الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة محمد بوضياف -المسيلة

كلية: الحقوق والعلوم السياسية

قسم: الحقوق

ميدان: الحقوق والعلوم السياسية

تخصص قانون إداري

مذكرة مقدمة ضمن متطلبات نيل شهادة الماستر الأكاديمـــي

بعنوان:

الأمن السيبراني (المفهوم والأهمية)

اعداد الطالبة

- قاقي سعاد

الأستاذ المشرف:

- د. مقروف محمد

لجنة المناقشة:

اللقب والاسم	الرتبة	الصفة
لعمارة عبد الرزاق	أستاذ محاضر	رئيســا
مقروف محمد	أستاذ التعليم العالي	مشرفا ومقررا
بوبعاية كمال	أستاذ محاضر	مناقشا

السنة الجامعية: 2024/2025

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة محمد بوضياف -المسيلة

كلية: الحقوق والعلوم السياسية

قسم: الحقوق

ميدان: الحقوق والعلوم السياسية

تخصص قانون إداري

مذكرة مقدمة ضمن متطلبات نيل شهادة الماستر الأكاديمـــي

بعنوان:

الأمن السيبراني (المفهوم والأهمية)

اعداد الطالبة:

- قاقي سعاد

الأستاذ المشرف:

- د. مقروف محمد

لجنة المناقشة:

اللقب والاسم	الرتبة	الصفة
	أستاذ محاضر	رئيســا
مقروف محمد	أستاذ التعليم العالي	مشرفا ومقررا
	أستاذ محاضر	مناقشا

السنة الجامعية: 2024/2025

ملحق بالقرار رقم ....1082.... المؤرخ في 27 ديسمبر 2020 .....

الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي

الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

أنا الممضي أسفله،

السيد(ة): ..قاقي سعاد.. الصفة: طالب، أستاذ، باحث ..طالبة..

الحامل(ة) لبطاقة التعريف الوطنية رقم 21 03 44 77 والصادرة بتاريخ 2024-04-04

المسجل(ة) بكلية / معهد ..الحقوق والعلوم السياسية.. قسم ..المسؤولية..

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه)،

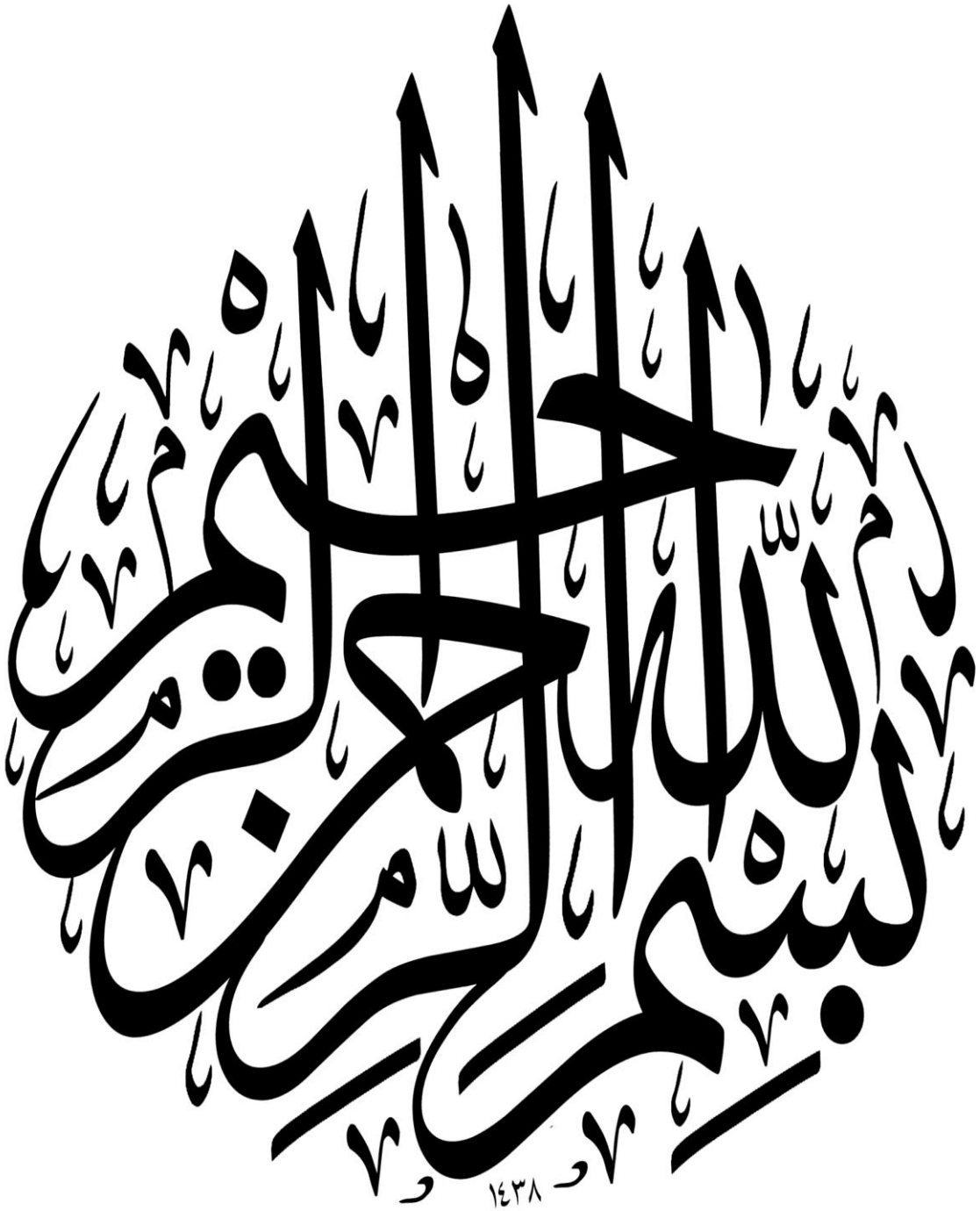
عنوانها:

الأمن السيبراني - المفهوم والأهمية -

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه .

التاريخ: 01 جوان 2025

توقيع المعني (ة)


بسم الله الرحمن الرحيم
١٤٣٨

شكر وعرفان

قال تعالى «قال ربي أوزعني أن أشكر نعمتك التي أنعمت علي وعلى والدي وأن أعمل صالحا ترضاه"

الحمد والشكر لله الذي وسع كل شيء رحمة وعلما على إتمام هذا العمل والصلاة والسلام على رسول الله سيدنا محمد عليه أفضل الصلوات، نتقدم بجزيل الشكر والتقدير والعرفان إلى أستاذنا الفاضل الدكتور " **مقروف محمد** " على الجهد المبذول لمساعدتنا في إعداد هذه المذكرة، فلم يبخل علينا بأي فكرة أو معلومة، وتابع المذكرة خطوة بخطوة إلى أن تمت وظهرت في شكلها ومضمونها الراهن، أدامه الله فخرا لنا ولخدمة العلم والوطن، وجزاه الله عن ذلك خيرا في الدنيا والآخرة.

وأجزل الشكر وافره إلى الأساتذة الذين قبلوا قراءة ومناقشة هذه المذكرة فلهم كل التقدير على الملاحظات التي سيسدونها، والتي ستثري هذه الدراسة بلا شك.

دون أن ننسى كل الأساتذة الذين ساعدونا وساهموا في تزويدنا بالمعلومات والمعارف ولم يبخلوا علينا شيء طوال مدة الدراسة.

إهـــداء

بعد مسيرةٍ دامت سنوات، حملت في طياتها الكثير من الصعوبات والمشقات والتعب، ها أنا اليوم أقف على عتبة التخرج، أقطف ثمرات جهدي وتعبي، وأرفع قبعتي بكل فخر.

أهدي هذا النجاح إلى من زيّن اسمي بأجمل الألقاب، إلى من دعمني بلا حدود وأعطاني بلا مقابل، إلى من علمني أن الدنيا كفاح، وسلاحها العلم والمعرفة إلى فخري واعتزازي :**والدي العزيز**.

وإلى من جعل الجنة تحت أقدامها، واحتواني قلبها قبل يدها وسهلت عليّ الشدائد بدعائها، والشمعة التي أنارت لي الليالي المظلمات سر قوتي ونجاحي، وردتي الجميلة :**والدتي الغالية**

وإلى أعزّ سند في الحياة بعد والدي، إلى نصفي الثاني وبيت أسراري إلى الداعم الكبير في مسيرتي :**أختي الغالية. وأهدي تحياتي إلى إخوتي جميعًا، حفظهم الله ورعاهم.**

ودون أن أنسى، أرسل تحياتي ومحبّتي إلى أولاد أختي **قيس وأوس**، وأتمنى من الله أن يوفقهما، ويجعل أيامهما بهجة وفرحًا، وأن ييسر لهما حياتهما، ويبلغا أعلى المراتب.

ولا أنسى أيضًا تحياتي لزملائي وزميلاتي طوال المسيرة الدراسية، ولصديقاتي المقربات :**شيماء، و آية، وخيرة**.

حظ موفق للجميع.

مقدمة:

يشهد العالم في العقود الأخيرة تحوّلاً جذريًا في طبيعة التهديدات الأمنية، حيث لم تعد المخاطر محصورة في النزاعات العسكرية التقليدية أو الهجمات المسلحة، بل امتدت إلى مجالات جديدة أكثر تعقيدًا وتجريدًا، وعلى رأسها الفضاء السيبراني. فقد باتت التهديدات الإلكترونية تشكّل جزءًا لا يتجزأ من أدوات الصراع الجيوسياسي، وأصبحت الدول توظفها في حروب غير معلنة، تستهدف من خلالها البنى التحتية الحيوية، والمؤسسات السيادية، والمنشآت الاقتصادية، بل وتمتد أحيانًا لتطال الأفراد وخصوصياتهم، مما يهدد الاستقرار المجتمعي والسلم الاجتماعي.

وفي ظل هذا الواقع، لم يعد الأمن السيبراني ترفًا مؤسساتيًا أو خيارًا مؤجلًا، بل غدا ضرورةً حتمية تمليها طبيعة العصر الرقمي ومتطلباته المتسارعة. فالحماية الفعّالة للفضاء السيبراني أضحت مرتبطة ارتباطًا وثيقًا بحماية السيادة الوطنية، وضمان استمرارية مؤسسات الدولة، وصون الأمن الداخلي، بل وتمتد لتشمل الأمن الاقتصادي والثقافي والاجتماعي للدول.

ولذلك، شهدت السنوات الأخيرة اهتمامًا متزايدًا من قبل الحكومات والمؤسسات الدولية بوضع أطر تشريعية وتقنية وتنظيمية لتعزيز الأمن السيبراني، وتكثيف التعاون الإقليمي والدولي في هذا المجال. وقد أدركت الجزائر، كغيرها من الدول، أهمية مواكبة هذه التطورات المتسارعة، خاصة في ظل تنامي الاعتماد على التكنولوجيا الرقمية في مختلف مناحي الحياة، من الخدمات الحكومية إلى القطاع المالي، ومن التعليم إلى الطاقة والنقل.

فالجزائر، باعتبارها دولة ذات موقع جيوسياسي محوري، وتواجه تحديات أمنية متعددة الأبعاد، تجد نفسها اليوم أمام ضرورة صياغة وتنفيذ سياسات واستراتيجيات وطنية فعّالة للأمن السيبراني. وهو ما يطرح جملة من التساؤلات حول مدى جاهزية الإطار القانوني، والتنظيمي، والمؤسساتي لمواجهة التهديدات السيبرانية، وحول مدى تطابق هذه السياسات مع المؤشرات والمعايير الدولية المعتمدة في هذا المجال.

ومن هذا المنطلق، يأتي هذا البحث كمحاولة علمية لتحليل واقع الأمن السيبراني في الجزائر، من خلال دراسة الاستراتيجية الوطنية في هذا المجال، وتقييم مدى فعاليتها، والكشف عن أوجه القوة والقصور فيها، مع تقديم توصيات تهدف إلى تعزيز القدرات الوطنية في حماية الفضاء السيبراني، ورفع مستوى الجاهزية السيادية في مواجهة التحديات الرقمية المعاصرة.

أهمية الموضوع

الأهمية العلمية : فمن الناحية العلمية، يُسهم البحث في إثراء الأدبيات المتعلقة بالأمن السيبراني، من خلال تحليل واقع الاستراتيجية الجزائرية في هذا المجال، واستعراض المفاهيم الحديثة ذات الصلة.

الأهمية العملية : أما من الناحية العملية، فتتمثل الأهمية في كون الموضوع يُلامس الأمن القومي مباشرة، ويمس حياة الأفراد ومصالح المؤسسات، كما يُسلّط الضوء على التحديات التي تواجه الجزائر في مجال الأمن السيبراني، ويبحث في مدى قدرتها على مواكبة التطورات العالمية، مما يُمكن صناع القرار من الاستفادة من نتائج البحث لتطوير السياسات الوطنية ذات الصلة.

أهداف البحث

أهداف هذا البحث تتمثل في التعرف على الإطار العام للأمن السيبراني ومفاهيمه الحديثة، وتحليل الاستراتيجية الجزائرية في مجال حماية الفضاء السيبراني، إضافةً إلى تقييم مدى مطابقة السياسات الجزائرية للمؤشرات والمعايير الدولية. كما يهدف البحث إلى تقديم توصيات من شأنها الإسهام في تحسين الأداء الوطني في مجال الأمن السيبراني.

أسباب اختيار الموضوع

جاء اختيار موضوع "الأمن السيبراني" استجابةً لجملة من الدوافع الموضوعية والذاتية التي تداخلت لتُشكّل أساسًا قويًا لهذا التوجه البحثي.

أسباب موضوعية : فمن الناحية الموضوعية، يفرض الواقع الدولي المتغير، وما يشهده من تصاعد متسارع في وتيرة الهجمات الإلكترونية، تحديات جديدة على صعيد الأمن القومي للدول، إذ باتت هذه التهديدات تمس بشكل مباشر سيادة الدول، واستقرار مؤسساتها، وسلامة بنيتها التحتية الحيوية. ويأتي هذا في ظل التحول الرقمي الشامل الذي يشهده العالم، والذي فرض واقعًا جديدًا لم يكن مألوفًا في العقود السابقة، وهو ما جعل من الأمن السيبراني أولوية استراتيجية لا يمكن تجاهلها.

إلى جانب ذلك، تبرز **ندرة الدراسات العلمية المتخصصة** في موضوع الأمن السيبراني ضمن السياق الجزائري، سواء من حيث التحليل البنيوي للاستراتيجية الوطنية أو من حيث مقارنتها بالمؤشرات والمعايير الدولية المعتمدة، مما خلق فراغًا بحثيًا يستدعي التناول والتحليل. كما أن الغموض النسبي الذي يكتنف ملامح

السياسات الجزائرية في هذا المجال، مقارنةً بتجارب إقليمية ودولية رائدة، شكّل دافعًا موضوعيًا إضافيًا للبحث والتقصي.

أسباب ذاتية : أما من الناحية الذاتية، فإن الاهتمام الشخصي للباحثة بقضايا الأمن الوطني والتحول الرقمي، بالإضافة إلى القناعة بأهمية استباق المخاطر الرقمية وبناء وعي استراتيجي لدى صانعي القرار والمجتمع على حد سواء، كان لهما الأثر الأكبر في اختيار هذا الموضوع. كما أن الرغبة في الإسهام العلمي في مجال لا يزال قيد التشكل والتطوير في الجزائر، وتعزيز الفهم الأكاديمي والعملي لهذه الظاهرة المتعددة الأبعاد، شكّلا دافعًا ذاتيًا قويًا لخوض غمار هذا البحث، ومحاولة تقديم معالجة شاملة تسهم في سد فجوة قائمة في الأدبيات الوطنية.

الصعوبات

واجهت الدراسة عدة تحديات، أهمها ندرة المصادر المحلية الحديثة المتعلقة بالسياسات الوطنية في هذا المجال، وغياب الشفافية في نشر بعض الإحصاءات والبيانات الرسمية المتعلقة بالهجمات السيبرانية في الجزائر.

الإشكالية

من خلال ما سبق ذكره يمكننا طرح الإشكالية الأتية :

إلى أي مدى استطاعت الجزائر بناء استراتيجية وطنية فعالة للأمن السيبراني ؟

المنهجية المعتمدة

تم الاعتماد على المنهج :

الوصفي : لدراسة النصوص القانونية والسياسات المعتمدة .

المقارن : لمقارنة وضع الجزائر بدول أخرى في المؤشرات الدولية.

خطة البحث

ولتناول هذا الموضوع، تم تقسيم البحث إلى فصلين رئيسيين: تناول الفصل الأول مقاربة معرفية حول الأمن السيبراني، حيث تطرّقنا في المبحث الأول إلى تعريف الأمن السيبراني، وبيان أبعاده ومعضلته، ثم انعكاسات التهديدات السيبرانية على الأمن القومي للدول، بينما خُصِّص المبحث الثاني لدراسة الجريمة السيبرانية، من خلال التطرق إلى الجرائم الإلكترونية، والإرهاب الإلكتروني، والحروب السيبرانية. أما الفصل الثاني، فقد ركّز على واقع الأمن السيبراني في الجزائر، حيث تناولنا في المبحث الأول الأطر النظرية والتطبيقية لاستراتيجيات الحماية المعلوماتية، ثم استعرضنا في المبحث الثاني السياسة العامة الجزائرية في مواجهة الجرائم السيبرانية، من خلال تحليل الأهداف الأمنية، والهيكل التنظيمي، والتدابير التقنية والإجرائية المتخذة، في حين خُصص المبحث الثالث لدراسة مفهوم المخاطر التقنية المرتبطة بالتطور التكنولوجي، مع التركيز على البرامج الضارة باعتبارها أبرز صور هذه المخاطر. ويُختتم البحث بخاتمة تتضمن أهم النتائج والتوصيات المقترحة.

الفصل الأول

مقاربة معرفية حول الأمن السيبراني

يمثل الأمن السيبراني أحد أعقد الإشكالات التي فرضتها البيئة التكنولوجية الحديثة، نتيجة التوسع الكبير في استخدام الإنترنت والاعتماد المتزايد على الفضاء الرقمي في مختلف المعاملات. وضمن هذا الإطار، أصبح من الضروري الوقوف على الأسس المفاهيمية لهذا المجال، عبر استعراض تعريفاته المتعددة، وأبعاده التقنية والاستراتيجية، فضلًا عن التحديات التي تفرضها التهديدات السيبرانية على الأمن القومي للدول. وعليه، يسعى هذا الفصل إلى تقديم مقاربة معرفية شاملة تُمهّد لفهم السياق العام للأمن السيبراني وتداعياته الراهنة.

