دور الأمن السيبراني في حماية نظم المعلومات: تجربة الجزائر

The role of Cyber security in protecting information systems: Algeria's experience

ناصر مراد [1]

مخبر تحديات النظام الضريبي الجزائري في ظل التحولات الاقتصادية

nacermourad@yahoo.fr

تاريخ الإستلام: 2025/04/29 تاريخ القبول: 2025/05/30 تاريخ النشر: 2025/11/22

ملخص:

حاليا يشهد العالم تزايداً كبيراً في حجم الهجمات السيبرانية التي إستهدفت مختلف الدول، وتعتبر المؤسسات المالية الأكثر عرضة لخطر هذه الهجمات السيبرانية، نظراً لدورها الحيوي في الوساطة المالية. و تترتب عن هذه الهجمات أضرار كبيرة على المؤسسة من خلال الخسائر المالية و فقدان الثقة مع المتعاملين الاقتصاديين. و في ظل الاستخدام الواسع لتكنولجيا المعلومات والاتصال في المؤسسات الاقتصادية، و انتشار استعمال الأنترنت خاصة في مجال التجارة الالكترونية، و التي صاحبها القرصنة الالكترونية، فقد ظهرت الجرائم الاقتصادية المرتبطة بالتطور التكنولوجي و ثورة الاتصالات. في هذا السياق أصبحت حماية نظم المعلومات ضرورة حتمية لمواجهة مختلف التهديدات السيبرانية.

لقد توصل الباحث إلى عدة نتائج أهمها: يوجد عدة آليات لمواجهة المخاطر السيبرانية، و التي تتوقف على مدى تأهيل العنصر البشري و التقني و التشريعي؛ البعد الدولي للأمن السيبراني ، مما يستدعي تعاون دولي لمواجهته.

الكلمات المفتاحية: الأمن السيبراني، المخاطر السيبرانية، نظم المعلومات، الجرائم السيبرانية، التهديدات السيبرانية.

تصنيف JEL: k41 ;Ll86, O33

.**Abstract:**

Currently, the world is witnessing a significant increase in cases of cyber-attacks that target various countries. Due to their vital role in financial intermediation, the financial institutions are considered the most vulnerable to these cyber-attacks. This type of attack causes severe damage to the institutions through financial losses and a decrease of economic operators trust. In light of the widespread adoption of information technology by companies, and the spread of the Internet use in the field of e-commerce,. For that reason, the economic crimes are linked to technological development and the communications revolution. In this context, the protection of information systems has become a necessity to confront various cyber threats.

The results concluded that there are several mechanisms for overcome cyber risks, all of which depend on the capabilities of the human, technical and legislative element. Furthermore, the international framework for cyber-security also calls for international cooperation to confront it.

Keywords: keywords1; Cyber security, cyber risks, information systems, cyber crimes, cyber threats .

Jel Classification Codes: K41.L86 .O33.

[1] المؤلف المراسل.

1. مقدمة:

أدى التطور التكنولوجي للمعلومات إلى إحداث ثورة في الاتصالات و المعاملات الرقمية، و تزامن ذلك مع ظهور جرائم إلكترونية خطيرة مثل التجسس السيبراني، التخريب الإلكتروني، سرقة البيانات الرقمية و الإختراقات الإلكترونية، و الذي تسبب في أضرار جسيمة على الأفراد و المؤسسات و كذلك على الدول. في هذا السياق أصبح الأمن السيبراني ضرورة حتمية لمواجهة مختلف الهجمات السيبرانية، و تجنب مخاطرها.

تشهد الجزائر منحنى تصاعديا في الهجمات السيبرانية، في ظل توجه الجزائر نحو تبني الحكومة الإلكترونية، لذلك أصبحت السلطات الجزائرية ملزمة على إيجاد الحلول و الإجراءات الضرورية لمواجهة التهديدات السيبرانية، في هذا السياق تبنت الجزائر إستراتيجية شاملة من أجل ضمان الأمن السيبراني، و حماية نظم المعلومات من مخاطر التهديدات السيبرانية.

1-1 إشكالية الدراسة

سنحاول من خلال هذه الدراسة معالجة الإشكالية التالية :ما هو دور الأمن السيبراني في حماية نظم المعلومات؟

و تتفرع هذه الإشكالية إلى الأسئلة الفرعية التالية :

- ماذا نقصد بالأمن السيبراني و ما هي خصائصه؟
- ما هي أهمية و أهداف الأمن السيبراني؟
- ما هي المخاطر السيبرانية التي تواجه نظم المعلومات و كيف يمكن مواجهتها؟
- ما هو واقع الأمن السيبراني في الجزائر؟

2-1 أهمية الدراسة

تكمن أهمية الدراسة في البحث عن المخاطر السيبرانية التي تواجه نظم المعلومات ، و التي تشكل أهم التهديدات على المستوى الدولي. بالإضافة إلى التطرق إلى السبل الفعالة لمواجهة المخاطر السيبرانية،و معرفة تجربة الجزائر في الأمن السيبراني .

