الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة 8 ماي 1945 قالمة
كلية العلوم الانسانية والاجتماعية

مذكرة تخرج لنيل شهادة الماستر:

قسم : علوم الإعلام و الإتصال و علم المكتبات

تخصص : إتصال و علاقات عامة

الموضوع :

الهجمات السيبرانية و أثرها على العلاقات السياسية الدولية
-العلاقات الجزائرية المغربية نموذجا-

إعداد الطلبة:
- برج اسمهان
- مسيود سميرة
- مزعاش أكرم

اشـــراف:
د. سردوك علي

اعضاء لجنة المناقشة

الرقم	الاسم و اللقب	الدرجة العلمية	الصفة	الصفة
01	عبد العزيز بوصفط	أستاذ محاضر أ	جامعة 08 ماي 1945 قالمة	رئيسا
02	علي سردوك	أستاذ محاضر أ	جامعة 08 ماي 1945 قالمة	مشرفا. مقررا
03	ابتسام خطاف	أستاذ مؤقت	جامعة 08 ماي 1945 قالمة	ممتحنا

السنة الجامعية: 2021-2022


بسم الله الرحمن الرحيم

الشكر والعرفان:

قبل كل شيء أشكر الله عز وجل في ما منحه لنا من صبر وطاقة لتحمل هذا العمل الشاق وفي تكملته

أما بعد قال الله عز وجل " واصبروا إن الله مع الصابرين "

أتقدم بكامل عبارات الثناء والتقدير لأستاذنا القدير الذي ساهم بشكل كبير في توجيهنا وإرشادنا طوال فترة بحثنا الأستاذ سردوك علي ، وكل الحب والاحترام لقسم الإتصال والعلاقات العامة ، كما نتوجه بجزيل الشكر للسادة الأفاضل أعضاء لجنة المناقشة لتفضلهم بمناقشة هذا الموضوع الأستاذ بوصفط عبد العزيز والأستاذة خطاف إبتسام ، وعلى القيمة العلمية المضافة من قبلهم ، وكل الحب والاحترام لكافة الأساتذة الذين ساهموا في وصولنا لهذه النقطة من مسيرتنا الجامعية والمهنية مستقبلا.

الإهداء:

إلى من كانت معي طول درب حياتي والتي كانت هي أساس نجاحي بدعائها الدائم وحضورها المستمر

إلى أمي الحبيبة حفظها الله وأطال في عمرها

"عائشة درويش"

إلى السند ومصدر العطاء والقوة والتحفيز في مسيرتي الدراسية

إلى من كان وجوده دعم لي

إلى أبي الغالي أدامه الله لي ورعاه

إلى إخوتي وسندي الثاني في الحياة

إلى ابنة أختي جويرية وكل العائلة التي شاركتني هذا العمل حتى في تفاصله الصغيرة

إلى من كانت دعواتهم ظاهرة حتى بعد انتقالهم إلى رحمة الله الواسعة إلى جدي "الخميسي درويش" وجدي "عمار برج"

إلى كل من صديقتي وأختي "إيمان زروقي" التي ساهمت في هذا الموضوع وبشكل كبير في تكملته إلى اللحظة الأخيرة

وإلى "يسرى طواهرية" التي أبدت هي الأخرى تفانيها معنا في هذا العمل

إلى كل من إدارة العلوم السياسية والإعلام الألي الذي كان إستقبالهم لنا برحابة صدر وسرور دائم

وإلى كل من درسنا معهم وتعلمنا وإستفدنا منهم

إلى جميع الأصدقاء من قريب وبعيد

أهدي هذا العمل المتواضع إلى كل هؤلاء

برج إسمهان

إلى من حملتني تسعة أشهر في بطنها

إلى من الجنة تحت أقدامها

إلى أغلى إنسانة على قلبي

إلى أمي الحبيبة ، أدامها الله لي وأطال في عمرها

إلى من تعب من أجلي ودعمني

إلى من كان سندا لي في مشواري الدراسي

إلى ينبوع العطاء

إلى والدي الغالي حفظه الله وأطال عمره

إلى من دعموني في مشواري الدراسي

إلى من حفزوني وشجعوني

إلى من لم يبخلوا عليا في شيء

إلى إخوتي الأعزاء حفظهم الله وأطال في عمرهم

إلى بنات أخي التوأم

إلى" روان ومرام" حفظهما الله تعالى

إلى أصدقاء المواقف الحقيقية

إلى إيمان زروقي و إسمهان برج

إلى يسرى طواهرية التي لم تبخل علينا بعلمها

إلى أصدقاء الدرب

إلى قسم الاعلام و الإتصال وعلم المكتبات

إلى قسم العلوم السياسية والإعلام الألي

إلى من دعمونا في مسيرتنا الدراسية مسيود سميرة

إلى ملاكي في الحياة ، إلى معنى الحب و الى معنى الحنان ، الى بسمة الحياة و سر الوجود ، الى من كان دعائها سر نجاحي ، الى كل حياتي الى اغلى شيئ في الدنيا ...

أمي الغالية رحام رزيقة

الى من كلله الله بالهيبة ، الى من علمني العطاء بدون انتظار ، الى من أحمل اسمه بكل افتخار و ستبقى كلماتك مترسخة في ذهني...

والدي عمار

الى سندي و رفيقي و صديقي ...

أخي الطاهر

الى من أرى التفاؤل بعينهم و السعادة في ضحكتهم و رفيقوا دربي في هذه الحياة

الى كل من تطلعوا لنجاحي بنظرات الأمل وإلى أبناء حيي

أصدقائي

إلى من شاركتني المشقة والعناء طبايبية قطر الندى

إلى زميلتا الدراسة اللتان شاركتان هذا العمل

أهدي هذا العمل المتواضع الى كل هؤلاء الذين ساهموا و لو بقدر قليل في انجاز هذه المذكرة

أكرم مزعاش

ملخص الدراسة:

تهدف هذه الدراسة إلى معالجة موضوع الهجمات السيبرانية وتأثيرها على العلاقات الدولية السياسية بين الجزائر والمغرب، حيث تناولت هذه الدراسة ماهية الهجمات الإلكترونية وانواعها والاستراتجيات التي إعتمدت عليها الجزائر للحد من هذا النوع من الهجمات وتداعيات هذه الأخيرة على الدولة الجزائرية ، وذلك بالإعتماد على المنهج الوصفي، كون هذه الدراسة تندرج ضمن البحوث الكيفية التي تهدف إلى جمع أكبر عدد ممكن من المعلومات الدقيقة والصحيحة حول موضوع البحث وتحليل تلك المعلومات المتحصل عليها من خلال أداة المقابلة.

وتمحورت إشكالية الدراسة حول ما هو دور الهجمات السيبرانية وتأثيرها على العلاقات الدولية السياسية الجزائرية المغربية ؟ حيث خلصت دراستنا إلى مجموعة من النتائج كان أبرزها :

- أن الهجمات السيبرانية تعد أحد الأسباب في قطع العلاقات بين الجزائر والمغرب
- تعرضت الجزائر للهجمات السيبرانية بسبب هشاشة منظومتها وبيئتها الإتصالية

الكلمات المفتاحية :

- الهجمات السيبرانية
- الإختراق الإلكتروني
- تكنولوجيا الإتصال الحديثة
- الفضاء السيبراني.

Study summary

This study aims to address the issue of cyber-attacks and its impact on international political relation between Algeria and Morocco

Where this study dealt with the nature and types of cyber-attacks and the strategies that Algeria relied on to reduce this type of attacks and the repercussions of the latter on the Algerian state, depending on the descriptive approach as this study falls within the qualitative research that aims to collect the largest possible number of accurate and correct information about this research topic and analyse that obtained information through interview

The problem of the study revoled around what is the role of cyber-attacks and their impact on the Algerian - Moroccan political international relations where our study concluded a set of results ,the most prominent of which were :

Cyber-attacks are one of the reasons for the severing of relations between Algeria and Morocco

Algeria has been exposed to cyber -attacks due to the fragility of its system and its communication structure.

Key words:

- Cyber attacks
- Electronic hack
- Modern communication technologie
- cyber space.

خطة البحث:

المقدمة.

الفصل الأول : الجانب المنهجي.

الاشكالية.

تساؤلات الدراسة.

أسباب اختيار الموضوع.

أهمية الدراسة.

أهداف الدراسة.

الدراسات السابقة.

تحديد المفاهيم و المصطلحات.

نوع الدراسة.

منهج الدراسة.

أدوات جمع البيانات.

عينة الدراسة.

حدود الدراسة.

الجانب النظري:

الفصل الأول: الهجمات السيبرانية.

المبحث الأول: ماهية الهجمات السيبرانية .

المطلب الأول: مفهوم الهجمات السيبرانية .

المطلب الثاني: خصائص الهجمات السيبرانية و أهدافها.

المطلب الثالث: نماذج عن الهجمات السيبرانية .

المبحث الثاني: طبيعة الهجمات السيبرانية و أنواعها.

المطلب الأول: طبيعة الهجمات السيبرانية .

المطلب الثاني: أنواع الهجمات السيبرانية و مخاطرها.

المطلب الثالث: دوافع الهجمات السيبرانية.

الفصل الثاني: تأثير الهجمات السيبرانية المغربية على العلاقات السياسية الجزائرية.

المبحث الأول: مخاطر الهجمات السيبرانية المغربية على الدولة الجزائرية.

المطلب الأول: أنظمة التجسس الإلكترونية التي تعرضت لها الجزائر .

المطلب الثاني: أضرار نظام بيغاسيوس على البنية الاتصالية في الجزائر.

المبحث الثاني: جهود الدولة الجزائرية في التصدي للهجمات السيبرانية.

المطلب الأول: الاستراتجيات الاتصالية المعتمدة من طرف الجزائر.

المطلب الثاني: تداعيات الهجومات السيبرانية على الجزائر.

الفصل الثالث: الجانب التطبيقي.

المقدمة

المقدمة:

تعد التكنولوجيا مظهرا من مظاهر العصر الحديث، وقد تداخلت مع حياتنا في كافة جوانبها، حتى أصبحت التكنولوجيا موجودة في كل بيت فهذا العصر هو عصرها وفيه تطورت وازدهرت ووصلت إلى أعلى مراتب الحداثة والتجدد.

فعلى إثر هذا التطور والذي ظهرت من خلاله مفاهيم عدة من أنترنيت الأشياء إلى الذكاء الإصطناعي إلى الأجهزة الإتصالية الحديثة والبرمجيات، برز مصطلح أخر في الأفق هو مصطلح الفضاء الإلكتروني التي تداولت البشرية على إستغلاله وكان لظهوره تماشيا مع الشبكة العنكبوتية أثر جوهري في مجالات الحياة ، الإقتصادي والتجاري والسياسي منه، وقد كان بطبيعة الحال للأجهزة الإتصالية والإلكترونية جزء كبير أو المساهمة الأكبر في هذا الفضاء الإلكتروني الذي منح بدوره فُتحة أو مجال لإبراز مفهوم آخر تحت جناحه، وهو ما يعرف بالهجمات السيبرانية .

فالتكنولوجيا الإتصالية التي ساعدت الفضاء الإلكتروني على الانتشار أكثر، أعطت هذا النوع من الهجمات سهولة في الإنتشار بشكل أسرع وأكثر مرونة،وهذا ما أدى إلى تفاقم الوضع وزيادة خطورة التكنولوجيا بصفة عامة وخصوصا في مجال كمجال الهجمات السيبرانية.

فقد دخلت وسائل الإتصال الإلكتروني في ساحة الصراعات البشرية لتحدث ثورة معلوماتية ضخمة في جل القطاعات ، الأمنية والعسكرية والسياسية وهذا التحول يكون كبير في مجال السياسات بين الدول وعلاقاتهم ؛ بحيث تطورت خلافاتهم ونزعاتهم من تقليدية إلى نزاعات كانت فيها الهجمات السيبرانية سلاحا حاسما وليدة اليوم والمستقبل في آن واحد.

فإن إستخدام الأجهزة الإتصالية والإلكترونية في الهجمات السيبرانية بمثابة هاجس وتحدي للدول التي وجب عليها أن تكون متيقظة كهذا المجال وواقعا ملموسا في نتائجه على دولة كدولتنا وإفتراضيا في اساليبه القتالية.

الجانب المنهجي

الجانب المنهجي:

الاشكالية :

لعل أبرز ما يميزنا اليوم كمجتمعات حديثة هو القفزة الهائلة في التطورات التكنولوجية أو ما يعرف بالعصر الرقمي خاصة تلك التي تخص الجانب الاتصالي حيث تعتبر هذه الأخيرة لها القدرة على التخزين و إرسال المعلومات من مكان إلى اخر و يتم كل هذا عن طريق العديد من الوسائل كالحاسوب و الهاتف و غيرها ، و نتيجة للتوسع في استخدام شبكة الانترنت الأمر الذي أدى إلى تفاقم مخاطر على المستوى المادي و المعنوي على حد سواء ، فنجد أن الأضرار المادية تتجلى في الاختلاس و النصب من خلال القرصنة لمواقع و أجهزة خاصة بالأفراد و المؤسسات، في حين تتمثل المعنوية منها في التأثير على سلوك الفرد و اتجاهاته و حتى مبادئه من خلال الترويج لأفكار و تحريضه على تغيير أرائه بغية تحقيق مصالح خفية ، و رغم كل هذا تعد الهجمات السيبرانية لها الأثر البالغ في تحطيم البنية الشبكية و الاتصالية للأجهزة الإلكترونية و سهولة اختراقها بسبب الاعتماد المفرط في أنظمة الحماية للأجهزة و على اعتبار أن طبيعة الفضاء الالكتروني و سهولة اختراقها بسبب الاعتماد المفرط في أنظمة الحماية للأجهزة و على اعتبار أن طبيعة الفضاء الالكتروني تتخطى الحواجز المكانية و الزمانية فقد اصبحت جل الدول تعتمد اعتمادا كليا على الأنظمة الالكترونية ، الأمر الذي يزيد من خطورة هذه الأخيرة لتجد الحكومات و الدول نفسها أمام تداعيات هي بغنى عنها ، فكانت الجزائر من ضمن الدول التي كانت نتائج الهجمات السيبرانية عليها متكررة من طرف المغرب و ذلك من خلال ما يسمى بنظام التجسس الإلكتروني بيجاسوس، و على إثر هذا سارعت الجزائر بغلق الحدود الجوية و قطع العلاقات الدبلوماسية معها

نهائيا ، لذا سعت الجزائر لمواجهة هذا النوع من الهجمات الإلكترونية و انتهاج مجموعة من التدابير كان أهمها وضع أنظمة اتصالية متطورة لاكتشاف الهجمات السيبرانية وحماية منظوماتها المعلوماتية عن طريق ما يعرف بالأمن المعلوماتي و عليه قمنا بطرح التساؤل التالي:

-ما هو تأثير الهجمات السيبرانية على العلاقات الدولية السياسية الجزائرية المغربية؟

تساؤلات الدراسة:

1-ماهي التحديات السيبرانية للجزائر؟

2-ماهي أهداف الهجمات السيبرانية؟

3-ماهي الأبعاد السياسية للهجمات السيبرانية على الجزائر؟

4-ماهي الاليات الاتصالية المعتمدة من قبل الدولة الجزائرية لمواجهة الهجمات السيبرانية؟

أسباب اختيار الموضوع:

أسباب موضوعية:

- معرفة انعكاس هذه الهجمات على البيئة الاتصالية في الجزائر.
- إعطاء صورة شاملة عن الموضوع من خلال توضيح العلاقة بين المغرب و الجزائر و الهجمات السيبرانية.
- الرغبة في التعرف على نظام بيغاسوس الجديد و خطورته على الجزائر في ظل التطور التكنولوجي.

أهمية الدراسة:

لقد شهدت الفترة الأخيرة تزايد الهجمات السيبرانية و من الصعب تحديد الجهة التي صدرت عنها هذه الهجمات ، ولهذا فإن أهمية هذا البحث تكمن في أنه يعالج موضوع جديد من خلال التعريف بالهجمات السيبرانية أنواعها وطبيعتها ، بالإضافة إلى تأثير هذه الأخيرة على الشبكة الاتصالية الجزائرية من خلال تعرضها لنظام التجسس المغربي بيغاسيوس .

أهداف الدراسة:

1. معرفة التحديات التي تواجهها الجزائر في ظل الهجمات السيبرانية
2. توضيح ابرز أهداف الهجمات السيبرانية على الجزائر .
3. التعرف على الأبعاد السياسية للهجمات السيبرانية ضد الجزائر.
4. توضيح الاليات والاستراتيجيات الاتصالية المعتمدة من قبل الدولة الجزائرية لمكافحة الهجمات السيبرانية.

الدراسات السابقة:

تعد الدراسات السابقة في موضوعنا قليلة و هذا راجع إلى كون الموضوع جديد ومزال في قيد البحث.

- الدراسة الأولى: الهجمات السيبرانية في ضوء القانون الدولي الإنساني (2021)

مضمون الدراسة:

تناولت هذه الدراسة ماهية الهجمات السيبرانية والجهود الدولية المباشرة للتنظيم القانوني للهجمات السيبرانية ، أما الجزء الثاني من هذه الدراسة فقد خصصت

لمعايير تحديد الاهداف العسكرية المشروعة أثناء الهجمات السيبرانية في القانون الدولي الإنساني إضافة إلى التحديات انطباق القانون الدولي الانساني على الهجمات السيبرانية.