الفصل الأول : مقاربة معرفية حول الأمن السيبراني

في العصر الرقمي المعاصر، أصبحت البيانات والمعلومات الرقمية تمثل ثروة استراتيجية، الأمر الذي جعل من الأمن السيبراني قضية محورية تتقاطع مع مختلف الأبعاد السياسية، الاقتصادية، التقنية والمعرفية. لم يعد الأمن السيبراني مجرد مسألة تقنية تتعلق بحماية الأنظمة والشبكات من الاختراقات، بل تحول إلى مجال معرفي متكامل يقتضي فهماً عميقاً لبنية التهديدات، وأنماط السلوك البشري، والأنظمة المعلوماتية، بل وحتى السياقات الجيوسياسية.

إن مقاربة الأمن السيبراني من منظور معرفي تتيح فهمًا أشمل وأعمق لطبيعة التحديات التي تواجه الأفراد والمؤسسات والدول في الفضاء الرقمي. فهي تتجاوز الطابع الأداتي للتكنولوجيا، لتسائل أنماط إنتاج المعرفة، وإدارة المخاطر، واتخاذ القرار في بيئة تتسم بالتعقيد والديناميكية. ومن هذا المنطلق، تتجلى الحاجة إلى بناء إطار معرفي متعدد التخصصات يدمج بين علوم الحاسوب، علم النفس، الدراسات الأمنية، ونظرية المعرفة، من أجل بلورة سياسات واستراتيجيات قادرة على الاستجابة لمتطلبات الأمن السيبراني الحديث.

المبحث الأول ماهية الأمن السيبراني

أصبح ظهور التهديدات والجرائم السيبرانية تحديًا كبيرًا للأمن القومي والدولي، لدرجة أن العديد من الباحثين اعتبروا الفضاء السيبراني بمثابة المجال الخامس في الحروب بعد البر والبحر والجو والفضاء. وهو ما استدعى ضرورة وجود ضمانات أمنية ضمن هذه البيئة الرقمية، تبلورت بشكل أساسي في ظهور الأمن السيبراني (Cyber Security) كبعد جديد ضمن أجندة حقل الدراسات الأمنية. وتتداخل العديد من المفاهيم مع الأمن السيبراني، مما يجعل العديد منها امتدادًا للمفهوم.

المطلب الأول : الأمن السيبراني

مع التقدم المتسارع في تكنولوجيا المعلومات والاتصالات، أصبحت الأنظمة الرقمية جزءًا لا يتجزأ من مختلف جوانب الحياة اليومية، من التعليم والصحة إلى الاقتصاد والإدارة. وقد رافق هذا التحول الرقمي ظهور تحديات جديدة تهدد أمن المعلومات وحماية البيانات، مما أفرز مفهوماً حديثًا يعرف بـ"الأمن السيبراني."

يُعد الأمن السيبراني من أهم الركائز التي تعتمد عليها الدول والمؤسسات والأفراد لحماية بنيتها الرقمية من التهديدات والهجمات الإلكترونية التي تتزايد تعقيدًا وخطورة. وفي ظل هذا الواقع، أصبح من الضروري

فهم هذا المفهوم وأبعاده المختلفة، والوقوف على أهميته ووسائل تحقيقه، وهو ما سيتم تناوله في هذا المطلب.

الفرع الأول : تعريف الأمن السيبراني

إن طبيعة الفضاء السيبراني الذي يتضمن عمليات الدخول والخروج إلى المواقع الإلكترونية، وتبادل البيانات وتخزينها، تفرض ضرورة وضع قواعد وآليات تحمي أنظمة المعلومات والبيانات من الاختراقات. وهذا ما يدفع كل مُستخدِم أو مهتم بهذا المجال إلى طرح السؤال: ما هو الأمن السيبراني؟

تختلف التعريفات وفقًا لاختلاف المنظورات بين من يركز على الجوانب التقنية والعملية (كالباحثين) وبين من يهتم بالجوانب التنظيمية والقانونية (كالهيئات الحكومية). وفيما يلي أبرز التعريفات:

التعريف الأكاديمي:

يرى العالمان Neittaanmäki Lehto و Pekka Marttiأن الأمن السيبراني هو: *"مجموعة الإجراءات الفعالة لمواجهة جرائم الكمبيوتر، بما في ذلك التدابير الوقائية والردعية."*

بينما يعرفه البروفيسور ريتشارد كيميرر Richard Kemmerer (من جامعة كاليفورنيا) بأنه: *"أدوات دفاعية تهدف إلى كشف محاولات القرصنة وإفشالها."*

ويؤيده الخبير إدوارد أموروزو Edward Amoroso في تعريفه: *"الوسائل التقنية التي تحد من مخاطر الهجمات على البرمجيات أو الشبكات، مثل مكافحة الفيروسات، وتشفير الاتصالات، وغيرها."*

التعريف الحكومي:

الولايات المتحدة الأمريكية (وزارة الدفاع):

"الإجراءات التنظيمية لحماية المعلومات الإلكترونية والمادية من الجرائم أو التخريب أو الحوادث العرضية."

الوكالة الأوروبية للأمن السيبراني:(ENISA) (أول من أصدرت التشريع في هذا المجال)[1] *قدرة الأنظمة المعلوماتية على مقاومة الاختراقات أو الحوادث غير المُخطَّط لها التي تستهدف البيانات المُخزَّنة أو المُتبادَلة."*

[1] - أول اتفاقية تناولت هذا الموضوع ، هي الاتفاقية التي صدرت في بودابست 2001

التعريف القانوني الجزائري:

ينص التشريع الجزائري على أن الأمن السيبراني: *"مجموعة الوسائل التقنية والتنظيمية والإدارية المُعتمَدة لمنع الاستخدام غير المُصرَّح به للبيانات، وحماية نظم الاتصالات من سوء الاستغلال، مع ضمان استعادة المعلومات في حال فقدانها."*

والمعلومات التي تحتويها وذلك بهدف ضمان توافر استمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة [1]لحماية المواطنين المستهلكين من المخاطر في الفضاء السيبراني

بالنسبة للاتحاد الدولي للاتصالات :

وفقًا للاتحاد الدولي للاتصالات، يُشير مصطلح "الأمن السيبراني" إلى مجموعة شاملة من الأنشطة التي تهدف إلى حماية البيئة السيبرانية، وتتضمن تطبيق سياسات وإجراءات أمنية، واعتماد مبادئ توجيهية، وتبنّي مقاربات فعّالة لإدارة المخاطر، بالإضافة إلى تنفيذ برامج تدريبية واستخدام تقنيات حديثة لحماية أصول المؤسسات والمستخدمين.

يمكن تناول تعريف الأمن السيبراني من بعدين رئيسيين:

من الناحية الهدفية :يُعد الأمن السيبراني وسيلة لتأمين الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات، مما يُساهم في تقليل الخسائر والأضرار الناجمة عن المخاطر والتهديدات المحتملة، مع ضمان استعادة الوضع الطبيعي سريعًا لتفادي توقف عجلة الإنتاج وتحويل الأضرار إلى خسائر دائمة.

من الناحية الوظيفية :يشمل الأمن السيبراني مجموعة من الإجراءات والوسائل والسياسات والمبادئ التوجيهية والمقاربات العملية لإدارة المخاطر، إضافة إلى التدريبات والممارسات المثلى والتقنيات الحديثة، والتي تُستخدم جميعها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين. [2]

الفرع الثاني : أبعاد الأمن السيبراني ومعضلته

إذا افترضنا أن الأمن القومي هو قدرة الدولة على حماية مصالحها الحيوية وضمان استقرار مجالات حياتها اليومية، وتوجيه مسيرتها نحو التقدم بثباتٍ وطمأنينة، فإن هذه الحماية ترتبط ارتباطًا وثيقًا بسلامة

[1] - ورد تعريف هذه الجريمة ضمن نص **المادة الثانية (2)** من القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق لـ 05 غشت سنة 2009 ، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ، ر ، ج ، ج ، عدد 47 ، الصادرة بتاريخ 16 غشت سنة 2009 ، ص 05
كما عددت المادة (87) من قانون العقوبات الجزاء المنتظر لكل من ثبت في حقه الاختراق، وبالتالي المساس بحقوق الدولة أو المواطن.

[2] - أنظر التقرير الصادر عن الاتحاد الدولي للاتصالات، حول "اتجاهات الاصلاح في الاتصالات للعام 2010-2011 . "

مصادر الثروة والحياة في العصر الحديث، والتي تشمل – بشكل رئيسي – البيانات والمعلومات .فهذه العناصر تُشكِّل جسر التواصل والاتصال، وتُعتبر ركيزةً للإبداع والابتكار والمنافسة العالمية. ومن هنا، يتضح أن الأمن السيبراني لا يقتصر على الجوانب التقنية فحسب، بل يمتد ليشمل أبعادًا استراتيجية شاملة: عسكريةً، واقتصاديةً، واجتماعيةً، وقانونيةً، وأمنيةً

الأبعاد العسكرية :

تتمثل الميزة النسبية للقوة السيبرانية في قدرتها على ربط الوحدات العسكرية عبر الشبكات الإلكترونية، مما يُسهِّل تبادل المعلومات بسرعة فائقة، وإصدار الأوامر العسكرية، وتنفيذ عمليات استهداف وتدمير الأهداف عن بُعد. إلا أن هذه الميزة قد تتحول إلى نقطة ضعف حاسمة إذا لم تُؤمَّن الشبكات الإلكترونية بشكلٍ فعّال ضد الاختراقات الخارجية، والتي قد تُستغَل لشن هجمات إلكترونية مضادة تستهدف شبكات القوات المسلحة وأجهزة الاستخبارات.

فالاختراقات السيبرانية قد تؤدي إلى تجسس على الأسرار العسكرية، أو تعطيل القدرات التشغيلية للدولة، مثل إعاقة نشر القوات بسرعة، أو قطع التنسيق بين الوحدات العسكرية والأنظمة الاقتصادية المرتبطة بها، أو شلّ أنظمة حيوية كالدفاع الجوي والتوجيه الإلكتروني. بل وقد تصل الخطورة إلى فقدان السيطرة على مراكز القيادة والسيطرة، مما يُهدد الأمن الوطني بشكلٍ مباشر[1].

الأبعاد السياسية :

تتمثل الأبعاد السياسية للأمن السيبراني في حق الدولة في حماية نظامها السياسي وسيادتها ومصالحها الاقتصادية، والتي تشمل واجبها نحو ضمان رفاهية شعبها. وفي عصرٍ تُعيد فيه التكنولوجيا تشكيل موازين القوى، أصبح الفرد – بفضل الثورة الرقمية – فاعلًا مؤثرًا في المشهد السياسي الداخلي، حيث يُتيح له الوصول إلى كمٍّ هائل من المعلومات تحليل خلفيات القرارات السياسية التي تتخذها حكومته، ونشرها عبر منصات التواصل أو الأجهزة الذكية.

وفي المقابل، يعتمد صنّاع القرار والفاعلون السياسيون على الأدوات الرقمية نفسها لتعزيز نفوذهم، عبر استهداف شريحة واسعة من المواطنين للترويج لسياساتهم، بغض النظر عن مدى مصداقية المضامين أو اتساقها مع المبادئ العامة. ويُظهر التاريخ أمثلةً واضحةً على هذا التأثير المزدوج للتكنولوجيا: فاستخدام الرئيس الأمريكي السابق باراك أوباما للشبكات الاجتماعية بكثافة خلال حملته الانتخابية (٢٠٠٨) حوّلها

[1] - إدريس عطية ، **مجلة الدراسات الاستراتيجية والعسكرية**، المركز الديموقراطي العربي برلين ، المجلة 02، العدد 06 مارس 2020 ص 05.

إلى أداة فعّالة لبناء التأييد الشعبي. بينما كشفت تسريبات "ويكيليكس" للوثائق الدبلوماسية السرية عن مدى هشاشة الثقة بين الدول، وتأثير الاختراقات الإلكترونية على العلاقات الدولية ومصداقية الأنظمة السياسية[1].

الأبعاد الاجتماعية :

تُعدُّ الأبعاد الاجتماعية للأمن السيبراني ركيزةً أساسيةً لبناء مجتمع رقمي واعٍ، حيث يبدأ تعزيز الأمن من خلال نشر الوعي السليم بمخاطر الفضاء الإلكتروني بين جميع مستخدمي الشبكة الدولية. ولا تقتصر الخطوات الوقائية على الحلول التقنية فحسب، بل تشمل أيضًا صياغة سياسات تثقيفية مُبسَّطة تشرح التحديات الإلكترونية، وتُعرِّف بالإجراءات الأمنية الوقائية والرادعة، وتُوجِّه الأفراد نحو الممارسات الآمنة.

ولتحقيق ذلك، يجب تنظيم حملات إعلامية مُنهجة تستهدف تثقيف المواطنين بمسؤولياتهم الرقمية، سواء في حماية بياناتهم الشخصية أو تجنُّب نشر المعلومات المضللة. كما يتطلَّب الأمر تعاونًا مؤسسيًّا بين الحكومات ومنصات التواصل والمؤسسات التعليمية لبناء "مجتمع معلوماتي مسؤول" قادر على مواجهة الهجمات الإلكترونية، والحدّ من انتشار الجرائم السيبرانية مثل التصيد الإلكتروني والابتزاز. فالتعليم المدني الرقمي ليس ترفًا، بل ضرورةٌ لتمكين الأفراد من التعامل الذكي مع التهديدات، وحماية أنفسهم ومجتمعاتهم من تداعياتها الواقعية[2].

وينبغي التشديد على واجب الأمن والمسؤولية الفردية والتدابير الرادعة، وكذلك التداعيات المحتملة في إطار القانون الجنائي التي تترتب على عدم احترام الالتزامات التي يوجبها الأمن. وبشكل أكثر عمومية، فإنه من الضروري توفير التثقيف والتدريب على تكنولوجيات المعلومات والاتصال، وليس فقط على الأمن والتدابير الرادعة، إذ يجب أن تُغرس الثقافة الأمنية داخل ثقافة تكنولوجيا المعلومات[3].

الأبعاد الاقتصادية :

يرتبط الأمن السيبراني ارتباطًا عضويًّا بالاقتصاد، لا سيما في عصر اقتصاد المعرفة الذي يعتمد على توسيع نطاق استخدام تقنيات المعلومات والاتصالات، حيث تُشكِّل البياناتُ – سواءً المُخزَّنة أو المُتداولة ركيزةً للقيمة الاقتصادية على جميع المستويات. فالتقنيات الرقمية تُعزز التنميةَ الاقتصادية للدول من خلال تمكينها من الاستفادة من الفرص التي تتيحها الشركات العالمية، مثل خفض تكاليف الإنتاج، وتحسين الكفاءة التشغيلية، والاندماج في الأسواق الدولية.

---

[1] - قوي بوحنية ، إدريس عطية ، **مجلة الدراسات الاستراتيجية والعسكرية**، المركز الديموقراطي العربي برلين ، المجلة 02، العدد 06 مارس 2020 ص 62 .

[2] - سمير بارة: مرجع سابق ذكر ، ص 62 .

[3] - سمير بارة ، المرجع السابق ، ص 62 .

ويزداد هذا الترابط تعقيدًا مع التحوُّل نحو المال الإلكتروني وانتشار الخدمات الرقمية، حيث تتسابق البنوك والمؤسسات المالية على استثمارات ضخمة في تطوير أنظمة دفع آمنة، بينما تُنظم الحكومات تشريعات صارمة لحماية المعاملات المالية من جرائم كغسيل الأموال والتهرب الضريبي، والتي تتخطى الحدود الجغرافية. إلا أن ضمان أمن هذه البيئة الرقمية يظل تحديًّا كبيرًا، خاصة مع تزايد الهجمات الإلكترونية التي تستهدف البنى التحتية المالية، مما يُهدد استقرار الأسواق ويُعرض الثقةَ في الأنظمة الاقتصادية للخطر.

من هنا، يُصبح الأمن السيبراني ضامنًا لاستمرارية الخدمات الرقمية، كالتجارة الإلكترونية والخدمات المصرفية عبر الإنترنت، والتي يعتمد عليها النمو الاقتصادي. فكلما زادت موثوقية هذه الخدمات وأمانها، ازداد إقبال الأفراد والشركات عليها، مما يُترجم مباشرةً إلى تعزيز أسس الاقتصاد الوطني وتنافسيته العالمية[1].

الأبعاد القانونية :

تتشابك الأبعاد القانونية للأمن السيبراني مع التطور التكنولوجي في علاقة تبادلية؛ فالتقنيات المتسارعة تفرض تحديث التشريعات لمواكبة الأعمال المشروعة وغير المشروعة في الفضاء الرقمي. ومع ذلك، لا تزال الجرائم السيبرانية تواجه فجوة تشريعية بسبب طبيعتها المعقدة، مثل صعوبة تعقب الجناة، ومرونة المفاهيم التقنية، وغياب الحدود الجغرافية، مما يستدعي تعاونًا دوليًّا فاعلًا في إطار قانوني عابر للحدود.

على صعيد الحماية، يجب أن تستند القواعد القانونية إلى فهمٍ شامل للمخاطر التقنية والبشرية، سواءً نتجت عن أخطاء غير مقصودة أو أفعال إجرامية مُتعمَّدة .وبالقياس على مبادئ الأمن التقليدي (تحديد التهديدات، وضع استراتيجيات الدفاع، وإعداد خطط الطوارئ)، يتطلَّب الأمن السيبراني إرساء آليات رادعة تشمل:

1. **تشريعات متخصصة** :تُعرِّف الجرائم الإلكترونية بوضوح، وتُحدد العقوبات المناسبة لها.
2. **هيكليات مؤسساتية** :إنشاء وحدات قضائية وشرطية مُتخصِّصة في التحقيق والملاحقة.
3. **تعزيز القدرات** :تدريب الكوادر القانونية على التعامل مع الأدلة الرقمية.
4. **المسؤوليات المتعددة** :إقرار مسؤوليات مدنية (تعويضات) وجزائية (عقوبات) ومهنية (التزامات المؤسسات).

[1] - إدريس عطية: مرجع سابق الذكر، ص 105.