3-1 أهداف الدراسة

تهدف هذه الدراسة إلى تسليط الضوء على دور الأمن السيبراني في حماية نظم المعلومات، مع تشخيص مختلف المخاطر السيبرانية التي تواجه نظم المعلومات، و معرفة آليات مواجهة المخاطر السيبرانية، مع إبراز واقع الأمن السيبراني في الجزائر.

4-1 منهج الدراسة

نعتمد في البحث على المنهج الوصفي التحليلي، و ذلك من خلال دراسة و تحليل مخاطر الأمن السيبراني، بالإضافة إلى تحديد و تحليل مختلف الطرق الفعالة لمواجة المخاطر السيبرانية، بالاعتماد على تجربة الجزائر.

5-1 خطة الدراسة

لمعالجة الإشكالية المطروحة و تحقيق الأهداف المسطرة سنستعرض العناصر التالية:

- تعريف و خصائص الأمن السيبراني
- أهمية و أهداف الأمن السيبراني
- أنواع الأمن السيبراني
- المخاطر السيبرانية التي تواجه نظم المعلومات
- آليات مواجهة المخاطر السيبرانية
- واقع الأمن السيبراني في الجزائر.

2. تعريف و خصائص الأمن السيبراني:

ظهر الأمن السيبراني سنة 1970، حينها لم يكن متطورا نظرا لقلة استعمال بيانات الحواسيب، حينها كان من السهل التعرف على الهجمات الالكترونية، و في الثمانينات تطور الأمن السيبراني نظرا لانتشار الأنظمة الإلكترونية بشكل واسع، و رافقه تعدد و تطور الهجمات الالكترونية. وفي التسعينيّات شهد العالم تطورا في الأجهزة الإلكترونية، وتزامن ذلك مع تطور حجم و تعقيدات الهجمات الإلكترونية، مما استدعى تطوير بروتوكولات الحماية للمواقع الإلكترونيّة.

يتكون الأمن السيبراني من كلمتين هما : الأمن و السيبراني، و نقصد بالأمن الحماية، أما السيبراني هو الواقع الإفتراضي أو فضاء الانترنت، ويعتبر مفهوم الأمن السيبراني من أكثر المفاهيم المثيرة للإهتمام والدراسة، حيث يوجد عدة نعاريف من أهمها ما يلي:

- عبارة عن (مجموعة الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به، وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين من المخاطر في الفضاء السيبراني). (منى الأشقر جبور، 2012، ص 16) .

- الأمن السيبراني هو(سلاح إستراتيجي بيد الحكومة والأفراد، لاسيما أن الحرب السيبرانية أصبحت جزء لا يتجزأ من التكتيكات الحديثة للحروب والهجمات ما بين الدول) . (أوس مجيد غالب العوادي، 2016، ص 6)

- الأمن السيبراني هو(المجال الجديد الخامس للحروب الحديثة بعد البر والبحر والجو والفضاء الحقيقي، وهو يمثل جميع شبكات الحاسب الآلي الموجودة حول العالم، ويشمل ذلك الأجهزة الإلكترونية المرتبطة من خلال شبكة الألياف البصرية والشبكات اللاسلكية، الفضاء السيبراني ليس الإنترنت فقط وإنما شبكات أخرى كثيرة متصلة).(ادريس عطية،2019،ص 105) و عليه الأمن السيبراني هو عملية حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية، التي تعمل إلى الوصول إلى المعلومات الحساسة أو تغييرها أو تدميرها، بغرض الإلحاق الضرر لمستخدميها.

و يحتوي الأمن السيبراني على عدة عناصر من الحماية تنتشر عبر أجهزة الكمبيوتر أو الشبكات أو البرامج أو البيانات التي يريد الشخص حمايتها، و يجب أن يكمل كل منها الآخر داخل المنظمة لإنشاء دفاع فعال في مواجهة الهجمات السيبرانية. و ذلك من خلال إكتشاف هذه الهجمات و معالجتها.

يرتكز الأمن السيبراني على مرتكزين أساسين هما : (ربيعي حسين و سمر محمود، 2022، ص 179)

- التقنية : تؤدي تكنولوجيا المعلومات دورا كبيرا في تحقيق الأمن السيبراني فهي ما يؤمن المعلومات المخزنة والمتداولة.
- التشريع : يؤدي التشريع دور العنصر الذي يستجيب لمتطلبات البيئة الرقمية في مجال التنظيم، ووضع الآليات القانونية الكفيلة لضمان الحماية الملائمة للفضاء السيبراني .

و يتميز الأمن السيبراني بعدة خصائص نلخصها فيما يلي:

- توسع مجال الأمن السيبراني بحيث له عدة أبعاد هي: اقتصادية، اجتماعية، ثقافية، قانونية، سياسية و عسكرية؛
- (الاستمرارية والتي يقصد بها ضمان تقديم الخدمة دون انقطاع) ؛ (قصعة سعاد، 2020، ص 380)
- (درجة عالية من التغيير و الترابط و سرعة التفاعل)؛ (بارة سمير، 2017، ص 258)
- لا يوجد أمن سيبراني مطلق لذلك فهو يتصف بالنسبية، بحيث لا يمكن القضاء على الهجمات السيبرانية، و إنما تقليصها و التقليل من أضرارها؛
- مرونة الأمن السيبراني بحيث يتكيف مع تطور الهجمات السيبرانية؛
- وسيلة دفاعية ضد الهجمات وعمليات القرصنة على نظم المعلومات؛
- البعد الدولي للأمن السيبراني.