اوجه التشابه والاختلاف:

تتفق هذه الدراسة مع دراستنا الحالية في كونها تتطرق الى ماهية الهجمات السيبرانية ، في حين الجزء الأول من التأطير النظري قد تناول أنواع الهجمات السيبرانية ، إلا ان الإختلاف يتجلى كون هذه الدراسة قد ركزت على تقييم مدى انطباق القانون الدولي الانساني على حالات تطبيقية للهجمات السيبرانية المغربية على الأنظمة الاتصالية في الدولة الجزائرية (الموصلي، 2021، صفحة 03).

- الدراسة الثانية: مستقبل السيادة الرقمية في ظل التكنولوجيا الحديثة (2020)

مضمون الدراسة:

تضمنت هذه الدراسة السيادة الرقمية في ظل التطور الهائل في التكنولوجيا حيث احتوى الفصل الثاني على مجتمع المعلومات والشبكات التواصل الاجتماعي في ضوء التطورات التكنولوجية، وكذلك كيف ساهمت التكنولوجيا في صعود الشركات التقنية العالمية وعلاقتها بالدول أما الفصل الثالث تكلمت الدراسة عن ماهية السيادة الرقمية و معالمها و انتهاكاتها، اما الفصل الرابع فتضمن الأمن السيبراني ودوره في الفضاء الالكتروني وتأثير السيادة الرقمية على بيانات الحوسبة السحابية.

أوجه الاختلاف والتشابه:

تختلف هذه الدراسة عن موضوعنا في كونها ركزت في تأثير التكنولوجيا الحديثة على السيادة الرقمية للدول وسيطرة كل من الدول الغربية على هذه التكنولوجيا ، في حين كانت نقطة التشابه مع دراستنا تتمثل في كونها قد استفدنا منها في تطرقها للأمن السيبراني والردع السيبراني ، إضافة الى تطرقها الى كيف ارتبطت التكنولوجيا بزيادة الهجمات السيبرانية على الدول (سلاوي، بلدي، خلة، و خلة، 2020، الصفحات 70-71) .

- الدراسة الثالثة: المشكلات الاخلاقية والقانونية المثارة حول شبكة الانترنت (2006)

مضمون الدراسة :

تناولت هذه الدراسة ماهية شبكة الانترنت و طبيعتها، اما الفصل الثالث والرابع فقد تطرقت الى المشكلات الاخلاقية والقانونية لشبكة الانترنيت.

اوجه التشابه و الاختلاف:

ان هذه الدراسة تتشابه مع دراستنا بحيث تناولت الهجمات المعلوماتية والتي تتشابه مع الهجمات السيبرانية الى حد كبير؛ والتي تعني اختراق المعلومات وانتهاك خصوصية الأشخاص.

بالاضافة الى انها كذلك عالجت الحرب المعلوماتية الإلكترونية والتي يكون الهدف منها استهداف نظام معين يخص حكومة أو دولة معينة وذلك من أجل تعطيل نظام العدو والحصول على معلوماته ، أما أوجه الاختلاف فتكمن في ان هذه الدراسة قد انصب اهتمامها على المشكلات الاخلاقية و الجانب القانوني منها ، في حين موضوعنا قد تمحور حول تأثير الهجمات السيبرانية على العلاقة الدولية بين الجزائر و المغرب من الناحية الاتصالية ، إضافة الى تطرقنا الى

نظام التجسس التابع للكيان الصهيوني التي استخدمته المغرب ضدنا وعطل الانظمة الاتصالية المستخدمة في الجزائر (بن جامع، 2007، صفحة 71).

نوع الدراسة:

دراسة وصفية حيث يتم في هذه الدراسة جمع المعلومات التي تحصل عليها الباحث بشكل كافي و دقيق عن موضوع الدراسة ، حيث تركز الدراسة الوصفية على تفسير الأوجه البارزة لأي موضوع ، و كذلك تسليط الضوء على ابرز النماذج التي تعرضت لهذا النوع من الهجمات ، إضافة الى تقديم بعض الاستراتيجيات الاتصالية من أجل التصدي لهذه الأخيرة و الحد منها.

منهج الدراسة:

إن المنهج الذي إتبعناه في موضوع بحثنا هو المنهج الوصفي، بإعتباره الملائم لطبيعة هذه الدراسة .

حيث يعرف المنهج الوصفي على أنه المنهج الذي يقوم على جمع المعلومات والبيانات حول الظاهرة المدروسة، دون أي تدخل من قبل الباحث .

كما يعرف هذا المنهج بأنه طريقة لوصف الموضوع المراد دراسته من خلال منهجية علمية صحيحة ، وتصوير نتائج التي تم التوصل إليها إما على شكل أرقام وإحصائيات معبرة أو على شكل بيانات كيفية ،وهذا ما يميزه كمنهج لدراسات والبحوث الإنسانية والإجتماعية بحيث يصلح كمنهج كمي أو كيفي (المحمودي، 2015، صفحة 46).

أدوات جمع البيانات:

المقابلة هي تقنية مباشرة للتقصي العلمي تستعمل إزاء الأفراد الذين تم سحبهم بكيفية منعزلة ، غير انها تستعمل في بعض الحالات إزاء مجموعات من أجل إستجوابهم بطريقة نصف موجهة والقيام بسحب عينة كيفية بهدف التعرف بعمق على المستجوبين (أنجرس، 2004، صفحة 197).

عينة الدراسة :

مفهوم العينة : يمكن تعريفها على أنها مجموعة جزئية من مجتمع الدراسة يتم إختيارها بطريقة مناسبة وإجراء الدراسة عليها ومن ثم إستخدام تلك النتائج المتحصل عليها من هذه العينة ،حيث كانت العينة المناسبة لموضوع بحثنا هذا هي العينة القصدية لأننا قمنا بإستهداف مجموعة من الأساتذة ،وقد إخترنا 14 أستاذ على إعتبار قربهم من الموضوع المدروس (بن مرسلي، 2010، الصفحات 169-170).

حدود الدراسة :

الإطار الزماني :

أجريت الدراسة من 2022-02-11 إلى غاية 2022-06-09.

الإطار المكاني :

تعتبر الهجمات السيبرانية بمثابة الهجمات الإلكترونية التي تعرضت إليها العديد من الدول ، لكن كان تركيزنا على الهجمات التي تعرضت إليها الجزائر في الأونة الأخيرة من طرف المغرب .

الفصل الأول

الفصل الأول: الهجمات السيبرانية :

المبحث الأول : ماهية الهجمات السيبرانية :

إن التطور الهائل الذي لعبته الثورة الرقمية والمعلوماتية شكل قفزة تكنولوجية، إذ نجد أن الفضاء السيبراني قد أصبح عنصر مؤثرا نظرا لما يحمله من أدوات تكنولوجية متطورة وقد باتت أكثر تأثيرا في الحسابات الإستراتيجية للدول . فالدولة التي لا تملك التكنولوجيا السيبرانية المحصنة أمنيا سيتعرض فضائها السيبراني المتضمن للمعلومات و الخدمات البنية التحتية الحيوية إلى الهجمات السيبرانية و التي بدورها تسبب دمار هائل.

المطلب الأول : مفهوم الهجمات السيبرانية :

في ظل الثورة المعلوماتية والرقمية الحديثة نجد ما يسمى بالفضاء السيبراني والذي يقوم على أساس بنية عالمية لتكنولوجية المعلومات و الإتصال (الموصلي، 2021، صفحة 07) .

إذ أن الهجمات السيبرانية لم تكن معروفة إلا في وقت قريب وهذا ما يشكل إحدى أهم التحديات الراهنة التي يواجهها المختصون ، وبالخصوص في تحديد طبيعتها أو عناصرها (الفتلاوي، 2016، صفحة 03) .

الهجمات السبرانية لغة و إصطلاحا:

إن هذا المصطلح أي الهجمات السبرانية لابد من التركيز فيه على جانبين الأول يتمثل في السيبرانبة في اللغة ،بينما سيركز الجانب الثاني على الهجمات السيبرانية إصطلاحا ، و ذلك من خلال التعريفات التي أوردها المتخصصون والفقهاء في هذا الجانب (الموصلي، 2021، صفحة 08).

أ/السبرانية في اللغة :

كلمة سايبر cyber يونانية الأصل ، وترجع إلى مصطلح kybernetes الذي ورد في مؤلفات الخيال العلمي ، ويعني القيادة أو التحكم عن بعد (حطيط، صفحة 02).

وتعني أيضا الشخص الذي يدير دفة السفينة stecromon وتستخدم مجازا لتعبر عن المتحكم govemon وقد إستخدمها أفلاطون من قبل للتعبير عن الحكم (الكر و بن مرزوق، 2018، صفحة 35) .

إن كلمة سيبرانية أو سايبرأوسيبراني تعتبر ترجمة حرفية لكلمة cyber والمشتقة من كلمة cyberntics وقد أستخدم هذا المصطلح cybernetics أكادميا لأول مرة من قبل عالم الرياضيات الأمريكي نوربرت وينت عام 1939 في كتابه الشهير : علم التحكم الألي أو التحكم والإتصال في الحيوان والأدلة ، وذلك للإشارة إلى أليات التنظيم الذاتي .

أما في ما يتصل بالبحث عن مصدر كلمة سايبر cyberفي معاجم اللغة العربية فنجد أنه لا يوجد مصطلح مقارب للسايبر cyber إذا جاء معنى هذه الكلمة .

في قاموس المورد الحديث فمعنى الكمبيوتري أو عصري جدا كما ورد معنى مصطلح cybernetics بأنه علم الضبط او علم التحكم الأوتوماتيكي (الموصلي، 2021، الصفحات 08-09) .

السيبرانية في قاموس المورد هي علم الضبط ، مصدرها cyberneticsوهو مصدر يتطابق مع مفهوم الهجمات السيبرانية ، أي ضبط الأشياء عن بعد و السيطرة عليها .

عرف قاموس مصطلحات الأمن المعلوماتي مصطلح السيبرانية بالقول : هجوم عبر الفضاء الإلكتروني يهدف إلى السيطرة على مواقع إلكترونية أو بنى محمية إلكترونية ، لتعطيلها أو تدميرها أو الإضرار بها (حطيط، صفحة 02) .

السيبرانية وهي مأخوذة من كلمة سيبر وتعني صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الإفتراضي ، فالسيبرانية تعني فضاء الأنترنيت.

أما قاموس OXFORD الإنجليزي فيعرفها على أنها(دراسة فاعلية العمل البشري بمقارنتها بفاعلية الألات الحاسبة تتصل بسمات و خصائص الحواسيب وتكنولوجيات المعلومات و الواقع الإفتراضي) .

أما في اللغة العربية بالرجوع إلى المختصين فيها ، فنجد هؤلاء المختصين يواجهون تحديات في الوصول إلى مصطلح مقارب لمصطلح cyber (عطية، 2022، صفحة 103) .

و جاء في قاموس المعاني بمعنى : تخيلي (الموصلي، 2021، صفحة 09).

ب/ الهجمات السيبرانية إصطلاحا :

لقد حاول العديد من الخبراء و الفقهاء القانونيين وضع تعريف محدد للهجمات السيبرانية ، وسنستعرض هذه التعاريف تبعا لوجهات النظر التي يتبناها اصحابها .

فقد عرفه فيورتس (fuertes) بالقول : هجوم عبر الأنترنيت يقوم على التسلل إلى مواقع إلكترونية غير مرخص بالدخول إليها ، بهدف تعطيل أو إتلاف

البيانات المتوفرة فيها أو الإستحواذ عليها ، وهي عبارة عن سلسلة هجمات إلكترونية تقوم بها دولة ضد دولة أخرى .

و قد عرفه شمت (schmitt)بالقول : مجموعة من الإجراءات التي تتخذها الدولة للهجوم على نظم المعلومات المعادية بهدف التأثير والإضرار بها ، وفي نفس الوقت للدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة.

و فيما يتعلق باللجنة الدولية للصليب الأحمر فقد عرفت الهجوم السيبراني بأنه: إستخدام أنشطة متعددة لتغيير أو إفساد أو خداع أو إضعاف أو تدمير أنظمة الحاسوب أو شبكات الحاسوب للخصم أو المعلومات أو البرامج المدرجة في هذه الأنظمة أو الشبكات أو التي ترسل من خلالها ، وقد تؤثر هذه الأنشطة أيضا في الكيانات المرتبطة بهذه الأنظمة و الشبكات ،و قد يستخدم الهجوم السيبراني في منع المستخدمين المرخص لهم من الولوج إلى الحاسوب أو خدمة معلومات (هجوم الحرمان من الخدمة) ، أو لتدمير الألات التي يتحكم فيها الحاسوب (الموصلي، 2021، صفحة 09) .

الهجمات السيبرانية : يمكن تعريفها بأنها فعلا يقوض من قدرات ووظائف شبكات الكمبيوتر لغرض قومي أو سياسي ، من خلال إستغلال نقطة ضعف معينة تمكن المهاجم من التلاعب بالنظام (بن مرزوق، 2017) .

التعريف الإجرائي للهجمات السيبرانية :

فمن خلال التعاريف السابقة يمكن القول : بأن الهجمات السيبرانية هي عبارة عن هجوم يتم عبر مواقع إلكترونية عبر الأنترنيت بطريقة غير شرعية وغير مسموح بالدخول لها، إذ هذه الأخيرة يقوم بها شخص أو مجموعة من الأشخاص

أو دولة ضد دولة أخرى ، بهدف تدمير أنظمة الحاسوب أو تعطيل البيانات والإستحواذ عليها .

المطلب الثاني : خصائص الهجمات السبرانية و أهدافها:

أ/ خصائص الهجمات السيبرانية :

1) تسطيع الهجمات السيبرانية إلحاق الضرر بالخصم ، مهما كانت طبيعتها من دون أن تتجاوز حد الفصل بين الحرب والسلام بشكل رسمي.
2) صعوبة تحديد مصدرها و كلفتها إذ لا تعلن عنها الدولة المنفذة غالبا فتبقى مجهولة المصدر لوقت طويل، إضافة إلى أن تحديد مصدرها يحتاج فرق مختصصة .
3) مؤثرة في الجانب السياسي والإقتصادي على صعيد الولي نتيجة إنتقال جزء كبير من الصراعات بين القوى العظمى في العالم بين شبكة الأنترنيت والوسط الرقمي مع تزايد أرتباط العالم بتقنيات وسائل الإتصال الإلكتروني.
4) تجوزها للعامل الجغرافي مكنها من تخطي الحدود والوصول أو التجسس على نظام أو شركة أو حتى دولة عن طريق إرسال فيروسات إلكترونية .
5) إنخفاض الكلفة المواجهة نسبيا بالمقارنة مع الحروب التقليدية فهي لا تحتاج لمعدات وجيوش مجهزة كما أن إحتمالية وقوع الضحايا في صفوف القوة المهاجمة تكون منعدمة (عبد الواحد، 2021، الصفحات 39-43) .

ب/ أهداف الهجمات السيبرانية :

- تهدف هذه الهجمات إلى تخريب و تعطيل عمل الأشخاص أو مؤسسات أو خدمات حكومية بخاصة البنية التحتية للدولة. (مكتبي، 2020) .

- تهدف كذلك الهجمات السيبرانية إلى تعطيل وسائل النقل برا وبحرا وجوا كما يمكن تغيير مسار الرحلات .
- تعطيل أنظمة الطاقة وقطع الكهرباء على مدن بأكملها.
- إضافة إلى أن الهجمات السيبرانية لها أهداف من الناحية المعلوماتية فالهجوم السيبراني هدفه تعطيل انظمة التحكم والصواريخ وتغيير مسارها أو شل حركتها من خلال التحكم في الانظمة الإتصالية أو الجهاز الذي يتحكم في هذه الصواريخ (علاو، 2022) .

كما تهدف الهجمات السيبرانية إلى الكشف عن البيانات والمعلومات الموجودة على الأجهزة أو تغيير الشبكات الأصلية الخاصة بالنظام بشبكات وهمية قريبة من الأصلية أو قد تصل إلى تعطيل أجهزة العدو أو الخصم إلكترونيا من خلال تعطيل أجهزة الاتصالات الخاصة بهذا الأخير (الحرب الإلكترونية و السيبرانية، 2021).

- كما نجد أيضا صراع سيبراني ذو طبيعة ناعمة ؛ والمقصود به صراع حول الحصول على المعلومات ، بهدف التأثير في المشاعر و أفكار الأفراد و شن حرب نفسية و إعلامية،وكذلك يهدف هذا الأخير إلى التأثير في طبيعة العلاقات الدولية ، كالدور الذي لعبه موقع ويكيليكس في الدبلوماسية الدولية .

المطلب الثالث : نماذج عن الهجمات السيبرانية:

1-<u>نموذج أكرانيا و روسيا :</u>

حسب المؤشر التنبؤي للهجمات الإلكترونية CAPI فإن لدى روسيا خبرة في الهجمات السبرانية وبث الدعايات والرسائل التي يمكن أن تؤثر في إستقرار الحكومة الأكرانية ولطالما استخدمت موسكو المعلومات المظلة في وسائل

التواصل الاجتماعي والهجمات الإلكترونية المتقطعة على شبكة الكهرباء الأكرانية.

اليوم تشهد الساحة الدولية تصاعدا للتوتر في العلاقات الروسية الأكرانية وكما هو معروف لقد قرعت في السنوات العشر الماضية طبول الحرب بين البلدين تارة وبين روسيا وحلف الناتو الداعم تارة أخرى ولكن طوال هذه الفترة ورغم تعظيم إمكانات اندلاع شرارة المعركة بحكم كثرة الأزمات والتوترات الرئيسية والفرعية فإن المشهد لعمل عسكري حقيقي لم يتطور في حين كان الأثر واضحا باستخدام هجمات كان هدفها شل الأنظمة المالية والبنية التحتية الحيوية في أوكرانيا .