ولا يقتصر الأمر على المستوى الوطني، بل يتعداه إلى تبني اتفاقيات دولية لملاحقة المجرمين الإلكترونيين، وحماية الضحايا عبر الحدود، مثل اتفاقية بودابست لمكافحة الجريمة السيبرانية. فغياب الإطار القانوني الموحَّد يُضعف جهود مكافحة اختراق البيانات، والقرصنة المالية، وغيرها من الجرائم التي تُهدد الأمن العالمي [1]

معضلة الأمن السيبراني العالمي :

تُشكِّل معضلة الأمن السيبراني العالمي تحديًّا وجوديًّا للدول، خاصة الكبرى منها، التي تبقى عاجزةً عن سد الثغرات الأمنية رغم امتلاكها إمكانيات تقنية وبشرية هائلة. وتكمن المفارقة في أن السبب الرئيسي لهذه الأزمة ليس ضعف الأنظمة التقنية، بل **الإهمال البشري** في تطبيق معايير الحماية الأساسية، وفقًا لتقرير الاتحاد الدولي للاتصالات (ITU) 2017الذي أكد وجود خللٍ منهجي في أنظمة حماية المعلومات حتى في الدول المتقدمة، رغم اعتبارها الأمن السيبراني أولوية دفاعية[2].

أبرز الثغرات التي تُعقِّد المواجهة:

ثغرات الأنظمة الحساسة:

تتعرض المواقع الرسمية والحكومية لاختراقات متكررة بسبب تأخر الكشف عن نقاط الضعف في أنظمة التشغيل، كما حدث في اختراق وكالة الأمن القومي الأمريكي (NSA)عام 2016، حيث فشلت الإجراءات الوقائية في حماية البيانات السرية ذات العواقب الاستراتيجية.

تعتمد الحلول غالبًا على ترقيع البرمجيات بدلًا من معالجة جذرية للثغرات، مما يُسهِّل على القراصنة تطوير هجمات أكثر تعقيدًا.

غياب الإجماع الدولي:

عدم التوافق على تعريف موحَّد للجرائم السيبرانية يعيق تطبيق العدالة، خاصة مع تورط جهات إرهابية تستغل المعاملات المالية الإلكترونية لتمويل عملياتها، مثل جماعات تستخدم العملات الرقمية لغسيل الأموال.

يؤدي ضعف التشريعات العابرة للحدود إلى تحوُّل الفضاء الإلكتروني إلى ساحة للابتزاز والضغط السياسي، كما في هجمات تعطيل البنى التحتية الحيوية (كالمحطات النووية) .

[1] - إدريس عطية المرجع السابق ص 06 ، ص 54 .
[2] - عبد الله بن عبد العزيز بن فهد العجلان، "الارهاب الإلكتروني في عصر المعلومات"، المؤتمر الدولي الاول حول حماية المعلومات الخصوصية في قانون الانترنت، القاهرة (مصر) 2 - 4 جوان 2008.

عجز القدرات البشرية:

تفوق التهديدات الإلكترونية سرعةَ تطوير الحلول الوقائية، خاصة في مجالات حماية البنى التحتية الحيوية (الطاقة، المياه، الاتصالات).

تحوَّل الفضاء السيبراني إلى ساحة صراعٍ غير مباشر بين الدول، حيث تُستخدم الهجمات الإلكترونية كأداة للضغط الجيوسياسي، كتخريب منشآت نفطية لدول مُستهدَفة.

تزايد الضحايا البشرية:

رصدت الإحصائيات الأمريكية 4000 هجوم يوميًا بواسطة برمجيات خبيثة منذ 2016، لكن المستقبل قد يشهد ارتفاعًا في الضحايا البشرية نتيجة اختراق أنظمة طبية أو نقل ذكية.

تضارب مصالح الشركات:

تُفضِّل الشركات متعددة الجنسيات استثمار الأموال في تطوير منتجات مربحة بدلًا سد الثغرات الأمنية، مما يخلق بيئة خصبة للقراصنة، كما في حالات تسريب بيانات العملاء بسبب إهمال تحديث أنظمة الحماية.

الفرع الثالث : انعكاسات التهديدات السيبرانية على الأمن القومي للدول

في خِضَمِّ التسارع التكنولوجي الذي يُعيد تعريف مفاهيم الأمن بمستوياته (القومي، الإقليمي، الدولي)، لم تعد النماذج التقليدية للأمن – القائمة على الترسانات العسكرية أو الردع النووي – قادرةً على مواكبة التعقيدات الجديدة. فالتحديات المُتشابكة، من أزمات سيبرانية إلى حروب معلوماتية، فرضت مفهومًا أشمل هو "**الأمننة**"، الذي يدمج التهديدات غير التقليدية ضمن أولويات الاستراتيجيات الوطنية، ويجعل من المعلومات سلاحًا استراتيجيًّا يفوق تأثير الأسلحة النووية في عصر تحكُّم البيانات بمصير الدول.

فالسيطرة على الفضاء الرقمي، وقدرة الاختراق الإلكتروني لشلّ البنى التحتية، وتحويل البيانات إلى أدوات ضغط جيوسياسي، أصبحت معادلةً جديدةً تُعيد تشكيل موازين القوى. وفي هذا السياق، يبدو الاستثمارُ في البرامج النووية مضيعةً للموارد أمام حتمية تحوُّل الدول إلى صناعة المعلومات وتقنياتها فائقة التطور، مثل:

الذكاء الاصطناعي لتعزيز الأمن السيبراني.

الحوسبة الكمومية لحماية الشبكات من الاختراقات.

إنترنت الأشياء لمراقبة البنى التحتية الحيوية.

فالهجمات الإلكترونية على منشآت الطاقة في أوكرانيا (2015)، وتعطيل أنظمة الصحة خلال جائحة كورونا، أثبتت أن تهديدات الفضاء الرقمي ليست افتراضية، بل قادرة على إحداث دمارٍ مكافئٍ لحروبٍ عسكرية. لذلك، فإن تطوير تقنيات المعلومات ليس خيارًا، بل ضرورةٌ لضمان البقاء في عالمٍ تُحدِّد فيه السيادةُ الرقميةُ مكانةَ الدول [1]

وفي خضم هذا التطور والتوجه الحتمي الذي يجب على الدول أن تلجأ نحو عالم المعلوماتية والتكنولوجيات الحديثة، برز تحدٍ خطير وهو كيفية التعامل أو الاستغلال الأمثل لهذه الأخيرة، بحيث تزامن التوسع والتراكم الهائل للمعلومات وتداخل شبكات الاتصال فيما بينها، تزامن مع توالي التهديدات الإلكترونية في المجال السيبراني، وبذلك أصبحت مسألة الأمن القومي للدول تحت الاختبار الدائم والتحدي المحتوم الذي تفرضه معادلة ضرورة حماية الأمن القومي للدولة بالتزامن مع مواكبة الانفتاح وركوب كافة سلالم التكنولوجيا وتحولاتها ومواجهة كافة التهديدات التي قد تحملها.
ولكن قبل الخوض في تفاصيل هذه التهديدات وطبيعتها، يجب معرفة أو التعرف على الهجمات السيبرانية، فهناك من يعرفها على أنها "فعل يُنفذ باستخدام قدرات وظائف شبكة الكمبيوتر لفرض أهداف قومية أو سياسية من خلال استغلال نقطة ضعف تمكن المهاجم من التلاعب بالنظام[2]."

وعلى ذلك، فإن الإرهاب الإلكتروني يعرض الدولة بأركانها ومؤسساتها الإلكترونية الرقمية للخطر، لأن أفعاله الناجمة عن جرائمه تتجاوز نطاقها المحلي إلى الوطني بأسره، بل إلى الدول الأخرى. أي أن ناتج جرائمه لا يظل محصوراً في نطاق ضيق، بل ينتقل إلى حدود أبعد بكثير من النطاق الواقعي المحلي والوطني، ويصل إلى النطاق الافتراضي عبر شبكاته على مستوى العالم[3].

أدَّت الثورة المعلوماتية إلى تحوُّلات جذرية في طبيعة التهديدات الأمنية، حيث لم تعد الدول قادرةً على الاعتماد على الإجراءات التقليدية كإغلاق الحدود أو التشويش على اتصالات الجيران لضمان أمنها. ففي الماضي، كانت التهديدات تنحصر في النزاعات الحدودية أو التنافس على الموارد أو التحالفات العسكرية، أما اليوم فقد تجاوزت هذه التهديداتُ الحواجزَ الجغرافية بفضل التطور التكنولوجي، فأصبحت الهجمات السيبرانية قادرةً على اختراق الأنظمة الإدارية والعسكرية للدول من أي مكان في العالم، باستخدام أدوات بسيطة تُحوِّل الفضاء الرقمي إلى ساحة حرب مفتوحة يشارك فيها الجميع :أفرادًا، وجماعات، وحتى دولًا[4].

---

[1] - إسماعيل صبري مقلد، ثورة المعلومات وحروب المستقبل المحتمل ، **مجلة آفاق المستقبل**، العدد 5 جويلية/أوت/سبتمبر 012 ، ص 13

[2] - رغدة البهي، مرجع سبق ذكر ، ص 09 .

[3] - مصطفى محمد موسى، **الإرهاب الالكتروني دراسة قانونية، أمنية، نفسية، اجتماعي**، مصر: دار الكتب و الوثائق القومية المصرية، العدد 009 ، ص 03

[4] - ذياب البد نية، **الأمن وحروب المعلومات**،: دار الشروق للنشر والتوزيع 302 ،ص 24 .

فئات التهديدات السيبرانية بناءً على أهدافها[1]:

تهديدات تُستهدَف بها الدول:

اختراق الأمن القومي :كالتجسس على المنشآت العسكرية أو النووية.

تدمير البنى التحتية الحيوية :مثل شبكات الطاقة، والنقل (الجوي، البري، البحري)، والأنظمة الصحية.

زعزعة الاستقرار الاقتصادي :عبر مهاجمة القطاعات المصرفية أو أسواق المال.

تهديد السلم الاجتماعي :كالتلاعب بمنصات التواصل لتفكيك النسيج المجتمعي.

تهديدات تُستهدَف بها الأفراد:

انتهاك الخصوصية :سرقة البيانات الشخصية أو تسريبها للابتزاز.

الجرائم المالية :كالاحتيال الإلكتروني أو اختراق الحسابات البنكية.

استغلال الفئات الضعيفة :كالتنمر الإلكتروني أو توزيع محتوى غير قانوني يستهدف الأطفال.

تعدي على الملكية الفكرية :سرقة براءات الاختراع أو القرصنة البرمجية.

إشكالية الحدود في الجرائم السيبرانية:

لم يعد مفهومُ الحدود التقليدي قائمًا في عصر المعلومات، فالجاني قد ينفذ هجومه من قارةٍ مختلفة عن موقع الضحية، كما في حالات اختراق الشبكات المالية الآسيوية من قراصنة في أوروبا، أو سرقة البيانات الحساسة لدولة أفريقية عبر خوادم في أمريكا. هذا التفكك الجغرافي يُصعِّب تطبيق القوانين المحلية أو الدولية، خاصةً مع صعوبة تحديد هوية الجناة الذين يعملون غالبًا تحت أسماء مستعارة، وبأدوات تكنولوجية متطورة تُمكِّنهم من التهرُّب من الملاحقة [2]

ويختلف حجم الاختراق أو الضرر الذي يمكن أن تتعرض له أي دولةٍ في العالم بسبب الهجمات السيبرانية، وذلك حسب قوَّتها ومدى تقدمها. فإذا كانت المعطيات الحالية تشير إلى أن كل دول العالم أضحت معرَّضةً للاختراق وللهجمات الإلكترونية المتعددة، إلا أن الدول المتقدمة تعد الأقل عرضةً؛ بسبب النظم الحمائية المعتمدة في هذا الشأن، والبنية التحتية للاتصالات التي تمتاز عن غيرها بالحس العالي

[1] - منى الأشقر جبور، مرجع سبق ذكر ، ص 04.

[2] - حجازي عبد الفتاح بيوم، **جرائم الكمبيوتر والانترنت والتشريعات العربية (دراسة مقارنة مع تطبيق على نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية)** ، القاهر : دار النهضة العربية: 009 ، ص 13 .

والوعي المجتمعي، وبالتالي فهي معرَّضة للهجمات الخارجية أكثر من الداخلية، مثلما يحصل من حينٍ لآخر في القضايا التي حدثت في الانتخابات الرئاسية الأمريكية سنة 2016، والتي اتُّهمت فيها دولة روسيا الاتحادية بالتدخل في الشأن الداخلي للولايات المتحدة الأمريكية وغير ذلك.

أما فيما يخص الدول المتخلفة، فالأمر هنا يعد غايةً في الصعوبة؛ بسبب أن هذه الهجمات السيبرانية تتوالى وتتكرر دائمًا وبشكل متسارع، سواء كان مصدرها داخليًّا أو خارجيًّا، وذلك بسبب هشاشة البنية التحتية، وأنظمة الاتصالات الضعيفة، وبالتالي تأخُّر رهيب في أنظمة الحماية، وكذا التوترات الاجتماعية المتكررة، وهو ما يفتح الباب أمام أطراف غير خاضعة للقوانين، وبالتالي التلاعب وتهديد الدولة في عمقها الاستراتيجي، ألا وهو أمنها القومي.

بالرجوع قليلًا إلى الوراء، وإلى سنوات بداية الألفية الجديدة، ومع التطور والانتشار الرهيب للنظم التكنولوجية وشبكة الإنترنت، باتت مسألة الأمن بصفة عامة على المحك، ليس فقط الأمن القومي للدول فحسب، بل مسألة الأمن الإقليمي، ووصولًا إلى الأمن الجماعي للبشرية والمنظومة الدولية. فالهجمات السيبرانية أضحت مصدر قلق ليس فقط للوضع الداخلي للأنظمة الحاكمة، وإنما قد تكون المسألة تمس الأمن الجماعي لتكتل أو هيئة قارية ككل، كالاتحاد الأوروبي مثلاً، والذي أُختُبِر لأكثر من مرة في هذا الشأن، ووُجهت أصابع الاتهام وقتها للولايات المتحدة الأمريكية بالتصنت على المكالمات لبعض قادة الاتحاد الأوروبي. وكذلك الشأن بالنسبة للاتحاد الإفريقي، الذي وضع أمن القارة وشعوبها على المحك لأكثر من مناسبة. وبالتالي، ومن خلال هذين المثالين البسيطين، يتجلى لنا خطورة التهديدات التي تعرضت لها المنظومة الدولية ككل، سواء كان المتهمون دولًا أو مؤسسات أو كيانات تابعة لدول ما وتحارب بالوكالة، أو أفرادًا هواة، وهو ما دفع بهذه الهيئات إلى التجمع في شكل تحالفات أو تكتلات خاصة في مجال المواجهة.

تأخذ الأحلاف السيبرانية عدة أشكال منها: شكل الأحلاف التقليدية، وكمثال على ذلك، يُعد تحالف الناتو السيبراني أحد أهم هذه الأمثلة، والذي يتجه نحو معالجة مجموعة واسعة من التهديدات، وتعزيز السياسة السيبرانية التي جاءت بموجب اتفاق إستونيا سنة 2007. وركز الحلف بشكل أساسي على تنفيذ تدابير الحماية الضرورية للجانب العسكري، حيث دفعت هجمات الفضاء الإلكتروني التي وقعت في إستونيا عام 2007 الحلف لإعادة التفكير في حاجته لسياسة دفاع إلكتروني، ومن ثم وضع الحلف للمرة الأولى في تاريخه سياسة رسمية للدفاع الإلكتروني، ثم تم توسيعها في يناير 2008، ترتكز على ثلاث دعائم أساسية:

1. **التضامن** :بمعنى تقديم المساعدة عند الطلب مع احترام مبدأ سيادة الدولة.

2. **عدم التكرار** :بمعنى تفادي الازدواجية غير الضرورية في الهياكل والقدرات على المستوى الدولي والإقليمي والوطني.

3. **التأمين** :من خلال التعاون القائم على الثقة، مع الأخذ في الاعتبار حساسية المعلومات ذات الصلة التي لا بد أن تكون متاحةً، وأماكن الانكشاف الممكنة التي يمكن أن تُعرَّض للاختلاف بصورة أسهل [1]

وفي سياق متصل، رفع الخبير الاستراتيجي الأمريكي، اللواء فلاديمير بيلوس، "سقف القناعة"، بقوله: "أن تبدأ المعركة في المستقبل بالتحول أكثر فأكثر باتجاه الفضاء الافتراضي، مع تنامي قدرة الدول المهاجمة على تطوير وإدارة سيناريو حرب المعلومات ضد دول أخرى، في محاولة لتدميرها من الداخل دون الحاجة لخوض حرب دامية أو مكلفة على المستوى الاستراتيجي؛ أي أنه بالإمكان إجبار العدو على الاستسلام دون استخدام الأسلحة التقليدية[2] ".

ومن المتوقع، مثلاً، نشوب حرب إلكترونية بين الصين والولايات المتحدة الأمريكية بعد تقرير (CIA) ، لأن الصين أصبح بمقدرتها تشويش الأنظمة والأجهزة وإلحاق الضرر بها وإدخال الفيروسات والبرامج الخبيثة .

وحرب الفضاء الإلكتروني لا تتضمن أي إراقة للدماء، ولكنها أخطر من الحروب العسكرية، لأنها تستطيع تدمير الأنظمة والأجهزة، مما يمنعها من العمل بشكل كامل ويتسبب في إتلافها.[3]

المطلب الثاني : الفضاء السيبراني

شهد العالم خلال العقود الأخيرة تحولاً جذريًا بفعل الثورة الرقمية، حيث ظهرت بيئة جديدة غير مادية تُعرف بـ"الفضاء السيبراني"، وهو الفضاء الذي تنشأ فيه وتتفاعل المعلومات عبر شبكات الحاسوب والإنترنت. ويُعد الفضاء السيبراني مجالًا افتراضيًا واسعًا يشمل كل ما يتعلق بالاتصال الرقمي، من المواقع الإلكترونية والبريد الإلكتروني إلى شبكات التواصل الاجتماعي والتطبيقات الذكية.

رغم أن الفضاء السيبراني ليس ملموسًا بطبيعته، إلا أن تأثيره يمتد إلى الواقع، حيث بات يشكل بعدًا جديدًا للعلاقات الاقتصادية، الاجتماعية، والسياسية، ويطرح تحديات قانونية وأمنية تتطلب فهمًا دقيقًا

[1] - محمد بوكبشة ، الأمن والدفاع السيبراني أولوية قصوى ، **مجلة الجيش** ، العدد 51 أكتوبر 2017 ص 34 .
[2] - سامر مؤيد عبد اللطيف، الحرب في الفضاء الرقمي رؤية مستقبلي، مجلة رسالة الحقوق، السنة السابعة العدد 2 2015 ، ص 2 .
[3] - المرجع السابق ص 04 .

لطبيعته. وفي هذا المطلب، سيتم التطرق إلى مفهوم الفضاء السيبراني، خصائصه، وأبعاده المختلفة التي جعلت منه عنصرًا أساسيًا في النقاشات المعاصرة حول الأمن والسيادة والخصوصية.