لقد حددت جمعية الأنترنت ISOC المبادئ الأساسية للأمن السيبراني، و التي تتمثل فيما يلي: (مجتمع الأنترنت، 2020، ص2)

- الوعي: يتعين على جميع الجهات المعنية في كل من القطاعين العام و الخاص فهم المخاطر التي تهدد أمنها، و مدى تأثير تلك المخاطر عليها و على الآخرين في النظام البيئي الخاص بالبنية التحتية لشبكة لانترنت.

- المسؤولية: يجب على جميع الجهات المعنية تحمل مسؤولية مواجهة المخاطر الأمنية في إطار مؤسساتها، مع الأخذ في الاعتبار للآثار المترتبة على اتخاذ إجراء ما أو التقاعس عن تنفيذه.

- التعاون: يجب إشراك جميع الجهات المعنية بما في ذلك المعنية خارج الحدود، في حوار مستمر حول الأمن السيبراني لمواجهة التهديدات الجديدة و المستمرة.

و تتوقف فعالية الأمن السيبراني على العناصر التالية:

- التكنولوجيا المتطورة؛
- العنصر البشري الكفء؛
- الاستراتيجيات المحكمة؛
- العنصر الأمني الردعي.

3- أهمية و أهداف الأمن السيبراني

يعرف الأمن السيبراني اهتماما واسعا من طرف أفراد المجتمع سواء على مستوى الأفراد أو المنظمات، حيث يشهد العالم ثورة تكنولوجية هائلة أدت إلى ظهور تحديات خطيرة تهدد وجوده، و ذلك من خلال زيادة التهديدات الإلكترونية مثل: السرقة والنصب والاحتيال والابتزاز، مما أدى إلى أضرار خطيرة تضر بالفرد و المنظمة، في هذا السياق استوجب البحث على

الآليات التي تمكننا من مواجهة هذه المخاطر، و ذلك عن طريق الأمن السيبراني الذي يعمل على الوقاية من الجرائم الإلكترونية.(و يشكل الأمن السيبراني هاجسا استراتيجيا للقوى العالمية والمتمثلة في الولايات المتحدة الأمريكية والصين وروسيا، إذ تدور في وقتنا الحالي حرب إلكترونية بين هذه القوى من أجل اختراق المعلومات والتأثير على أسعار البورصة والعملات وغيرها من المنشآت). (مصطفى إبراهيم سلمان الشمري، 2021، ص 164)

تكمن أهمية الأمن السيبراني في حماية و تأمين نظم المعلومات من الهجمات السيبرانية على المستوى الإقليمي و العالمي، فهذا الأمن يحمي معلومات الأفراد و المنظمات، بحيث يحفظها من كافة المخاطر والأضرار، في شكل جرائم إلكترونية كسرقة البيانات و الإبتزاز. على هذا الأساس أصبح الأمن السيبراني ضرورة حتمية لحماية بيانات الأفراد و المنظمات.

و يهدف الأمن السيبراني لوضع أفضل أنظمة الحماية للحفاظ على معلومات المستخدمين وبيانات الأجهزة محميّة ضد الخرق والسرقة والضّياع والتلف، و يمكن تلخيص أهداف الأمن السيبراني في العناصر التالية:

- توفير بيئة أمنة موثوقة للتعاملات في مجتمع المعلومات؛
- توفير المتطلبات اللازمة للحد من المخاطر والجرائم الإلكترونية التي تستهدف المتعاملين؛
- تعزيز حماية أنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات و بيانات؛
- سد الثغرات في أنظمة امن المعلومات؛
- التصدي للهجمات السيبرانية التي تستهدف منظمات القطاع العام والخاص؛
- مواجهة البرمجيات الخبيثة التي تعمل على إحداث أضرار بالغة للمتعاملين؛
- التخلص من نقاط الضعف في أنظمة الحاسب الآلي والأجهزة المحمولة ؛
- الحد من التجسس والتخريب الإلكتروني على مستوى الحكومة والأفراد و المنظمات؛
- اتخاذ التدابير اللازمة لحماية الأفراد والمنظمات من المخاطر المحتملة في مجال استخدام الإنترنت؛
- تدريب الأفراد على آليات وإجراءات جديدة لمواجهة التحديات الخاصة باختراق أجهزتهم التقنية بقصد الضرر بمعلوماتهم الشخصية ؛
- صمود البني التحتية من الهجمات الإلكترونية؛
- العمل على حفظ الحقوق المترتبة على الاستخدام المشروع للشبكات المعلوماتية؛
- حماية المصلحة الفردية والعامة، و الذي ينعكس إيجابا على الاقتصاد الوطني .

