المدرسة الوطنية العليا للعلوم السياسية

قسم العلاقات الدولية

تأثير التهديدات السيبرانية على الأمن المجتمعي الجزائري

مذكرة مقدمة لاستكمال متطلبات الحصول على شهادة الماستر

تخصص: علاقات دولية

من اعداد:

شايب محمد

تحت اشراف الأستاذ:

حمزاوي ميلود

أعضاء لجنة المناقشة

فراني حياة	المدرسة الوطنية العليا للعلوم السياسية	رئيسا
حمزاوي ميلود	المدرسة الوطنية العليا للعلوم السياسية	مشرفا ومقررا
أوبعيش هجيره	المدرسة الوطنية العليا للعلوم السياسية	ممتحنا

السنة الجامعية: 2025/2024م

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

قال تعالى

وَإِذْ قَالَ إِبْرَاهِيمُ رَبِّ اجْعَلْ هَٰذَا بَلَدًا آمِنًا وَارْزُقْ أَهْلَهُ مِنَ الثَّمَرَاتِ مَنْ آمَنَ مِنْهُم بِاللَّهِ وَالْيَوْمِ الْآخِرِ قَالَ وَمَن كَفَرَ فَأُمَتِّعُهُ قَلِيلًا ثُمَّ أَضْطَرُّهُ إِلَىٰ عَذَابِ النَّارِ وَبِئْسَ الْمَصِيرُ

(سورة البقرة الاية126)

الشكر والتقدير

الحمد لله الذي وفقنا لإتمام هذا العمل فاللهم لك الحمد حتى ترضى ولك الحمد إذا رضيت ولك

الحمد بعد الرضا

أولا وقبل كل شيء أتقدم بجزيل الشكر والامتنان وكل عبارات الاحترام والتقدير والمحبة الى الأستاذ الدكتور

"حمزاوي ميلود"

على مساعداته وتوجيهاته المستمرة التي قدمها لي، ووقوفه الدائم معي لإنجاز هذا العمل.

فلك مني أرقي عبارات الشكر استاذي على ما قدمته لي من نصائح وتوجيهات، وفقك الله ورعاك.

شكر لكل اساتذتي الافاضل الذين اخذت منهم العلم في مختلف الاطوار الدراسية من مدرسة حصيري شريف ومتوسطة ابن سينا إلى متقنة رضا حوحو وختاما بالمدرسة الوطنية العليا للعلوم السياسية.

كما أتقدم بالشكر الى الأساتذة الأفاضل أعضاء لجنة المناقشة على قبولهم مناقشة هذا العمل.

كما لا يفوتني بهذه المناسبة ان أوجه شكري وامتناني الى كل من ساندني وقدم لي النصح والارشاد ومد لي يد العون من قريب او بعيد.

شكرا لكم جميعا.

الإهداء

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

الحمد لله الذي وفقنا لهذا الامر اللهم لك الحمد حتى ترضى

أهذي هذا العمل المتواضع:

الى اعزوأغلي انسانة في حياتي، الى من منحتني القوة والعزيمة طوال مشواري الدراسي

أمي

الى من وضعني في الامام وربني وعلمني الصواب وساندني في الحياة

أبي

الى أخي عبد الرزاق وأخي ياسين الى اختي شيماء وريمة الذي كانوا دائما سند لي ومصدر اعتزازي

فكانوا خير معين لي وفقكم الله

For me

الملخص

تتناول هذه المذكرة موضوع "تأثير التهديدات السيبرانية على الأمن المجتمعي في الجزائر"، من خلال تحليل الظاهرة في بعدها المفاهيمي والميداني. تنطلق الدراسة من فرضية أن التهديدات السيبرانية لم تعد مجرد مخاطر تقنية، بل باتت تشكل تهديداً مباشراً لاستقرار المجتمعات، خاصة في الدول النامية ذات البنية الرقمية الضعيفة.

ركزت الدراسة على توسيع مفهوم الأمن ليشمل الأبعاد الاجتماعية والثقافية والاقتصادية، مبرزة كيف تؤثر الهجمات الرقمية في تماسك المجتمع، والثقة في الدولة، والاستقرار العام. وتناولت المذكرة الحالة الجزائرية من خلال تحليل نماذج للهجمات السيبرانية، وآثارها السياسية والاقتصادية والثقافية، مع تقييم الاستراتيجيات الوطنية والدولية للتصدي لها.

اعتمدت المذكرة على مناهج متعددة: وصفي تحليلي، استقرائي، مقارن، كما استندت إلى اقترابات مثل الأمن الإنساني، الحوكمة الرقمية، والنظرية النقدية. وخلصت إلى ضرورة تطوير وعي سيبراني مجتمعي، وتعزيز القدرات الرقمية للدولة، وإصلاح المنظومة القانونية بما يواكب تحديات الفضاء السيبراني.

الكلمات المفتاحية:

التهديدات السيبرانية – الأمن المجتمعي – الأمن السيبراني – الجزائر – الفضاء الرقمي

Abstract (in English):

This thesis explores the impact of cyber threats on societal security in Algeria, analyzing both the conceptual framework and the real-world implications. It argues that cyber threats have evolved beyond technical risks to become a direct challenge to the social fabric and internal stability, particularly in developing countries with weak digital infrastructure.

The study expands the concept of security to include its social, cultural, and economic dimensions. It highlights how cyber-attacks affect social cohesion, public trust in state institutions, and national stability. The Algerian case is analyzed through examples of cyber incidents and their political, economic, and cultural effects, alongside an evaluation of national and international response strategies.

The research adopts a multi-method approach: descriptive-analytical, inductive, and comparative, supported by theoretical frameworks including human security, digital governance, and critical theory. It concludes that Algeria must enhance cyber awareness, build stronger digital capacity, and reform its legal system to effectively counter cyber threats and protect societal security.