الفرع الأول : تعريف الفضاء السيبراني

أصبح العِلمُ الذي كان في الماضي حِكرًا على قلَّةٍ من العلماء، يعيش اليوم في عالَمٍ افتراضيٍّ، حتى غَزا أدراجَ المكاتب الضخمة والمراكز البحثية المهمة، وصار الأفرادُ يَحصلون عليه بشكلٍ افتراضيٍّ. كما فرضَ علينا نمطًا مُحددًا في تعاملاتنا، مما جعل هذا الإنجازَ الفريدَ محطَّ اهتمام الجميع (أفرادًا، مؤسساتٍ، أنظمةً... إلخ) في أيِّ مكانٍ من العالم، بحثًا عن تلك المعلومة بأيِّ ثمنٍ.

وفي ظلِّ طغيان المعلومات وتطوُّرها في مجالاتٍ متعددة، أصبح من الضروريِّ البحثُ عن الإطار المناسب لضمان سلامتها؛ حتى تؤدِّيَ غرضها، وتُؤمِّنَ حمايةَ البعض من نزوات البعض الآخر. ومن هنا، برزتْ أنظمةُ المعلومات لتقوم بهذه المهمة، عبر طرح مجموعةٍ من الوسائل التي تسمح لمجموعاتٍ من الأفراد (طبيعيين أو اعتباريين) بالتواصل بشكلٍ مُستمرٍّ أو مؤقَّتٍ؛ لتبادل المعلومات (صورٍ، أصواتٍ، تقاريرَ... إلخ)، ليس فقط عبر الأجهزة الفردية (كالحواسيب الشخصية)، بل امتدَّتْ إلى مجالاتٍ عدَّة، مثل: الهواتف النقَّالة، ومواقع الإنترنت، ومؤسسات الهيئات الرسمية (كوزارة الدفاع الوطني والوزارات السيادية ... إلخ)، على أن يكون القاسمُ المشترك بين الجميع هو احترامُ قواعد المعاملات[1] .

تعريف الفضاء السيبراني:

تتفق جميع الدراسات العلمية على أن هذا الفضاء هو بيئة افتراضية تعتمد في بنيتها على التكنولوجيا الحديثة، لتسهيل التعامل والتواصل بين مختلف الفواعل (سواء أكانوا أشخاصًا أم هيئات حكومية أو غير حكومية) عبر شبكات إلكترونية (كالحاسوب) ذات استقلالية عن وسائل الاتصال التقليدية. وبمعنى آخر، فإن كل المعلومات والمعاملات المتداولة فيه، بقدر ما تُسهِّل عملية الاندماج بين أجهزة الاتصالات والأقمار الصناعية والفضاء الإلكتروني، بقدر ما تفتح الباب أمام عمليات الاختراق[2].

ومن بين العلماء الذي يُعتبرهم الباحثونَ بمثابة الأب الروحي والمؤسس لهذا الفضاء، عالمُ الرياضيات الأمريكي الأستاذ **نوربرت وينر(Norbert Wiener)** ، الذي استطاع وضع تعريف دقيق لهذا الفضاء قائمًا على ما أسماه "**علم التحكُّم والاتصال في الحيوان والآلة**"، بهدف نقل الرسائل بين الإنسان والآلة أو

[1] - أيريك ليوبولد-سيرج لوست، ترجمة فتحي علي زمال، "أمن المعلومات"، **المملكة العربية السعودية، مدينة الملك عبد العزيز للعلوم والتقنية**، 2014، ص 10

[2] - **عادل عبد الصادق، "الفضاء الالكتروني والرأي العام : تغير المجتمع والادوات والتأثير"**، المركز العربي لأبحاث الفضاء الالكتروني: قضايا استراتيجية العدد 2459 ، 2013

بين الآلة والآلة. ويُعَدُّ هذا العلم (السيبرنيتيكا) أساسًا لفكرة التحكُّم في الآليات والأنظمة، سواء أكانت بيولوجية أم إلكترونية. [1]

بعد الحرب العالمية الثانية، أحدث التطور التكنولوجي، خاصة مع ظهور الإنترنت، مجموعة من المفاهيم التي أصبحت تعبّر عن هذا الفضاء، مثل الفضاء الرقمي، الدفاع الإلكتروني، الهجوم الإلكتروني، والجريمة الإلكترونية، حيث حلّ الكمبيوتر محلّ الآلة التي تحدث عنها نوربير وينر.

وقد عبّر عن هذه الوضعية بدقة كل من الأستاذ **ألان فريدمان**، الباحث في معهد الأمن السيبراني (الولايات المتحدة الأمريكية)، و**بيتر سيبنجر**، المتخصص في السياسة الخارجية في مركز بروكينغز، حيث قالا إن هذا الفضاء الجديد، بقدر ما يوفر من المرونة والسهولة في التواصل بين المجتمعات في جميع أنحاء العالم وفي مختلف المجالات، فإنه في المقابل يخلق تحديات أمنية معقدة لمواجهة الخروقات .

الفرع الثاني: أقسام الأخطار والتهديدات في الفضاء السيبراني

تنقسم التهديدات السيبرانية إلى ثلاث فئات رئيسية، بناءً على تصنيفات **وكالة الاتحاد الأوروبي لأمن الشبكات والمعلومات:(ENISA)**

التهديدات الإجرامية:(Cybercrime)

تشمل جرائم مثل الاختراق، وسرقة البيانات، وبرامج الفدية. وفقًا لتقرير **فيريزون:(2021)**

57%"من الهجمات السيبرانية في 2020 استهدفت سرقة بيانات شخصية أو مالية [2]

التهديدات الاستخباراتية:(Cyber Espionage)

تهدف إلى سرقة أسرار دولة أو شركات. تُشير دراسة لـ **كلارك وناك (2010)** إلى أن:

"الصين وروسيا تستخدمان مجموعات قرصنة مُنظمة لاستهداف البنى التحتية الحيوية للدول الغربية [3]

التهديدات العسكرية:(Cyberwarfare)

[1] - Dans son livre *« Cybernetics or Control and Communication in the Animal and the Machine »*, publié en 1947, il a proposé ce concept pour promouvoir une vision unifiée des domaines naissants de l'automatique, de l'électronique et de la théorie mathématique de l'information. (*National Cyber Security Strategy 2016-2021 UK, page 16.*)

[2] - Verizon, *2021 Data Breach Investigations Report* (New York: Verizon Communications, 2021), p 23.

[3] - Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security* (New York: HarperCollins, 2010), p 112.

تتضمن هجمات تعطيل أنظمة الطاقة أو الاتصالات. في 2010، شهد العالم هجوم **ستاكسنت (Stuxnet)**الذي دمَّر أجهزة طرد مركزي إيرانية، وهو ما صنَّفته **الأمم المتحدة** كأول حرب سيبرانية[1]

الفرع الثالث: الأبعاد الأمنية للتهديدات والمخاطر

لضمان أمن الفضاء السيبراني، يجب معالجة الأبعاد التالية:

البُعد التقني:

تطوير أنظمة تشفير متقدمة مثل **بروتوكول TLS 1.3** لحماية البيانات.

وفقًا لـ **المعهد الوطني للمعايير والتكنولوجيا(NIST)** ، فإن: "التحديثات الأمنية الدورية تُقلل من ثغرات الأنظمة بنسبة 40 % [2]

البُعد القانوني:

تفعيل قوانين مثل **القانون العام لحماية البيانات (GDPR)** في الاتحاد الأوروبي، الذي يُلزم الشركات بحماية بيانات المستخدمين.

يُشير **تقرير اليونسكو (2019)** إلى أن: 65%"من الدول لديها تشريعات جزئية لمكافحة الجرائم السيبرانية [3]

البُعد الاستراتيجي:

تبني استراتيجيات وطنية لأمن المعلومات، كالاستراتيجية الأمريكية **(Cybersecurity Strategy 2023)**التي تركز على": تعاون القطاعين العام والخاص لمواجهة الهجمات المُنظمة."

البُعد الاجتماعي :

زيادة الوعي بمخاطر التصيد الاحتيالي(Phishing) ، حيث تُظهر إحصاءات **شركة سيمانتك (2022):** 30%"من المستخدمين يقعون ضحية رسائل التصيد بسبب نقص الوعي[4]

[1] - United Nations Office for Disarmament Affairs, *Report on Developments in the Field of Information and Telecommunications* (New York: UNODA, 2013), p 17.

[2]- National Institute of Standards and Technology, *NIST Cybersecurity Framework* (Gaithersburg: NIST, 2020), p 34.

[3] - UNESCO, *Global Survey on Cyber Legislation* (Paris: UNESCO Publishing, 2019), p 89.

[4] - Symantec, *Internet Security Threat Report 2022* (Mountain View: Symantec Corp, 2022), p 41.

المبحث الثاني: الجريمة السيبرانية

تُمثل الجرائم السيبرانية تهديدًا متناميًا في العصر الرقمي، حيث تُستغل التكنولوجيا لتنفيذ أفعال غير مشروعة تُهدد الأفراد والمؤسسات والدول .وتنقسم هذه الجرائم إلى ثلاثة فروع رئيسية:

المطلب الأول : الجرائم الإلكترونية

تُعرف الجرائم الإلكترونية بأنها أفعال ضارة تُرتكب باستخدام الحواسيب أو الشبكات الرقمية، سواء كانت تستهدف البيانات أو الأنظمة أو الأفراد. وتشمل أنواعًا متعددة، منها:

الاختراقات :(Hacking) الوصول غير المصرح به إلى الأنظمة لسرقة البيانات أو تعطيلها. على سبيل المثال، اختراق حسابات البنوك الإلكترونية لسرقة الأموال.

البرمجيات الخبيثة :(Malware) مثل الفيروسات وبرامج الفدية (Ransomware) التي تشفر الملفات وتطلب فدية لفك تشفيرها. فيروس (2017) "Wanna Cry" الذي أصاب أكثر من 200,000 جهاز في 150دولة يُعد مثالًا بارزًا.1

هجمات الحرمان من الخدمة :(DDoS) تُعطل الخدمات الإلكترونية بإغراق الخوادم بطلبات وهمية. في 2016، تعرضت مواقع مثل "تويتر" و"نيتفليكس" لهجمات أوقفت خدماتها لساعات.

تشكل هذه الجرائم تحديًا للقوانين التقليدية، إذ يصعب تتبع الجناة بسبب إخفاء الهوية في الفضاء السيبراني. وتُقدَّر الخسائر العالمية الناجمة عنها بنحو 6 تريليونات دولار سنويًّا بحلول 2025 .

المطلب الثاني: الإرهاب الإلكتروني

يُشير الإرهاب الإلكتروني إلى استخدام التقنيات الرقمية لتنفيذ أعمال إرهابية تهدف إلى بث الرعب أو الإضرار بالبنية التحتية الحيوية. وتتمثل أساليبه في:

التجنيد والدعاية :تستغل الجماعات الإرهابية منصات مثل "تيليغرام" أو "دارك ويب" لنشر الأفكار المتطرفة. على سبيل المثال، استخدم تنظيم "داعش" مواقع إلكترونية لعرض مقاطع فيديو تروّج للعنف.

[1] - Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (New York: Doubleday, 2019),p 45.

[2] - Cybersecurity Ventures, "Cybercrime Damages $6 Trillion by 2025," *Cybersecurity Ventures*, 2020, accessed June 15, 2023, https://cybersecurityventures.com/.

الهجمات على البنية التحتية :مثل تعطيل شبكات الطاقة أو أنظمة النقل. في 2015، اخترق قراصنة شبكة كهرباء أوكرانيا، مما تسبب في انقطاع التيار عن 230,000 شخص.1

التسريب الإلكتروني :نشر معلومات سرية لزعزعة الاستقرار. تسريبات "ويكيليكس" (2010) كشفت وثائق دبلوماسية حساسة أثرت على العلاقات الدولية.

تُظهر هذه الهجمات تحول الإرهاب إلى الفضاء الرقمي، مما يتطلب تعاونًا دوليًا لمواجهته عبر تشريعات صارمة وتقنيات متقدمة.

المطلب الثالث: الحروب السيبرانية

الحروب السيبرانية هي صراعات بين دول أو كيانات كبرى باستخدام الهجمات الإلكترونية لتدمير البنى التحتية أو التجسس. وتتميز بغياب الحدود الجغرافية وصعوبة إثبات المسؤولية. من أبرز أمثلتها:

هجمات التجسس :مثل اختراق وكالة الأمن القومي الأمريكية (NSA) من قبل "إدوارد سنودن" (2013)، الذي كشف برامج مراقبة جماعية.2

الهجمات التخريبية :فيروس(2010) "Stuxnet" ، الذي دمر أجهزة تخصيب اليورانيوم في إيران، ويُعتقد أن إسرائيل والولايات المتحدة شاركتا في تطويره.

الحرب الإعلامية :كالتدخل الروسي المزعوم في الانتخابات الأمريكية (2016) عبر اختراق البريد الإلكتروني للحزب الديمقراطي.

تُهدد الحروب السيبرانية الأمن العالمي، إذ قد تؤدي إلى أزمات اقتصادية أو انهيار أنظمة اتصالات حيوية. وتدعو الحاجة إلى اتفاقيات دولية تُجرم هذه الهجمات، مثل مبادئ بودابست (2001)لمكافحة الجريمة السيبرانية. 3

[1] - Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown, 2014), 204.

[2] - Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (New York: Metropolitan Books, 2014), 89.

[3] - Council of Europe, *Convention on Cybercrime* (Budapest: Council of Europe, 2001), Article 2.

خلاصة الفصل:

في خلاصة مبحثنا الأول تناولنا مفهوم الأمن السيبراني من منظوره الشامل؛ حيث عرفناه بأنه منظومة متكاملة من الإجراءات والتقنيات والضوابط الهادفة إلى حماية أنظمة المعلومات والشبكات والبيانات من الهجمات الإلكترونية والاختراقات. كما استعرضنا أبعاده المتعددة، سواء التقنية أو السياسية أو الاقتصادية أو الاجتماعية أو القانونية، مع الإشارة إلى أهمية توفير بيئة رقمية آمنة في ظل تسارع التحول الرقمي وانتشار الفضاء السيبراني.

أما في المبحث الثاني فتطرقنا إلى الجريمة السيبرانية، وهي الأنشطة الإجرامية التي تُرتكب باستخدام تقنيات الحواسيب والإنترنت، واستعرضنا أنواعها المختلفة مثل الاختراق، والتصيد الاحتيالي، والبرمجيات الخبيثة (مثل فيروسات الفدية)، والهجمات الموزعة لتعطيل الخدمة، والتجسس الإلكتروني والإرهاب السيبراني. كما ناقشنا التحديات التي تفرضها هذه الجرائم على الأمن القومي والاستراتيجيات المتبعة لمكافحتها، مشددين على ضرورة تبني منهجيات متكاملة تجمع بين الجوانب التقنية والقانونية والاستراتيجية والاجتماعية للتصدي لهذه الظاهرة المتطورة.

بهذا نكون قد غطينا معًا الأسس النظرية والتطبيقية للأمن السيبراني والجرائم السيبرانية، مما يؤكد الحاجة إلى وعي متزايد وتحديث دائم للإجراءات الدفاعية لمواجهة التحديات التي يفرضها العالم الرقمي اليوم.

الفصل الثـــاني:

الأمن السيبراني في الجزائر

بعدما تم التطرق إلى مجموعة من النقاط المفاهيمية في موضوع الأمن السيبراني في الفصل الأول من الدراسة، وكذلك تناول مجموعة من النقاط ذات الصلة به، والتحدث عن إحدى أهم الهيئات والمؤسسات الدولية التابعة للأمم المتحدة التي تهتم بمجال تكنولوجيا المعلومات والتطورات الحاصلة في هذا الشأن عموماً، والأمن السيبراني وكل ما يحيط به على وجه الخصوص؛ سيتم التحدث في البداية عن الاستراتيجية الجزائرية في مجال الأمن السيبراني بالتحديد السياسة العامة لحماية المعلومات بجوانبها وأهداف الحماية.

وكمبحث ثانٍ في هذا الفصل، كان من الضروري وضع مجموعة من الآليات والضوابط التي يمكن من خلالها تطوير الاستراتيجية الجزائرية في مجال الأمن السيبراني، وذلك ضمن الاجتهادات التي يحاول الباحث القيام بها والخروج في الختام بعدة نقاط لم تكن موجودة سابقاً ضمن خطط برنامج صانع القرار الجزائري.

وفي ختام هذا الفصل، سيتم طرح عدد من التوصيات المستنتجة في هذا الشأن، والتي يمكن لصانع القرار الجزائري الرجوع إليها والاعتماد عليها كنموذج من الاجتهادات الخاصة بالباحث.

الفصل الثاني: الأمن السيبراني في الجزائر

يشهد العالم في العقود الأخيرة تحولات متسارعة في مجال التكنولوجيا والرقمنة ، ما أدى إلى بروز تهديدات جديدة تمس بالأمن الوطني والسيادة الرقمية للدول، وعلى رأسها التهديدات السيبرانية. وفي هذا السياق، لم تكن الجزائر بمنأى عن هذه التحديات، إذ عرفت طفرة رقمية مهمة في قطاعات متعددة، مثل الإدارة الإلكترونية، المعاملات المالية، الاتصالات، والتعليم عن بُعد. إلا أن هذا التحول الرقمي، رغم ما يحمله من فرص، قد أفرز أيضًا مخاطر سيبراني متزايدة تستهدف البنى التحتية الحيوية، البيانات الحساسة، وحتى الأفراد.

إن الأمن السيبراني في الجزائر بات يشكل أحد الرهانات الاستراتيجية للدولة، التي بدأت تدرك أهمية بناء منظومة متكاملة لحماية فضائها الرقمي. وقد ظهرت خلال السنوات الأخيرة عدة مبادرات في هذا الاتجاه، سواء على مستوى التشريع، عبر سن قوانين خاصة بالجريمة الإلكترونية، أو من خلال إنشاء هيئات مختصة بالأمن السيبراني ومراكز استجابة للطوارئ المعلوماتية.

غير أن الطريق نحو تحقيق أمن سيبراني فعّال ومستدام في الجزائر لا يزال يتطلب تضافر الجهود على مستويات متعددة: تطوير البنية التحتية التكنولوجية، تعزيز الكفاءات البشرية، رفع الوعي المجتمعي، وتكثيف التعاون الإقليمي والدولي.

من هذا المنطلق، تكتسي دراسة واقع الأمن السيبراني في الجزائر أهمية بالغة، لفهم التحديات القائمة، وتقييم الاستراتيجيات المتبعة، واستشراف سبل تعزيز القدرة الوطنية على مواجهة التهديدات الرقمية في بيئة متغيرة ومعقدة.