4- المخاطر السيبرانية التي تواجه نظم المعلومات

لقد تضاعف عدد الهجمات السيبرانية ثلاث مرات على مدار العقد الماضي مع تزايد اعتمادنا على الخدمات المالية الرقمية خاصة في ظل الوباء العالمي كوفيد 19، و تشكل الخدمات المالية الأكثر استهدافا للهجمات السيبرانية و التي أصبحت مصدر تهديد للاستقرار المالي.

وقد أصبحت أدوات القرصنة أقل تكلفة وأكثر سهولة وأشد قوة، مما يتيح للقراصنة إلحاق ضرر أكبر مقابل نسبة ضئيلة من التكلفة. ويؤدي التوسع في الخدمات القائمة على شبكة الانترنت إلى زيادة فرص القرصنة. ويستهدف المهاجمون المؤسسات الكبيرة والصغيرة، والبلدان الغنية والفقيرة، ويعملون عبر الحدود، لذلك يجب أن تكون مواجهة الجريمة

السيبرانية والحد من مخاطرها مسؤولية مشتركة بين دول العالم. و نلخص المخاطر السيبرانية التي تواجه نظم المعلومات فيما يلي:

- البرامج الضارة: يتسّم هذا الخطر بأنّه من أشهر أنواع المخاطر التي تُهدد الأمن السيبراني، إذ تتسلل بعض البرامج إلى الأنظمة، بهدف الوصول غير المصرح به للبرامج والملفات، وإلحاق الضرر بها، من خلال سرقتها أو حذفها.

- سرقة كلمة المرور: عند الدخول إلى الحساب، قد يتبين وجود تغيير في كلمة المرور، وهذا مؤشر على أنّ شخص ما تمكّن من اختراق النظام والحصول على كلمة المرور، مما يشكل خطر على البيانات السرية الموجودة في النظام.

- التنصت: يتمثل هذا الخطر في قدرة أحد الأشخاص على الاستماع للبيانات المتنقلة بين المستخدم والمضيف، وهذا يمثل سرقة المعلومات عن النظام.

- هجمات التصيد: يكون التصيد على شكل رسائل من جهات رسمية تتضمن طلب بعض البيانات الهامة، وقد يقع بعض الأشخاص في الخطأ، ويُقدّم معلومات هامة للمتصيدين من خلال النقر على رابط آخر مشبوه. (و حسب دراسة قام بها نادي خبراء المعلومات و الأمن الرقمي الفرنسي سنة 2020، فإن 80 % من الشركات الفرنسية قد استهدفت بهجمات التصيد). (ساعد ، 2022، ص 71)

- رفض خدمة الموزع: يستهدف هذا الخطر عادةً الخوادم الرئيسية، حيث يُوقف المستخدم مواقع الويب التي تُحاول الوصول للبيانات.

- هجوم عبر الموقع: و ذلك من خلال استهداف مواقع الويب الضعيفة، وتحميل عدد من الرموز الخطيرة عليها، و عند دخول أحد المستخدمين لهذه المواقع قد يتعرّض النظام الخاص به للسرقة، أو التسبب بتعطل الخدمات الرئيسية فيه.

- هجوم SQL: و ذلك من خلال برنامج لمعالجة البيانات، بحيث يُتاح للأطراف الخارجية الوصول للمعلومات الحساسة غير المتاحة، عن طريق عدد من البرمجيات.

- برامج الفدية: تُثبّت عدد من البرامج الضارة على الأنظمة، ممّا يؤدي إلى منع الوصول إلى النظام، وبالتالي يطلب الطرف الخارجي من المستخدم دفع الفدية مقابل إزالة هذه البرامج.

- فيروس طروادة: يعمل فيروس طروادة على الدخول للنظام من خلال تنكّره ببرامج قانونية من خلال التنبيهات التي تُظهر للمستخدم حاجة النظام الخاص به، حينها تستطيع البرامج الضارة الدخول للنظام من خلال عملية المسح.

-هجوم حفرة الماء: و هو من الأخطار التي تستهدف المنظمات، خاصةً مواقع الويب الخاصة بالمنظمة، وعادةً ما يكون بشكل متكرر وبهدف إلحاق الضرر بهذه المواقع.

و ينتج عن هذه المخاطر عدة أضرار تنعكس سلبا على أداء المنظمة و تتمثل فيما يلي: (ساعد بوقرص ، 2022، ص 66)

- إعتراض البيانات؛

– إتلاف وتخريب البيانات؛

– سرقة الهويات الرقمية؛

– تعطيل المصالح والخدمات؛

– التجسس على الشبكات و كشف أسرار المستخدمين

– الإبتزاز؛

– التحايل والتصيُّد؛

– التأثير السلبي على الرأي العام.