هذا وقد جاء المؤشر التنبؤي للهجمات الإلكترونية CAPI الذي ابتكره أنطون داهبورا المدير التنفيذي لمعهد جونز هوبكنز لأمن المعلومات مع خبير الأمن السيبيراني والشؤون العالمية تيري طومسون المحاظر في وكالة الاستخبارات الباكستانية تنبؤوا بهذه الهجمات السيبرانية التي شنت أخيرا على المصالح الأوكرانية كما حدث في هجوم Notpetyo لعام 2017 الذي شنته روسيا ضد شركة برمجيات أوكرانية تسببت في خسائر المليارات من الدولارات جراء أضرار التي لحقت بالاقتصاد العالمي .

هذا ويعتمد هذا المؤشر CAPI على نظام تسجيل من 5 أجزاء يسعى إلى فهم أفضل لسبب انخراط الدول في الصراع السيبراني، ويكون بمنزلة مقياس للتنبؤ بالهجمات السيبرانية المستقبلية مع استمرار نمو الأمن السيبراني باعتباره جانبا مهما من جوانب الأمن القومي في ظل تزايد هذه الهجمات السيبرانية .

وبالرجوع إلى التوتر الروسي الأوكراني يقوم المؤشر التنبؤي للهجمات الإلكترونية CAPI بفحص وتعيين درجات المخاطر في 5 فئات :

1-حيازة القوى السيبرانية المنظمة ذات المعرفة .
2-الدافع الوطني .
3-عدم الخوف من التداعيات.
4-التوافق مع إستراتيجية الأمن القومي.
5-الضعف التكنولوجي للهدف.

بناءا على هذه الفئات الخمس فإن الدول القومية المكونة من دولة معتدية ودولة دفاعية تعطي درجات تتراوح من 1 إلى 5 في كل مجال من المجالات الخمس المذكورة سابقا .

وجود قوة سيبرانية منظمة وواعية الدوافع المحتملة لمهاجمة الهدف عدم الخوف من التداعيات اتساق الهجوم الإلكتروني مع استراتيجية الأمن القومي الشاملة للبلد ونقاط الضعف التكنولوجية في الهدف ، والنتيجة كانت ارتفاع درجات الخطر بين روسيا وأوكرانيا التي أعلى مستوى ممكن هي درجة 25 من أصل 25 .

وتشير هذه الدرجة إلى مدى توغل روسيا المحتمل في أوكرانيا وإلى تاريخ روسيا في الهجمات السيبرانية الناجمة عن الحكومة الأوكرانية والبنية التحتية الحيوية، بالإضافة إلى ممارسة الروس المستمرة لتجربة التقنيات القرصنة الجديدة . وثمة نموذجان للهجمات الإلكترونية الروسية على أوكرانيا :

أولا : التوغل في جرجيا 2008 وإحتلال شبه جزيرة القرم عام 2014 وفي كلا الحالتين استخدمت روسيا هجمات حرمان الخدمة على شبكة الكمبيوتر وتم

تحديد هذا النهج في العقيدة العسكرية الروسية بما في ذلك الحرب السياسية والاقتصادية وحرب المعلومات .

ثانيا : وقد شنت روسيا هجمات سيبرانية في عامي 2015 و2016 قصيرة ولكن خطيرة على شبكة الكهرباء ويشير الباحثين إلى أن روسيا قد استخدمت نفس أسلوب أو الطريقة التي استخدمتها لحالتي هجومات جورجيا وجزيرة شبه القرم ، هذا وتعتبر من أوائل الدول التي استغلت الفضاء السيبراني في حروبها و تعتمد الاستراتيجية الروسية في نزاعها مع أوكرانيا على الأسلحة الإلكترونية بإعتبارها قوة مضاعفة في الحروب (خالد، 2022) .

نموذج إيران :

تعرضت إيران إلى عدة هجمات سيبرانية ، كان من أبرز هذه الهجمات تلك التي شنتها الولايات المتحدة وإسرائيل ضد إيران وهو ما يعرف بهجوم stuckient ، ويعد هذا الأخير جزء من عملية أكبر من الهجمات الإلكترونية عرفت تحت إسم الألعاب الأولمبية dperationdlympic games، حيث عمل هذا الهجوم على تخريب برنامج النووي لإيران من خلال وضع أو إنزال فيروس على نظام التشغيل الذي يدير عملية تخصيب اليورانيوم في موقع ناتانز النووي مما أدى هذا إلى إتلاف عدد كبير من وحدات الطرد المركزي (شادي، 2019، صفحة 99) .

هذا ويعد فيروس stucksent عبارة عن برنامج خبيث يهاجم أنظمة التحكم الصناعية المستخدمة على نطاق واسع فقد عثر على هذا الفيروس لأول مرة من قبل شركة بيلاروسية تدعى vimsblock ada حيث صرحت أنها عثرت عليها في أحد أجهزة الكمبيوتر لأحد عملائها الإيرانيين.

حيث أشارت شركة سيمنانيك التي تعمل في مجال برنامج الأمن الإلكتروني والبرنامج المضادة للفيروسات أن إيران تأتي في طليعة الدول المستهدفة من ناحية الإصابات التي حققها برنامج ستكسنتو أن ما يقارب 60 بالمئة من أجهزة الكمبيوتر التي تعرضت لهجوم في هذا التطبيق الخبيث كانت في إيران .

هذا وقد كان من الصعب معرفة من قام بهذا الهجوم بالتحديد على إيران لكن كانت أصابع الإتهام موجها لكل من الولايات المتحدة الأمريكية وإسرائيل كون الولايات المتحدة الأمريكية لديها خلافات و صراع مع دولة إيران منذ عهد جورش بوش الإبن وإسرائيل لديها تخوف من كون إيران دولة نووية (غربي و شرقي، 2020، الصفحات 101-102).

نموذج الصين :

الصين أكبر هدف للهجمات الإلكترونية في العالم :

حسب مقال عرضته قناة العين الإخبارية فإن الصين قد تعرضت لأكثر من 800 مليون هجوم إلكتروني يوميا في عام 2018 وبلغت ذروت هذه الهجمات الإلكترونية في شهر أغسطس في وقت رفضت فيه الحكومة الصينية إدعاءات بأنها وراء الهجوم الإلكتروني على البرلمان الأسترالي أظهر بحث حديث ان الصين هي أكبر هدف لتلك الهجمات في العالم .

هذا وأفادت شركة الأمن السيبراني الصينية knouwnsec و مقرها بكين بأن النظمات الصينية عانت في المتوسط من أكثر من 800 مليون هجوم سيبراني من هجمات الحرمان من الخدمة أو ما يعرف ب DDOS يوميا في عام 2018 و بلغت ذروتها في شهر أغسطس عندما وصلت الهجمات إلى اكثر

من 4.9 مليار في اليوم الواحد لتصبح بذلك أكثر دولة تعرض للهجمات السيبرانية في العالم .

وهجمات DDOS عبارة عن هجوم إلكتروني يقوم فيه المتسللون بإغراق موقع معين بسيل من البيانات غير اللازمة، مما يسبب بطئ الخدمات وصعوبة وصول المستخدمين له وقال التقرير إن معظم المتسللين 97 بالمئة منهم كانوا من القراصنة المحليين في حين أن 3 بالمئة الباقين كانوا من الخارج وتستهدف هذه الهجمات الخارجية عادة المواقع الحكومية والمالية وتأتي معظم هذه الهجمات من دول مثل الولايات المتحدة الأمريكية وكوريا الجنوبية و اليابان ، و أضافت knounsec السيبراني الصيني أن الضغط على هذه الهجمات السيبرانية على المواقع الحكومية يتزايد خاصة خلال الأحداث الخاصة و الحساسة مثل الأحداث السياسية و العسكرية .

بكين 11 مارس 2022 رصدت الصين هجمات سيبرانية تستهدف شبكة الأنترنيت الخاصة بها منذ أواخر فبراير حسبما أفادت به هيئة الأمن السيبراني الصينية تحاول منظمات خارجية من خلال هذه الهجمات السيطرة على الحواسيب في الصين، لشن هجمات الفن الوطني للإستجابة لحالات الطوارئ لشبكة الكمبيوترو مركز التنسيق في الصين إضافة إلى ان الفريق أكد أن معظم الهجمات الإلكترونية كانت من طرف الولايات المتحدة الأمريكية و بعضها في ألمانيا و هولندا كما أكد الفريق إلى أنه قد تم التعامل مع هذه الهجمات في الوقت المناسب إلى أقصى حد (عادل، 2019).

نموذج الولايات المتحدة الأمريكية :

لقد تم إستهداف مجموعة من المواقع الأمريكية إذ تعرضت هذه الأخيرة إلى طلبات بلغت مليون طلب في الثانية ، و هذا ما أدى إلى ضغط الأجهزة الخادمة وبالتالي تعطلت الأجهزة الخادمة للخزانة العامة و الخدمة السرية و هيئة التجارة الفيدرالية ووزارة النقل ، كذلك أصيب موقع مؤشرا ناسداك و بورصة نيويورك التجارية و بورصة نيويورك المالية وموقع هيئة البريد بواشنطن ، غير أن الهجمة التي إستهدفت البيت الأبيض فشلت وهذا راجع إلى تعاونها مع شركة تعرف باسم أكاماي حيث أي تحرك على الأنترنيت يهدف إلى الإتصال بالبيت الأبيض يتم تحويل مساره و ذلك بتمريره عبر أقرب جهاز خادم للمتصل من مجموعة تربوا على 20 ألف جهاز خادم حول العالم ، وهذا بهدف منع أول هجمة لتعطيل موقع البيت الأبيض (إيه كلارك و كيه كنيك، 2012، صفحة 40).

كذلك فقد تعرضت شركة سوني بيكسرر الامريكية للهجوم و كان ذلك في عام 2014 ، ويرجع السبب في هذا إلى فيلم تم إنتاجه من قبل هوليود ، و قد كان هذا الفيلم عن زعيم كوريا الشمالية كيم يونغ أون ، بالإضافة إلى هذا فقد تعرضت أنظمة الإتصال الإلكترونية التابعة لوزارة الدفاع الأمريكي pentagon إلى هجمات سيبرانية و ذلك في عام 1998 -2000 ، فهذا الهجوم تسبب في الحصول و الإستحواذ على الالات من الملفات الأكثر سرية وخصوصية ، و بهذا فالولايات المتحدة الأمريكية قد ألقت اللوم رسميا على روسيا الإتحادية ، لكن هذه الأخيرة أنكرت ذلك كليا عن هذا الهجوم .

وقد كشف تقرير لوكالة الإستخبارات الأمريكية عن عملية قرصنة على الإنتخابات الرئاسية الأخيرة و كان هذا في عام 2017 حيث جاء في هذا التقرير بان الرئيس الروسي فلاديمير بوتين قد أعطى امر بإقامة حملة تأييد لمصلحة

الرئيس ترامب خلال الإنتخابات ، وهذا بهدف تسوية سمعة الوزيرة هيلاري كلينتون التي كانت نترشحة للإنتخابات من أجل التأثير عليها في الإنتخابات وهذا ما أدى إلى خسارتها في الإنتخابات ، حيث أرجعت الوزيرة هيلاري السبب في هذه الخسارة إلى القرصنة الروسية ، وجاء رد ترامب على هذه الإتهامات بالسخافة ووصفتها روسيا بأنها تفوق الوقاحة ، في حين أن ويكيليكس نفت التورط الروسي ، كما صرحت وكالة الإستخبارات المركزية الأمريكية عن أدلة كثيرة تثبت أن من كان وراء الهجمات الإلكترونية هم ققراصنة من الروس مرتبطين بالكرملين ، وكذلك القرصنة المعلوماتية التي إخترقت حسابات البريد الإلكتروني لكيلنيون ومدير حملتها جون بوديستا ، وقادة الحزب الديمقراطي وقد نشرت على موقع ديكليكس ، أما سي أي إيه لم تفصح عن تلك الأدلة وقد صرحت عن أن هدف روسيا هو تحويل إنتخابات الرئاسة لصالح ترامب (عادل ع.، 2009، الصفحات 206-208).

المبحث الثاني : طبيعة الهجمات السيبرانية و أنواعها :

المطلب الأول : طبيعة الهجمات السيبرانية :

1. الهجمات السيبرانية وسيلة أم أسلوب قتال :

إن هناك العديد من الوسائل والأساليب التي يتم إستعمالها في القتال لذلك من المهم جدا التمييز بين هذه الوسائل والأساليب وعليه لابد من بيان طبيعة الهجمات السبرانية هل هي وسيلة أم أسلوب للقتال أم الإثنين معا .

أ-الهجمات السيبرانية وسيلة للقتال :

هنا نرجع الهجمات السيبرانية حسب إستخدامها ، فإذا أستخدمت هذه الأخيرة بغرض التسلل إلى أنظمة إلكترونية معدة للحماية وكذلك تنظيم سير عمل منشأت

حيوية ، وتم السيطرة عليها وتدميرها وتعطيل أنظمتها ، فهنا تكون الهجمات السيبرانية وسيلة للقتال أي سلاحا تهاجم به العدو.

ولكن نجد أن المجتمع الدولي يواجه العديد من الإشكاليات من خلال طريقة التعامل مع الهجمات السيبرانية وذلك من النقاش والجدل حول تصنيف الانشطة السيبرانية كسلاح وكذلك خضوعها لإتفاقيات معينة بالحد من التسلح لهذا ذهب بعض الخبراء بقولهم بأن الهجمات السيبرانية ووصفها بأنها سلاح ليست صحيحة ولا يمكن أن تكون كذلك .

وهذا راجع لإفتقاد الهجمات السيبرانية إلى الطاقة الحركية وأنها لاتخضع للتنظيمات الدولية المتعلقة بإستخدام الأسلحة وهذا مخالف للواقع .

فالسلاح الحقيقي هو الذي يحدث أضرارا سواءا مادية أو جسدية أو يخلف أثارا وراءه إذ يستعمل من أجل الهجوم على العدو أو الدفاع أو يستعمل التهديد أو التخويف .

وفي حديث اللجنة الدولية للصليب الأحمر عن الأسلحة السبرانية نجدها قد أشارت إلى أن تقييم مشروعية الأسلحة الجديدة له مصلحة في كافة الدول .

ب-الهجمات السبرانية أسلوب قتال :

إذا ساعدت الهجمات السيبرانية توجيه وتخطيط العمليات العسكرية وسهلت القوة العسكرية التقليدية ، فهنا تعتبر أسلوبا للقتال ، وذلك من خلال إستخدامها في توقيف عمليات الإتصال في المطارات سواءا كانت عسكرية أو مدنية ، ففي هذه الحالة لم تقم بتحقيق الهدف فقط بل تعدت ذلك إلى تمهيد وفتح الطريق امام القوات العسكرية لتكون بذلك قد حققت أفضلية عسكرية على العدو او الطرف

الأخر ، ولهذا يمكن إعتبارها أسلوب للقتال وإدراجها ضمن التخطيطات والتكتيكات العسكرية .

ومن هنا نتوصل إلى أن الهجمات السيبرانية تكون وسيلة وأسلوب للقتال في وقت واحد ، وذلك من خلال الأهداف المستخدمة لتحقيقها ، فقد طالبت اللجنة الدولية للصليب الاحمر للدول الاطراف في إتفاقيات جنيف وكان هذا اثناء إنعقاد المؤتمر الدولي الثامن والعشرين للصليب الاحمر والهلال الأحمر والذي تم إنعقاده عام 2003 ، بأن تخضع كل الأسلحة الجديدة والوسائل والأساليب الحربية الجديدة لإستعراض دقيق ومتعدد التخصصات (الموصلي، 2021، الصفحات 12-13).

المطلب الثاني : أنواع الهجمات السيبرانية و مخاطرها :

أ/ أنواع الهجمات السيبرانية :

1- الفيروسات(virus): يعتمد فيها الهاكرز هنا إلى زج الفيروسات وديدان الأنترنيت ونشرها في شبكات المعلومات الوطنية والأنترنيت بقصد إحداث خلل مؤقت أو دائم في ملفات ونظم التشغيل المستهدفة، والفيروسات كما حددها التقرير الصادر عن المركز القومي للحاسبات في الولايات المتحدة الامريكية : هي برامج مهاجمة تصيب أنظمة الحاسب بأسلوب يماثل إلى حد كبير الفايروسات الحيوية التي تصيب الإنسان (خالد، 2022، صفحة 08).
2- برامج القنابل المعلوماتية : تعرف القنبلة المعلوماتية باسم (الشفرة الموقوتة)؛ وهي نوع من أنواع الهجمات عبارة عن برامج الخبيثة صغيرة الحجم يتم إدخالها بطرق غير قانونية وإخفائها مع البرامج

الأخرى وهذه البرامج من الناحية الشكلية ليست ملفا إلكترونيا واحد وإنما هي شفرة اتصالية إلكترونية وذلك بتقسيمها إلى مجموعة معينة و متفرقة الأماكن في الحاسوب ،بحيث يصعب التعرف عليها وتتجمع فيما بينها بحسب الأمر المعطى لها من زمان و مكان معينين لذلك لا يمكن اكتشافها لأشهر وهذا النوع من البرامج تستخدم لتدمير المعلومات والبيانات الإتصالية والإلكترونية وتدمر أنظمتها الإتصالية. (الموصلي، 2021، صفحة 17).

3- هجوم حجب الخدمة (A.denial.of.service DOS) : هو نوع من الهجمات التي تتعرض لها الشبكة و ينتج عن هجوم DOS نوعا من قطع خدمة الشبكة على المستخدمين أو الأجهزة أو التطبيقات وهي نوعان : - إرسال كمية هائلة من البيانات مما يسبب في وجود بطء في الغرسال او الإستقبال أو تعطل الجهاز او الخدمة.