Keywords (in English):

Cyber threats – Societal security – Cybersecurity – Algeria – Digital space

عرف العالم بعد نهاية الحرب الباردة تحولات جوهرية في المفاهيم السياسية والدولية، ولم تعد القضايا العسكرية التقليدية تلعب دورا مهيمنا في الدراسات الأمنية والعلاقات الدولية، وانما تعدت ذلك الى مفاهيم جديدة تهتم بالجانب غير العسكري، من بينهما التوسع في مفهوم الأمن ومسألة الأمن المجتمعي وتأثره بما أفرزته ظاهرة العولمة التي اعتبرها البعض أنها أدت الى تحولات سلبية أثرت على خصوصيات المجتمعات، ومن أهم ما أفرزته العولمة مواقع التواصل الاجتماعي التي سهلت التواصل بين المستخدمين عبر مختلف انحاء العالم، وبذلك أصبحت هذه الوسائل فضاء مؤثر في الحياة اليومية يسمح بنقل مختلف القضايا السياسية والاجتماعية مع تسهيل طرق إيصال المعلومات عبر وسائل متعددة سواء الصور، الفيديو، التسجيلات الصوتية وغيرها ليصبح بذلك فضاء متاح تروج عبره مختلف القضايا دون وجود رقابة على ذلك وهذا ما اثر على الأمن المجتمعي بشكل عام والمجتمعات الجزائرية بشكل خاص نتيجة ارتفاع أعداد كبيرة ومتزايدة من مختلف فئات المجتمع.

حيث شهد العالم خلال العقود الأخيرة تطورات هائلة في مجال التكنولوجيا والاتصال، أدت إلى بروز الفضاء السيبراني كأحد أهم الميادين الحيوية التي تؤثر في مختلف أوجه الحياة السياسية، الاقتصادية، الاجتماعية وحتى الثقافية. فقد أصبح هذا الفضاء، بكل ما يحتويه من شبكات وأنظمة معلوماتية، مكوناً محورياً في البنية التحتية للدول، ووسيلة رئيسية للتواصل والتبادل ونقل المعرفة، لكنه في المقابل فتح الباب واسعاً أمام نوع جديد من التهديدات الأمنية ذات الطابع غير التقليدي، والمعروفة باسم "التهديدات السيبرانية."

لقد تميزت هذه التهديدات بطابعها المعولم، وقدرتها على اختراق الحدود الجغرافية، وعدم التمييز بين الدول المتقدمة والنامية، ما جعلها تمثل تحدياً جديداً للأمن القومي والمجتمعي على حد سواء. فمع تزايد الاعتماد على التكنولوجيا الرقمية، أصبحت المجتمعات عرضة لهجمات إلكترونية تستهدف مؤسسات الدولة، البنى التحتية الحيوية، والمواطنين الأفراد، وتنعكس آثارها سلباً على الاستقرار العام، والنسيج الاجتماعي، والثقة في المؤسسات، ما يجعل من التصدي لها ضرورة استراتيجية ملحة.

وفي هذا السياق، لم تكن الجزائر بمنأى عن هذه الظاهرة؛ فخلال السنوات الأخيرة، عرفت البلاد تصاعداً في وتيرة التهديدات السيبرانية، خاصة في فترات الاضطراب السياسي أو النقاشات المجتمعية الحادة، حيث تم استغلال الفضاء الرقمي لبث حملات تضليل إعلامي، ونشر أخبار كاذبة، والتشكيك في مؤسسات الدولة، فضلاً عن محاولات اختراق قواعد بيانات حساسة تابعة لمؤسسات حكومية. إن خطورة هذه التهديدات تكمن في كونها لا تستهدف فقط البنى المادية، بل تتجاوز ذلك إلى المساس بالأمن الثقافي والفكري، وتوجيه الرأي العام، وخلق فجوات مجتمعية تهدد التماسك الداخلي.

وتكتسي دراسة موضوع "تأثير التهديدات السيبرانية على الأمن المجتمعي الجزائري" أهمية قصوى، بالنظر إلى تزايد ارتباط الأمن المجتمعي، كأحد مكونات الأمن القومي، بالمجال السيبراني. فالأمن المجتمعي لا يتعلق فقط بحماية المواطنين من الأخطار المادية، بل يمتد ليشمل حماية الهوية الثقافية، وتحصين الوعي الجماعي من الاختراقات الفكرية والمعلوماتية، وضمان استمرارية الثقة بين المجتمع ومؤسسات الدولة.

إن معالجة هذا الموضوع تقتضي فهماً متعدد الأبعاد، يستند إلى مقاربة شاملة تأخذ بعين الاعتبار الجوانب السياسية، القانونية، التكنولوجية، والاجتماعية للتهديدات السيبرانية، وتحلل انعكاساتها على السلم المجتمعي. كما يستوجب البحث الوقوف على الاستراتيجية الجزائرية لمواجهة هذه التهديدات، والتحديات التي تعترض جهودها في هذا المجال، في ظل ضعف البنية الرقمية الوطنية، وقصور الوعي السيبراني لدى فئات واسعة من المجتمع.