وتشكل المخاطر السيبرانية من أهم المخاطر في القرن الواحد والعشرين، بحيث أصبح االمفهوم الحديث للأمن لا يقتصر فقط على الجوانب العسكرية، بل يواكب كل التهديدات التي تعرقل الاقتصاد الرقمي وتدفق المعرفة، (فقد أسقطت تكنولوجيا المعلومات والاتصالات مفهوم الحدود الجغرافية بين الدول، مما يضع السيادة الوطنية على المحك، خاصة مع اختراق المواقع الحكومية الرسمية والتجسس المعلوماتي على الدول). (أميرة عبد العظيم و محمد عبد الجواد، 2020، ص 375)

و يواجه الأمن السيبراني عدة صعوبات تقلل من فعاليته، و نلخص هذه الصعوبات فيما يلي:

- زيادة تطور و تعقد الهجمات السيبرانية على البيانات؛

- زيادة و انتشار الهجمات السيبرانية بشكل واسع، مما أدى إلى زيادة عدد الحروب السيبرانية والتجسس السيبراني؛

- ظهور تقنيات جديدة و الذي ساهم في الابتكار في الهجمات السيبرانية؛

- إخفاء هوية المستخدمين، و الذي يصعب الكشف عنهم؛

- نقص الموارد البشرية المتخصصة في مجال الأمن السيبراني؛

- التشفير له نقاط ضعف وكلمة المرور دوما قابلة للتقليد؛

- استخدام الروبوتات الآلية لنشر المعلومات الخاطئة؛

- استخدام مواقع التواصل الاجتماعي التي تتيح الدّخول إلى معلومات المستخدم بكل سهولة؛

- (لقد أدى استخدام شبكات الحواسيب إلى خلق نظم معلومات متكاملة تحقق مركزية البيانات، مما أتاح لمرتكبي الهجمات السيبرانية فرصة الوصول إلى كافة ملفات بيانات و برامج المؤسسة)؛ (علوطي لمين، 2009، ص 170)

- (افتقار الشركات العاملة في الميدان إلى رؤية صحيحة حول الكيفيات المستعملة في شبكاتها، مما سمح للقراصنة بالدخول والخروج بطريقة سهلة)؛ (جمال بوازدية، 2019، ص 1276)

- قلة الخبرة لدى المشرعين القانونيين و القضاة للتعامل مع التهديدات السيبرانية؛

- ضعف أنظمة الحماية بسبب استخدام الاتصال غير الآمن بالإنترنت؛

- ضعف التنسيق الدولي في مواجهة الهجمات السيبرانية.

5- آليات مواجهة المخاطر السيبرانية:

في ظل التهديدات السيبرانية المتزايدة و المخاطر الجسيمة المترتبة عنها على مستوى الأفراد و المنظمات، أصبح من الضروري البحث عن الآليات الفعالة لمواجهة هذه المخاطر، (كما أن صناع القرار في الولايات المتحدة الأمريكية، دول الاتحاد الأوروبي، روسيا، الصين والهند وغيرها من الدول، يصنفون الأمن السيبراني كأولوية في سياساتهم الدفاعية الوطنية، إضافة إلى إعلان أكثر من 130 دولة حول العالم عن تخصيص أقسام وسياسات خاصة بالحرب السيبرانية ضمن فرق الأمن الوطني، إذ تضاف جميع هذه الجهود إلى الجهود الأمنية التقليدية لمحاربة الجرائم الإلكترونية والاحتيال الإلكتروني و الأوجه الأخرى للمخاطر السيبرانية) . (علي زياد علي،2020، ص 57)

و يمكن تلخيص طرق استخدام الهجمات السيبرانية و كيفية مواجهتها في الجدول التالي:

الجدول رقم 01 : طرق استخدام الهجمات السيبرانية و كيفية مواجهتها

البيان	الأمن السيبراني الاجتماعي	الأمن السيبراني الاقتصادي	الأمن السيبراني العسكري
القيم المهددة	- الدين –الشباب – التراث - الأخلاق	- الجودة -التنافسية -المعاملات المالية - التطور الاقتصادي	- العقيدة العسكرية - ثقة الشعب بالجيش و الأمن
أهداف الهجمات السيبرانية	- نشر الإنحراف - التحريض على العنف - تشكيك الشعب بقدراته	- تدمير التنمية الاقتصادية - سرقة الأموال - تدمير التجارة الإلكترونية - إيقاف التصدير و الاستيراد -إلحاق الخسائر الاقتصادية	-الحصول على معلومات تخص التسليح - التجسس على الاستخبارات - امكانية إعادة توجيه القتال و الصواريخ الذكية - التجسس على البيانات الرقمية.
استراتيجيات مواجهة الهجمات السيبرانية	- توصية الهيئات الشخصية و الأجهزة الأمنية المختصة الوطنية -توجه و تركز الدفاع الشعبي الإلكتروني	- ضرورة توعية الخبراء و المختصين بمخاطر التهديدات السيبرانية - الحرص على استمرار عدم انقطاع الاتصال بشبكة الانترنت	- الهجوم الإلكتروني المضاد - محاكاة عملية الإختراق الأمني العملياتي - تطوير ترسانة السلاح الرقمي
آليات مواجهة الهجمات السيبرانية	-الشبكات الاجتماعية - البريد الالكتروني - مواقع وسائل الإعلام - تقنيات الحماية الالكترونية	- مواقع الحماية من الفبروسات - إدخال نشاط أمن المعلومات إلى الشركات -تحفيز مواقع الأنترنت الإحتياطية	- توفير برامج الحماية - تجهيز منشات الهجوم الإلكتروني - توظيف الأنظمة الإلكترونية في الهجوم على مواقع العدو
المسؤول عن المواجهة	كل من لديهم القدرة على عمل السلاح الرقمي	مديرية المعلوماتية في المؤسسات	وحدات خاصة بتقييم إحداثيات داخل الجيش و المخابرات تكون مهمتها الدفاع و الهجوم