المبحث الأول: "استراتيجيات الحماية المعلوماتية: الأطر العامة والتطبيقات العملية"

في ظل الاعتماد المتزايد على تكنولوجيا المعلومات في مختلف المجالات، أصبحت حماية البيانات والمعلومات أولوية قصوى للحكومات، المؤسسات، وحتى الأفراد. ومع تصاعد التهديدات السيبرانية وتطور أساليب الاختراق والتجسس الإلكتروني، لم يعد من الكافي الاعتماد على وسائل الحماية التقليدية، بل أصبح من الضروري اعتماد استراتيجيات متكاملة وشاملة لضمان أمن المعلومات وسلامتها.

تتطلب حماية المعلومات وضع أطر عامة تستند إلى معايير تقنية، تنظيمية، وقانونية، إضافة إلى تطبيقات عملية تأخذ بعين الاعتبار طبيعة الأنظمة المستخدمة وحجم التهديدات المحتملة. ويهدف هذا المبحث إلى تسليط الضوء على أبرز الاستراتيجيات المعتمدة في مجال الحماية المعلوماتية، من حيث المبادئ التي تقوم عليها، وأهم الآليات والتقنيات المستخدمة، مع تقديم نماذج تطبيقية تساعد في فهم كيفية تفعيل هذه الاستراتيجيات على أرض الواقع.

المطلب الأول: الأطر النظرية لاستراتيجيات الحماية المعلوماتية

تُعد الأطر النظرية حجر الأساس لأي استراتيجية فعّالة في مجال الحماية المعلوماتية، إذ تضع المبادئ العامة والتصورات المفاهيمية التي تُوجّه السياسات والإجراءات العملية لاحقًا. وتشمل هذه الأطر مجموعة من النماذج والنظريات التي تفسر كيفية حماية المعلومات، وتحدد مستويات الأمن المطلوبة، والعوامل المؤثرة في اختيار وسائل الدفاع المناسبة.

تتنوع هذه الأطر بين ما هو تقني يركّز على البنى التحتية الرقمية، وما هو تنظيمي يركّز على سياسات الاستخدام والحوكمة، إضافة إلى الأطر القانونية التي تضبط الحقوق والواجبات المتعلقة بالأمن المعلوماتي. وسيتناول هذا المطلب أبرز الأطر النظرية التي تشكل الخلفية الفكرية لاستراتيجيات الحماية المعلوماتية، مع بيان دورها في بناء أنظمة حماية متكاملة وفعّالة.

الفرع الأول: مفهوم الحماية المعلوماتية وأهميتها

تُعد الحماية المعلوماتية أحد الأعمدة الرئيسية في نظم أمن المعلومات الحديثة، وهي تشمل جميع الإجراءات والتدابير الفنية والتنظيمية التي تهدف إلى الحفاظ على سرية وسلامة وتوافر المعلومات. وتبرز أهمية الحماية المعلوماتية في ظل التحول الرقمي السريع الذي يشهده العالم، حيث أصبحت البيانات المورد

الأكثر قيمة للدول والمؤسسات على حد سواء. فالهجمات السيبرانية لم تعد تقتصر على إحداث خلل في الأنظمة التقنية فحسب، بل باتت تشكل تهديداً مباشراً للأمن القومي والاقتصادي للدول[1].

من هذا المنطلق، أصبحت الحماية المعلوماتية ذات أولوية قصوى لدى الحكومات والمنظمات، خاصة في القطاعات الحيوية مثل الصحة، والمال، والطاقة، حيث يمكن أن يؤدي خرق أمني واحد إلى تداعيات كارثية. ولهذا، فإن فهم الحماية المعلوماتية لا يقتصر على الجانب التقني، بل يمتد ليشمل الجوانب القانونية والتنظيمية وحتى الاجتماعية.[2]

الفرع الثاني: النماذج النظرية لاستراتيجيات الحماية

لقد طُورت عدة نماذج نظرية لتأطير مفهوم الحماية المعلوماتية ووضعها ضمن أطر عملية قابلة للتنفيذ. من أبرز هذه النماذج نموذج CIA Triad، الذي يرتكز على ثلاثة عناصر أساسية: السرية (Confidentiality)، السلامة(Integrity) ، والتوافر .(Availability) ويُعتبر هذا النموذج حجر الزاوية في معظم سياسات الحماية، حيث يسعى إلى ضمان أن تكون المعلومات محفوظة من الوصول غير المصرح به، وأن تظل دقيقة وغير معدلة، ومتاحة عند الحاجة[3].

كما ظهرت نماذج أخرى أكثر تعقيدًا مثل نموذج Parkerian Hexad، الذي يضيف عناصر أخرى مثل الأصالة(Authenticity) ، والامتلاك(Possession) ، والمنفعة(Utility) ، وهو ما يعكس توسع نطاق المخاطر وتعقيد بيئة المعلومات الحديثة[4].

[1] - محمد العابد، *أمن المعلومات: المفاهيم والاستراتيجيات* (بيروت: دار المنهل، 2020)، ص 35.
[2] - خالد الزهراني، "الحماية المعلوماتية بين النظرية والتطبيق"، *مجلة دراسات أمنية*، العدد 14 (2021): 112.
[3] - James F. Ransome and Anmol Misra, *Core Software Security: Security at the Source* (Boca Raton, FL: CRC Press, 2014), 29
[4] - Eric D. Knapp and Joel Thomas Langill, *Industrial Network Security* (Waltham: Syngress, 2015), 76.

المطلب الثاني: التطبيقات العملية لاستراتيجيات الحماية المعلوماتية

بعد وضع الأطر النظرية التي تُوجّه سياسات الحماية المعلوماتية، تأتي مرحلة التنفيذ العملي التي تُترجم تلك المبادئ إلى أدوات وتقنيات وإجراءات ملموسة. وتشمل التطبيقات العملية مختلف الوسائل التقنية والتنظيمية التي تُعتمد لحماية نظم المعلومات من التهديدات السيبرانية، بدءًا من الجدران النارية وبرمجيات مكافحة الفيروسات، مرورًا بأنظمة التشفير وإدارة الوصول، وصولًا إلى خطط الاستجابة للحوادث والنسخ الاحتياطي.

تكتسب هذه التطبيقات أهميتها من كونها تمثل خط الدفاع الفعلي في مواجهة الهجمات الإلكترونية، كما تختلف باختلاف طبيعة المؤسسة وحجم البيانات ونوع التهديدات. لذلك، يُعنى هذا المطلب باستعراض أبرز التطبيقات العملية المعتمدة في مجال الحماية المعلوماتية، مع التركيز على فعاليتها، تحديات تنفيذها، وأمثلة واقعية توضح كيفية توظيفها في البيئات الرقمية الحديثة.

الفرع الأول: الأدوات والتقنيات المستخدمة في الحماية

في العصر الرقمي، لا يمكن تحقيق الحماية المعلوماتية من دون الاستعانة بمجموعة من الأدوات والتقنيات المتطورة. ومن أبرز هذه الأدوات جدران الحماية(Firewalls) ، وأنظمة كشف التسلل(IDS/IPS) ، وبرمجيات مكافحة الفيروسات، وكذلك تشفير البيانات سواء أثناء النقل أو في التخزين. كما أصبحت تقنيات التعلم الآلي والذكاء الاصطناعي تلعب دورًا متزايدًا في الكشف الاستباقي عن التهديدات وتحليل سلوك المستخدمين بحثًا عن أنماط مريبة[1].

إضافة إلى ذلك، تُستخدم تقنيات إدارة الهوية والوصول (IAM) لضمان أن كل مستخدم داخل النظام يتمتع بالصلاحيات المناسبة فقط، مما يقلل من فرص الاستغلال أو الخطأ البشري الذي يُعد أحد أبرز أسباب خروقات البيانات[2].

[1] - Kevin Mitnick, *The Art of Invisibility* (New York: Little, Brown, 2017), 150.
[2] - Susan M. Gates, "Access Control and Identity Management," *Journal of Information Security*, vol. 8, no. 2 (2019): 98–105.

الفرع الثاني: التحديات والاتجاهات المستقبلية

رغم التطور الكبير في أدوات الحماية، فإن التحديات لا تزال قائمة. من أبرز هذه التحديات الهجمات المتقدمة المستمرة(APT) ، والهندسة الاجتماعية، وثغرات سلسلة التوريد، إضافة إلى تعقيد البنى التحتية السحابية والبيئات متعددة النظم. كما أن هناك نقصاً في الكوادر البشرية المؤهلة في مجال الأمن السيبراني، ما يزيد من حدة المخاطر[1].

من جهة أخرى، تتجه استراتيجيات الحماية نحو التحول من الحماية التقليدية إلى الأمن الاستباقي، حيث يُستخدم التحليل التنبئي والتعلم الآلي لتحديد التهديدات قبل وقوعها. كما برزت مفاهيم مثل Zero Trust Securityالتي تفترض انعدام الثقة التلقائية داخل وخارج الشبكة، وتفرض التحقق المستمر من الهوية والصلاحيات[2].

المبحث الثاني : استراتيجيات الجزائرية في مواجهة الجرائم السيبرانية

مع مطلع الألفية وموازاة التطور الهائل في تكنولوجيا المعلومات، أصبح من الضروري أن تتحرك الدول لمكافحة التهديدات السيبرانية وتبني نظام دفاعي سيبراني يُحسِّن أداء مؤسساتها من جهة، ويجعل سياساتها أكثر فعالية وتكاملاً من جهة أخرى. أدت هذه الحاجة إلى خلق برامج متعددة وهياكل متخصصة تُعنى بالدفاع والأمن السيبراني تماشيًا مع التطور التكنولوجي للأجهزة الرقمية الحديثة[3]. إذ إن قدرة الدولة، مهما كان مستوى تطورها المعلوماتي، على مواجهة المخاطر الناتجة عن الحروب المعلوماتية تتجاوز حدود الواقع الممكن؛ وبالتالي، فإن أقصى ما يمكن للدولة فعله هو زيادة قدرتها على الدفاع والردع للحد من التهديد المعلوماتي الذي يمتد عبر عدة محاور ليظل ضمن حدود يُمكن تحملها.

ومن المحتمل أن تزيد صعوبة تلك المهمة إذا وصل الهجوم على نظم المعلومات وقواعدها في دولة الخصم إلى مستوى التهديد الاستراتيجي الأكثر فتكًا، مما يُبرز من أهم تداعيات التطور التكنولوجي بروز

[1] - مركز الدراسات السيبرانية، "التهديدات الأمنية الحديثة في الشرق الأوسط"، تقرير خاص، 2023

[2] - John Kindervag, "No More Chewy Centers: Introducing Zero Trust," Forrester Research Report, 2010

[3]- إلهام غازي، **الدفاع السيبراني** : مجلة الجيش، العدد 163 أكتوبر 2018 ص 6.

المشكلات التي تهدد الأمن القومي الجزائري، وعلى رأسها الجرائم المعلوماتية. تُعد الجرائم المعلوماتية والإلكترونية صنفًا جديدًا من الجرائم وتتخذ أشكالًا متعددة، أبرزها جرائم الاختراق التي تهدف إلى الاستيلاء على اشتراكات وأرقام سرية وإرسال الفيروسات، إلى جانب الجرائم المتعلقة بالمواقع المعادية، خاصةً تلك السياسية التي، وإن كانت تعبر عن تنامي القيم الحضارية الديمقراطية، غالبًا ما تكون مصدرًا للأخبار الفاسدة التي تخلق شرخًا بين النظام السياسي ومواطنيه. كما تشمل هذه الجرائم جرائم القرصنة والنسخ غير المرخص، بالإضافة إلى جرائم التجسس الإلكتروني بفعل التقنيات عالية التقدم، والإرهاب الإلكتروني الذي يتم من خلاله الاستيلاء على المعلومات وتدميرها وتعطيلها في عصر الازدهار الإلكتروني[1].

ومن هذا المنطلق، كانت السياسات والخطط المسطرة لدى صانع القرار في الجزائر تهدف إلى مواكبة التحولات والتطورات العالمية في هذا المجال، خاصةً إذا ما استرجعنا السنوات الأخيرة من القرن العشرين التي عاشت البلاد تحت ضغط التوترات الأمنية التي خلفت دمارًا وخسائر فادحة في الأرواح والعتاد والممتلكات، وشكلت ظاهرة الإرهاب الصورة نالأبرز للتهديد الذي يواجه كيان الدولة الجزائرية وأمنها القومي. ولم يقتصر الأمر على نمط وسلوك معين تجاه فئة أو مؤسسة بعينها، بل امتد ليشمل جميع الجهات الخاضعة لسلطة الدولة الجزائرية.

ومن أهم التحديات التي برزت مع بداية القرن الحادي والعشرين هي التحولات الهائلة في مجال التكنولوجيا والرقمنة عبر كافة المجالات، وهو أمر استدعى وقوف صانع القرار الجزائري عنده، إذ يمثل تحولًا بالغ الصعوبة وغير آمن على الدول التي تفتقر إلى رؤية واضحة لتبني الإيجابيات ومواجهة السلبيات. وإدراكًا للطبيعة الحاسمة والفعالة للدفاع السيبراني، عملت الجزائر منذ سنوات على تبني هذا المفهوم ووضعه في قلب سياساتها وآلياتها، لا سيما في الخطط العسكرية؛ فقد أصبح النظام المعلوماتي والرقمي أمرًا لا يمكن تجاهله داخل المؤسسات والقطاعات المختلفة. ويمتد إطار الدفاع السيبراني إلى أبعد من مجرد حماية الحواسيب؛ ليصل إلى تأثير مباشر على الأمن القومي من خلال حماية النظم الإلكترونية للدولة ومواجهة الهجمات السيبرانية[2]. وهذا يقودنا إلى دراسة الاستراتيجية الجزائرية في هذا المجال والتعرف على أهم الآليات المعتمدة

[1] - سارة بودح، الإستراتيجية الجزائرية في انفاق على التسلح في ظل التهديدات الأمنية الجديدة 2010- 2014 ، **مذكرة لنيل شهادة الماستر أكاديمي تخصص العلوم السياسية والعلاقات الدولية** ، منشور ، جامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية ،السنة الجامعية 2015/2014 .

[2] - الهام غازي، مرجع سبق ذكر ، ص 17.

لدى صانع القرار، مما يتيح استخلاص النتائج الجوهرية مع الأخذ في الاعتبار المقومات والإمكانيات والمكانة التي تحتلها الجزائر كدولة محورية في قارة إفريقيا والعالم العربي والإسلامي.

المطلب الأول: السياسة العامة لحماية المعلومات

في عالم تتسارع فيه وتيرة التحول الرقمي وتزداد فيه التهديدات السيبرانية تعقيدًا، أصبحت الحاجة إلى تبني سياسة عامة فعّالة لحماية المعلومات أمرًا لا غنى عنه لضمان أمن واستقرار البنى التحتية الرقمية. وتشكل السياسة العامة لحماية المعلومات الإطار المرجعي الذي يُحدد التوجهات الكبرى للدولة أو المؤسسة في مجال أمن المعلومات، من حيث المبادئ، الأهداف، والأولويات، كما تُنظم العلاقة بين مختلف الفاعلين المعنيين بالحماية المعلوماتية.

وتقوم هذه السياسة على مزيج من التدابير التشريعية، التنظيمية، والتقنية، وتُراعي التوازن بين حماية البيانات وحرية الاستخدام، بما يضمن الثقة في البيئة الرقمية. ويهدف هذا المطلب إلى تسليط الضوء على مفهوم السياسة العامة لحماية المعلومات، مكوناتها الأساسية، والأدوار التي تلعبها في مواجهة المخاطر السيبرانية المتزايدة.

الفرع الأول : الاستراتيجية المحددة

تُعَدُّ الاستراتيجية المحددة حجر الزاوية في بناء سياسة حماية المعلومات، حيث تُركِّز على تحديد الأهداف الواضحة وآليات التنفيذ. تشمل هذه الاستراتيجية ثلاث ركائز رئيسية:

أهداف الحماية :تشمل ضمان سرية المعلومات (Confidentiality) عبر تشفير البيانات، وسلامتها (Integrity)من خلال تقنيات كالتوقيع الإلكتروني، وتوافرها (Availability) بأنظمة النسخ الاحتياطي.[1]

[1] - أحمد عبد الله، *أمن المعلومات: المفاهيم والتطبيقات* (القاهرة: دار النشر التقنية، 2020)، ص 45.

الأطر المعيارية :كاعتماد معايير دولية مثل ISO/IEC 27001 لإدارة أمن المعلومات، أو إطار عمل NIST SP 800-53الخاص بالضوابط الأمنية.[1]

التطبيقات العملية :مثل استخدام جدران الحماية (Firewalls) لمنع الاختراقات، وأنظمة كشف التسلل (IDS)لمراقبة الشبكات، وخطة الاستجابة للحوادث Incident Response Plan) لتقليل الأضرار.[2]

مثال تطبيقي: تطبيق شركة "أ "لاستراتيجية تعتمد على تشفير البيانات الحساسة باستخدام خوارزمية AES-256، مع تدقيق دوري لالتزام الموظفين بالسياسات.[3]

الفرع الثاني: الجانب الهيكلي

يشير الجانب الهيكلي إلى البنية التحتية التكنولوجية والمادية التي تدعم أمن المعلومات. يتضمن:

البنية الشبكية الآمنة :تصميم شبكات مُجزَّأة (Network Segmentation) لعزل البيانات الحساسة، واستخدام شبكات افتراضية خاصة (VPN) للاتصالات الخارجية.[4]

التقنيات الدفاعية :كأنظمة منع الاختراق (IPS) ونُظُم التحديث التلقائي للبرامج Patch) (Managementلإغلاق الثغرات.[5]

الأمن المادي :حماية مراكز البيانات بالبطاقات الذكية وكاميرات المراقبة، وتطبيق معايير مثل TIA-942 لتصميم مراكز البيانات [6] .

[1] - John Smith, *Cybersecurity Frameworks: **A Global Perspective*** (New York: TechPress, 2019), 78.

[2] - محمد خالد، *الحماية من الهجمات السيبرانية* (الرياض: **مركز الأمن الإلكتروني، 2021**)، ص 112.

[3] - "Case Study: Implementing AES-256 in Enterprise Systems," ***Journal of Information Security* 14**, no. 3 (2022): 34.

[4] - Laura Davis, *Secure Network Architectures* (London: Cyberbooks, 2020), p 89.

[5] - "Best Practices in Patch Management," *International Journal of Cybersecurity* 7, no. 2 (2021): p 56.

[6] - عمر فاروق، *الأمن المادي لتكنولوجيا المعلومات* (دبي: دار المستقبل، 2019)، ص 67.