لذا، تسعى هذه المذكرة إلى الإحاطة بجوانب هذه الظاهرة المركبة، من خلال تحليل طبيعتها، ودوافعها، وآلياتها، وكشف تأثيراتها على الأمن المجتمعي في الجزائر، واستعراض التجارب الدولية الناجحة التي يمكن الاستفادة منها في صياغة سياسة وطنية فعالة للأمن السيبراني، تضمن الحماية الوقائية، والاستجابة السريعة، وبناء مجتمع رقمي آمن ومتين. وعلى اعتبار ان البحث العلمي يستند الى خطوات بحثية، فقد تم تقسيم الدراسة لمجموعة من الفصول تمثل أولها في الإطار النظري لمفهوم التهديدات السيبرانية والامن المجتمعي واهم المقاربات المفسرة لتطور مفهومهما تطورهما اما في الفصل الثاني تناولنا التأثير السيبراني على الامن المجتمعي الجزائري سياسيا، اقتصاديا، اجتماعيا وثقافيا. اما الفصل الثالث كان حول استراتيجيات مواجهة التهديدات السيبرانية وتعزيز الامن المجتمعي من سياسات وتشريعات وطنية الى جهود وتعاون دولي لمكافحة التهديدات السيبرانية.

1. المشكلة البحثية

شهد العالم في العقود الأخيرة ثورة رقمية هائلة رافقتها تحولات جذرية في طرق التواصل وتخزين المعلومات وإدارتها، ما فتح المجال أمام تهديدات جديدة تتجاوز الحدود الجغرافية والسيادية للدول. في هذا السياق، لم تعد التهديدات الأمنية محصورة في النطاق العسكري أو التقليدي، بل برزت التهديدات السيبرانية كواحدة من أخطر أشكال التهديدات المعاصرة، لما تحمله من قدرة على ضرب البنى التحتية الحيوية، وتعطيل المؤسسات، وزعزعة الثقة العامة، بل والتأثير في السلم الاجتماعي والسياسي داخل الدول.

وفي الحالة الجزائرية، ومع تسارع وتيرة الرقمنة، ازداد انكشاف المجتمع الجزائري على الفضاء السيبراني، مما جعله عرضة لموجة من الهجمات السيبرانية التي تستهدف مختلف قطاعات الحياة السياسية، الاقتصادية، الثقافية والاجتماعية. وهو ما يدفع إلى التساؤل حول مدى تأثير هذه التهديدات على الأمن المجتمعي الجزائري، وكيفية إدراكها والتعامل معها.

وعليه تتمثل إشكالية الدراسة في التساؤل المحوري التالي:

ما مدى تأثير التهديدات السيبرانية على الأمن المجتمعي في الجزائر، وما طبيعة الاستجابات الوطنية والدولية الكفيلة بالحد من هذا التأثير؟

وينبثق عن هذا التساؤل الرئيسي جملة من الأسئلة الفرعية، من بينها:

- ما هي أبرز التهديدات السيبرانية التي تواجه الجزائر؟ وما خصائصها؟
- كيف تؤثر هذه التهديدات على الأبعاد السياسية والاقتصادية والثقافية والاجتماعية للأمن المجتمعي؟
- ما هي الاستراتيجيات المتبعة وطنياً ودولياً لمواجهة هذه التهديدات؟ وهل هي فعالة؟

الفرضيات:

- إن ضعف البنية التحتية الرقمية في الجزائر، إلى جانب تزايد الاعتماد على الفضاء السيبراني، يجعل البلاد عرضة بشكل خاص للهجمات التي تستهدف البنى التحتية الحيوية للبلاد وقواعد البيانات الحكومية، مما يؤثر سلباً على استقرار الدولة وثقة المواطنين بمؤسساتها
- يؤدي الاستغلال المتزايد للمنصات الرقمية في الجزائر لنشر المعلومات المضللة وخطاب الكراهية، خاصة خلال فترات الاضطراب السياسي، إلى تآكل النسيج الاجتماعي وتقويض الأمن الثقافي والفكري، مما يهدد تماسك الهوية الوطنية الجزائرية.
- على الرغم من الجهود التشريعية والمؤسساتية التي تبذلها الجزائر لمواجهة التهديدات السيبرانية، فإن فعالية استراتيجيتها الوطنية تظل محدودة بسبب قصور الوعي السيبراني العام لدى المواطنين والفجوات في الكفاءات التقنية المتخصصة داخل مؤسسات الدولة.

1. مجالات الدراسة

- **المجال الموضوعي** :دراسة التهديدات السيبرانية في علاقتها بالأمن المجتمعي، مع التركيز على حالة الجزائر.
- **المجال المكاني** :يركز البحث على الحالة الجزائرية كمجال جغرافي واجتماعي لتحليل ظاهرة التهديدات السيبرانية.
- **المجال الزمني** :يغطي البحث الفترة ما بين 2015 إلى 2024، وهي المرحلة التي شهدت تصاعدا في الهجمات السيبرانية.

2. اهمية الدراسة

تكمن أهمية هذه الدراسة في أنها تسلط الضوء على إحدى أخطر التهديدات الأمنية غير التقليدية التي تواجه الجزائر والعالم المعاصر، والمتمثلة في التهديدات السيبرانية، من خلال تناولها كعامل تهديد للأمن المجتمعي بكل أبعاده. وتزداد هذه الأهمية بالنظر إلى ما يلي:

- الطابع المستحدث والمعقد للتهديدات السيبرانية، والتي تختلف عن التهديدات الكلاسيكية في عدم مركزيتها، وغموض مصدرها، وسرعة انتشارها.
- النقص في الدراسات المحلية التي تتناول الأثر المجتمعي للتهديدات السيبرانية، مقارنة بالاهتمام الأكاديمي العربي والدولي.
- أهمية رفع الوعي المؤسساتي والمجتمعي بأثر هذه التهديدات، ودور الدولة والمجتمع في مواجهتها.
- الحاجة إلى بناء استراتيجية وطنية متكاملة للتصدي لمخاطر الفضاء السيبراني، بما يعزز الأمن الوطني الشامل.