المصدر: أحمد السيد النجار، محمد عبد الهادي علام، حروب المعلومات: من يواجهها؟مجلة الأهرام، العدد 139، مصر، 2015 ص 26 .

بالإضافة لما سبق يمكن إدراج بعض التدابير التي نراها ضرورية لتوفير الأمن السيبراني ، و التي تتمثل فيما يلي:

- ضرورة توفير التكنولوجيا الحديثة لمنح المنظمات والأفراد أدوات الأمن السيبراني اللازمة لمواجهة الهجمات السيبرانية، و الاعتماد على الذكاء الاصطناعي ،مع مسايرة تطور الهجمات السيبرانية؛

- توعية الأفراد بخطورة الهجمات السيبرانية، و بأهمية الأمن السيبراني لمواجهة هذه المخاطر، لتحقيق درجة عالية من الحماية في عالم رقمي سهل الاختراق؛
- تدريب الأفراد على كيفية التعامل مع المخاطر السيبرانية، لتجنب أو تقليص حجم الأضرار الناجمة عنها؛
- عدم تثبيت البرامج و التطبيقات من مواقع غير رسمية؛
- يجب أن تكون كلمة السر قوية و معقدة لا يمكن للغير معرفتها؛
- (إستخدام الجدران النارية التي تمنع التسلل و الاقتحام و القرصنة و هجوم الفيروسات الموجهة من خارج النظام عبر شبكة الانترنت)؛ (عبده نعمان صالح محمد الشريف، 2008، ص 124)
- سن ترسانة قانونية قوية تعمل على ردع الجرائم السيبرانية، قصد إقامة فضاء سيبراني آمن؛
- ضرورة التنسيق والتعاون الدولي أمنياً وإجرائياً وقضائياً في مواجهة الجرائم السيبرانية؛
- ضرورة وجود هيأة مختصة ذات كفاءة عالية في مواجهة الجرائم السيبرانية، و ذلك من الناحية العلمية و العملية و الفنية؛
- تمكين السلطات القائمة بالضبط والتحقيق و الملاحقة القضائية، في مجال الجرائم السيبرانية، مع تزويدهم بآليات تقنية متطورة، لكشف مختلف هذه الجرائم.

6- واقع الأمن السيبراني في الجزائر

تشير الإحصائيات المسجلة في الجزائر أن الجريمة السيبرانية شهدت منحاً تصاعدياً، (حيث سجلت سنة 2017 أكثر من 2.500 جريمة سيبرانية تتعلق أبرزها بانتهاك الحريات الشخصية، و التهديد عبر الأنترنت و الابتزاز و القرصنة الإلكترونية). (جمال بوازدية، 2019، ص 1280)

وهو ما ينبأ بخطورة الوضع، لا سيما في ظل توجه الجزائر نحو تبني الحكومة الإلكترونية، لذلك أصبحت السلطات الجزائرية ملزمة بإتخاذ الإجراءات اللازمة لمواجهة الجرائم الإلكترونية ، فهي تعمل على إيجاد الحلول والإجراءات اللازمة لمواجهة هذه التهديدات. في هذا السياق توجهت الجزائر إلى وضع إستراتيجية شاملة من أجل ضمان الأمن السيبراني، وذلك من خلال وسائل قانونية وتقنية لمقاومة الاستخدام غير الشرعي لشبكة الأنترنت قصد حماية نظم المعلومات من مخاطر التهديدات السيبرانية.

تتمحور استراتيجية الأمن السيبراني حول تعزيز وتحيين الإطار القانوني المتعلق باستعمال تكنولوجيات الإعلام والاتصال وتامين نظم المعلومات، وتقوم أساسا على سبعة 07 محاور هي :(ربيعي حسين و سمر محمود، 2022، ص 187)

- جانب وظيفي وتنظيمي يهدف إلى تنفيذ أعمال الأمن السيبراني بشكل موجه ضمن سلسلة وظيفية وتنظيمية مكرسة لضمان تجانس الأعمال؛
- جانب قانوني يهدف من خلاله على تعزيز الإطار القانوني لضمان أمن المنظومة المعلوماتية بشكل مستمر؛
- جانب الموارد البشرية يسمح بتوفير مورد بشري ذو كفاءة عالية في مجال النشاطات العملياتية والتسيير في مجال الدفاع السيبراني؛

- جانب تقني يعمل من خلاله على رفع القدرات التقنية للحماية واليقظة وضمان القدرة على الرد السريع على الهجمات السيبرانية؛

- جانب الوقاية والتحسيس لمستخدمي الجيش والقطاعات الأخرى بخطر استخدامات تكنولوجيا الإعلام والاتصال ؛

- جانب التعاون في مجال الدفاع السيبراني إلى جانب جيوش الدول الصديقة والشريكة من أجل ضمان نقل واكتساب الخبرات وتطويرها؛

- جانب البحث والتطوير الذي تعتبر جانبا حاسما في إستراتيجية الأمن السيبراني من خلال القدرة على تشخيص المشكلات وإيجاد الحلول لها.