- الحزم المنسقة بشكل ضار يحدث هذا عندما يتم إرسال حزمة منسقة بشكل ضار إلى جهاز مستضيف أو تطبيق بحيث لا يتمكن المستقبل من معالجتها و هناك نوع أخر يندرج ضمن هجوم حجب الخدمة و هو هجوم حجب الخدمة الموزع متشابه مع هجوم DOS و لكنه ينشأه من مصادر متعددة منسقة. (حمود، 2022).

4- أحصنة طروادة :يعتبر نوع من االبرامج الضارة ، حيث يقوم هذا الأخير على التلاعب بأجهزة الكمبيوتر المستهدفة ، و إلهامها بأن هذا البرنامج سيؤدي وظيفة مفيدة ، حيث حصان طروادة يستطيع الوصول إلى الكمبيوتر المصاب دون تصريح ، كما يمكن لهذا البرنامج أن يسبب أضرار خطيرة و ذلك عن طريق حذف الملفات و تدمير المعلومات على النظام ، بالإضافة إلى إنشاء باب

خلفي على أجهزة الكمبيوتر التي تسمح لمستخدمي البرامج الخبث الوصول إلى النظام ، و ربما بتسوية المعلومات السرية أو الشخصية ، على عكس الفيروسات و الديدان ، فبرنامج أحصنة طروادة يتكاثر من خلال إصابة ملفات أخرى .

5-الإختراف الإلكتروني : و هو عبارة عن نظام أو برنامج إلكتروني إلكتروني يتم إنشاءه من أجل إستغلال معلومات الخصم و تدميرها و كذلك إتلاف نظامه الحاسوبي ، و هذا بهدف التقدم على الخصم أمنيا و عسكريا و سياسيا . و هناك عدة مستويات تميز هذه المواجهة سواءا على المستوى الفردي أو المؤسساتي أو على مستوى الدول . حيث يتخذ الإختراق الإلكتروني عدة أشكال ، و لكن يتم إدراجها في وظيفة واحدة و تتمثل في الدخول إلى لب معلومات الخصم والحصول عليها و المستخدمة لاجل ذلك نظام حسوبي يضرب البنية المعلوماتية للفئة المستهدفة (محمود، 2021، الصفحات 55-56).

6-الفدية : تعتبر هذه الهجمة برمجة خبيثة ، إذ تقم بمطالبة فدية مالية من أجل الضحية ، حتى لا يتم تسريب معلومات خاصة بالضحية ، فهذه الأخيرة قد اثرت على 300000 جهاز حاسوب في 150 دولة في العالم ، كما تسببت هجمات wannacry في تعطيل بيانات أساسية و استراتيجية على مستوى العالم .

فهذا التعطيل قد مس وزارات حكومية و بنوك و مقدمي خدمات اتصالات وغيرها ، فإن ظهور هذه الهجمات يهدد إنهيار الأنظمة التي تقوم بحماية المجتمع عند قيامه بمهامه الأساسية في كثير من البلدان ، لذافالخطر يتزايد من هذه الهجمات الضارة لأنها تتم عن طريق دول عالمية في بعض الأحيان .

إن تجربة هجمات wannancry وضحت بأن البيانات التحتية للكثير من المؤسسات قد تكون لها قابلية عالية للتعطيل بسبب هذه الهجمات و مثال على ذلك

ما تعرض له قطاع الطاقة الأوكرانية في عام 2015 من إعتداءات أدت بدورها إلى التسبب في غلق مؤقت لأكثر من 30 محطة توليد الطاقة فرعية و قطع إمداد الطاقة عن اكثر من 230 الف شخص. (بانقا ع.، 2019، صفحة 16) ، إن فيروسات الفدية إذا نجحت في الوصول إلى النظام فإنها تقوم بتشفير الملفات الخاصة بالخصم ,وهنا لايستطيع هذا الأخير بفك تشفير الملفات الموجودة على النظام ، و هنا يكون المصاب أمام خياران فالأول يتمثل في الإستسلام و تقديم الفدية المطلوبة أما الثاني يتمثل في القيام بزيارة الموقع الإلكتروني noransom.kaspersty.com مع معرفة إذا كان المصاب يمتلك برنامج فك التشفير الذي يقوم بتشفير الملفات (سعد، 2020، صفحة 18).

7.-تصيد المعلومات : إن هذا النوع من الهجمات يعتبر من الأساليب التي تشكل إستخدامها مضرا لتكنولوجيا المعلومات و الغتصالات ، بالإضافة إلى تهديد أمن الانترنيت حيث هذه الأخيرة تتمكن من جعل مستخدمي الانترنيت يقومون بفضح معلومات سرية ، أو القيام بجرائم كتبييض الأموال ، و كذلك التعدي على الملكية الفكرية ، بالإضافة إلى أنها تسهل عملية الإبتزاز .

وإن عمليات التصيد تتم عن طريق البريد الإلكتروني ، و هنا يتم توجيه رسائل إلى المرسل يطلب منه إعطاء بياناته كرقم الحساب المصرفي بغرض تحويل مبالغ مالية معينة إليه ، مقابل نسبة مئوية من المال و كذلك قد يطلب من المرسل تعديل كلمة المرور أو التأكيد عليها أو تعديل المعلومة أو بيان شخص أخر ،مما يساعد منفذين هذا النوع من الهجمات للدخول إلى نظام مالي من خلال إستخدام هوية الشخص المستهدف .

و لكن هذه المحاولات في الوصول إلى المستهدف لا تقتصر على البريد الإلكتروني ، بل تتعدى ذلك إن تكون عن طريق التراسل المباشر ، حيث نجد

القراصنة يقومون بتوجيه رسائلهم عن طريق وصلات بمجرد الضغط عليها يحمل برنامج التجسس أو فيروس على الجهاز الذي يتم عبره الإتصال .

و من هنا فإن إحدى الشركات التي تقدم خدمات تحويل الأموال بالولايات المتحدة الأمريكية فقد تعرض نظامها للإقتحام من قبل مجرمون ، حيث تمكنوا من الوصول إلى أصحاب ملايين بطاقات الإئتمان و أرقامها ورموز الأمان فيها (جبور، 2016، صفحة 56).

8-تجسس المعلومات spyware information :

إن وسائل التجسس التقني و المعلوماتي ؛ تعتبر من أشهر أسلحة الحروب الإلكترونية ، حيث تم إستخدام هذا السلاح منذ بداية إستعمال الإنساني لوسائل الإتصال والتواصل . وهذه الأخيرة أي وسائل التجسس المعلوماتي عدة أشكال، فمنها ما يتم عبر التجسس والتنصت على المعلومات الصادرة من أجهزة الحواسيب، أو الصادرة عن المحطات الطرفية ،أو إعتراض المراسلات الإلكترونية الصادرة عن الأقمار الصناعية , وكذلك الهواتف المحمولة ، وغيرها من وسائل التجسس المعلوماتي ذات الطابع القديم أو الحديث (محمود، 2021، الصفحات 49-50) .

9- الرسائل الصامتة messages silent : وهي عبارة عن برمجة تقنية مخصصة للهواتف ، إذ هذه الرسائل يتم برمجتها للهواتف المحمولة الذكية من خلال فئة الجيل الثالث وهنا حامل الهاتف يمكنه الشعور بوصولها ،بحيث تساعد مرسلها على تحديد مكان تواجد الشخص بدقة ، وهذا يتم عن طريق إستخدام معادلة تقوم بإحتساب قوة إشارة الموجات المنبعثة من الجهاز المحمول تبعا لأقرب ثلاث مراكز مستقلة لهذه الموجات ، وهذه التقنية قد أثارت العديد من

الأزمات في المجتمعات الغربية ، كونها تحتوي على جانب من التعدي على الخصوصية (محمود، 2021، صفحة 58) .

ب/ مخاطر الهجمات السيبرانية :

إن الهجمات السيبرانية باتت الأخطر وأكثر فتكا على الأطراف الفاعلة من الدول ، كما تزداد خطورة هذه الأخيرة في ظل التطور التكنولوجي ، خاصة الدول المتقدمة التي تستخدم الإدارة الإلكترونية .

1-مخاطرها على الأفراد :

لقد أدي ظهور الحاسبات الألية والإعتماد على شبكات الأنترنيت بكثرة إلى تغيير شكل الحياة في العالم وتشكيل خطرا وتهديدا لسلامة الفرد ، إذ أصبح هذا الإختراع بمثابة لغم داخل كل بيت خاصة بعد الدخول إلى شبكة المعلومات الدولية .

ومن هنا فغن الحفاظ على خصوصية كل فرد اصبح من المستحيلات ، وذلك نظرا إلى تزايد الهجمات السيبرانية التي تهدد هذه الخصوصية (شاوشة، 2020، الصفحات 41-42) ، وهذا من خلال سرقة البيانات الشخصية وتسريبها وكذلك إستخدامها بدون إذن بالإضافة إلى إختراق أنظمة المعلومات ، ويتم أيضا الإعتداء على الملكية الفكرية والإحتيال . (جبور، 2016، صفحة 32).

كما نجد أيضا ان هذه الهجمات تقوم بالتهديد والإبتزاز المعلوماتي وهو ما يمثل خطرا كبيرا على الأفراد ، حيث شهدت شبكة الأنترنيت حالات للإبتزاز المعلوماتي وذللك عن طريق أشخاص تمكنو بإستخدام وسائل مختلفة من إختراق نظام الامن للبريد الإلكتروني أو التنصت أو التجسس على حلاقات الدردشة عبر

مواقع التواصل التواصل الإجتماعي وهذا النوع من الهجمات عادة ما يستهدف الشخصيات المعروفة سواءا الحكومية او العسكرية.

ومثالا على ابتزاز الشخصيات ما حدث في امريكا حيث نفذ مخترقون هاكرز المعروفون بإسم ارايفيل الذين قاموا بتهديد الرئيس الأمريكي دونالد ترامب بنشر معلوماته الشخصية ، حيث قام المخترقون بالمطالبة بفدية تقدر ب 42 مليون دولار (شاوشة، 2020، الصفحات 41-42).

1-مخاطرها على المؤسسات :

إن الهجمات السيبرانية تشكل خطرا كبيرا على المؤسسات وذلك من خلال إختراق شبكات اتصالاتها والوصول الى قواعد البيانات التي تتضمن المعلومات الحيوية عن أنشطتها وخدماتها المختلفة .وبالتالي فقد اصبح التجسس على مختلف أنشطة الشركات مصدر قلق . كذلك من مخاطر هذه الهجمات على المؤسسات إسقاط موقع المؤسسة على الأنترنيت وذلك عن طريق تلقي الشبكة العديد من الرسائل المولدة تلقائيا دون توقف إلى أن تصل إلى تعطيل الموقف وتعجزه عن الخدمة تماما حتى يسقط وبالتالي تسقط معه جميع المعاملات التجارية والمالية الإلكترونية التي يوفرها موقع المؤسسة لعملائه وشركائه وإضافة إلى هذا هناك رسائل أخرى تتعرض لها المؤسسات مثل فك شيفرة السرية للبيانات التي تتم تبادلها خارجيا مع الأخرين سواءا كانوا عملاء أو وكلاء او ماشابه ذلك ، ومثال ذلك ما قام به الشاب من النرويج الذي جعل العالم يعرف تهديدا وكان ذلك من خلال نشر برامج في عدة أسطر وهذا الأخير يتم من خلاله فك الشيفرة الرقمية التي تبث بها أفلام عن الشبكة لهذا ما يسمى السطو على المؤسسات .

3-مخاطرها على الدول:

إن الهجوم الإلكتروني يعتمد على نشاط او فعل مقصود ومتعمد فذلك لدوافع سياسية من أجل التأثير على الدول والرأي العام العالمي إذ يعتبر الفضاء الإلكتروني عاملا مساعدا وسيلة في تنفيذ هذا العمل الإلكتروني ، ولقد شهدت الاونة الأخيرة إرتباطا واسعا بين الانترنيت والهجوم السبراني ، إذ نجد الحروب الوقعة التقليدية قد تحولت إلى حروب رقمية ، ولهذا نجد أن الهجوم الإلكتروني أصبح يشكل خطرا كبيرا على الدول فيما يمكن أن يخلف أضرارا جسيمة وخسائر مالية ضخمة كتعطيل عمليات التحويل المالي ، وكذلك الدخول والولوج إلى شبكات التحكم في المرافق العامة وهذا ما يتسبب في شلل البنى التحتية الأساسية أو تدميرها كليا ، ومن هنا قد أصبحت الدول معرضة للدمار الشامل وهذا ليس عن طريق الأسلحة التقليدية بل عن طريق الأسلحة البيولوجية المعلوماتية والتي تتمثل جيوش الفيروسات التي تقوم هذه الأخيرة بتحطيم البنية المعلوماتية ومن الأسلحة التي يعتمد عليها الهجوم الرقمي في تنفيذ عملياته القنابل الإلكترونية والتي تقوم بتعطيل الإتصالات والتشويش عليها والتنصت على المكالمات وكذلك بث معلومات مظلة بالإضافة إلى هذا استهداف شبكات الحاسوب وتخريبها عن طريق نشر فيروسات ومسح الذاكرة الخاصة بالأجهزة المعادية .

إن الهجوم الإلكتروني يشكل تهديدا لكافة الدول فهو يهدد سياستها وأمنها واقتصادها. (شاوشة، 2020، الصفحات 46-49)

1-مخاطرها على التجارة الإلكترونية:

1 المخاطر الأمنية للهجمات على التجارة الإلكترونية:

نظرا للإستخدام الواسع لتكنولوجيا المعلومات والإعتماد عليها بشكل كبير تتفاقم مخاطر الهجمات السبرانية بشكل كبير . بالإضافة إلى الثغرات الأمنية المتعددة في التعاملات التجارية الإلكترونية حيث تندرج هذه المخاطر في النقاط التالية:

أ) القرصنة أو تعطيل نظام المعلومات :

هناك العديد من الوسائل الهجومية الشائعة لتخريب وتدمير المعطيات التي تتم في التعاملات التجارية ، إذ نجد على سبيل المثال الفيروسات فهي واحدة من هذه الوسائل الشائعة بكثرة .

وللقرصنة عدة مخاطر تتمثل في :

خرق الحماية المادية وهذا يتبع عن طريق التفتيش في المخلفات التقنية والمقصود بها بحث المخترقون في مخلفات المؤسسة التي قد تساعدهم في إختراق نظام المعلوماتي للمؤسسات التجارية والمالية وقد تكون هذه المخلفات إما عبارة على أوراق مكتوبة كلمة سر أو قد تكون أقراص صلبة التي تم رميها بعد استعمالها .

الإلتقاط السلكي : وهو تنصت أو إستنزاف المعلومات وهذا عن طريق سلك يتم ايصاله مع شبكة توصيلات النظام. والطريقة قد تكون معقدة أو سهلة وهذا حسب نوع الشبكة.

ب)استغلال الشبكات الإجتماعية المعلوماتية :

مخاطر محرك غوغل Google إن هذا الأخير يعتبر من أهم محركات البحث في العالم وهذا لإحتوائه على الكم الهائل من المعلومات اللامتناهية التي يتم تحميلها

وتغييرها من ثانية إلى أخرى بالإضافة إلى الرغبة في الرد وتقديم الأجوبة والمعلومات ، وهذا بغض النظر عن عدد الصفحات الغير منتهية التي جعلت منه الوسيلة الهامة في بث الأفكار الشائعة وكيفية قرصنة المواقع والحصول على كلمات سر. ولهذا فإن شركة غوغل قد تلقت العديد من الشكاوي بسبب التعدي على خصوصية الأفراد وذلك عن طريق أمور غير قانونية وهذا لإنعدام الرقابة (شاوشة، 2020، الصفحات 50-51) .

ثانيا :المخاطر التجارية للهجمات السبرانية:

إن الهجمات الإلكترونية لا تختصر فقط في التهديد الأمني بل تصل إلى التهديدات التجارية إذ نجد من هذه الأنشطة:

- موقع الشبكة المعلوماتية في المعاملات التجارية:

يعتبرالهجوم السبراني أكثر خطورة وهذا نظرا للتطور المتسارع لتكنولوجيا المعلومات والإعتماد عليها بشكل كبير في جل التعاملات مما يساعد في التحكم الكامل بإتصالات الأفراد ، وهذا ما أدى إلى اتساع سرعة عملياتهم والذي أصبح من الصعب مكافحة هذه الهجمات ، ولهذا فإن الوظيفة الرئيسية للتجسس على التعاملات الإقتصادية تتمثل في منع التبادلات التجارية وهذا عبر وسائل التكنولوجيا ، بالإضافة إلى التجسس على المحادثات عبر الهاتف والأنترنيت والتطلع على الوثائق الرسمية وكذلك مهاجمة المراكز الرئيسية الإقتصادية بتخريب الحواسيب أو أنظمة الإتصال وقاعدة البيانات (شاوشة، 2020، صفحة 53).

بالإضافة إلى مخاطر الهجمات السبرانية على الدول والأفراد والمؤسسات نجد ما يسمى بمخاطر الجيل الجديد من الهجمات السبرانية حيث تميزت هذه

الأخيرة بأنها هجمات محدودة ومؤقتة في العقد الأخير أي أنها لا تؤثر على قطاع كبير من المستخدمين وأيضا لا تكون سبب في شلل الأنترنيت أو التلاعب بالخدمات الحكومية وإيقاف خدماتها بصورة كبيرة إلا بإستثناء الهجمات التي لها طابع عسكري مثل: ستاكسن نت وكان إستخدام هذا الفيروس ضد مواقع إيران النووية التي تسبب في تعطيل أجهزة الطرد المركزي ، إذ نجد كذلك هذه الهجمات بدورها استهدفت الحسابات البنكية وإخترقت المواقع الإلكترونية والصفحات الرسمية على مواقع التواصل الإجتماعي.