الفرع الثالث: الجانب التنظيمي

يركز الجانب التنظيمي على السياسات والإجراءات التي تُنظِّم عمل الأفراد والفرق لتحقيق الأمن المعلوماتي. أبرز عناصره:

السياسات الداخلية :مثل سياسة استخدام البريد الإلكتروني، وسياسة الوصول إلى البيانات (Access Control Policy)القائمة على مبدأ "أقل صلاحية.(Least Privilege) " [1]

التوعية والتدريب :إجراء دورات تدريبية سنوية للموظفين حول التصيد الاحتيالي (Phishing) وحماية كلمات المرور.[2]

الإدارة والمساءلة :تعيين مدير لأمن المعلومات(CISO) ، وتطبيق إجراءات التدقيق (Auditing) لمراقبة الالتزام بالسياسات.[3]

المطلب الثاني: أهداف الحماية الأمنية

لا تقتصر الحماية الأمنية للمعلومات على مجرد منع الاختراقات أو التصدي للهجمات السيبرانية، بل تمتد لتشمل مجموعة من الأهداف الاستراتيجية التي تسعى إلى ضمان سلامة البيئة الرقمية واستمراريتها. وتعد هذه الأهداف حجر الأساس في بناء سياسات أمن معلومات فعّالة، إذ توجّه الجهود التقنية والتنظيمية نحو حماية البيانات وضمان خصوصيتها، وتوفير بيئة رقمية موثوقة وآمنة.

وتتنوع أهداف الحماية الأمنية بين ما هو تقني، كالحفاظ على سرية المعلومات وسلامتها وتوافرها)مبادئCIA) ، وما هو إداري واستراتيجي، مثل تعزيز الثقة الرقمية، حماية البنية التحتية الحساسة، وضمان

[1] -Sarah Johnson, *Corporate Cybersecurity Policies* (Berlin: SecurePub, 2021), 102.

[2] -Impact of Cybersecurity Training on Employee Behavior," *Journal of Organizational Security* 5, no. 4 (2022): 45.

[3] - خالد أحمد، *إدارة أمن المعلومات في المؤسسات* (القاهرة: دار التكنولوجيا، 2020)، ص 88.

الامتثال للأنظمة والتشريعات .ويهدف هذا المطلب إلى استعراض هذه الأهداف بمختلف أبعادها، وبيان دورها في تحقيق الأمن السيبراني المستدام.

الفرع الأول: أهداف الحماية الأمنية

تهدف الحماية الأمنية إلى ضمان سلامة المعلومات والأنظمة من خلال مجموعة من الإجراءات التي تعكس مبادئ السرية(Confidentiality) ، والتكاملية (Integrity)، والتوافر(Availability) ، المعروفة اختصارًا بـ .CIAوتتمثل هذه الأهداف في:

السرية:(Confidentiality)

ضمان أن المعلومات لا تُكشف إلا للأشخاص المخوَّلين بالوصول إليها. ويُحقَّق ذلك عبر آليات مثل التشفير، والمصادقة(Authentification) ، والتحكم في النفاذ .(Control d'Accès) على سبيل المثال، تُستخدم كلمات المرور المعقدة وتقنيات التشفير لحماية البيانات الحساسة من الوصول غير المصرح به

التكاملية:(Integrity)

التأكد من دقة المعلومات وعدم تعرضها للتعديل أو التخريب. تُطبَّق تقنيات مثل التوقيعات الرقمية والخوارزميات (كـ SHAأو (MD5للكشف عن أي تغييرات غير مشروعة في البيانات أثناء نقلها أو تخزينها

التوافر:(Availability)

ضمان استمرارية عمل الأنظمة وإتاحة المعلومات للمستخدمين المخوَّلين عند الحاجة. يشمل ذلك حماية البنية التحتية من هجمات حجب الخدمة (DDoS) وتوفير نسخ احتياطية دورية لاستعادة البيانات في حالة الكوارث

الحماية المادية والشخصية:

تشمل تأمين الأجهزة المادية (مثل الخوادم) من الاختراقات، وتدريب الموظفين على الإجراءات الأمنية لتجنب الأخطاء البشرية، مثل تسريب كلمات المرور أو الوقوع في فخ الهندسة الاجتماعية

الامتثال للقوانين والسياسات:

توافق الإجراءات الأمنية مع التشريعات المحلية والدولية، مثل حماية البيانات الشخصية وفقًا للائحة العامة لحماية البيانات (GDPR) أو المعايير المحلية

الفرع الثاني: مستويات الحماية الأمنية

تعتمد مستويات الحماية على تصنيف المعلومات وفقًا لدرجة حساسيتها وأهميتها، وتشمل:

المعلومات عالية السرية:(Top Secret)

تشمل البيانات التي قد تؤدي إلى أضرار جسيمة للأمن الوطني أو المؤسسة إذا تم الكشف عنها. تُطبَّق عليها إجراءات مشددة مثل التشفير المتقدم، والوصول المقيد لفريق مُحدَّد، والتخزين في بيئات معزولة

مثال: الخطط العسكرية أو الأسرار التجارية.

المعلومات السرية:(Secret)

بيانات حساسة لكنها أقل خطورة من الفئة السابقة. تتطلب مصادقة ثنائية (Two-Factor Authentication) وتدقيقًا دوريًا لسجلات الوصول

مثال: التقارير المالية الداخلية

.

المعلومات الحساسة غير المصنفة:(Confidential)

معلومات لا تُصنَّف كسرية لكنها تحتاج إلى حماية من الوصول العشوائي. تُستخدم سياسات التحكم بالصلاحيات (Role-Based Access Control) للحد من انتشارها

مثال: بيانات الموظفين الشخصية.

المعلومات غير المصنفة:(Public)

بيانات متاحة للجميع ولا تحتاج إلى إجراءات أمنية خاصة، لكن يجب ضمان تكاملتها لتجنب التلاعب.
مثال: المنشورات الإعلامية الرسمية .

الفرع الثالث : التدابير التقنية والاجرائية للأمن السيبراني

لقد أدرك المشرع الجزائري جيدًا أن المواجهة الفعالة للإجرام الإلكتروني لا تكون فقط من خلال إرساء قواعد قانونية موضوعية ذات طبيعة ردعية، وإنما يجب أن تصاحب هذه القواعد إجراءات أخرى وقائية وتحفظية، من شأنها تفادي وقوع الجريمة الإلكترونية أو على الأقل الكشف عنها في وقت مبكر يسمح بتدارك مخاطرها. وهو ما استدركه المشرع بتضمين القانون رقم 22-06 [1]- المعدل لقانون الإجراءات الجزائية – تدابير إجرائية مستحدثة تتعلق بالتحقيق في الجرائم الإلكترونية، وتتمثل في مراقبة الاتصالات الإلكترونية وتسجيلها والتسرب.

ويقصد باعتراض المراسلات، اعتراض أو تسجيل أو نسخ المراسلات التي تكون في شكل بيانات قابلة للإنتاج والتوزيع والتخزين والاستقبال والعرض، والتي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية، وذلك في إطار البحث والتحري عن الجريمة وجمع الأدلة حولها.

[1] - القانون رق 06 - 22، المؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر سنة 2006، المتضمن تعديل وتتميم الأمر رقم 155-66 المؤرخ في 18 صفر عم 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، ج ، ر ، ج ، ج عدد رقة 48 ، الصادرة بتاريخ 24 ديسمبر سنة 2006، المعدل والمتمم ، ص 4 .

وقد أشار المشرع الجزائري إلى ظروف وكيفية اللجوء إلى هذا الإجراء في المادة 65 مكرر 5 من قانون الإجراءات الجزائية. وبموجب هذه المادة، يسمح المشرع الجزائري لسلطات التحقيق والاستدلال، إذا استدعت ضرورة التحري في الجريمة المتلبس بها أو التحقيق في الجريمة الإلكترونية، باللجوء إلى إجراء اعتراض المراسلات السلكية واللاسلكية، وتسجيل المحادثات والأصوات، والتقاط الصور، والاستعانة بكل الترتيبات التقنية اللازمة لذلك، بهدف الكشف عن ملابسات الجريمة وإثباتها، دون التقيد بقواعد التفتيش والضبط المألوفة[1].

ومع ذلك، فإن المشرع الجزائري لم يمنح هذا الحق بشكل مطلق، بل أحاطه بمجموعة من الضمانات القانونية التي تحد من تعسف سلطات الاستدلال والتحري، وتصون الحقوق والحريات العامة والحياة الخاصة للأفراد.

المطلب الثالث: مفهوم المخاطر التقنية

رغم ان المعرفة التقنية العالية قدمت للبشرية خدمات جليلة مما جعل حياتنا أكثر رفاهية ومكنت الناس من سد مختلف احتياجاتهم، إلا انها حملت في طياتها اخطارا كامنة تهدد حياة الناس في مختلف المجالات كما قد تمس شرف واعتبار الناس، وحتى أرزاقهم لأنه لا يمكن اكتشافها في حدود المعرفة التقنية السائدة وقت الانتاج او وقت طرح المنتج للتداول، الامر الذي يجعل اي منتج بما فيه البرمجيات والخدمات الكترونية، التجارة الالكترونية، الرقمنة يحمل في طياته مخاطر غير متوقعة.

لدفع هذه المخاطر او بناء المسؤولية القانونية المترتبة على ظهورها يجب الاخذ بعين الاعتبار مسألتان اساسيتان[2] هما اولا ان هذه المخاطر لا تكون معروفة لمن يقوم بتصميم نظم المعلومات او التطبيقات والبرمجيات او لمن يصنعها او يطورها، لان واقع الامر انها مجهولة غير معلومة يقينا بحكم مستوى المعرفة

[1] - أسمهان بوضياف، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مقال منشور في مجله الأستاذ الباحث للدراسات القانونية والسياسية الصادرة عن جامعة محمد بوضياف المسيلة ، الجزائر ، المجلد 03 ، العدد 03 ، منشور بتاريخ 01-09- 2018 ، ص 364 .
2 - درع حماد ، المسؤولية المدنية عن مخاطر التطور التقني ، مجلة كلية الحقوق ، جامعة النهرين ، مجلد9، ع16،العراق ،2006/5/5،ص209.

السائدة وقتها وثانيا فان سلامة المستهلك او المستخدم لها لها اعتبارها لان الهدف الاساسي لأي قانون ينظم هذه المسائل هو حماية الامن والسلم الاجتماعيين.

الفرع الأول: تعريف المخاطر

عامة تتعدد تعريفات المخاطر فنجد من يعرفها تتعدد التعريفات المتعلقة بمفهوم المخاطرة فهناك من يعرفها على أنه[1]: "التعرض لظرف معاكس، أي هي حالة يكون فيها إمكانية أن يحدث انحراف معاكس عن النتيجة المرغوبة المتوقعة أو ألمأمولة كما عرفها آخر[2] على أنها: "الأحداث غير المرئية، وغير المرغوبة في المستقبل وهي التي تجلب حلاوة الحياة ومرارتها".

كما فرق الفقه بين المخاطرة والخطر والمجازفة[3] فإن كانت المخاطرة هي إمكانية حدوث انحراف معاكس للنتيجة المرجوة فإن الخطر هو السبب في الخسارة، أما المجازفة فإنها اختيار سلوك أو إتيان عمل ما مع تجاهل أو عدم التأكد من النتيجة المرجوة التي يغلب عليها أو يتساوى فيها الربح والخسارة، فالمجازفة تحمل عنصر الشك في النتيجة وعدم اليقين من صحة العمل المقدم، والمخاطرة تحمل في معناها الخطر وعنصر المجازفة معا.

الفرع الثاني: ضبط مفهوم المخاطر الناجمة عن المعرفة التقنية العالية

من الصعوبة بمكان بلورة تعريف موحد لمفهوم مخاطر التقنية العالية لأنها اوسع من حصرها في تعريف واحد [4]من جهة، وان التطور المعرفي يخضع لعوامل واعتبارات يصعب تحديدها لأنها تتغير تبعا للمستوى العلمي والتكنولوجي ثم ان مخاطر التقنية العالية تجعلها مرنة، غير قابلة للقولبة غير ان تهديدها لمبدأ ضمان سلامة الانسان[5] باعتباره قيمة عليا يجعلها قابلة للتوحيد ضمن نموذج واحد .

1 - طارق عبد العال حماد، "إدارة المخاطر"، دار الجامعية، الإسكندرية، 2003. ص 16. –كذلك انظر: أسامة عزمي سلام وآخرون، "الخطر والتأمين"، دار الحامد، الأردن/ 2007، ص 22.

2 - خالد وهيب الراوي، "إدارة المخاطر المالية"، دار الميسرة، طبعة 2، الأردن، 2011، ص 7.

3 - منصور بختة، مسؤولية لبنوك في عقود الائتمان ،اطروحة دكتوراه في العلوم السياسية ،تخصص قانون ، منشور ، جامعة ابو بكر بلقايد ،تلمسان كلية الحقوق والعلوم السياسية سنة المناقشة 2014-2015 ، ص 306، 307.

4 - درع حماد ، المرجع السابق ، ص210.

5 - محمد بودالي ، حماية المستهلك في القانون المقارن دار الكتاب الحديث ،2006،الجزائر ،ص403.

تقوم فكرة مخاطر التقنية العالية على فكرة ان المنتج لم يكن به عيب وقت انتاجه او طرحه للتداول ، إلا ان تقدم المعارف التقنية بعد ذلك اظهر وكشف عن وجود مخاطر معينة فيه ، مما يكون لنا صورة من صور الاستحالة المطلقة[1] التي لا يكون بمقدور الناس جميعا كشفها .

يشير مولر MULLER [2] الا ان :"الامر يتعلق بأضرار ناجمة عن خطورة في المنتج لم يكن من الممكن توقعها طبقا للمعرفة العلمية والفنية لحظة صنعها ، فلا الصانع ولا اي شخص اخر يمكنه ان يتكهن بان المنتج ينطوي على مخاطر عند استعماله ...ولا يمكن ان تظهر مخاطره الا بعد انتشاره الواسع في السوق ".

ومنه يجب اطلاق منتج ما للتداول مثلا تطبيق معين او تقنية عالية جديدة فيتخلى المنتج ارادیا عن حيازته له ، ثم تحديد حالة المعرفة العلمية او الفنية لان مخاطر التقنية ملازمة لصناعة لتكنولوجيا التي تحمل في طياتها مخاطر ومجاهيل قد لا تعيها او تدركها ارادة الانسان.

ونقصد بحالة المعرفة السائدة "مستوى الخبرة الفنية والمعرفة العلمية الثابتة في صناعة محددة لحظة وضع تصور فني للمنتج "[3].

الفرع الثالث: البرامج الضارة كأحد أهم صور المخاطر التقنية

تنقسم برامج الكمبيوتر من حيث الاداء الذي تقوم به الى نوعين، برامج تشغيلية، وبرامج تطبيقية، وهما يختلفان اساسا في اداء كل منهما لمهامه، فالبرامج التشغيلية لها وظيفة اجرائية، فهي تسيطر على العمليات الاساسية للأداء الاولي داخل الكمبيوتر فهي مجموعة اوامر تؤدي بها عملها المرسوم لها وفقا للنظام المبنية عليه.

[1] -درع حماد ، المرجع السابق، ص210

[2] -MULLER :l'assurance ,responsabilité civil,R.G.AT1970.

[3] - درع حماد ، المرجع السابق، ص217.

اما البرامج التطبيقية فتقوم بتوجيه اسام الكمبيوتر ضمن النظام الذي وضع لها وفق لأوامر البرامج **التشغيلية** المثبتة بالكمبيوتر [1] .

وهناك نوع ثالث من البرامج تعرف بالبرامج الضارة او الخبيثة ، وهي عبارة عن تعليمات برمجية تتسبب في الحاق الضرر او تعطيل الاستخدام العادي لأجهزة الكمبيوتر او الشبكات او المنصات الرقمية ، وذلك من خلال الاختراق والوصول غير المصرح به .

وتلجأ البرامج الضارة الى خداع المستخدمين الاعتياديين لمنع الاستخدام الطبيعي للجهاز ، و/او الولوج للمنصة او الصفحة ، من خلال اتباع اسلوب واحد او اكثر مثل البريد الالكتروني للتصيد او الثغرة الامنية للنظام او محرك الاقراص USB المحمول الذي اصابته العدوى ، او فتح موقع ضار حيث يفتح هذا البرنامج نافذة خلفية يتسلل من خلالها الفيروس للنظام وهو ما يعرف بهجمة الجذور الخلفية [2] حيث صمم هذا الفيروس ليكون مخفيا وكامنا لأطول مدة ممكنة .

كذلك نجد التصيد الاحتيالي الذي يتم عن طريق رسائل الايميل الاحتيالية المخادعة ، كذلك نجد برامج التجسس وهي تستهدف الحياة الخاصة للأشخاص وبياناتهم الخاصة او المالية ، حيث تقوم بتثبيت نفسها وتغيير اعدادات الجهاز كما تقلل من اداءه .

كما تعد الفيروسات المصممة لتعطيل التشغيل العادي للجهاز عن طريق تعديل بياناته او اتلافها او حذفها او منع وصول مالكها اليها ، وتنتشر عن طريق الملفات الضارة ومن اشهرها برامج الفدية .

وتعد هجمات الاستغلال ومجموعات الاستغلال من اخطر هذه البرمجيات لأنها تستغل الثغرات الامنية لتجاوز اجراءات الحماية الامنية للكمبيوتر من خلال تضمين كود شل shellcode في احد الهجمات مما يمكنهم من تنزيل المزيد من البرامج الضارة ، وأما البرمجيات عديمة الملفات خطيرة جدا لأنها تثبت نفسها في

[1] - احمد ضاعن السمدان ، الحماية القانونية المدنية لبرامج الكمبيوتر ، صورها وتطبيقاتها في القانون المقارن وفي دول الخليج ، ابحاث مؤتمر الكويت الأول للقانون والحاسب الالي ، ط1، 1994، الكويت ،ص41،42 ن كذلك محمد حسام محمود لطفي ، الحماية القانونية لبرامج الحاسب الالي، ابحاث مؤتمر الكويت الول للقانون والحاسب الالي ، ط1، 1994، الكويت،ص21 .

[2] - حسن الفني، تعريف والامن السيبراني،/http://portal.aridmy/ar-ly/account

ذاكرة النواة مما يصعب اكتشافها والتخلص منها ، لان معظم برامج مكافحة الفيروسات لم تصمم لاكتشافها والتعرف عليها وتحييدها .

تعد هجمات ضد سلسلة التوريد[1] من البرامج الضارة لأنها تستهدف المطورين ومقدمي البرامج من خلال النجاح في الوصول الى اكواد المصدر في التطبيقات الموثوقة ، بعد العثور على بروتوكول شبكة غير امن او بنية تحتية للخادم غير محمية او اجراء ترميز أي تشفير غير امن حيث تعدل اكواد المصدر ويتخفى البرنامج الضار في صورة عملية انشاء البرامج وتحديثها .