و لتجسيد استراتيجيه الأمن السيبراني، يوجد هيئات متخصصة تحرص على مواجهة كافة الجرائم بما فيها التهديدات السيبرانية، و التي تتمثل فيما يلي:

- مركز الوقاية من جرائم الإعلام الآلي و الجرائم المعلوماتية للدرك الوطني:

أنشئ سنة 2008، و يهدف إلى تأمين منظومة المعلومات لخدمة الأمن العمومي، و ذلك من خلال تحليل بيانات الجرائم المعلوماتية المرتكبة، و تحديد هوية مرتكبيها ، قصد حماية نظم المعلومات، خاصة تلك المستعملة في البنوك و المؤسسات الرسمية، و يعمل هذا المركز على التكوين المستمر لأفراده حتى يوفر القوى المؤهلة ذات الكفاءة العالية حتى يتمكن من مواجهة مختلف الجرائم السيبرانية.

- المعهد الوطني للأدلة الجنائية و علم الإجرام للدرك الوطني:

أنشئ سنة 2004 بموجب مرسوم رئاسي 133/04، و دخل حيز الخدمة ابتداء من 01 جانفي 2009 ، و يهدف إلى تقديم المساعدات التقنية للمحققين، و يضم عدة مصالح أهمها: مصلحة البصمات ، مصلحة البيئة و مصلحة الإعلام الآلي، و يتم على مستوى هذه المصلحة رصد و مراقبة و تتبع عمليات الاختراق و القرصنة المعلوماتي، و كذا اكتشاف المعلومات المسروقة و تفكيك البرامج المعلوماتية. (عادل غزال، 2014، ص 64)

- المصلحة المركزية لمكافحة الجريمة المعلوماتية:

أنشئت سنة 2011، و هو تابع لمديرية الأمن الوطني ، و يهدف إلى مكافحة التهديدات الأمنية الناجمة عن الجرائم الإلكترونية سواء على المستوى الوطني أو الدولي، في هذا السياق تتعامل مع الهيئات الدولية المختصة في مكافحة الإجرام مثل أنتربول و أفريكوم، أما على المستوى المحلي فهي تتعامل مع الشرطة العلمية و المكاتب اللامركزية المختصة في الإجرام.

- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها:

أنشئت سنة 2009 ، و دخلت حيز الخدمة سنة 2015 بعد صدور المرسوم الرئاسي رقم 261-15 المؤرخ في 08 أكتوبر 2015، و من أهم مهامها ما يلي:

- استغلال المعطيات المتوفرة بطريقة تسمح بمتابعة كل ما يجري في الفضاء السيبراني من نشاطات غير شرعية؛

- تعزيز التنسيق بين مختلف الفاعلين في الميدان والتشديد على ضرورة التعاون بين القطاعين العام والخاص والمجتمع المدني، قصد نشر ثقافة المواجهة لكل الممارسات التي تخالف القانون في الفضاء السيبراني؛

- العمل على إقامة إطار مركزي للمعلوماتية ، يتم من خلالها جمع المعطيات، قصد الرصد المستمر للتهديدات واقتراح الحلول المناسبة؛

- (التنسيق والتعاون بين مختلف الأجهزة الأمنية، المالية والإدارية التي لها علاقة مباشرة بأنشطة تكنولوجيا الإعلام، من اجل تحديد المسؤوليات لفرض مراقبة صارمة بعد حصر المجالات المستهدفة من طرف محترفي الجريمة الالكترونية)؛ (جمال بوازدية 2019، ص 1281)

- اقتراح الأرضية اللازمة لتجسيد الإستراتيجية الوطنية لمواجهة الجرائم الالكترونية.

7. خاتمة:

يشهد العالم ثورة تكنولوجية هائلة أدت إلى ظهور تحديات خطيرة تهدد وجوده، و ذلك من خلال زيادة التهديدات الإلكترونية، في كافة المجالات: الاقتصادية و الاجتماعية و الثقافية و السياسية و العسكرية، مما أدى إلى أضرار خطيرة تضر بالفرد و المنظمة، في هذا السياق استوجب مواجهة هذه المخاطر، و ذلك عن طريق الأمن السيبراني الذي يعمل على الوقاية من الجرائم الإلكترونية، كما تطلب تبني إستراتيجية سيبرانية، و استحداث إطار قانوني و مؤسساتي لمواجهة مختلف التهديدات السيبرانية.