وهذه الهجمات المحدودة والمؤقتة ظلت على هذه الحالة الى أن جاء ما يعرف بهجوم أنترنيت الأشياء ، وقد وقع في الو.م.أ وكان ذلك في يوم الجمعة 21 أكتوبر2016 ، وهنا كان التحول الرئيسي في شكل نوعية الهجمات السيبرانية ، حيث إستطاع بعض القراصنة من السيطرة على أجهزة تشغيل الموسيقى ، وتأمرت متعلقة بالأنترنيت وبعض الأدوات الإلكترونية المنزلية التي تعكس مفهوم أنترنيت الأشياء والتي يتم استخدامها لإطلاق هجوم إلكتروني على العديد من المواقع الإلكترونية مثل : تونيت ونتفليكس ، وكذلك بعض الشركات مثل شركة dyn DNS والذي نتج عن هذا الهجوم إغراق الخوادم المشتغلة بمليارات الطلبات التي تتعدى من قدرة الخوادم على معالجة البيانات والإستجابة للطلبات ، وبالتالي إنقطاع الخدمة عن الكثير من المستخدمين لمدة من الزمن تصل إلى الساعة ، وهذه الهجمات لم تتوقف عند هذا الحد بل تعدت إلى هجمات أخرى ، فبعد حالة إنقطاع الخدمة جاءت هجمات الفدية الخبيثة" Ransomware حيث هذه الأخيرة قد تسببت في خسائر مالية كبيرة فقد أدت إلى إيقاع قطاع الصحة في بريطانيا عن العمل وإلغاء العديد من العمليات الجراحية وكذلك أدت إلى تأجيل

الحالات الصحية الطارئة ، إذن فإن هذه الهجمات لقد كان لها تأثير على قطاع كبير من المستخدمين في وقت قياسي (خليفة، 2019، الصفحات 108-109).

المطلب الثالث: دوافع الهجمات الإلكترونية :

إن الهجمات الإلكترونية التي تصيب أنظمة المعلومات او الانظمة الحاسوبية والشبكات التي تحفظ وتخزن فيها المعلومات وتنقل عبرها تتمثل في عناصر وهي كالأتي :

1-وجود الدافع :

قد يكون الهجوم الإلكتروني بدافع الرغبة في الإنتقام من الطرف المستهدف ، أو من أجل الحصول على المال أو كذلك الرغبة في الأستئثار بأكثر قدر من الزبائن ، وهذا بحث بين الشركات المنافسة ، لذا قد نجد شركة ما تقوم بمهاجمة أنظمة المعلومات وإخنراق المواقع التابعة للشركة المستهدفة وكذلك تعطيلها وهذا العمل العمل لا يقوم به أي شخص بل محترفين في هذا المجال ، وذلك كله من أجل منع وصول الزبائن لموقع الشركة . فالدافع أيضا قد يكون رغبة المهاجم في إثبات قدراته الفنية ، بالإضافة قد كون دافع الهجوم بأغراض سياسية ومثال على هذا ما حدث لموقع الجزيرة في 27 مارس 2003 م لأن المهاجمين كان في إعتقادهم أن قناة الجزيرة كانت منحازة للجانب العراقي في ظل الغزو الأمريكي للعراق ومن نتائج هذا الهجوم ظهور العلم الأمريكي على شاشة التلفزيون القسم الإنجليزي مكتوبا عليه ما معناه : دعوا الحرية تدق ناقوسها . أي أن أمريكا قد جاءت من أجل تحرير العراقيين (حزام القريطي، 2022، صفحة 39). وكذلك من الدوافع السياسية نجد أن الهجوم يتمثل إختراق أجهزة العدو من شبكات الأنترنيت وأنظمة المعلومات الخاصة ، وهذا من أجل تعطيل خدماته في كافة

المجالات عن طريق سرقة قواعد معلوماته السرية وتخريبها أو تعطيلها (الجواد، 2020، صفحة 45).

2/ وجود طريقة لتنفيذ الهجوم :

إن من أجل تحقيق هجوم ناجح لابد أن يكون للمهاجم تصور وخطة واضحة ومدروسة تحقق الغرض . وهذا ما يميز المهاجم المحترف من المهاجم غير المنحرف .

ولهذا من أجل صد الهجمات أو تكون أضرارها خفيفة ، يجب معرفة طرق الهجوم وخططه وكذلك متطلبات نجاح التنفيذ .

3/ وجود ثغرات :

ونقصد بهذه الأخيرة أن هناك نقطة ضعف في تصميم أو تهيئة البرمجيات ، أو قواعد تخزين المعلومات أو في الاجهزة التي يتم فيها حفظ المعلومات ، بالإضافة إلى معدات أو برامج تشغيل الشبكات التي تمر المعلومات عبرها (حزام القريطي، 2022، صفحة 40).

وأيضا من الدافع نجد هناك دوافع فردية غذ أن محاولات الإختراق او الهجوم على مستوى الفرد يبدأ بين الأفراد ، وذلك بدافع التباهي والإفتخار بالنجاح في إختراق أجهزة أصدقائهم الأخرين ، كذلك بدافع التحدي ، لكن مع مرور الوقت فهذه الحالة أصبحت هواية عند بعض الأفراد مما أدى ببعض الأفراد إلى تشكيل منتديات للتدريب على الإختراق ، وقد تفاقمت هذه المشكلة وتزايدت خاصة بعد إقالة المبرمجين من بعض الشركات المنافسة ، مما أدى إلى إفراغ جل غضيهم تجاه تلك الشركات وذلك لغرض الإنتقام من شركاتهم التي كانت سبب في إقالتهم من عملهم .

أما فيما يخص الدوافع الإقتصادية ، إن ما يجري بين الشركات العالمية من منافسات تجارية . فإن عملية الإختراق أصبحت جد مهمة للعديد من تلك

الشركات ، وهذا بدافع الإطلاع على كل معلومات الشركات المتنافسة من أجل تحقيق أرباح تجارية بالإضافة إلى محاولة ضرب إقتصاديات الدول الأخرى وهذا من خلال الإطلاع على معلومات تخص تلك الإقتصاديات و اليات نموها بغرض الحد منها (الشميري و علي إسماعيل، 2020، صفحة 280).

خلاصة:

نستنتج أن الهجمات السيبرانية عبارة عن هجوم تقوم به دولة ضد أخرى بطريقة غير قانونية بهدف تعطيل وظيفة شبكة الكمبيوتر والحصول على معلومات سرية، وفي ظل التطور التكنولوجي أصبحت الهجمات السيبرانية تشكل وسيلة وأسلوب للقتال في الوقت نفسه ، ويتضح أن الهجمات السيبرانية لا تقتصر على نوع واحد بل على مجموعة من الأنواع المتعددة وهذه الأخيرة كانت لها مخاطر على كافة المستويات.

الفصل الثاني

الفصل الثاني: تأثير الهجمات السيبرانية المغربية على العلاقات السياسية الجزائرية:

إن الدولة الجزائرية كغيرها من الدول تتعرض للعديد من المخاطر، والتي تمثلت في الهجمات السيبرانية ، التي شهدتها في الآونة الأخيرة وكل هذا جاء نتيجة للثورة التكنولوجية الحديثة وتطورها ، خاصة بعد إنتشار وسائل التواصل الإجتماعي والعديد من المواقع الإلكترونية والتي تهدد إستقرار الوطن. إذ أن هذه الهجمات تستهدف الجزائر من كل الدول ،لكن في الفترة الأخيرة قد تعرضت لهجمات من طرف المملكة المغربية ،مما أدى إلى زيادة حدة التوتر العلاقات السياسية بين الدولتين، وهذا كان نتيجة لإستخدام المغرب نظام تجسس بيغاسيوس والذي كان بمثابة القطرة التي أفاضت الكأس بين البلدين .

المبحث الأول : مخاطر الهجمات السيبرانية المغربية على الدولة الجزائرية:

لقد نجحت العديد من الحكومات في استخدام تقنيات متطورة للتجسس من خلال الشبكة العنكبوتية على الدول أو المنظمات و مراقبة المعلومات التي يتم تداولها حول العالم ، وتعتبر الدولة الجزائرية من بين الدول التي تعرضت لهذا التجسس من قبل المملكة المغربية من خلال برنامج يعتبر الأخطر في العالم وهو نظام بيغاسيوس الإسرائيلي.

المطلب الأول: أنظمة التجسس الإلكترونية التي تعرضت إليها الجزائر :

لقد تعرضت كيانات ووزارات الدولة الجزائرية إلى هجمات إلكترونية مست بمنظوماتها وبنيتها الإتصالية وخذا من خلال إستخدام مجموعة من الأنظمة التجسسية بغية الحصول على معلومات سرية هامة وإستعمالها كورقة ضغط على الجزائر ,وكان من بينها برنامج الفدية ونظام بيغاسيوس حيث تم تسليط الضوء على نظام بيغاسيوس الإسرائيلي .

1-نظام بيغاسيوس:

يعتبر نظام بيغاسيوس(pegasus)أحد البرامج أو الفيروسات الخبيثة والتجسسية التي أنتجتها شركة (كوادريم)وهي فرع من الشركة الأم NSO groupe للكيان الصهيوني ويعد من أكثر البرامج تطورا ولديه القدرة على إختراق مليارات الأجهزة التي تعمل بأنظمة تشغيل IOS أو أند رويد .

اول كشف في العالم عن نظام التجسس بيغاسيوس جاء عام 2016 حيث كشف تقرير Citizenlab وهو مختبر دولي في الأبحاث التقنية مقره في Toronto canada عن ثغرة تم إستغلالها من قبل برنامج تجسس متطور للغاية ووفقا لهذا التقرير قد تم إختراق هاتف الناشط الإماراتي أحمد منصور وقد أدى هذا الإختراق بسجن الناشط الإماراتي أحمد منصور ، وقد سميت الثغرة على هاتف منصور Zéro clik .

هذا ويعد نظام بيغاسيوس من البرامج الخبيثة التي تعمل بطرق مختلفة وجزء من تطويرها يتعلق بتطوير آليات الإستهداف الإتصالية ، ففي السابق كان يتم إستهداف الأشخاص من خلال رابط إلكتروني أو رسالة .

لكن مع بيغاسيوس هناك أنماط إستهداف حديثة ، إذ يكفي أن تقوم جهة معينة بالإتصال بالشخص المستهدف لفترة ما بين 8إلى 10 ثوان ليتم تنزيل وتثبيت البرنامج حتى لو لم يتم الرد على المكالمة .

وعادة هناك طرق معينة يمكن للشخص إكتشاف إستهدافه ، لكن مع برنامج بغاسيوس الأمر مختلف تماما لكونه برنامج ذكي جدا فيصعب على شخص غير تقني أو مهندس كشفه .

وبالنسبة لنظام بيغاسيوس المؤشرات التقنية يصعب على غير الخبير كشفها ، لأن الإختراق الإلكتروني الناجح هو الإختراق الصامت الذي لا يمكن الكشف عنه .

فقد إستهدف بشكل أساسي نشطاء حقوق الإنسان والصحفيين والسياسيين على وجه الخصوص وبالتالي الإستهداف يكون محدد (مسحال، قناة الجزيرة، 2021).

المطلب الثاني : أضرار نظام بغاسوس على البنية الإتصالية في الجزائر :

على اعتبار أن نظام بيغاسيوس يعد من البرامج الإلكترونية الضارة ، فكانت أضراره تتشابه نوعا ما أو إلى حد كبير مع البرامج الخبيثة الأخرى وهي كالتالي :

1 - الزيادة في استخدام وحدة المعالجة المركزية .

2 - الانخفاض في سرعة عمل الأجهزة الإلكترونية .

3 - تعطيل النظام الإتصالي للحصول على المعلومات أو الملفات المراد الوصول إليها .

4 - تخريب الملفات الإلكترونية الحساسة وتغييرها قصد تشويه الحقيقة أو حتى سرقتها للضغط على الدولة الجزائرية (الغزال، 2019).

5_ الوصول إلى المعلومات الخاصة ، خاصة أن أجهزة الكومبيوتر أصبحت مركزية أكثر

6_ التلاعب النفسي لمستخدمين الأنترنيت لأداء أو تحقيق هدف معين

7_ تشفير الملفات والمجلدات الإلكترونية مما يتيح الولوج إلى ملفات إلكترونية مسبقا (Machine Learning to Predict the Likelihood of a Personal Conputer to Be Infected with Malware, 2019) .

8_ من أضرار نظام بيغاسيوس كما قلنا سابقا التجسس وذلك حتى على قائمة الاتصالات الموجودة في الأجهزة سواء للهواتف أو الحواسيب.

9- من أضراره أيضا أنه قد يحدث استنزاف للبطارية الغير المبرر لأجهزة الاتصال (خطورة الفيروسات و البرمجيات الخبيثة على أجهزة الحاسب ، 2021).

بمعنى أخر فإن نظام بيغاسيوس التجسسي عمل على الإضرار بشكل مباشر بالعاملين بالموارد والكفاءات والأهم من ذلك الإضرار ب البنى التحتية للمنظومة الإتصالية .

مع العلم أن الجزائر تعتبر من أضعف الدول في مجال التكنولوجيات والأجهزة الإتصالية وبالتالي بنية إتصالية ضعيفة وبالتالي كثرت الثغرات الإلكترونية التي عمل نظام كنظام بيغاسيوس للتجسس على استغلالها .

المبحث الثاني : جهود الدولة الجزائرية في التصدي للهجمات السيبرانية :

نظرا لتزايد الهجمات السيبرانية وخطورتها ، فإن الدولة الجزائرية تحاول وتبذل مجهودات مستمرة للتصدي ومكافحة هذه الهجمات ،إذ تقدم بعض السبل والطرق من أجل السيطرة على هذه المخاطر ، ويظهر هذا من خلال ضرورة التحلي بالعقيدة الأمنية والجزائرية بالمزبد من اليقضة والتحكم في التكنولوجيا الحديثة . بالإضافة يجب ترقية وتكوين مستوى الأفراد في مجال أمن وحماية المعلومة .

المطلب الأول : الإستراتجيات الإتصالية المعتمدة من طرف الجزائر :

في إطار رسم السياسة الأمنية العامة ، عملت الجزائر على وضع مخطط لتفادي إختراق أنظمة المعلومات الإلكترونية الحساسة لرئاسة الجمهورية ، وزارة الدفاع ، أجهزة الأمن .

يعتبر الأمن السيبراني كإحدى الأولويات والإستراتيجيات لمواجهة أو التصدي لهذا النوع من الهجمات ، حيث كانت الدول الرائدة في مجال التصدي للهجمات السيبرانية قد أثبتت أن النجاعة في التطبيق وفعالية الوسائل المستعملة لا يمكن لها أن تتجسد ما لم يكن هناك تنسيق وتخطيط محكم ، وعليه ترجمت الجزائر إلى رسم إستراتجياتها مركزة على النقاط التالية :

- تحديد المخاطر.
- محاولة إيجاد الثغرات الإلكترونية في الأنظمة الإتصالية الجزائرية ومعالجتها .
- إتخاذ التدابير اللازمة كالتكوين في البرمجيات الإلكترونية .
- التكوين والتربية الإتصالية والتحصين الإلكتروني.
- التحديث الإلكتروني للبنية الإتصالية للمعلومات الإلكترونية (بوازدية، 2019، الصفحات 16-17) .
- التعلم الالي للتنبؤ باحتمالية إصابة جهاز كمبيوتر ببرامج ضارة.
- إجراء تقييم أمني بما في ذلك اختبار الاختراق و التحقق من الأمن أثناء إقتناء الأجهزة الإلكترونية.
- تحديد العوامل التي تزيد من خطر الإصابة بالبرامج الضارة و اتخاذ الإحتياطات اللازمة للوقاية من الهجمات الإلكترونية .
- تطوير الترسانة الإلكترونية للأجهزة حتى تتماشى مع عصر الرقمنة .

- التوعية المستمرة للأفراد والمواطنين من خلال التحذير من إستخدام مواقع التواصل. الإجتماعي التي باتت تمثل ملاذا آمنا لهؤلاء المهاجمين السيبرانيين.

إضافة إلى أن الإستراتيجية الإتصالية السياسية في الجزائر فتمثلت في :

- توفير مايعرف بالدفاع الإلكتروني من خلال مراقبة الأنظمة التي تحمي الدولة من كافة التهديدات.
- متابعة حالة تقدم نشاطات تجسيد السياسة الشاملة للدفاع السيبراني الرامية لضمان فعالية الحماية ضد التهديدات السيبرانية التي تستهدف أنظمة الإتصالات والمعلومات الإلكترونية (بونيف، 2019، الصفحات 08-09) .

هذا وكما يمكن أن تنتهج الجزائر مجموعة من التقنيات التكنولوجية التي يمكن عدها كأحد الإستراتيجيات الإتصالية التي يمكن أن تعتمد عليها مستقبلا الدولة الجزائرية والمتمثلة في :

1-<u>التقنية الأولى:</u> جدران الحماية أو ما يعرف بالجدران الناري (Firewall) حيث يعتبر من أهم وسائل الدفاع التقنية لمواجهة الهجمات الإلكترونية ومنعها من إختراق الأجهزة الإلكترونية ، أما البرامج الضارة يمنعها من الدخول أو التسلل إلى الجهاز وهذه التقنية ظهرت لها عدة أجيال فالجيل الأول ويعرف بمرشحات العبوة وهي مخصصة لنقل البيانات الإلكترونية من الحواسيب على شبكة الانترنت وهنا يجب أن تتطابق العبوة لشروط الجدار حتى يسمح بمرورها وإذا كانت عكس ذلك سوف يتم رفضها من طرف جدران الحماية ويتم التخلص منها .