3. أهداف الدراسة

تسعى هذه الدراسة إلى تحقيق جملة من الأهداف العلمية والمعرفية والعملية، من أبرزها:

- الإحاطة بالمفاهيم النظرية المتعلقة بالأمن السيبراني والأمن المجتمعي.
- الكشف عن طبيعة التهديدات السيبرانية وأنواعها ومصادرها.
- تحليل التأثيرات السياسية والاقتصادية والثقافية والاجتماعية لهذه التهديدات على المجتمع الجزائري.
- تقييم الاستراتيجيات الوطنية والدولية لمواجهة التهديدات السيبرانية.
- تقديم مجموعة من التوصيات التي يمكن أن تسهم في تعزيز قدرات الدولة الجزائرية في حماية فضائها الرقمي.

4. أسباب اختيار الموضوع

تم اختيار هذا الموضوع للأسباب التالية:

- حداثة الظاهرة السيبرانية وخطورتها المتزايدة في العالم والجزائر على وجه الخصوص.
- الفراغ الأكاديمي النسبي في تناول العلاقة بين الأمن السيبراني والأمن المجتمعي في السياق الجزائري.
- الرغبة في المساهمة العلمية في إثراء حقل دراسات الأمن غير التقليدي، والتقاطع بين الأمن والمجتمع والفضاء الرقمي.
- طابع الموضوع العملي والآني، ما يمنحه أهمية مضاعفة على صعيدي البحث العلمي وصنع السياسات العامة.

5. مناهج الدراسة:

تعد مناهج البحث العلمي الأدوات الأساسية التي يعتمد عليها الباحث لفهم الظواهر وتحليلها. ونظرا للطبيعة المركبة والمتعددة الأبعاد لموضوع التهديدات السيبرانية وتأثيرها على الأمن المجتمعي، فقد تم الاعتماد على مجموعة من المناهج المتكاملة، وهي:

ا- المنهج الوصفي التحليلي

التعريف:

هو منهج يقوم على رصد ووصف الظواهر والمفاهيم كما هي، ومن ثم تحليلها وربطها بعواملها المؤثرة.

دوره في الدراسة:

استخدم هذا المنهج لتحديد المفاهيم النظرية الأساسية المرتبطة بالأمن السيبراني، الأمن المجتمعي، التهديدات الرقمية، وما إلى ذلك.

كما مكن الباحث من وصف واقع التهديدات السيبرانية في الجزائر، من حيث طبيعتها ومصادرها وتكرارها.

ساعد في تحليل العلاقة بين هذه التهديدات وبنية المجتمع الجزائري من حيث الاستقرار، الثقة العامة، والأمن الشامل.

ب المنهج الاستقرائي

التعريف:

يرتكز على الانطلاق من الجزئيات والوقائع الملموسة وصولا إلى تعميمات واستنتاجات كلية.

دوره في الدراسة:

استخدم لاستقراء الوقائع والحالات الواقعية للهجمات السيبرانية في الجزائر.

مكن من بناء فهم تدريجي لتأثير تلك الوقائع على الأمن السياسي، الاقتصادي، الثقافي والاجتماعي.

تم توظيفه في استنتاج فرضيات ميدانية بناء على أحداث ملموسة مثل اختراق "صيدال"، التسريبات الحكومية، أو هجمات على بنوك ومؤسسات تعليمية.

ج- المنهج المقارن

التعريف:

هو منهج يهدف إلى مقارنة الظواهر في بيئات مختلفة لاستخلاص أوجه التشابه والاختلاف.

دوره في الدراسة:

استخدم لمقارنة الاستراتيجيات الجزائرية في الأمن السيبراني مع نماذج وتجارب دولية ناجحة مثل إستونيا، فرنسا، وغيرها.

ساعد على تحديد الفجوات والتحديات في المنظومة الجزائرية مقارنة بالدول الأخرى، واستلهام دروس قابلة للتطبيق.

كما مكن من تحليل الفوارق في الأطر القانونية والتنظيمية بين الجزائر وتلك الدول.

ج- المنهج الكيفي

وقد تمثل ذلك في:

- تحليل محتوى الظاهرة من خلال توصيف التهديدات السيبرانية وتفسير آثارها.
- الاعتماد على حالات واقعية مثل اختراق صيدال ووزارة العدل وتحليل تداعياتها السياسية والاقتصادية.
- استخدام الدراسات السابقة والمراجع النظرية لاستخلاص أبعاد التأثير المجتمعي.

6. الاقترابات **والنظريات المعتمدة**

في العلوم السياسية والعلاقات الدولية، يشير مصطلح "الاقتراب" إلى الزاوية أو الإطار التحليلي الذي يستخدم لتفكيك وفهم الظاهرة. وفي هذه الدراسة، تم اعتماد عدة اقترابات تتكامل فيما بينها لفهم التأثيرات متعددة المستويات للتهديدات السيبرانية على الأمن المجتمعي:

ا- اقتراب الأمن الإنساني

الشرح:

يقوم هذا الاقتراب على توسيع مفهوم الأمن ليشمل أمن الأفراد والمجتمعات، وليس فقط الدول .يتناول الأمن من حيث ضمان الحياة الكريمة، حرية التعبير، الحق في الخصوصية، والأمن من الخوف والعوز.

دوره في الدراسة:

مكن من النظر إلى التهديدات السيبرانية ليس فقط كخطر على الدولة، بل كتهديد مباشر لسلامة وأمان الأفراد.

ساعد على تحليل التأثيرات الاجتماعية والنفسية للهجمات مثل الابتزاز الإلكتروني، سرقة البيانات الشخصية، التنمر الإلكتروني، والتضليل الإعلامي.

وفر أرضية لتحليل انعكاسات ضعف الحماية السيبرانية على الثقة المجتمعية في مؤسسات الدولة.