1.7 نتائج الدراسة:

من خلال هذه الدراسة توصلنا إلى النتائج التالية:

-يكتسي الأمن السيبراني أهمية بالغة، و ذلك نظرا للمخاطر الجسيمة للهجمات السيبرانية؛

-توسع مجال الأمن السيبراني بحيث له عدة أبعاد هي: اقتصادية، اجتماعية، ثقافية، قانونية، سياسية و عسكرية؛

-يوجد عدة آليات لمواجهة المخاطر السيبرانية، و التي تتوقف على مدى تأهيل العنصر البشري و التقني و التشريعي؛

-يواجه نظم المعلومات عدة مخاطر سيبرانية تهدد وجوده؛

-البعد الدولي للأمن السيبراني ، مما يستدعي تعاون دولي لمواجهته؛

-يتطلب الأمن السيبراني زيادة الاهتمام والتعبئة والتكيُّف مع التطور السريع للفضاء السيبراني، و ذلك من خلال تبني إستراتيجية شاملة لمواجهة الجرائم السيبرانية؛

-تولي الجزائر اهتماما كبيرا للأمن السيبراني، و ذلك نظرا لتزايد حجم الهجمات السيبرانية و خطورتها.

2.7 التوصيات:

لتحقيق الأمن السيبراني نضع التوصيات التالية:

-ضرورة العمل على ضمان أمن المعلومات وشبكات الأنترنت خلال خطوات مهمة تعتمد على مجموعة كبيرة من وسائل قانونية وتقنية و بشرية؛

-نشر الوعي لدى مختلف شرائح المجتمع، و الداعية إلى نشر ثقافة الأمن السيبراني؛

-ضرورة تدريب العنصر البشري قصد تأهيله على التقنيات الحديثة المستعملة في الفضاء السيبراني؛

-إنشاء هيئات تحكيم متخصصة في القضايا السيبرانية؛

-ضرورة سن نصوص عقابية صارمة، لردع الهجمات السيبرانية؛

-ضرورة التنسيق و التعاون الدولي في مواجهة الهجمات السيبرانية، سواء في مجال التحقيق أو تسليم المجرمين، أو التدريب و التأهيل؛

-ضرورة توفير المقومات الضرورية لإنجاح الإستراتيجية الشاملة التي تبنتها الجزائرمن أجل ضمان الأمن السيبراني.

8. قائمة المراجع:

1- أحمد السيد النجار، محمد عبد الهادي علام، حروب المعلومات: من يواجهها؟مجلة الأهرام، العدد 139، مصر، 2015 .

2- ادريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مجلة مصداقية،المجلد 01،العدد 01، الجزائر، 2019 .

3- أميرة عبد العظيم و محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، المجلد 3، العدد 35 ، 2020.

4- أوس مجيد غالب العوادي، الأمن المعلوماتي السيبراني ، مركز البيان للدراسات والتخطيط، بيروت، 2016.

5- بارة سمير، الأمن السيبراني في الجزائر: السياسات و المؤسسات، المجلة الجزائرية للأمن الإنساني، الجزائر، العدد الرابع، 2017.

6- جمال بوازدية، الإستراتيجية الجزائرية في مواجهة الجرائم السيبرانية : التحديات و الآفاق المستقبلية، مجلة العلوم القانونية و السياسية، المجلد 10، العدد 01، الجزائر، 2019 .

7- ربيعي حسين و سمر محمود، الحروب السيبرانية : المخاطر و استراتيجيات تحقيق الأمن السيبراني الدولي و الداخلي، المجلة الجزائرية للأمن الإنساني، المجلد 07، العدد 02، الجزائر، 2022.

8- عادل غزال، مشاريع الحكومة الإلكترونية من الإستراتيجية إلى التطليق، مشروع الجزائر: الحكومة الإلكترونية نموذجا، مجلة المكتبات والمعلومات، العدد 34 ، الجزائر، 2014.

9- عبده نعمان صالح محمد الشريف، الحكومة الإلكترونية كإستراتيجية و طرق الإثبات و الحماية لمعاملاتها، مجلة علوم الاقتصاد و التسيير و التجارة، العدد 18، الجزائر، 2008.

10- علوطي لمين، تحديات الأمن الإلكتروني في المؤسسة، مجلة أبحاث اقتصادية و إدارية، العدد 06، الجزائر، 2009.

11- علي زياد علي، الصراع والأمن الجيوسيبراني في الساحة الدولية: دراسة في استراتيجيات الاشتباك الرقمي، دار أمجد للنشر والتوزيع، عمان، 2020 .

12- مجتمع الأنترنت، المبادئ التوجيهية المتعلقة بتأمين البنية التحتية للانترنت في الدول العربية، 2020.

13- مصطفى إبراهيم سلمان الشمري، الأمن السيبراني وأثره في الأمن الوطني العراقي، مجلة العلوم القانونية والسياسية، المجلد 10 ، العدد 01 ، 2021.

14- منى الأشقر جبور، «الأمن السيبراني: التحديات ومستلزمات المواجهة ، المركز العربي للبحوث القانونية والقضائية، 2012.