أما الجيل الثاني وهو ما يسمى ب فلتر محدد الحالة هذا الجيل يقوم بمراقبة مجموعة من المعلومات الإلكترونية المستقبلة ويقارنها بمجموعة المعلومات الإلكترونية الواردة ضمن نفس السياق والتي لا تتطابق مع قواعده يقوم برفضها

وهذا يدل على أنها زرعت في السياق وليست جزء منه وهذا ما قد يدل على أنها عبارة عن برامج ضارة .

والجيل الثالث والأخير والذي من المستحسن أن تعمل به الجزائر في ظل تعرضها للهجمات السيبرانية من خلال برنامج بيغاسيوس هو ما يسمى" بطبقات التطبيقات" (Application Layer Firewall) .

2 - التقنية الثانية : وتعتبر من أكثر آليات إعتمادا في التصدي للهجمات السيبرانية الإلكترونية وهي معروفة بمضادات الفيروسات (Antivirus) فهي تعمل على كشف البرامج الخبيثة التي تلحق الضرر بالأجهزة الإلكترونية ومنعها من سرقة البيانات والمعلومات الإلكترونية الشخصية كما لها القدرة على التصدي لبرامج التجسس وبرامج أحصنة طروادة وغيرها من البرامج الإلكترونية ضارة ، فهناك أسلوبين يتم إعتمادها من طرف هذه التقنية الأسلوب الإلكتروني الأول هو رصد نظام للإشتباه في تصرفات البرنامج والتحقق والفحص في هذا البرنامج ، أما الأسلوب الثاني مضاهاة ملف (File Emulation)

ويتم تنفيذ هذا الأخير في بيئة إفتراضية ، وبتالي من خلال هذين الأسلوبين يستطيع مضاد الفيروسات من معرفة ما إذا كان البرنامج الإلكتروني ضار أو لا.

3 التقنية الثالثة : وهي تقنية أنظمة كشف التسلل (Intrusion Detection Systems) يمكن لدولة الجزائرية إنتهاجها في نطاق التصدي لتعطيل الحواسيب المركزية من خلال جهاز إستشعار للتنبيه عن بداية وقوع إختراق الذي تحتوي عليه هذه الآلية الأخيرة (عبد الواحد، 2021، الصفحات 58-59-60-61) .

المطلب الثاني: تداعيات الهجومات السيبرانية على الجزائر:

أدت العلاقة الشاسعة بين الدول بالفضاء الإلكتروني ، وما خلفته من هجمات سيبرانية إلى جملة من التداعيات سواء من الناحية السلبية أو الإيجابية من نتائج هذه الأخيرة على دول عديدة أبرزها الجزائرو يمكن إبرازها كتالي:

1/تصاعد المخاطر الإلكترونية خاصة مع قابلية الهجوم على منشآت حكومية خاصة من خلال الهجوم عليها عبر وسيط وحامل للخدمات أو شل عمل أنظمتها المعلوماتية ،الأمر الذي يؤثر في وظائف المنشآت .وبالتالي فإن التحكم في مثل هذا الأمر يعد أمرا خطيرا على الدولة الجزائرية.

2/ من تداعيات الهجمات السيبرانية أنها أدت إلى قطع العلاقات مع المغرب وزيادة الإحتقان بين البلدين .

3/ الهجوم السيبراني من خلال نظام بيغاسيوس على الجزائر كان بمثابة نقلة تصورية لما ستكون عليه النزاعات مستقبلا.

4/ كان من أبرز التداعيات التي شكلتها أو أحدثتها الهجمات السيبرانية على الجزائر هي تحديث القدرات الدفاعية والهجومية والإستثمار في البنية التحتية المعلوماتية وتأمينها من خلال تأمين الأجهزة الإتصالية (james, 2022).

5/من تداعيات الهجمات السيبرانية من الناحية السياسية ،فأنها تهدد بتفكيك الوحدة الدولية كما أيضا تؤدي إلى ضعف ثقلها السياسي في المحافل الدولية .

6/ شل أنظمتها وشبكاتها الإتصالية والمعلوماتية وبالتالي فإن التحكم في تنفيذ مثل هذا النوع من الهجمات يعد بمثابة أداة سيطرة إستراتيجية جد مهمة .

7/ هذا و قد عملت الهجمات السيبرانية على دفع الرأي العام للنهوض ضد النظام الجزائري مما أدى إلى التفرقة بين الشعوب الجزائرية وإثارة النزاعات بينهم (كافي، 2022) .

خلاصة:

شكلت الهجمات السيبرانية خطورة كبيرة على الجزائر من طرف الدولة المغربية التي إستخدمت نظام بيغاسيوس الإسرائيلي الذي كان بمثابة الهجمة الإلكترونية لإختراق العديد من الهواتف و الحواسيب ، مخلفا وراءه الكثير من الأثار التي تمثلت في قطع العلاقات بين الدولتين بصفة نهائية ، في حين أن الدولة الجزائرية عملت على مواجهة هذه الهجمات عن طريق الهجمات عن طريق مجموعة من الاستراتيجيات والتدابير الإتصالية.

الجانب التطبيقي

الجانب التطبيقي:

جدول يمثل مجموعة من الأساتذة الذين تم إجراء مقابلة معهم في إطار موضوع البحث:

الإسم واللقب الأستاذ	التخصص	الرتبة	الوقت وتاريخ إجراء المقابلات
مرزوقي حسام الدين	إعلام و إتصال	أستاذ مساعد أ	سا من 13:00إلى15.00 2022-05-11
زيايتة يونس	إتصال تنظيمات	دكتور أستاذ محاضر.ب	سا من 13:40إلى 13:57 2022-05-14
حموش عبد الرزاق	إعلام وإتصال	دكتور	سا من11:20إلى 12:00 2022-05-15
غول لخضر	علم إجتماع تنمية	دكتورأستاذ محاضر.ب	سا من 14:00إلى 14:30 2022-05-16
دندان عبد الغاني	علاقات دولية	أستاذ محاضر	سا من 10:00إلى10:43 2022-05-19
حميداني سليم	علاقات دولية وعلوم سياسة	دكتور	سا من 10:10إلى10:30 2022-05-22
عبادنة محمد أمين	إتصال مؤسساتي	دكتور	من12:30إلى12:45 2022-05-22
بن سعدون	علوم سياسية وعلاقات	أستاذ محاضر	سا من 11:15إلى 11:55

اليامين	دولية		2022-05-23
حلاسي سمير	ذكاء إصطناعي وبرمجة	أستاذ محاضر	سا من 14:00إلى 14:30 2022-05-25
مزيان رياض	علاقات دولية	أستاذ محاضر	سا من 11:20إلى11:40 2022-05-26
زودة مبارك	تكنولوجيا الإعلام والإتصال الحديثة	دكتور أستاذ محاضر.ب	سا 10:52 2022-05-30
فراق محمد أمين	الأمن السيبراني	أستاذ محاضر	سا من10:30إلى 11:00 2022-05-29
برحومة نبيل	شبكات وأنظمة	أستاذ محاضر	سا من 11:15-11:30 2022-05-29
شهرة شمس الدين	الحساب الحاسوبي وتحسين الأداء	أستاذ محاضر	سا من 11:10إلى11:45 2022-05-31

المصطلحات الأكثر تكرارا :

من المفاهيم المتكررة أثناء المقابلة نجد:

*الموقع الجيوستراتيجي.

*الوضع السياسي.

*الحراك.

*الدفاع السيبراني.

*تخصيص ميزانية.

*قطع العلاقات.

*الصحراء الغربية.

*العلاقات الدبلوماسية.

*مسؤولين كبار.

*تسريب المعلومات.

*المنظومة المعلوماتية.

*التوعية.

*التمكن من التكنولوجيات.

تحليل أسئلة المقابلة:

س1: ماهي أبرز الأسباب التي جعلت الجزائر ضمن قائمة الدول العربية الأكثرإستهدافا؟

ج1: وقد تمت الإجابة عن هذا السؤال من طرف جميع الاساتذة وبإختلاف التخصصات بإجابة موحدة تمثلت في أن الأسباب راجعة إلى :

موقعها الجيوستراتيجي و الجيوسياسي ،وكذلك الثروات التي تمتاز بها كالزئبق بالإضافة إلى وضعها السياسي غير المستقر وكذلك الحراك الذي شهدناه في الآونة الأخيرة ،نضيف إلى ذلك توجهات السياسة الخارجية للجزائر التي تجعلها في حالة تضاد مع مجموعة من الدول سواء العربية أو الإفريقية والأوروبية منها أو في ما يخص تصورها للأداء الخارجي خاصة ضد إسرائيل.

يضاف إلى ما سبق طبيعة التوتر السياسي مع المغرب منذ عقود، ما يجعل المنظومة المعلوماتية للجزائر أحد أهداف الاختراق المعلوماتي للجارة الغربية.

أما بالنسبة للجانب التقني فالسبب تمثل في ضعف وهشاشة البينية المعلوماتية والأجهزة الإلكترونية ،إضافة إلى عدم وجود أليات مراقبة وتدقيق لمعرفة التهديدات والإختراقات في وقتها.

وهناك سبب أخر يجعل الجزائر تتعرض للهجمات السيبرانية وهو عدم وجود نظام إنذار مبكر يخص هذا النوع من الهجمات وعدم وجود ثقافة بشأن هذه الهجمات وطبيعتها ومحتواها .

أيضا توجد مسألة أخرى تمثلت في عدم وجود إرادة على مستوى فوقي للتصدي بحزم تجاه هذا الخطر، كذلك ضعف المنظومة الإتصالية في التصدي لهذه المسائل(مرزوقي و زودة و زيايتة و عبادنة وغول و شهرة و حميداني و حلاسي و فراق و بن رحومة و دندان و مزيان و بن سعدون و حموش ، 2022).

س2 ماهي أبرز التحديات التي ستواجه الجزائر في ظل زيادة تعرضها للهجمات السيبرانية ؟

ج2 تمت الإجابة عن هذا السؤال ب:

- إلتزام الجزائر بتطوير بنيتها التحتية الإلكترونية أو الرقمية .
- وضع إستراتجية وطنية على المدى الطويل ؛ أي من 5 إلى 10 سنوات.
- تعميم إستخدام التكنولوجيات والخروج بإستراتجيات وحلول للتعامل مع البيانات وتحليلها والإعتماد على تقنيات الذكاء الإصطناعي .
- إنشاء مراكز أبحاث وأقطاب تكنولوجية حقيقية .

- عدم الإقتصار على وزارة الدفاع فقط للحماية من الهجمات السيبرانية (مرزوقي ، 2022) .

* في حين أجاب الأستاذ على هذا السؤال ب:

تعويض النقص في الجانب الأمني من خلال الحماية الأمنية التقنية والحماية التكنولوجية من خلال تطوير التقنيات التكنولوجية (غول، 2022) .

*أما الأستاذ سليم حميداني فقد أجاب ب:

- يجب تصحيح الوضع أي تقييم الأضرار الواقعة على المنظومة السيبرانية في الجزائر من خلال إعادة هيكلة المنظومة وتكييفها وتحديثها .
- سد منافذ الإختراق من خلال منظومات رقابة حديثة .
- التكوين الداخلي للقوى العاملة في هذا المجال والكوادر البشرية .
- الإرتقاء بالبحث العلمي وذلك من خلال فهم التهديدات الإلكترونية جيدا قبل مواجهاتها .
- تنسيق الجهود الداخلية و الخارجية لتصدي لهذه الهجمات .
- لابد من فهم طبيعة ومصدر التهديدات ومحاولة الإعتراض لها بطرق تناسبها (حميداني، 2022) .

*أما بالنسبة للأساتذة فتمثلت إجابتهم في :

- تطوير وتكوين متخصصين في مجال الدفاع السيبراني.
- تخصيص ميزانية معتبرة من اجل تكوين أفراد وتجهيز مؤسسات أمنية مختلفة، كالجيش والدرك الوطني والشرطة من أجل التصدي لمثل هذه الهجمات.
- هذا وقد أضاف الأستاذ عبد الغاني دندان نقطة أخرى والمتمثلة في الفطنة واليقظة من طرف الدولة الجزائرية في مجال أمن المعلومات (دندان و زياتة و حموش، 2022) .

*وقد أجاب الأستاذ عن التحديات ب:

- يجب على الجزائر حماية مؤسساتها السيادية في الفضاء السيبراني وزيادة فاعلية أنظمة الأمان السيبراني في مواجهة هذه الهجمات (عبادنة، 2022) .

* ومن جهتهما، يقترح كل من الأستاذين مايلي:

تأمين العسكري والمجتمعي ، الإقتصادي والثقافي الإلكتروني، ومن تحدياتها أيضا هي تأمين الشبكة حتى لا تتعرض للإختراق ، سياسة الرقمنة يمثل التحدي الأول والأصعب للجزائر (حلاسي و بن سعدون ، 2022) .

* في حين أجاب الأستاذ عن هذا السؤال بالإجابة التالية:

- المساس بالسيادة الوطنية .

- زعزعة الأمن المعلوماتي.

- حدوث فوضى داخلية أو مجتمعية تخلق جماعات معارضة على إعتبار وجود أقليات مثل القبائل (مزيان، 2022) .

*بالإضافة إلى أن الأستاذ كانت إجابته متمثلة في :

- من التحديات التي صادفت الجزائر هي أن كل يوم يتم إختراع أنظمة إختراقات متطورة عن سابقتها بحكم التطور التكنولوجي .

- التكوين الحالي والمستقبلي للأطر .

- التحديث المستمر للأجهزة التكنولوجية (فراق، 2022).

س3: مع تفاقم وتعرض الجزائر إلى الهجمات السيبرانية في الأونة الأخيرة لابد من وضع إستراتيجيات إتصالية للحفاظ على أمنها الوطني .

- **ماهي أبرز الإستراتيجيات الإتصالية؟**

- **ما درجة فاعلية هذه الإستراتجيات ضد الهجمات السيبرانية المغربية ؟**

ج3: وكان في هذا الصدد الإجابات عن هذا السؤال من طرف كل من الأساتذة متمثلة في :

الإستراتيجية الأولى تشمل إستراتيجية توعوية من خلال حملات توعية للأذهان حول الهجمات السيبرانية ،وكذلك كيفية إستخدام الأجهزة الإتصالية والإلكترونية، إنشاء شبكة داخلية لحماية المعلومات الحساسة من الإختراق (حموش و عبادنة و حلاسي 2022).

في حين أضاف الأستاذ إستراتيجية أخرى تمثلت في التنسيق والتفاعل بين الهيئات والجهات المعنية من وزارة الدفاع ووزارة الداخلية ومركز التكنولوجيات والإتصالات الجزائرية كل هذا يعمل على التنسيق فيما بينها للتصدي للهجمات السيبرانية (حموش، 2022).

*في حين الأستاذين تمثلت إجابتهم في :

من الإستراتيجيات أن الجزائر قد قامت بنقل جميع بيانات الأفراد والجزائرين حماية عالية وقبل ما تحدث الهجمات السيبرانية قامت بتعزيز المنظومة .

- كذلك تعزيزنظام المراقبة على المعلومات والبيانات المستخدمة في الأنظمة وكذلك على وسائل الإعلام والإتصال دون تقييد الحريات .
- تواجد أنظمة مضادة للقرصنة، إذا نجد جامعات ومنهم جامعة قالمة قد إقتنوا أنظمة مضادة لحماية البيانات الطلبة والأساتذة أما على المستوى الحكومي تم تطوير شبكة الأمن الإلكتروني .
- يمكن إستحداث شرطة أمنية متخصصة في مجال المعلوماتي والنظر في القضايا .

- تواجد كفاءات جزائرية ومبدعين للتصدي للهجمات السيبرانية الإلكترونية.
- لابد من البحث عن الثغرات الموجودة ومحاولة غلقها ، وتعزيز نظام الأمن الإلكتروني من المواقع الرسمية للرئاسة الحكومية للوزارة والمؤسسات الرسمية .
- الرقابة الإلكترونية المستمرة للمعلومات الداخلة والخارجة للجهات الرسمية (دندان و مزيان، 2022).

*في حين كانت الإجابة عن الشطر الثاني من السؤال من طرف الأستاذين التي تمثلت في :

- تستمد درجة الفاعلية من التحكم العالي في التكنولوجيا.

*وقد جاء في إجابة الأستاذ سليم حميداني عن الشطر الأول من السؤال المتمحور حول الإستراتيجيات في:

- إعتماد الجزائر على إستراتيجية وهيا الإبقاء على الجانب الورقي التقليدي وهذا ما قلل الأضرار الإلكترونية.
- فتح المجال البحثي في الجامعات والتعليم العالي للإهتمام بالهجمات السيبرانية وجعلها موضوعا للبحث لمذكرات التخرج والمشاريع البحثية .
- محاولة إيجاد أليات موازية لحماية المعلومات (دندان و مزيان، 2022).

أما بالنسبة للإجابة عن درجة الفاعلية فقد كانت إجابته متمثلة في إن الهجمات السيبرانية لم يتضح حجمها الفعلي في التأثير فقط وبالتالي درجة فاعلية هذه الإستراتيجيات غير محددة.

*في حين كانت إجابة الأستاذ متمثلة في:

- بناء وإعادة هيكلة قطاع تكنولوجيا الإتصال مع تكوين أطراف في القطاع تماشيا مع التطورات الحاصلة في هذا المجال.
- ودرجة الفاعلية فتكون لها فاعلية كبرى إذا ما توفرت الشروط السابقة (غول، 2022) .