ب -لاقتراب البنيوي-الوظيفي

الشرح:

يركز هذا الاقتراب على دراسة البنى الاجتماعية (مثل الدولة، الأسرة، التعليم، الإعلام...) ووظائفها المختلفة، وكيف تؤثر عليها أو تتأثر بالمتغيرات الجديدة.

دوره في الدراسة:

ساعد على تحليل تأثير الهجمات السيبرانية على وظائف الدولة الحيوية، مثل التعليم، الأمن، الصحة، والإدارة.

مكن من فهم كيف أن الخلل في منظومة الأمن السيبراني يمكن أن يحدث اضطرابا وظيفيا في بنى المجتمع.

مثلا: اختراقات قواعد البيانات الصحية أو التعليمية تهدد استقرار النظام المؤسسي.

ج- الاقتراب القانوني و المؤسساتي

يتناول القواعد والتشريعات المنظمة للسلوك الدولي في مجال الامن السيبراني وعلاقات التعاون او الصراع

دوره في الدراسة :

ساعد على تحليل الاتفاقيات الدولية مثل اتفاقية بودابست، و مقارنتها بالتشريعات المحلية

د -اقتراب "النظرية النقدية في العلاقات الدولية"

الشرح:

يعيد هذا الاقتراب طرح الأسئلة حول مصادر السلطة والمعرفة والتكنولوجيا، ويبرز الاختلالات في بنية النظام الدولي، خصوصا في مجال الهيمنة الرقمية والتفاوت في القدرات السيبرانية.

دوره في الدراسة:

استخدم لتوضيح كيف تعاني الدول النامية مثل الجزائر من تبعية رقمية وتكنولوجية، تجعلها عرضة للتهديدات.

كشف عن فجوة السيادة الرقمية، وأن جزءا من التهديد السيبراني مرتبط بالبعد الجيوسياسي العالمي (مثلا السيطرة الغربية على نظم التشغيل والخوادم ومنصات البيانات).

مكن من طرح توصيات تدعو إلى تعزيز الاستقلال الرقمي والسيادة المعلوماتية كجزء من الأمن الوطني.

نظرية الأمننة(Securitization Theory)

المنظر الرئيسي :باري بوزان – مدرسة كوبنهاغن

تنظر إلى الأمن كعملية اجتماعية – سياسية، حيث يتم "تأطير" مسألة معينة (مثل التهديد السيبراني) على أنها تهديد وجودي لمجتمع أو دولة.

في المذكرة، جرى تناول التهديدات السيبرانية كأخطار تمس بقاء المجتمع الجزائري واستقراره، وهذا يمثل عملية "أمننة" للفضاء الرقمي.

الفصل الأول: الإطار النظري لمفهوم التهديدات السيبرانية والأمن المجتمعي

تمهيد

يشهد العالم المعاصر تحولات جذرية فرضتها الثورة الرقمية، لم تعد معها مفاهيم الأمن التقليدية كافية لفهم التعقيدات الجديدة في البيئة الدولية. فقد برزت قضايا أمنية غير عسكرية، على رأسها التوسع في مفهوم الأمن ليشمل الجانب المجتمعي ومسألة الأمن المجتمعي وتأثره بما أفرزته ظاهرة العولمة التي اعتبرها البعض أنها أدت إلى تحولات سلبية أثرت على خصوصيات المجتمعات، ومن أهم ما أفرزته العولمة مواقع التواصل الاجتماعي التي سهلت التواصل بين المستخدمين عبر مختلف أنحاء العالم، ليصبح بذلك فضاء مؤثرا في الحياة اليومية يسمح بنقل مختلف القضايا السياسية والاجتماعية وبذلك أصبحت هذه الوسائل مؤثرة، مع تسهيل طرق إيصال المعلومات عبر وسائل متعددة سواء الصور، التسجيلات الفيديو، الصوتية وغيرها ليصبح بذلك فضاء متاح تروج عبره مختلف القضايا دون وجود رقابة على ذلك وهذا ما اثر على الأمن بشكل عام والمجتمعات بشكل خاص والمجتمعات الجزائرية نتيجة ارتفاع أعداد كبيرة ومتزايدة من مختلف فئات المجتمع. شهد العالم خلال العقود الأخيرة تطورات هائلة في مجال الاتصال، والتكنولوجيا، أدت إلى بروز الفضاء السيبراني كأحد أهم الميادين الحيوية التي تؤثر في مختلف أوجه الحياة، السياسية، الاقتصادية، الاجتماعية وحتى الثقافية. فقد أصبح هذا الفضاء، بكل ما يحتويه من شبكات ونظم معلوماتية، مكونا محوريا في البنية التحتية للدول، ووسيلة رئيسية للتواصل والتبادل ونقل المعرفة، لكنه في المقابل فتح الباب واسعا أمام نوع جديد من التهديدات ذات الطابع غير التقليدي، والمعروفة باسم "التهديدات السيبرانية". لقد تميزت هذه التهديدات بطابعها المعولم، وقدرتها على اختراق الحدود الجغرافية، وعدم التمييز بين الدول المتقدمة والنامية على حد سواء. يهدف هذا الفصل إلى بناء إطار مفاهيمي راسخ لهذين المصطلحين المحوريين، التهديدات السيبرانية والأمن المجتمعي، من خلال استعراض نشأتهما، تعريفاتهما المختلفة، وأبرز المفاهيم المرتبطة بهما. سيتم تحليل طبيعة التهديدات السيبرانية كشكل من أشكال التهديدات المعاصرة ذات الطابع المعولم وقدرتها على اختراق الحدود، كما سيتناول الفصل مفهوم الأمن المجتمعي كبعدٍ متزايد الأهمية ضمن منظومة الأمن القومي الشامل، وذلك لوضع الأساس النظري اللازم لفهم طبيعة التفاعل والتأثير المتبادل بينهما، والذي سيتم بحثه في الفصول التالية.