المبحث الثاني: استراتيجيات الجزائرية في مواجهة الجرائم السيبرانية

مع مطلع الألفية، وبالتوازي مع التطور الهائل في تكنولوجيا المعلومات، كان من الضروري أن تتحرك الدول من أجل مكافحة التهديدات السيبرانية وتبني نظام دفاعي سيبراني يمكنها من تحسين أداء مؤسساتها من جهة، وجعل سياستها أكثر فعالية وتكاملًا من جهة أخرى. هذه الحاجات خلقت برامج متعددة وهياكل متخصصة، تتمثل مهامها في الدفاع والأمن السيبراني، بما يتماشى مع التطور التكنولوجي للأجهزة الرقمية الحديثة. [2]

إن قدرة الدولة، مهما كان مستوى تطورها المعلوماتي، على مواجهة المخاطر التي تسببها الحروب المعلوماتية تَخرُج عن حدود الواقع الممكن. ويترتب على ذلك أن أقصى ما يمكن للدولة أن تفعله هو أن تزيدَ بدرجة ما من قدرتها على الدفاع والردع؛ للحد من التهديد المعلوماتي الذي يشمل مداه العديد من المحاور، كي تُبقي هذا التهديد ضمن حدود يمكن تحمُّلها .وربما يزيد من صعوبة تلك المهمة أن الهجومَ على نظم المعلومات وقواعدها في الدولة الخَصمِ قد يصل في شموله إلى مستوى التهديد الاستراتيجي، وهو الأشد فتكًا[3].

من أبرز نتائج التطور التكنولوجي ظهور مشكلات تهدد الأمن القومي الجزائري، وتتصدرها الجرائم المعلوماتية. إذ تُعتبر الجرائم المعلوماتية والإلكترونية فئة جديدة من الجرائم التي تظهر بأشكال متعددة، من

[1] - microsoft.com/ar/security/business/zerotrust/maturity-model-assissment-cool, البرامج الضارة وكيف تعمل
[2] - إلهام غازي ، الدفاع السيبراني مجلة الجيش العدد 63 أكتوبر 2018 ص 46 .
[3] - إسماعيل صبري ، مرجع السابق الذكر ص 43 .

أبرزها جرائم الاختراق التي تهدف إلى الاستيلاء على اشتراكات وأرقام سرية للآخرين، أو إرسال الفيروسات. كما توجد جرائم مرتبطة بالمواقع المعادية، وخصوصًا المواقع السياسية، التي رغم تعبيرها عن نمو القيم الحضارية الديمقراطية، غالبًا ما تكون مصدرًا للأخبار الزائفة التي تُحدث فجوة بين النظام السياسي والمواطنين. إضافة إلى ذلك، تبرز جرائم القرصنة والنسخ غير المشروع، إذ تُعد الجزائر من البلدان التي عانت بشدة من هذه الظاهرة. ولا نغفل كذلك جرائم التجسس الإلكتروني التي تعتمد على تقنيات متطورة للتجسس على الدولة، بالإضافة إلى الإرهاب الإلكتروني الذي يتم من خلاله الاستيلاء على المعلومات أو تدميرها وتعطيلها في ظل ازدهار العصر الرقمي[1].

ومن هذا المنطلق، سعَت السياسات والخطط التي رسمها صانعو القرار في الجزائر إلى مواكبة كل تلك التحولات والتطورات العالمية، خاصةً إذا نظرنا إلى الوراء؛ إذ عاشت البلاد ما يعادل السنوات العشر الأخيرة من القرن العشرين.

تحت ضغط التوترات الأمنية التي خلَّفت الدمارَ والخسائرَ الفادحةَ في الأرواح والعتاد والممتلكات، والتي مثَّلت ظاهرةُ الإرهاب إحدى أهم الصور المهدِّدة لكيان الدولة الجزائرية وأمنها القومي، فإنها لم تقتصر على نمطٍ وسلوكٍ مُحدَّدٍ تجاه فئةٍ أو مؤسسةٍ معينة، بل تجاوزت كلَّ ما هو خاضعٌ لسلطتها.

ومن أهم التحديات التي أفرزتها بدايةُ القرن الحادي والعشرين هي التطوراتُ والتحولاتُ الهائلةُ التي شهدها العالمُ في مجال التكنولوجيا والرقمة عبر كافة المجالات، وهو أمرٌ كان لزامًا على صانع القرار الجزائري الوقوفُ عنده. فقد أصبح هذا التحولُ في غاية الصعوبة، بل وغير آمنٍ على الدول التي تفتقر إلى رؤيةٍ واستشرافٍ لإيجابياته وسلبياتِه.

وإدراكًا للطبيعة الحاسمة للدفاع السيبراني، عملت الجزائرُ مُنذ سنواتٍ على تبني هذا المفهوم ووضعه في صميم السياسات والآليات، لاسيما في الخطط العسكرية .فقد أضحى النظامُ المعلوماتي والرقمي أمرًا لا يمكن تجاوزُه داخل المؤسسات والقطاعات، ويمتد إطارُ الدفاع السيبراني إلى أبعد من مجرد ضمان سلامة

[1] - سارة بودح ، الاستراتيجية الجزائرية في الانفاق على التسلح في ظل التهديدات الأمنية الجديدة 2010 -2014 ، مذكرة لنيل شهادة الماستر أكاديمي في تخصص الهلوم السياسية والعلاقات الدولية ، جامعة قاصدي مرباح ورقلة ، السنة الجامعية 2015/2014 ص 54 .

الحواسيب وأمنها؛ ليصل إلى حدٍّ يكون له تأثيرٌ مباشرٌ على الأمن القومي .وبالتالي، يعمل هذا الدفاعُ على حماية النظم الإلكترونية الخاصة بالدولة، وما تواجهه من حروبٍ إلكترونية. كما يُمكِّن الدفاعُ السيبراني من التصدي للتهديدات المحدقة بالشبكات والأجهزة الرقمية الحسَّاسة للمؤسسات الكبرى[1]

المبحث الثالث : الأمن السيبراني في السياسة الأمنية الجزائرية

في ظل التغيرات الجيوسياسية المتسارعة والاعتماد المتزايد على التكنولوجيا الرقمية، أصبحت التهديدات السيبرانية من أبرز التحديات التي تواجه الدول، باعتبارها تهديدات عابرة للحدود يصعب التنبؤ بها أو السيطرة عليها بالوسائل التقليدية. وفي هذا السياق، أدركت الجزائر أهمية الأمن السيبراني كجزء محوري من سياستها الأمنية الشاملة، ليس فقط لحماية بنيتها التحتية المعلوماتية، بل أيضًا لضمان استقرارها السياسي والاقتصادي والاجتماعي.

وقد عملت الدولة الجزائرية على تطوير مقاربة استراتيجية تأخذ بعين الاعتبار خصوصيات الفضاء السيبراني، من خلال تعزيز الإطار التشريعي، وإنشاء مؤسسات مختصة، وتكثيف التنسيق بين القطاعات الأمنية والتقنية، إلى جانب تنظيم ملتقيات وطنية تهدف إلى رفع الوعي وتكوين الكفاءات. ويأتي هذا المبحث لتحليل موقع الأمن السيبراني ضمن السياسة الأمنية الجزائرية، من خلال الوقوف على التوجهات الرسمية، المؤسسات الفاعلة، والتحديات الراهنة التي تواجه الدولة في هذا المجال الحيوي.

المطلب الأول : مكانة الأمن السيبراني في السياسة الأمنية الجزائرية

مع تصاعد الهجمات الرقمية وتعاظم التهديدات على أمن الدولة، حرصت الجزائر على وضع الأمن السيبراني في صلب أولوياتها كجزء لا يتجزأ من استراتيجيتها الأمنية الشاملة. فقد بدأت الدولة ترسيخ ذلك من خلال تأسيس بنية مؤسساتية قوية، تشمل مراكز متخصصة لمكافحة الجريمة المعلوماتية، تتبعها الأجهزة

[1] - إلهام الغازي ، المرجع السابق ، ص 47 .

القضائية مثل المعهد الوطني للأدلة الجنائية للدرك، ومصلحة الدفاع السيبراني التابعة للجيش الوطني الشعبي، إلى جانب مصلحة مركزية في مديرية الأمن الوطني

الفرع الأول : مكانة الأمن السيبراني في السياسة الأمنية الجزائرية

تحتل قضية الأمن السيبراني مكانة متزايدة في السياسة الأمنية الجزائرية، خاصة مع تصاعد التهديدات الرقمية العالمية. تُعرِّف الجزائر الأمن السيبراني بأنه "مجموع الوسائل التقنية والتنظيمية والإدارية التي تُستخدم لمنع الاستخدام غير المصرح به للمعلومات الإلكترونية، واستعادة البيانات، وضمان استمرارية عمل النظم المعلوماتية، وحماية خصوصية المواطنين من المخاطر السيبرانية" (ص. 14). تعكس هذه التعريفات إدراكاً رسمياً لضرورة تكييف التشريعات والأطر الأمنية مع التحديات الحديثة.

في هذا الإطار، أقرت الجزائر قانوناً خاصاً بجرائم الكمبيوتر والإنترنت (القانون رقم (04–09، الذي يُجرم الاختراقات غير المشروعة، وسرقة البيانات، والقرصنة الإلكترونية، مع فرض عقوبات تصل إلى السجن لمدة 10 سنوات. كما أنشأت هيئات مختصة مثل **الوكالة الوطنية لأمن المعلومات** (ANSI)لتنسيق الجهود بين القطاعات الحكومية والخاصة في مواجهة الهجمات السيبرانية.

وتتجلى مكانة الأمن السيبراني في الاستراتيجية الوطنية الجزائرية من خلال:

دمج الأمن السيبراني في الأمن القومي :تُعتبر حماية البنية التحتية الحيوية (كالطاقة والاتصالات) أولوية، نظراً لارتباطها المباشر بسلامة الدولة واستقرارها الاقتصادي

التعاون مع المنظمات الدولية :انضمت الجزائر إلى اتفاقية **بودابست لمكافحة الجريمة السيبرانية** (2001)، مما يعزز تبادل الخبرات مع الدول الأخرى

بناء القدرات البشرية :تُدرّس مقررات الأمن السيبراني في الجامعات، مثل برنامج الماجستير في "الدراسات الاستراتيجية والأمنية" بجامعة الجزائر 3، لتعزيز الكفاءات المحلية

الفرع الثاني: أسباب اهتمام الجزائر بالأمن السيبراني

حماية البنية التحتية الحيوية :تُعد الجزائر عرضة لهجمات تستهدف قطاعات حيوية مثل الطاقة والنقل، خاصة مع اعتمادها المتزايد على الأنظمة الرقمية. فالهجمات على محطات الكهرباء أو شبكات الاتصالات قد تُعطل الخدمات الأساسية

مكافحة الإرهاب الإلكتروني :تواجه الجزائر تهديدات من جماعات إرهابية تستخدم الفضاء السيبراني للتجنيد ونشر الدعاية، مثلما حدث مع تنظيم القاعدة في بلاد المغرب الإسلامي

الحفاظ على الأمن القومي :تشكل الهجمات السيبرانية تهديداً للأمن الداخلي، خاصة مع تسريبات البيانات الحكومية أو اختراق أنظمة الدفاع. على سبيل المثال، أشارت تقارير إلى محاولات اختراق أنظمة المراقبة الحدودية الجزائرية .

الالتزام بالمعايير الدولية :تهدف الجزائر إلى مواكبة التوصيات الصادرة عن الاتحاد الدولي للاتصالات (ITU)لتعزيز الثقة في التعاملات الرقمية، خاصة في ظل التوجه نحو التحول الرقمي .

الحد من الخسائر الاقتصادية :تُقدر الخسائر المالية الناجمة عن الجرائم السيبرانية في الدول النامية بنحو 2.2 مليار دولار سنوياً، مما يدفع الجزائر إلى تعزيز آليات الحماية .

المطلب الثاني: أبرز التهديدات التي تواجه الأمن السيبراني الجزائري

تتفق العديد من الدوائر العلمية على أن الجرائم المستحدثة في الفضاء السيبراني (كالجرائم الإلكترونية، الإرهاب الإلكتروني، والحروب الإلكترونية) أصبحت لا تعرف حدودًا؛ فقد ألغت عنصرَي الزمان والمكان، وأفقدت الدول إمكانية التحالف لمواجهتها. فالدقة المتناهية في تنفيذ الاختراقات جعلت الانتصار شبه محقق حتى على المؤسسات العسكرية، وإن لم تُفعَّل اليقظة المعلوماتية (المراقبة المستمرة لهذا الميدان) حتى يتم الاستباق في وضع الآليات الكفيلة بالتأقلم مع التحديات التي تفرزها التطورات التكنولوجية، فإن هذا الخطر من شأنه المساس بالأمن.

بالنسبة للجزائر، فإن موقعها الجغرافي جعل منها فضاءً مفتوحًا مغاربيًا، متوسطيًا، وأفريقيًا لتلاقي وتقاطع التهديدات اللاتماثلية التي تركت آثارها على مسألة الأمن الوطني. وإذا أضفنا إلى ذلك المخاطر السيبرانية، فإن الجزائر كغيرها من الدول أصبحت إحدى ضحايا هذه التحديات، وأصبحت في حاجة إلى تصميم وتطوير إستراتيجية أمنية متعددة التخصصات (الجوانب التشريعية، التنظيمية، البشرية، المالية، التقنية، والمعلوماتية) حتى يتسنى لها تأمين الثورة الرقمية للأفراد والمؤسسات، وبالتالي التصدي للخطر. في هذا الإطار، توجهت الجزائر إلى طرح تصورات ورسم سياسة أمنية مزدوجة (الأمن السيبراني) للتحكم في أنظمة المراقبة لحماية المنظومة المعلوماتية للمؤسسات والمواطنين من جهة، ومواجهة الأخطار من جهة ثانية. ولتدارك النقائص، تجتهد الجزائر في الجبهة الخارجية من خلال التعاون المتعدد التخصصات، للاستفادة من تجارب غيرها من الدول.

من هذا المنطلق، وفي إطار رسم السياسة الأمنية العامة، طرح صناع القرار في الجزائر مخططًا وطنيًا لتفادي الوقوع في مأزق أمني جديد (اختراق أنظمة المعلومات الحساسة لرئاسة الجمهورية، وزارة الدفاع الوطني، أجهزة الأمن)، آخذين بعين الاعتبار من جهة الأزمة الأمنية التي تحاصر البلاد في شقها المتوسطي، المغاربي، والساحل الأفريقي، ومن جهة ثانية، الحفاظ على الحقوق الشخصية والحريات الفردية وفق ما تضمنته المواثيق الدولية والقوانين الوطنية.[1] وسوف نطرح تصور أو مقاربة الجزائر للموضوع من خلال النقاط التالية:

الفرع الأول : على المستوى الوطني

أُدرج الأمن السيبراني كإحدى الأولويات في برنامج المواجهة ضد الجريمة الإلكترونية والإرهاب الإلكتروني، بل أصبح يشكل جزءًا لا يتجزأ من استراتيجيات الدفاع، لأن الدروس المستخلصة من الدول التي لها تجربة في هذا المجال، أثبتت أن النجاعة في التطبيق وفعالية المعايير والوسائل المستعملة لا يمكن لها أن تتجسد ما لم يكن هناك تخطيط محكم وتنسيق بين الفاعلين في الميدان. وعليه، توجهت الجزائر إلى رسم إستراتيجيتها مركزة على النقاط التالية:

[1] - حليمة نايت الصغير ، **الجريمة الالكترونية وإجراءات مواجهتها في التشريع الجزائري** 2022/2021 ، مذكرة لنيل شهادة الماستر أكاديمي في تخصص القانون الجنائي وعلوم جنائية ، منشور ، جامعة محمد بوضياف المسيلة ، كلية الحقوق والعلوم السياسية ، السنة الجامعية 2022/2021 ص 16 .

من الناحية القانونية :اعتمد المشرع الجزائري في سن الأحكام القانونية لمحاصرة الجريمة الإلكترونية على ثلاثة معايير متفق عليها إلى حد ما لدى الفقهاء والتشريعات المقارنة:

أولًا :وسيلة الجريمة المتمثلة في استخدام تكنولوجيات الاتصال.

ثانيًا :موضوع الجريمة المتمثل في المساس بالأنظمة المعلوماتية.

ثالثًا :الجانب الشرعي والمتمثل في العقوبات المحددة في القانون.

ويهدف المشرع من هذه الخطوة إلى تحديد النطاق الذي تنشط فيه الجريمة الإلكترونية حتى يتسنى للفاعلين التحكم في الموضوع. ومن خلال القراءة التحليلية لمواد القوانين المستحدثة أو المعدلة، يتضح أن المشرع الجزائري قد طرح تصورًا يتوفر على العلاج الوقائي والردعي لمحاصرة الجرائم السيبرانية من الجوانب التالية:

أولًا :تم تعريف الجريمة الإلكترونية وإدراجها ضمن الأعمال المعاقب عليها قانونًا (المادة 02 من القانون رقم 09-04 المؤرخ في 2009.05.09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها). كما تبنى القانون النقاط الأساسية المذكورة في المعيار الأول والثاني. أما المعيار الثالث، فقد تناوله المشرع من خلال إدراج المادة 323 من القانون 10-05 الصادر في 2005.06.20 المتضمن الدليل الإلكتروني (انظر القانون المدني طبعة 2014). كما تم تعديل المواد (65، 79، 143، 156، 212، 238، 720) من قانون الإجراءات الجزائية، والمواد (303، 333، 394، 396) من قانون العقوبات المتضمنة تجريم وتسليط العقاب على كل من يثبت في حقه اختراق أنظمة معلومات المؤسسات أو الأفراد بطريقة غير شرعية. كما جاءت المادة 87 من نفس القانون صريحة في تجريم وتسليط العقاب على كل من يثبت تورطه في أعمال الإشادة والتجنيد لصالح الجماعات الإرهابية (الإرهاب الإلكتروني)[1].

[1] - نايت الصغير حليمة ، المرجع السابق ، ص 11 .