* هذا وقد أضاف الأستاذ إجابة أخرى متمثلة في :

- تكوين مراكز خاصة لمواجهة الهجمات على مستوى المؤسسات العسكرية والأمنية والرسمية للدولة ، وأنظمة العمل في البنوك والإدارات .
- نشر الثقافة الإلكترونية والرقمية .
- إنشاء هيئات متخصصة للتواصل والحماية .
- التواصل الجماهيري عبر وسائل الإعلام المختلفة .

أما عن درجة فاعليتها فتمثلت إجابته في:

- زيادة فاعلية برامج الحماية الإلكترونية .
- زيادة تأمين المؤسسات الإستراتيجية للدولة لحماية بيناتها وأجهزتها (بن سعدون، 2022).

*هذا وقد أجاب الأستاذ عن هذا السؤال ب:

الإستراتيجية الأولى متمثلة في التصدي للهجمات السيبرانية من خلال ما يعرف بالذكاء الإصطناعي .

والإستراتيجية الثانية متمثلة في فك التشفير والذي يستخدم في تشفير المعلومات (فراق، 2022) .

س4: فيما تمثلت النتائج الهجمات السيبرانية على الجزائر عامة وبصفة خاصة على البنية الإتصالية في الجزائر ؟

ج4: * كان قد أجاب عليه الأستاذ بالإجابة المتمثلة في:

النتائج تتطلب معطيات لمعرفة الضرر بأرقام صحيحة على إعتبار أن التعرض للهجوم السيبراني للمراكز الحساسة في الدولة يمس بأمنها (حموش، 2022).

*أما الأستاذ فقد كانت إجابته متمثلة في :

أن الهجمات السيبرانية كانت محدودة لأن الجزائر ليست منظومة معلوماتية متكاملة وإنما هي منظومة قطاعية لأن الجانب الإتصالي متقدم في قطاعات

ومتأخر في جدا في قطاعات أخرى ، فالثقافة السائدة في الجزائر هي المزج بين الورقي والإلكتروني وهذا مزال يحافظ على سلامة المعلومات وقدرة إستعادتها ولهذا هذه الهجمات السيبرانية لم تكن إلا مجرد إختراقات وتعطيل وقتي في مواقع أو بث أخبار كاذبة (حميداني، 2022) .

*أما الأستاذ فقد تمحورت إجابته في :

أن الهجمات السيبرانية كانت نتائجها متمثلة في ضرب السيادة الوطنية والإخلال بالقوانين الدولية بصفة عامة (غول، 2022).

*أما الأستاذ فقد تمثلت إجابته في :

الإنتهاك والتعدي الإلكتروني الممنهج كان له الأثر البارز على ثقة التي كانت بين البلدين (زودة، 2022).

*أما الأستاذ دندان عبد الغاني متمثلة في أن الجزائر لم تتعرض لأضرار كثيرة بالنسبة للجوانب الإتصالية (دندان، 2022) .

*في حين اجاب الأستاذ عن نتائج الهجمات السيبرانية ب :

أن الولوج إلى مراكز القرار السياسي (الإختراق الامني) يعكس مدى خطورة الوضع الأمني ودرجة العداء والكراهية خاصة في شبكة التواصل الإجتماعي (مزيان، 2022).

س5: هل زيادة التوتر في العلاقات الدولية بين الجزائر والمغرب راجع إلى الهجمات الإلكترونية ؟ أم هناك خلفيات أخرى وراء هذا التوتر بين البلدين ؟

ج5: وكان قد اجاب عليه كل من الأساتذة :

في أن الهجمات السيبرانية ليست السبب في توتر العلاقات بين الجزائر والمغرب ، بل راجع إلى خلفيات أخرى وتوتر قديم وليس حديث ؛ اي هي مجرد تحصيل حاصل ، بحيث شملت جوانب سياسية تمثلت في موقف الجزائر من الصحراء الغربية وكذلك بشأن الوضع الإقليمي والدولي ،إضافة إلى الموقف الثابت للجزائر

للقضية الفلسطينية هذا من جهة ومن جهة أخرى مشكلة التطبيع المغرب مع الكيان الصهيوني ، وتجنيد عملاء من المغرب والجزائر لضرب سمعة الدولة الجزائرية من خلال المواقع الإلكترونية وإستفزاز الرأي العام وتحريضه(حموش و مرزوقي و زيايتة و غول و عبادنة و حميداني و مزيان و بن سعدون و زودة و دندان ، 2022) .

ولهذا كان أي سبب من الأسباب يعد بمثابة الحجة في قطع العلاقات.

س6:.هل يعد قطع العلاقات الجزائرية المغربية سنة 2021 هو أحد الأسباب في شن الدولة المغربية لهذه الهجمات على الجزائر؟

ج6 ¨في هذا السؤال قد أجاب الأساتذة كتالي:

- إن قطع العلاقات بين الجزائر والمغرب سنة 2021 ليس وليد الهجمات السيبرانية بل تعتبر أحد الأسباب في قطع هذه العلاقة و ليست السبب الوحيد و الأساسي , لأن قبل سنة 2021 كانت هناك خلفيات ،إذ أن المغرب يعتبر نفسه في عداء مع الجزائر ،والجزائر تعتبر نفسها في حالة عدم إنسجام مستمر مع المغرب بالإضافة إلى هذا فالجزائر تعد محط أنضار العديد من الدول ؛ لأن مواقفها ثابتة ومبدئها قائم على الحفاظ على السيادة وعدم التدخل في الشؤون الداخلية للدول الأخرى ،وكذلك رفضها للقاعدة الأمريكية على أراضيها في حين بعض الأطراف الأخرى بوجود هذه القواعد ،والهجمات السيبرانية تعتبر أداة من أدوات التهديدات الأمنية(مرزوقي و غول وحميداني و دندان و حموش و عبادنة و مزيان و بن سعدون و زودة ، 2022) .

س7: ما تأثير الهجمات السيبرانية على الدولة الجزائرية على الصعيد السياسي؟

ج7:* كانت إجابة الأساتذة كالتالي:

-التأثير يكمن في التجسس على الهواتف الإتصالية لكبار المسؤولين ومعارضين سياسيين .

-التأثير يكمن أيضا في الإتفاقية التي أجرتها الولايات المتحدة الأمريكية حول سيادة المغرب على الصحراء الغربية .

كما كان التأثير في قطع العلاقات وتعمق الأزمة بسبب هذه الهجمات الإلكترونية (مرزوقي و زياتة و حموش و غول ، 2022).

*في حين كانت إجابة الأستاذ عن هذا السؤال متمثلة في:

- ينظر إلى الهجمات السيبرانية على أنها مؤشر على ضرورة إستجابة الدولة لتهديدات المعاصرة وأنها يجب أن تكيف وضعها في ظل التطورات التكنولوجية الراهنة.

- كما عملت الهجمات الإلكترونية على التأثير على الجزائر من خلال إعطاء مبرر لتعامل مع البث الإلكتروني والمواقع الإتصالية تجاه الوجود الأجنبي الإعلامي ونقل الصورة والمعلومة المغلوطة وغير ذلك (حميداني، 2022) .

*أما إجابة الأستاذ فقد تمثلت في :

-كون الدولة يجب أن تكون أكثر تحفظا من خلال مراقبتها لمواقعها الإلكترونية و لمؤسساتها السيادية التي تمثلها (عبادنة، 2022) .

*إضافة فقد كانت من ضمن الإجابات على هذا السؤال إجابة الأستاذ التي تمثلت في :

- التشويه على النشاط الديبلوماسي للدولة الجزائرية .

- تعقب الجزائر في المحافل الدولية والمنظمات الدولية لتشويه على مخرجات الديبلوماسية الجزائرية .

محاولة تحريف وتزييف صورة وسمعة الجزائر عبر مواقع إلكترونية لدى الأخرين .

وعلى مستوى السياسة الداخلية فتمثل التأثير في :

التأثير على الأسرة وفئة الشباب ،وتشكيكها في منظومتها المختلفة في إطار ما يعرف بحروب الجيل الرابع.

زرع الشك والريبة لدى الشباب لخلق نوع من فقدان الثقة والأمن والإستقرار (بن سعدون، 2022) .

*في حين أجاب الأستاذ عن هذه التأثيرات ب:

أن الهجمات السيبرانية لم تؤثر من الناحية السياسية بل كانت سياسة الفعل ورد الفعل من خلال الأجهزة التكنولوجية وبرامج التجسس من طرف المغرب ،وقطع العلاقات من طرف الجزائر (مزيان، 2022).

س8: كيف تحدث الهجمات الإلكترونية من خلال نظام بيغاسيوس التجسسي؟

ومن هم أبرز ضحاياه؟

وقد تمت الإجابة عن هذا السؤال من طرفالأساتذة ب:

إن حدوث الهجمات الإلكترونية تتم عن طريق زرع نظام بيغاسيوس في الهواتف الذكية و في أنظمة الكومبيوتر وأجهزة لوحية إلكترونية وأجهزة الإعلام الالي، كما يمكن أن تتم الهجمة الإلكترونية في نظام بيغاسيوس من خلال التسلل إلى تطبيقات التواصل الإجتماعي المتواجدة في الهواتف ، كذلك يعتمد هذا النظام على ما يسمى(زيرو كليك) فبمجرد الحصول على رقم الهاتف بالنسبة للشخص المعني فإن إمكانية الوصول وإمكانية تنزيل المعلومة وفك التشفير متاحة بسهولة دون وعي من صاحب الهاتف ،كما أيضا يمكن لهذا النظام الوصول إلى التسجيلات الصوتية والصور والرسائل ،بل تعدى الأمر إلى تشغيل كاميرات هواتف الضحايا (حموش و زياتة و حميداني و دندان و مرزوقي و بن سعدون و فراق و حلاسي و زودة ، 2022).

*أما الأستاذ فقد كانت إجابته حول هذا السؤال متمثلة في :

تحدث الهجمة السيبرانية عادة عندما يعمل المبرمج خطأ في تطوير نظام معين وهنا المهاجم يستغل هذه الثغرات ليخترق أو يسرق البيانات والمعلومات المتواجدة إلكترونيا وهو على دراية مسبقة بهذا البرنامج وثغراته .

بالإضافة إلى أنه حتى لو لم يتم الرد فإن الإختراق قد تم بالفعل ، وهذا التجسس يؤدي إلى الإبتزاز والمساومة وأحيانا تعطيل أنظمة عمل هيئات ومؤسسات .

أبرز ضحايا نظام بيغاسيوس يتمثلون في :

مسؤولين كبار ومسؤولون في المستويات المدنية و المستويات العسكرية .

أما بالنسبة للأستاذ دندان عبد الغاني والأستاذ زيايتة يونس ب :

الضحايا لا تكون شخص ،بل مؤسسات وكذلك البرلمان ووزارة العدل ،كذلك يتم إستهداف قواعد البيانات الخاصة بالمؤسسات الأمنية كالدرك و الشرطة و الاجهزة الإلكترونية ومن هنا تعتبر المؤسسات إحدى البنى الأساسية للدولة الجزائرية (شهرة، 2022).

ملخص المقابلة:

من خلال المقابلات التي أجريناها مع مختلف الأساتذة بمختلف التخصصات، من علاقات دولية وعلوم سياسية إلى إعلام ألي، واتصال وعلاقات عامة.

خرجنا بمجموعة من النتائج كانت قد أجابت على التساؤلات الفرعية للدراسة والمتمثلة في:

أن الهدف من الهجمات السيبرانية على الجزائر راجع إلى زعزعة الأمن الوطني للدولة الجزائرية، والإخلال باستقرارها الداخلي والخارجي على حد سواء، كذلك ظرب منظوماتها الإتصالية والمعلوماتية للدولة الجزائرية وهذا ما جعل الجزائر تقف أمام تحديات هي بغنى عنها كانت متمثلة في تعميم استخدام التكنولوجيات والخروج باستراتيجيات وحلول للتعامل مع الهجمات السيبرانية .

إضافة إلى وضع استراتيجيات على المدى الطويل من 5إلى10سنوات، وكذلك كان من ناحية أخرى من الصعب عليها كدولة إعادة هيكلة منظومتها المعلوماتية من الصفر وهذا ما جعلها تعيد تكييفها بما يتماشى مع تكنولوجيات الحاصلة، في حين كان التحدي الأصعب للجزائر هو التطور المستمر في مجال التكنولوجيا .

لكن رغم كل هذا كان للهجمات السيبرانية ملامسة في الجانب السياسي تمثلت في التجسس على كبار المسؤولين والمعارضين السياسيين، وعلى إثر هذا كله عملت الجزائر على وضع مجموعة من الآليات الإتصالية المعتمدة للحد من الهجمات السيبرانية كان أبرزها متمثل في نشر حملات توعوية للأذهان حول هذا النوع من الهجمات وكذلك القيام بدورات تكوينية لحماية الأفراد والإدارات العامة والحساسة في الدولة .كما عملت الجزائر على إنشاء شبكة داخلية لحماية المعلومات الحساسة من الاختراق الإلكتروني وذلك بالتنسيق والتفاعل بين جميع الهجمات والهيئات من مركز التكنولوجيات والاتصال إلى وزارة الدفاع الداخلية هذا وكانت الجزائر قد قامت بنقل جميع بيانات أفراد الجزائريين لحمايتها من أي اختراق وتعزيز

المنظومة الإلكترونية ونظام المراقبة ونشر أنظمة مضادة في كل من الجامعات والمنشآت الخاصة والعامة في الجزائر، كما قد تذهب أو تلجأ الجزائر إلى تطوير استراتيجياتها مستقبلا إذا ما تم مواصلة هذا النوع من الهجمات عليها ،وذلك من خلال الاعتماد على تقنية الذكاء الاصطناعي من أجل محاربة الهجمات الإلكترونية.

خاتمة

خاتمة :

نستنتج في الأخير أن الهجمات السيبرانية أصبحت حتمية نظرا لظروف التي نشأت فيها ، ولما تم إستخدامها فيها من نطاق سلبي في مجال كمجال العلاقات الدولية السياسية، فالدول باتت تهاجم أنضارها من الدول الأخرى وهو مرأته الجزائر من دولة المغرب من اختراقات عطلت وشلت بنيتها الإتصالية ومنظومتها المعلوماتية من خلال نظام كنظام بجاسوس .

إضافة إلى تشكيل هذه الهجمات السيبرانية خطرا على أمن وإستقرار الدولة الجزائرية.

النتائج :

-من خلال الجوانب التي تم التطرق لها و تداولها في هذه الورقة البحثية ، توصلنا إلى النتائج التالية :

1) الهجمات السيبرانية أصبحت تشكل خطرا كبيرا في كل الأنظمة المعلوماتية للمؤسسات و الشركات وأكثر عرضة للإختراق ، وهذا من أجل الابتزاز و المساومة
2) تعتبر الهجمات السيبرانية واحدة من الأسباب التي أدت إلى زيادة حدة النزاعات والصراعات بين الجارتين الدولة الجزائرية والمغربية ، مما أدى إلى قطع العلاقات بصفة نهائية.
3) ما جعل الدولة الجزائرية أكثر عرضة لهذه الهجمات راجع إلى ضعف المنظومة المعلوماتية وهشاشتها.
4) الثورة التكنولوجية الحديثة لها ذلك الأثر الكبير في العلاقات السياسية القائمة بين الدول .
5) أصبحت الجزائر تملك المقومات البشرية لمواجهة تحديات الهجمات السيبرانية.

6) أصبح من غير المختلف عليه أن أمن الدول لم يعد متعلقا فقط بحمايتها من الهجمات العسكرية ، بالأسلحة التقليدية و إنما إمتد و إتسع ليشمل الحاجة لحماية مجتمعاتها و منشاتها وبنيتها الحيوية من التعرض للهجمات باستخدام تكنولوجيا الإتصال و المعلومات.
7) توجه الجزائر نحو تخصيص ميزانيات ومبالغ مالية في مجال الأمن السيبراني .
8) تعدد أنظمة الإختراق وتطورها ما جعل من الجزائر تدرك مدى خطورتها وتتوجه إلى تدابير الوقاية الإلكترونية.
9) الاعتماد على التشفير الإلكتروني للمعلومات الحساسة والخاصة بأمن الدولة الجزائرية.
10) تعرض الجزائر إلى الهجمات السيبرانية راجع إلى موافقتها السياسية الثابتة وموقعها الاستراتيجي .
11) من بين الاستراتيجيات التي ظلت الجزائر تعتمد عليها لحماية الأمن الوطني هي بقاء اعتمادها على الجانب التقليد بأكثر منه الحديث.

التوصيات:

1) تقوية أنظمة الحماية السيبرانية داخل المؤسسات الجزائرية في كل القطاعات ودون استثناء .
2) تنظيم دورات تكوينية في قطاع تكنولوجيا الإعلام تتماشى مع التطورات الحاصلة للموظفين الساميين و العاديين في القطاعات الحساسة .
3) تشجيع وتثمين البحث العلمي في قطاع الأمن السيبراني .
4) تفعيل وتشجيع التربية الإعلامية كمدخل أولي لنشر الوعي المعلوماتي.
5) تفعيل مشروع الحكومة الإلكترونية في الجزائر ، ما يجعل أنظمة الحماية منسقة ومنسجمة مع كافة قواعد البيانات للمؤسسات و الإدارات الجزائرية.

6) إنشاء ومراقبة أنظمة الهجمات السيبرانية عبر مختلف ربوع الوطن.