المبحث الأول: مفهوم التهديدات السيبرانية

عرفت البيئة الدولية مع تسارع الرقمنة تطورا لافتا في أنماط التهديدات الأمنية، حيث لم تعد تقتصر على الهجمات المسلحة التقليدية، بل ظهرت تهديدات رقمية عابرة للحدود يصعب التنبؤ بمصدرها أو توقيتها. يندرج ضمن هذا السياق مفهوم "التهديدات السيبرانية" الذي أصبح يحظى بأهمية متزايدة في أدبيات الأمن المعاصر. يتناول هذا المبحث التعريفات المختلفة لهذا المفهوم، وخصائصه، وطبيعته التقنية، والفرق بينه وبين غيره من المفاهيم المشابهة، كما يستعرض تطور الأمن السيبراني كحقل معرفي واستراتيجي، وأنواعه، وأبرز ملامحه في السياق الدولي.

المطلب الأول: الإطار النظري للأمن السيبراني

الفرع الأول: مفهوم الامن السيبراني

يقصد بالتهديدات السيبرانية تلك الهجمات التي تتم باستخدام آليات وشبكات الانترنيت وأجهزة الحاسوب التي، وتهدف الى إلحاق الضرر بالأجهزة والشبكات الالكترونية ذات الاتصال بالأنترنيت. 1

كما تعرف التهديدات السيبرانية بأنها: فعل يقوض من قذرات ووظائف شبكة الكمبيوتر لغرض قومي أو سياسي، من خلال استغلال نقطة ضعف ما تمكن المهاجم من التلاعب بالنظام.2

و تعد التهديدات السيبرانية من أبرز التحديات الأمنية في العصر الرقمي، نظراً لتعدد أشكالها وسرعة تطورها، حيث يشير مفهوم التهديد السيبراني إلى "مجمل الأفعال العدائية التي تُمارس عبر الفضاء الرقمي، والتي تهدف إلى الإضرار بالأنظمة المعلوماتية، أو سرقة وتخريب البيانات، أو التأثير على سلوك المستخدمين، أفراداً ومؤسسات ويشمل هذا المفهوم طيفاً واسعاً من الأنشطة، من أبرزها: الاختراقات الأمنية، والتجسس الرقمي، وهجمات حجب الخدمة، وهجمات الفدية، و الدعاية الرقمية، بالإضافة الى التزييف العميق الذي يستخدم لتظليل الرأي العام.[3]

وهذه التهديدات لا تقتصر على الجوانب التقنية فحسب، بل تتداخل مع أبعاد سياسية واقتصادية واجتماعية، وتؤثر بشكل مباشر في أمن الدول واستقرار المجتمعات، ما يستدعي مقاربة شاملة قائمة على التوعية، وسن القوانين، وتطوير آليات الحماية.[4] وقد عرفتها القيادة الاستراتيجية الامريكية بانها تطويع

---

[1] عبد الله جعفري، "التهديدات السيبرانية وتأثيرها على الأمن القومي الجزائري"، المجلة الإفريقية للدراسات القانونية والسياسية، العدد 8 (2022): 247.

[2] رغدة البهي، "الردع السيبراني: المفهوم، الإشكاليات، والمتطلبات"، مجلة الدراسات الإعلامية، العدد 5 (2018): 209.

[3] عبد الله محمد سيد، "الأمن السيبراني: التهديدات والتحديات في البيئة الرقمية المعاصرة "القاهرة: مكتبة الإنجلو المصرية، 2020،ص 35.

[4] عبد الكريم حسام،" التحولات الرقمية وأمن المعلومات" عمّان: دار الصفاء للنشر والتوزيع، 2021،ص 48.

عمليات نظام الكمبيوتر بهدف منع الخصوم من الاستخدام الفعال لها، فضلا عن التسلل الى أنظمة المعلومات وشبكات الاتصال بهدف جمع وحيازة وتحليل البيانات التي تحتويها.[1]

لذلك تعتبر التهديدات السيبرانية أحد الاشكال الحديثة للتهديدات الأمنية باعتبارها مرتبطة ارتباطا وثيقا بأنظمة المعلومات وشبكات الاتصال، وهي بذلك نتاج التطور التكنولوجي الذي وصلت اليه تكنولوجيا الاعلام والاتصال بمختلف أنواعها واشكالها.

وقد شهد القرن الحالي تطورا هائلا في وسائل الاتصال ومقابل التباين بين مستخدمي الشبكة ظهرت استخدامات غير مشروعة، مما أدي إلى ظهور جرائم مختلف عن الجرائم التقليدية عابرة للقارات وقد سميت بالجرائم المعلوماتية أو الإلكترونية أو جرائم الانترنت لمكافحة هذه الجرائم كان لابد من قيام نظام يكافحها لذا أنشئ الأمن السيبراني..

أما مصطلح (الأمن السيبراني) فهو مكون من كلمتي (الأمن) السيبراني، و(السيبراني)، وهذا المصطلح المركب نظرا لحداثة مصطلح الأمن فقد اختلفت عبارات الباحثين ووجهات نظرهم في تحديده، وضبط التعريفات، وماذا تعني السيبرانية مفهومه. وسأورد شيئا من تلك تعريف الأمن: لقد تعددت معاني الأمن في اللغة منها الثقة، الحفظ، الأمان، السلم، التصديق، الدين، القوة الإجارة وطلب الحماية، والمراد به هنا الأمن ضد الخوف، وإطلاق لفظ الأمن مجردا يؤدى إلى نوع من الالتباس وخلط بين المعاني، إنما بحسب طبيعة الموقف المراد التعبير عنه بأحد هده المعاني.[2]

ج- **تعريف الأمن اصطلاحا:** الأمن عدم توقع المكروه في زمن آت.