بالإضافة إلى ذلك، تدعمت الإجراءات القانونية بآلية تقنية جديدة تتمثل أولًا في صدور القانون 16-03 المؤرخ في 2016.06.19 المتضمن البصمات الجنائية في الإجراءات الجزائية لتحديد هوية الأشخاص. كما تم تعزيز الجهات القضائية على المستوى الوطني بأربعة محاكم خاصة وهي المحاكم المتخصصة (الجزائر، قسنطينة، وهران، ورقلة)، لتسهيل عمليات البحث والتحري لذوي الاختصاص من الأجهزة الأمنية والبت في القضايا المعروضة دون الرجوع إلى الوصاية. كما شمل التشريع بعض المجالات التي يحتمل أن تشملها الجريمة والتي لها صلة بمجال الحريات الخاصة على غرار قانون الملكية الفكرية، الثقافية، حقوق المؤلف (قانون 03-05 و03-06 الصادرين بتاريخ 2003.07.19)، وقانون مكافحة تبييض الأموال (01-05 الصادر بتاريخ 2005.02.05)، وقانون الوقاية ومكافحة المخدرات (04-18 الصادر بتاريخ 2004.12.25).

ثانيًا: تمت مُطابقة التشريع الداخلي مع ما جاء في التشريعات الدولية، وخاصة الاتفاقية الدولية المبرمة في عاصمة المجر بودابست بتاريخ 23 نوفمبر 2001، والتي تتناول الجرائم السيبرانية. وتُعتبر هذه الاتفاقية بمثابة المرجعية القانونية لكل التشريعات الدولية الصادرة في هذا المجال. ومن أبرز النقاط التي شملتها المطابقة:

استعمال المصطلحات المعمول بها في مجال الإعلام الآلي وتكنولوجيات الاتصال، مثل: "معطيات الإعلام"، و"معطيات متعلقة بالاختراق"، و"مُموِّل الخدمات" [1]، بهدف تسهيل عمل المختصين في الإعلام الآلي لفهم العمل المطلوب أو الملف المطروح بدقة.

الدخول غير الشرعي إلى الأنظمة المعلوماتية [2] . وتكمن أهمية تجريم هذا الفعل في تحديد نقاط الضعف بالأنظمة المستهدفة وإمكانية كشف هوية الجاني.

الاعتراض غير الشرعي للمكالمات والمعطيات المتبادلة، سواء في إطار خاص أو مهني [3].

[1] - المادة الأولى من الاتفاقية ومقدمة القانون الجزائري 04.09
[2] - المادة الثانية من الاتفاقية والمادة 394 مكرر من قانون العقوبات الجزائري
[3] - المادة الثالثة من الاتفاقية والمادة 303 من قانون العقوبات الجزائري

المساس بنزاهة أو سلامة المعطيات [1]، حيث إن الحصول على المعطيات بطريقة غير شرعية قد يُغيِّر مسار المعلومة في جانبها المهني أو الشخصي، مما يجعل هذا الفعل من أخطر التهديدات الإلكترونية.

المسؤولية المعنوية للجهات المكلفة بتسيير مجالات تكنولوجيا الإعلام، والتي تبقى ضامنةً –حسب القانون– لسلامة الأنظمة المعلوماتية [2].

التعاون الدولي لضمان سلامة الإجراءات القانونية (كالنيابة القضائية وتسليم المجرمين)، وهو من أهم العناصر التي ركزت عليها الاتفاقية في الباب الثالث والمواد 614 إلى 713 من قانون الإجراءات الجزائية، والمادة 15 من القانون 09–04. إذ يُعد هذا التعاون سبيلًا أساسيًا للخبراء للحد من الجريمة الإلكترونية، رغم ما قد تثيره طلبات التسليم من إشكالات تتعلق بسيادة الدول.

يُعتبر التعاون الإقليمي والدولي في مجال مكافحة التهديدات السيبرانية بالنسبة للدولة الجزائرية شكلاً من أشكال المؤشرات الخمسة التي أقرها الاتحاد الدولي للاتصالات السلكية واللاسلكية سابقًا.

ب) الآليات المؤسساتية:

سنعتمد في هذه الدراسة على الهيئات والمؤسسات التي وضعتها الجزائر في طليعة مجال مكافحة الجرائم السيبرانية، وهي:

- مؤسسة الجيش الوطني الشعبي.
- الدرك الوطني.
- الأمن الوطني.

استراتيجية الجيش الوطني الشعبي في مجال الأمن السيبراني:

[1] - المادة الرابعة من الاتفاقية والمادة 394 مكرر من قانون العقوبات الجزائري
[2] - المادة 12 من الاتفاقية والمادة 394 مكرر من قانون العقوبات الجزائري

أُحدثت بتاريخ 11جوان 2015)على مستوى دائرة الاستعمال والتحضير لأركان الجيش الوطني الشعبي (مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة، وأُوكلت لها مهمة حماية المنظومات والمنشآت الحيوية للبلاد ضد كل أنواع الجرائم السيبرانية.

تتمحور استراتيجية الدفاع السيبراني للجيش الوطني الشعبي حول سبعة عشر محورًا، وهي:

1. **الجانب الوظيفي والتنظيمي** :تكون أعمال الدفاع السيبراني ضمن الجيش الوطني الشعبي مُوجَّهةً ومنفَّذةً في إطار سلسلة وظيفية أو تنظيمية مكرسة لضمان تجانسها وفعاليتها.
2. **الجانب القانوني** :تحيين وتعزيز الإطار القانوني المتعلق باستعمال تكنولوجيات الإعلام والاتصال عموماً، وتأمين منظومات الإعلام خصوصاً.
3. **الجانب البشري** :تُعدُّ جاهزية موارد بشرية تقنية ذات كفاءة عالية في مجال الدفاع السيبراني هدفاً أساسياً لضمان نجاح إدخال هذا المجال في النشاطات العملياتية والتسييرية للجيش.
4. **الجانب التقني** :تقوية القدرات التقنية للحماية والكشف والرد على الهجمات السيبرانية، مع ضمان يقظة دائمة تجاه الوسائل المستخدمة من قبل المهاجمين.
5. **الجانب الوقائي والتوعوي** :التركيز على الوقاية وتوعية مستخدمي الجيش الوطني الشعبي بالمخاطر الناجمة عن استخدام تكنولوجيات الإعلام والاتصال في الإطارين المهني والشخصي.
6. **الجانب البحثي** :تحقيق درجة من الاستقلالية التكنولوجية عبر استخدام وسائل تقنية مُطوَّرة محلياً، خاصةً تلك المُخصَّصة للحماية ضد التهديدات السيبرانية.
7. **جانب التعاون** :تعزيز التعاون مع جيوش الدول الشريكة في مجال الدفاع السيبراني؛ لتمكين الجيش الوطني الشعبي من الاستفادة من الخبرات والوسائل التكنولوجية المتقدمة.

وتجسيداً لذلك، باشرت الدولة الجزائرية (وخاصةً مؤسسة الدفاع الوطني) إعداد برامج خاصة لمجابهة الجريمة الإلكترونية والحد من انتشارها، وإنشاء أجهزة جديدة تتلاءم أدوارها وتجهيزاتها مع متطلبات هذا المجال. وقد أصبحت الحماية السيبرانية جزءاً لا يتجزأ من أي منظومة دفاعية، حيث تمكَّن الجيش الوطني الشعبي من مواكبة التطورات التكنولوجية العالمية، وتأمين نطاقه المعلوماتي، وحماية الفضاء الرقمي لكافة الناشطين فيه

خلاصة الفصل:

يتناول الفصل الثاني من الدراسة موضوع الأمن السيبراني في الجزائر، من خلال تحليل الاستراتيجية الوطنية لحماية المعلومات والبيانات، وتحديد الأطر النظرية والعملية لهذه الاستراتيجية. يبدأ الفصل بتوضيح مفهوم الحماية المعلوماتية وأهميتها، ثم يعرض النماذج والنظريات التي تدعم حماية البيانات، مثل نموذج "CIA Triad"، كما يستعرض أدوات الحماية المستخدمة كجدران الحماية وتشفير البيانات، والتحديات التي تواجه الجزائر في هذا المجال، مثل نقص الكفاءات وتطور الهجمات السيبرانية. كما يتناول الفصل الاستراتيجية الجزائرية لمكافحة الجرائم الإلكترونية، من خلال توضيح السياسة العامة لحماية المعلومات، والهيكل التنظيمي، والتشريعات ذات الصلة. ويبرز أهمية تبني تدابير تقنية وإجرائية مثل مراقبة الاتصالات واعتراض المراسلات وفقًا للقانون، لمواجهة التهديدات الإلكترونية. وينتهي الفصل بتسليط الضوء على المخاطر التقنية الناجمة عن المعرفة الحديثة، وعلى رأسها البرامج الضارة، مع التركيز على الحاجة إلى رؤية وطنية شاملة تدمج بين الجوانب التقنية والتنظيمية والتشريعية لضمان أمن الفضاء السيبراني في الجزائر.

الخاتمة

خاتمة:

ختامًا، يُعدّ الأمن السيبراني من أبرز التحديات التي تواجه الدول في العصر الرقمي، لما له من تأثير مباشر على استقرارها السياسي، وأمنها الاقتصادي، وسلامة بنيتها التحتية الرقمية. ومن خلال هذه الدراسة، حاولنا تسليط الضوء على واقع الاستراتيجية الجزائرية في مجال الأمن السيبراني، واستعراض أهم الآليات القانونية والتنظيمية والتقنية المعتمدة لحماية الفضاء السيبراني الوطني، في ظل التحولات التكنولوجية المتسارعة. ونأمل أن تساهم هذه المذكرة في إثراء الجهود البحثية وتوعية صناع القرار بأهمية تطوير منظومة الأمن السيبراني كأولوية وطنية لضمان حماية الأفراد والمؤسسات والدولة ككل.

النتائج:

من خلال هذه الدراسة استخلصنا النتائج التالية :

1. يشكل الأمن السيبراني عنصرًا أساسيًا في حماية الأمن القومي للدول، بما في ذلك الجزائر، في ظل تزايد الهجمات الإلكترونية.
2. تبنت الجزائر مجموعة من السياسات والقوانين ذات الصلة بحماية الفضاء السيبراني، لكنها ما تزال بحاجة إلى مزيد من الفعالية والتكامل.
3. يواجه تطبيق هذه الاستراتيجيات تحديات متعددة، أبرزها النقص في الكفاءات البشرية المؤهلة، وضعف الوعي الأمني لدى الأفراد والمؤسسات.
4. تركز الاستراتيجية الجزائرية أساسًا على الحماية التقنية، في حين أن البعد التوعوي والتدريبي لا يزال محدودًا نسبيًا.
5. هناك حاجة لتعزيز التنسيق بين الجهات الحكومية والخاصة في التصدي للتهديدات الإلكترونية.
6. يشكل غياب التعاون الإقليمي والدولي الفعال عائقًا أمام مواجهة الجريمة السيبرانية العابرة للحدود.

من خلال هذه النتائج ارتقينا الى بعض التوصيات :

التوصيات:

استنادًا إلى ما سبق، توصي الدراسة بما يلي:

1. تعزيز الإطار التشريعي المتعلق بالأمن السيبراني وتحديثه بما يتماشى مع التحديات الجديدة.
2. إدراج التربية الرقمية ضمن المناهج الدراسية لنشر الوعي الأمني لدى الناشئة.
3. الاستثمار في تدريب الكفاءات الوطنية وتكوين مختصين في مجال الحماية المعلوماتية.
4. تطوير بنية تحتية سيبرانية resilient تعتمد على أحدث التقنيات العالمية.
5. تفعيل التعاون الإقليمي والدولي لمكافحة التهديدات السيبرانية وتبادل الخبرات والممارسات الفضلى.
6. إنشاء هيئة وطنية مستقلة تُعنى حصريًا بتنسيق وتقييم الاستراتيجية الوطنية للأمن السيبراني.

قائمة المصادر

والمراجع

قائمة المصادر والمراجع

I. المصادر والمراجع باللغة العربية

أولا : النصوص القانونية

القوانين والأوامر والمراجع التشريعية

1. القانون الجزائري رقم 06-22، المؤرخ في 2006/12/20، المعدل للأمر رقم 155-66 (قانون الإجراءات الجزائية).
2. القانون الجزائري رقم 09-04، المؤرخ في 2009/05/09، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
3. القانون الجزائري رقم 16-03، المؤرخ في 2016/06/19، المتضمن البصمات الجنائية في الإجراءات الجزائية.

ثانيا : الكتب

1. ذياب البد نية، *الأمن وحروب المعلومات*، دار الشروق للنشر والتوزيع، 2003.
2. حجازي عبد الفتاح بيوم، *جرائم الكمبيوتر والإنترنت والتشريعات العربية*، دار النهضة العربية، 2009.
3. أيريك ليوبولد-سيرج لوست، ترجمة فتحي علي زمال، *أمن المعلومات*، مدينة الملك عبد العزيز للعلوم والتقنية، المملكة العربية السعودية، 2014.
4. عمر فاروق، *الأمن المادي لتكنولوجيا المعلومات*، دار المستقبل، دبي، 2019.
5. أحمد عبد الله، *أمن المعلومات: المفاهيم والتطبيقات*، دار النشر التقنية، القاهرة، 2020.
6. محمد العابد، *أمن المعلومات: المفاهيم والاستراتيجيات*، دار المنهل، بيروت، 2020.
7. خالد أحمد، *إدارة أمن المعلومات في المؤسسات*، دار التكنولوجيا، القاهرة، 2020.
8. محمد خالد، *الحماية من الهجمات السيبرانية*، مركز الأمن الإلكتروني، الرياض، 2021.

ثالثا : المقالات والدراسات

1. منى جبور الأشقر، "الأمن السيبراني: التحديات ومستلزمات المواجهة"، *اللقاء السنوي للمختصين في أمن وسلامة الفضاء السيبراني*، لبنان، 2012.

2. سامر مؤيد عبد اللطيف، "الحرب في الفضاء الرقمي رؤية مستقبلية"، *مجلة رسالة الحقوق*، السنة السابعة، العدد 2، 2015.
3. سمير بارة، "الأمن السيبراني في الجزائر: السياسات والدفاع"، *المجلة الجزائرية للأمن الإنساني*، 2017.
4. محمد بوكبشة، "الأمن والدفاع السيبراني أولوية قصوى"، *مجلة الجيش*، العدد 51، أكتوبر 2017.
5. إلهام غازي، "الدفاع السيبراني"، *مجلة الجيش*، العدد 163، أكتوبر 2018.
6. أسمهان بوضياف، "المجرمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر"، *مجلة الأستاذ الباحث للدراسات القانونية والسياسية*، المجلد 03، العدد 03، 2018.
7. إدريس عطية، *مجلة الدراسات الاستراتيجية والعسكرية*، المركز الديمقراطي العربي برلين، المجلد 02، العدد 06، مارس 2020.
8. قوي بوحنية وإدريس عطية، *مجلة الدراسات الاستراتيجية والعسكرية*، المركز الديمقراطي العربي برلين، المجلد 02، العدد 06، مارس 2020.
9. رغدة البهي، "الردع السيبراني: المفهوم والإشكاليات والمتطلبات."
10. جمال بوازدية، "الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية: التحديات والآفاق المستقبلية."

الأطروحات والمذكرات الجامعية

1. سارة بودح، *الاستراتيجية الجزائرية في الانفاق على التسلح في ظل التهديدات الأمنية الجديدة 2010-2014*، مذكرة ماجستير، جامعة قاصدي مرباح ورقلة، 2015/2014.
2. نايت الصغير حليمة، *الجريمة الإلكترونية وإجراءات مواجهتها في التشريع الجزائري*، مذكرة ماجستير، جامعة محمد بوضياف المسيلة، 2022/2021.

التقارير

1. مصطفى محمد موسى، *الإرهاب الإلكتروني: دراسة قانونية، أمنية، نفسية، اجتماعية*، دار الكتب والوثائق القومية المصرية، العدد 009

ثانياً: المراجع باللغة الأجنبية

Ouvrages (كتب)

1. Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security*, نيويورك: HarperCollins, 2010.

2. Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*, نيويورك: Doubleday, 2019.

Articles et études (مقالات ودراسات)

1. Verizon, *2021 Data Breach Investigations Report*, نيويورك: Verizon Communications, 2021.
2. Symantec, *Internet Security Threat Report 2022*, Mountain View: Symantec Corp, 2022.

Lois et Jurisprudences (قوانين وسوابق)

1. Council of Europe, *Convention on Cybercrime*, 2001 ,بودابست.

4. Sites internet (مواقع إلكترونية)

1. الفضاء الإلكتروني والرأي العام: تغير المجتمع والأدوات والتأثير"، المركز "عادل عبد الصادق، العربي لأبحاث الفضاء الإلكتروني.
2. "تعريف الأمن السيبراني"حسن الفني، http://portal.aridmy/ar-ly/account/.
3. Microsoft, "البرامج الضارة وكيف تعمل" ، https://www.microsoft.com/ar/security/business/zerotrust/maturity-model-assessment-cool.

Rapports (تقارير دولية)

1. United Nations Office for Disarmament Affairs, *Report on Developments in the Field of Information and Telecommunications*, نيويورك: UNODA, 2013.
2. National Institute of Standards and Technology, *NIST Cybersecurity Framework*, Gaithersburg: NIST, 2020.
3. UNESCO, *Global Survey on Cyber Legislation*, باريس: UNESCO Publishing, 2019.
4. تقرير الاتحاد الدولي للاتصالات (ITU) ،"2011-2010 اتجاهات الإصلاح في الاتصالات".

فهرس

المحتويات

فهرس المحتويات

ملخص

تتناول هذه المذكرة موضوع الأمن السيبراني في ظل التحولات الرقمية المتسارعة، مركزة على الاستراتيجية الجزائرية لمواجهة التهديدات السيبرانية. تبرز الدراسة أهمية حماية البنية التحتية الرقمية للدولة وتعزيز الأطر القانونية والتنظيمية لمواجهة الجرائم الإلكترونية. كما تسلط الضوء على التحديات التقنية والبشرية التي تواجه الجزائر، وتقترح آليات للتطوير مثل تعزيز الوعي، وتكوين الكفاءات، وتحديث التشريعات. وخلصت الدراسة إلى ضرورة اعتماد مقاربة شاملة تجمع بين الجوانب التقنية والقانونية والاستراتيجية لضمان فضاء سيبراني آمن.

الكلمات المفتاحية :الأمن السيبراني، الجزائر، الجريمة الإلكترونية، حماية المعلومات، السياسة الأمنية

Abstract

This thesis addresses the issue of cybersecurity amid rapid digital transformation, focusing on Algeria’s strategy to counter cyber threats. The study highlights the importance of protecting the nation's digital infrastructure and strengthening legal and regulatory frameworks to combat cybercrime. It also discusses the technical and human challenges Algeria faces and suggests development mechanisms such as awareness enhancement, capacity building, and legal reform. The study concludes that a comprehensive approach combining technical, legal, and strategic dimensions is essential to ensure a secure cyber environment.

Keywords: cybersecurity, Algeria, cybercrime, information protection, security policy