الملاحق

الملاحق :

1- شعار شركة إن أس أو منتجة برنامج بيغاسيوس

المصدر : www.marefa.org

2-برامج الإختراق :

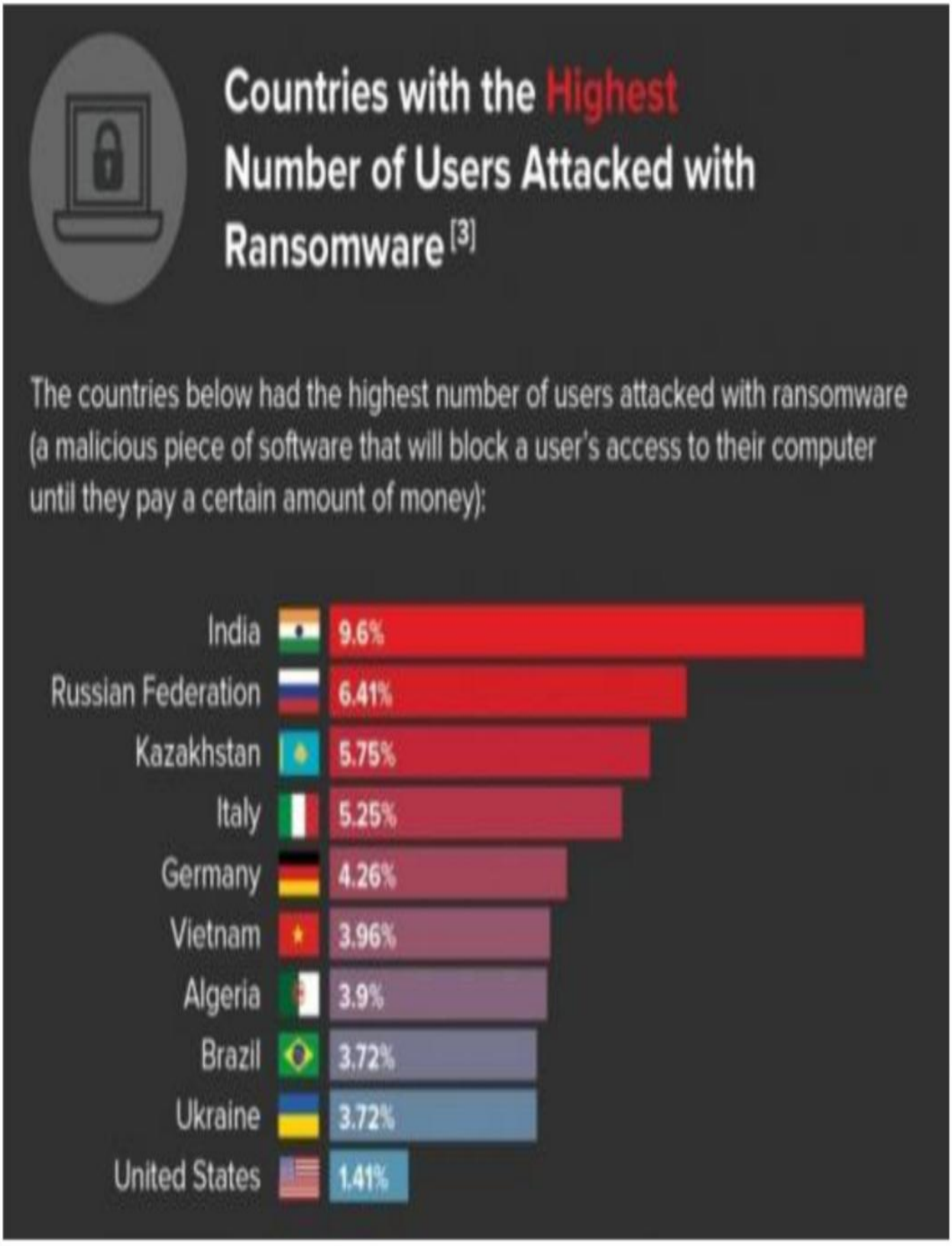
المصدر : www.lusailnews.net

3-جدول يوضح الترتيب العالمي للدول حسب الرقم القياسي العالمي للأمن السيبراني :

البلد	الرقم القياسي	الترتيب العالمي
الولايات المتحدة الأمريكية	0.824	1
كندا	0,794	2
أستراليا	0.765	3
ماليزيا	0.765	3
عمان	0.765	3
نيوزيلندا	0.735	4
النرويج	0.735	4
اسرائيل	0.676	6
تركيا	0.647	7
قطر	0.618	8
مصر	0.588	9
فرنسا	0.588	9
المغرب	0.559	10
تونس	0.529	11
السودان	0.441	14
الإمارات العربية المتحدة	0.353	17
البحرين	0.294	19
إيران	0.294	19
ليبيا	0.294	19
المملكة العربية السعودية	0.294	19
الأردن	0.206	22
الجزائر	**0.176**	**23**
بربادوس	0.176	23
بيلاروس	0.176	23
بليز	0.176	23
بنين	0.176	23
البوسنة والهرسك	0.176	23
بوتسوانا	0.176	23
ملاوي	0.176	23
سوريا	0.176	23
البهاما	0.147	24
موريتانيا	0.147	24
دولة فلسطين	0.147	24
بوروندي	0.118	25
كمبوديا	0.118	25
لبنان	0.088	26
هايتي	0.059	27
العراق	0.029	28
الصومال	0.029	28
هندوراس	0.000	29
ليسوتو	0.000	29

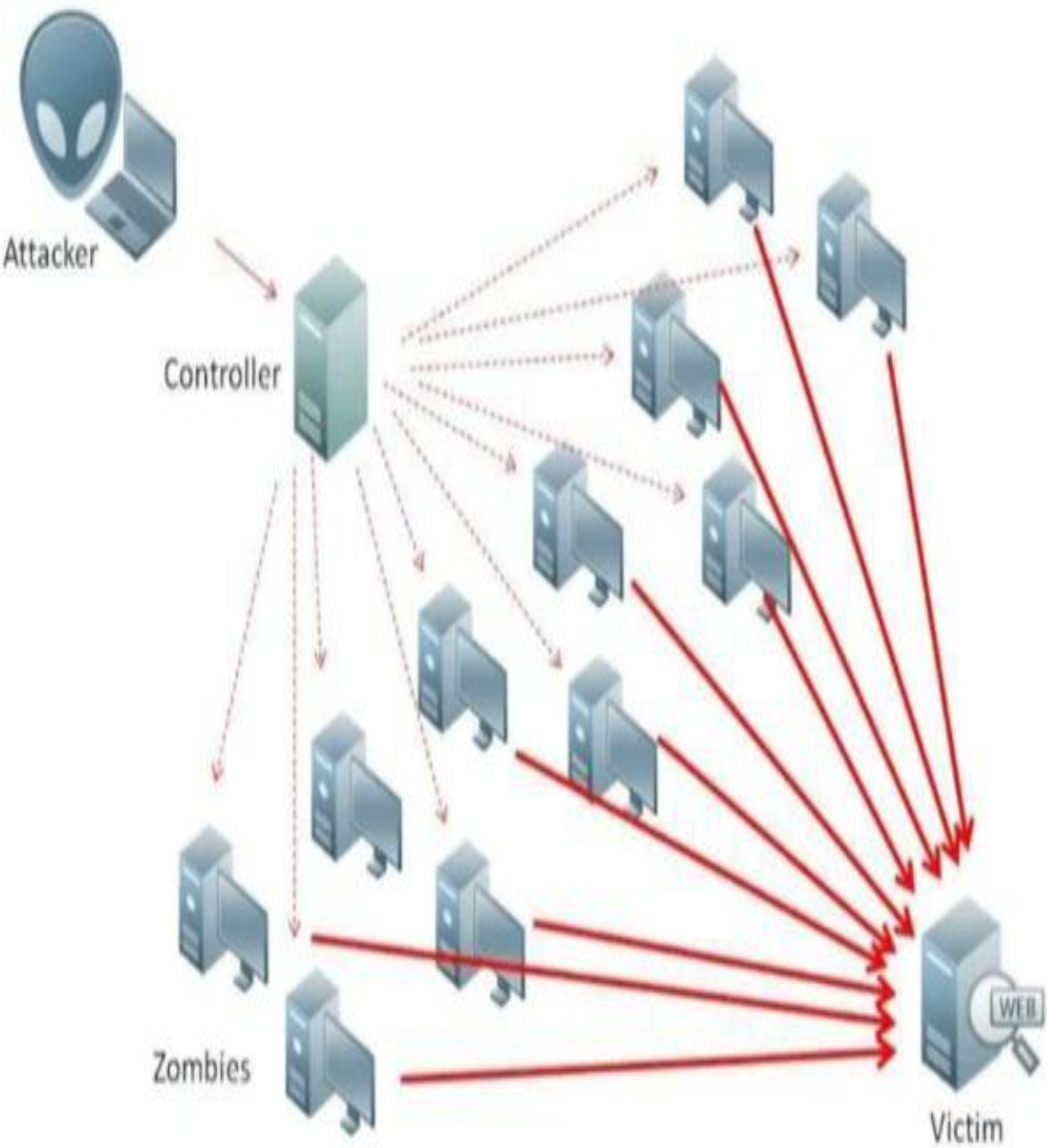
المصدر : الاتحاد الدولي للاتصالات ، **تقرير حول الرقم القياسي العالمي للأمن السيبراني وسمات السلامة السيبرانية** ، جنيف : الاتحاد الدولي للاتصالات ، مكتب تنمية الاتصالات ، أفريل ، 2015 ، ص ص 01-06.

الدول الأكثر تعرضا لفيروس الفدية:



المصدر : https://www.comparitech.com

طريقة عمل برنامج هجوم DDOS:



المصدر: https://ar.safetydetectives.com

قائمة المصادر والمراجع

قائمة المصادر والمراجع العربية:

1. (12 أكتوبر, 2021). تاريخ الاسترداد 24 ماي, 2022، من خطورة الفيروسات و البرمجيات الخبيثة على أجهزة الحاسب : https://www.maw9i3i.net

2. *الحرب الإلكترونية و السيبرانية*. (2021). تم الاسترداد من ttps://alkhandaeq.com

3. أحمد أبيس الفتلاوي. (2016). الهجمات السيبرانية : مفهومها و المسؤلية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر. *المحقق الحلي للعلوم القانونية و السياسية*، 3.

4. أحمد بن مرسلي. (2010). *مناهج البحث العلمي*. الجزائر: ديوان المطبوعات الجزائرية.

5. إدريس عطية. (24 02, 2022). مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري.

6. اليامين بن سعدون. (23 05, 2022). (أكرم مزعاش، المحاور) قالمة، علوم سياسية.

7. إيمان كافي. (09 02, 2022). أمن الدول و الأفراد على المحك. *الشعب*.

8. إيهاب خليفة. (2019). *مجتمع ما بعد المعلومات*. القاهرة: دار العربي للنشر و التوزيع.

9. بشرى سلاوي، عبد النور بلدي، مروة خلة، و سارة خلة. (2020). مستقبل السيادة الرقمية في ظل التكنولوجيات الحديثة. قالمة، قسم العلوم الإعلام و الإتصال والمكتبات: كلية العلوم الإنسانية والإجتماعية.

10. بلال بن جامع. (13 01, 2007). المشكلات الأخلاقية والقانونية المثارة حول شبكة الأنترنيت. قسنطينة، قسم علم المكتبات: كلية العلوم الإنسانية والإجتماعية.

11. تامر مسحال. (26 جانفي, 2021). تاريخ الاسترداد 08 أفريل, 2022، من قناة الجزيرة:
https://m.youtube.com/watc?v=p7pMOEhEi4

12. تامر مسحال. (بلا تاريخ). *قناة الجزيرة* . تم الاسترداد من ما خفي أعظم - الإمارات.

13. جمال بوازدية. (13 فيفري, 2019). الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية. *مجلة العلوم القانونية و السياسية*، من 1 إلى 32.

14. حسام الدين مرزوقي . (11 05, 2022). (إسمهان برج، المحاور) قالمة، علوم الإعلام والإتصال وعلم المكتبات.

15. دحان حزام القريطي. (2022). *الأمن السيبراني وحماية امن المعلومات*. الإسكندرية: دار الفكر الجامعي.

16. رولا حطيط. (بلا تاريخ).
https://l.facebook.com/l.php?u=https%3A%2F%2Fwww.bahethcenter.net%2Fuploaded%2Ffiles%2F%25D8%25A7%25D9%2584%25D8%25B3%25D9%258A%25D8%25A8%25D8%25B1%25D8%25A7%25D9%2586%25D9%258A%25D8%25A9%2520%25D8%25AF.%2520%25D8%25B1%25D9%2588%25D9%2584%25D8%25A7%2520%2.%25D9%2588%25D9%2584%25D8%25A7%2520%2.
تاريخ الاسترداد 12 03, 2022

17. رؤى حمود. (2022). تاريخ الاسترداد 01 04, 2022، من أبرز أنواع الهجمات السيبرانية: https://www.rmg-sa.com

18. رياض مزيان. (26 05, 2022). (أكرم مزعاش، المحاور) قالمة، قسم العلوم السياسية.

19. ريتشارد إيه كلارك، و روبرت كيه كنيك. (2012). *حرب الفضاء الإلكتروني*. أبو ظبي: دار الإمارات العربية المتحدة.

20. ريما مكتبي. (13 06, 2020). *قناة العربية*. تاريخ الاسترداد 18 03, 2022، من مهمة خاصة الحرب السيبرانية.

21. سامي محمد بونيف. (30 06, 2019). دور الإستراتيجيات الإستباقية في مواجهة الهجمات السيبرانية. *الردع السيبراني نموذجا*، صفحة من1 إلى 18.

22. سليم حميداني. (22 05, 2022). (إسمهان برج ، و سميرة مسيود، المحاورون) قالمة، قسم العلوم السياسية.

23. شمس الدين شهرة. (31 05, 2022). (إسمهان برج، و سميرة مسيود، المحاورون) قالمة، قسم الإعلام الألي.

24. صلاح مهدي هاوي الشميري، و زيد محمد علي إسماعيل. (2020). الأمن السيبراني كمرتكز جديد في الإستراتيجية العراقية. صفحة 280.

25. صلاح حيدر عبد الواحد. (جويلية, 2021). حروب الفضاء الإلكتروني ، دراسة في مفهومها و خصائصها وسبل مواجهتها. 39 43. عمان.

صلاح حيدر عبد الواحد. (28 جويلية, 2021). حروب الفضاء الالكتروني ؛دراسة في مفهومها و خصائصها و سبل مواجهتها. عمان، قسم العلوم السياسية، عمان.

26. عبد الصادق عادل. (2009). الإرهاب الإلكتروني القوة في العلاقات الدولية نمط جديد و تحديات مختلفة. القاهرة: مركز الدراسات السياسية و الإستراتيجية.

27. عبد الغاني دندان. (19 05, 2022). (سميرة مسيود، و إسمهان برج، المحاورون) قالمة، قسم العلوم السياسية.

28. عبد الوهاب منصور شادي. (2019). حروب الجيل الخامس أساليب التفجير من الداخل على الساحة الدولية. دار العربي للنشر و التوزيع.

29. عدنان الغزال. (29 جوان, 2019). *صحيفة الوطن* . تاريخ الاسترداد 12 أفريل, 2022، من أعراض البرامج الحاسوبية الضارة : www-alwatan-com-sa.cdn.ampproject.org

30. علم الدين بانقا. (2019). *مخاطر الهجمات الإلكترونية السيبرانية وأثارها الإقتصادية دراسة حالة دول مجلس التعاون الخليجي*. الكويت.

31. عنترة بن مرزوق. (2017). الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية.

32. غيث علاو. (2022). *الهجمات السيبرانية أكبر من حرب نووية بوسائل إلكترونية*.

33. لخضر غول. (16 05, 2022). (سميرة مسيود، المحاور) قالمة، قسم علم الإجتماع.

34. مبارك زودة. (30 05, 2022). (إسمهان برج، المحاور) قالمة، قسم الإعلام والإتصال وعلم المكتبات.

35. محمد سرحات علي المحمودي. (2015). *مناهج البحث العلمي*. صنعاء: دار الكتب.

36. محمد الأمين عبادنة. (22 05, 2022). (سميرة مسيود، المحاور) قالمة.

37. محمد الكر، و عنترة بن مرزوق. (15 04, 2018). البعد الإلكتروني للسياسة الأمنية. 35.

38. محمد علي محمود. (2021). تأليف *حروب الفضاء الإلكتروني و علاقاتها بحروب الجيل الخامس* (الصفحات 55-56).

39. محمود محمد سعد. (2020). *الحرب السيبرانية*.

40. منى الأشقر جبور. (2016). *السيبرانية هاجس العصر*. المركز العربي للبحوث القانونية و القضائية.

41. نور أمير الموصلي. (2021). الهجمات السيبرانية في ضوء القانون الدولي الإنساني. 07. سوريا، القانون الدولي الإنساني، سوريا.

42. هديل عادل. (24 02, 2019). تاريخ الاسترداد 09 04, 2022، من http://al-ain.com

43. وليد محمود خالد. (21 02, 2022). *قناة الجزيرة*. تاريخ الاسترداد 09 04, 2022، من eljazeera.net

44. ياسمينة شاوشة. (2020). الإرهاب الإلكتروني بين مخاطره و أليات مكافحته. *نيل شهادة الماستر في الحقوق*، 41-42. الحقوق و العلوم السياسية، البويرة/الجزائر: جامعة أكلي محند أولحاج.

قائمة المصادر الأجنبية:

1. (2019). Consulté le 24, 2022, sur Machine Learning to Predict the Likelihood of a Personal Conputer to Be Infected with Malware: https://scholar.smu.edu/datasciencereview/vol2/iss2/9

2. james, h. (2022, 03 09). *knowledge hub.* Consulté le 05 25, 2022, sur legal consequences of a cyber attack: https://harrperjames.co.uk