– **تعريف السيبرانية:** مأخوذة من كلمة (سيبر) وتعني صفة لأي شيء مرتبط بثقافة الحواسيب او تقنية المعلومات او الواقع الافتراضي، فالسيبرانية تعني فضاء الانترنيت.

د- تعريف مصطلح الأمن السيبراني:

عرف بأنه امن الشبكات، والأنظمة والمعلوماتية، والبيانات، والمعلومات والأجهزة المتصلة بالأنترنت. وعليه فهو مجال يتعلق بإجراءات، ومقاييس، ومعايير الحماية المفروض اتخاذها، او الالتزام بها، لمواجهة التهديدات ومنع التعديات والحد من آثارها في أقسى واسوأ الأحوال.

وأيضا عرف بأنه: عبارة عن مجموع الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام غير للمصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية

[1] بن صابر، بلقاسم، وحيدرة محمد. "الهجمات السيبرانية ومواجهتها في ضوء القانون الدولي المعاصر ".مجلة حقوق الإنسان والحريات العامة، جامعة مستغانم، المجلد 2، العدد 4 (يونيو 2017)ص 185

[2] عادل عبد الصادق، "أسلحة الفضاء الالكتروني في ضوء القانون الدولي الإنساني"، القاهرة، المركز العربي لأبحاث الفضاء الالكتروني 2016ص 13

البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني. كما عرف الأمن السيبراني: بأنه النشاط او العملية او القدرة او الامكانية او الحالة التي يتم بموجبها حماية نظم المعلومات والاتصالات والمعلومات الواردة فيها او الدفاع عنها ضد الضرر او الاستخدام أو التعديل غير المصرح به او الاستغلال.[1]

الفرع الثاني: المفاهيم المرتبطة بالأمن السيبراني

هناك العديد من المفاهيم المرتبطة بالأمن السيبراني، ومن أهمها ما يلي:

ا- الفضاء السيبراني: وعرفته الوكالة الفرنسية لأمن أنظمة الإعلام وهي وكالة حكومية مكلفة بالدفاع السيبراني الفرنسي بأنه: فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الالية للمعطيات الرقمية.

فهو بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية، مكون من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين او مستعملين. كما ان هناك من عرف الفضاء السيبراني بوصفه الدراع الرابعة للجيوش الحديثة.

ا- الردع السيبراني: يعرف الردع السيبراني بأنه منع الاعمال الضارة ضد الأصول الوطنية في الفضاء والأصول التي تدعم العمليات الفضائية، ويرتكز الردع السيبراني على ثلاث ركائز هي عماد استراتيجية الدفاع السيبراني تتمثل في: مصداقية الدفاع، والقدرة على الانتقام، والرغبة في الانتقام

ب-الجريمة السيبرانية: مجموعة الأفعال والاعمال غير القانونية التي تتم عبر معدات او أجهزة الكترونية او شبكة الانترنت او تبث عبرها محتوياتها، وهي ذلك النوع من الجرائم التي تتطلب الالمام الخاص بتقنيات الحاسب الالي ونظم المعلومات لارتكابها او التحقيق فيها ومقاضاة فاعليها. فهي الجريمة المتصلة باستخدام تقنيات المعلومات والاتصالات.

ج-القوة السيبرانية: يعد جوزيف س ناي من أبرز المهتمين بالقوة السيبراني، حيث يعرفها بانها القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني، أي انها القدرة على استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني، والتأثير على الاحداث المتعلقة بالبيئات التشغيلية الأخرى وذلك عبر أدوات سيبرانية[2]

أهمية الأمن السيبراني: يعد الهدف الأسمى للأمن السيبراني هو:

تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحويه من بيانات

[1] د. جبور الأشقر،" السيبرانية: هاجس العصر "بيروت: المركز العربي للبحوث القانونية والقضائية2009 ،ص 26

[2] دحان حيزام القريطي: "الامن السيبراني وحماية امن المعلومات ". دار الفكر الجامعي، الاسكندرية2022 ص 14ص16

1.التصدي لهجمات وحوادث امن المعلومات التي تستهدف الأجهزة

2.سد الثغرات في أنظمة امن المعلومات

3.مقاومة البرمجيات الخبيثة، وما تحدثه من اضرار بالغة للمستخدمين

4.الحد من التجسس والتخريب الالكتروني على مستوى الحكومة والافراد[1]

المطلب الثاني: تطور الأمن السيبراني

الفرع الأول: نشأة الأمن السيبراني

ظهر الأمن السيبراني مع نهاية الحرب الباردة، وظهور مصطلح حرب الإنترنت أو الحرب السيبرانية، التي جاءت مع بداية اعتماد الدول على أجهزة الكمبيوتر في مؤسساتها وتطوير وحدة المعالجة المركزية في هذه الأجهزة، التي دخلت في عمل المؤسسات والحكومات وحتى في الحياة اليومية، واقتصر دور الأمن السيبراني في الفترة الأولى على الحماية من الفيروسات والبرمجيات الخبيثة.

وظهر أول فيروس رقمي في سبعينيات القرن العشرين على شبكة "أربانت"، إحدى أوائل الشبكات في العالم لنقل البيانات باستخدام تقنية تبديل الرزم، وكان على شكل رسالة نصية بسيطة لم تتسبب بأضرار تقنية لكنها دفعت إلى اتخاذ تدابير وقائية

وفي عام 1983، طوّر معهد ماساتشوستس للتقنية نظام اتصالات يعتمد على التشفير، أصبح أساسا لتطوير تقنيات الأمن السيبراني الحديثة.

وشكل ظهور الإنترنت ثورة نوعية في حياة البشرية، إذ بدأ استخدامه في المجالين الأمني والعسكري وتسابقت الدول في تطويره مع مطلع تسعينيات القرن العشرين، حتى سميت تلك الفترة بـ"الحرب السيبرانية الباردة" أو "سباق التسلح السيبراني"، وظهرت حينئذ هجمات التصيد الاحتيالية "فيشينغ" والتجسس الإلكتروني و"الهجوم الموزع لحجب الخدمة" (دي دي أو إس).

وظهرت الحاجة دوليا إلى وجود قوة غير مادية إلى جانب القدرات العسكرية والاقتصادية، فبدأت الدول تولي اهتمامها بالقوة السيبرانية لتأثيرها على المستويين المحلي والدولي.

ومع انفجار الثورة المعلوماتية ودخول العصر الرقمي، واعتبار عدد من الباحثين الفضاء السيبراني بمثابة المجال الخامس في الحروب بعد البر والبحر والجو والفضاء، ظهرت الحاجة لتوفير ضمانات أمنية، خاصة مع بداية ظهور التهديدات والجرائم السيبرانية مع دخول القرن الـ 21.

[1] مرجع نفسه، ص18

ودخل الأمن السيبراني ضمن حقل الدراسات الأمنية، وظهرت تقنيات متطورة مثل التشفير والأمان السحابي والكشف عن التهديدات بالذكاء الاصطناعي، ومع ذلك فإن الهجمات السيبرانية مجال معقد وسريع التطور، مما يستلزم استجابات أمنية سريعة تضاهي وتيرة نموه السريع

الفرع الثاني: الامن السيبراني كحقل معرفي

ومع تصاعد المخاطر، أصبح الأمن السيبراني عنصرا أساسيا في الأمن القومي، وبدأت الدول تتعامل مع الفضاء السيبراني بوصفه ساحة حرب جديدة، لا تقل أهمية عن البر والبحر والجو. فظهرت مفاهيم مثل "الحرب السيبرانية"، و"الردع السيبراني"، و"الهجمات الممولة من الدول"، كما شُكلت جيوش إلكترونية متخصصة للقيام بعمليات هجومية ودفاعية في الفضاء الرقمي. ودفع ذلك إلى تنظيم اتفاقيات دولية ومؤتمرات تُعنى بوضع أطر قانونية لأخلاقيات الحرب في الفضاء السيبراني، رغم استمرار التحديات المتعلقة بتحديد مصدر الهجمات، ومساءلة الفاعلين غير الحكوميين.

في الوقت ذاته، تطورت تقنيات الأمن السيبراني بشكل كبير، مع الاعتماد على الذكاء الاصطناعي والتعلم الآلي في الكشف الاستباقي عن التهديدات، وتطوير أنظمة تحليل السلوك، والتشفير المتقدم، وتقنيات المصادقة متعددة العوامل. كما بات للأمن السيبراني دور محوري في حماية البنى التحتية الحيوية مثل شبكات الكهرباء، والمياه، والنقل، والخدمات الصحية، مما عزز من مركزه في الخطط الاستراتيجية الوطنية والتنموية.

مع تسارع التحول الرقمي في تسعينيات القرن العشرين وبداية الألفية الجديدة، بدأ الأمن السيبراني يتحول من مجرد إجراءات وقائية بسيطة إلى منظومة متكاملة من السياسات والتقنيات والاستراتيجيات. فقد أدى انتشار الإنترنت وتوسع استخدام البريد الإلكتروني، والمواقع الإلكترونية، والأنظمة المتصلة بالشبكات إلى تضاعف التهديدات الرقمية، وظهور هجمات أكثر تعقيدًا كالهجمات الموزعة لحجب الخدمةDDoS) وهجمات التصيد الإلكتروني**(Phishing) ، وتسريبات البيانات الحساسة. هذا التحول فرض على الحكومات والشركات الكبرى تطوير بنى تحتية سيبرانية متقدمة، وإنشاء وحدات متخصصة للأمن السيبراني، وتبني معايير دولية لإدارة أمن المعلومات.

** هجمات إلكترونية تستهدف الأفراد أو المؤسسات لسرقة معلومات شخصية أو مالية من خلال خداعهم لإدخال هذه المعلومات في مواقع ويب مزيفة أو مشاركتها عبر البريد الإلكتروني أو الرسائل النصية

ومع تصاعد المخاطر، أصبح الأمن السيبراني عنصرا أساسيا في الأمن القومي، وبدأت الدول تتعامل مع الفضاء السيبراني بوصفه ساحة حرب جديدة، لا تقل أهمية عن البر والبحر والجو. فظهرت مفاهيم مثل "الحرب السيبرانية"، و"الردع السيبراني"، و"الهجمات الممولة من الدول"، كما شكلت جيوش إلكترونية متخصصة للقيام بعمليات هجومية ودفاعية في الفضاء الرقمي. ودفع ذلك إلى تنظيم اتفاقيات دولية ومؤتمرات تُعنى بوضع أطر قانونية لأخلاقيات الحرب في الفضاء السيبراني، رغم استمرار التحديات المتعلقة بتحديد مصدر الهجمات، ومساءلة الفاعلين غير الحكوميين.

في الوقت ذاته، تطورت تقنيات الأمن السيبراني بشكل كبير، مع الاعتماد على الذكاء الاصطناعي والتعلم الآلي في الكشف الاستباقي عن التهديدات، وتطوير أنظمة تحليل السلوك، والتشفير المتقدم، وتقنيات المصادقة متعددة العوامل. كما بات للأمن السيبراني دور محوري في حماية البنى التحتية الحيوية مثل شبكات الكهرباء، والمياه، والنقل، والخدمات الصحية، مما عزز من مركزه في الخطط الاستراتيجية الوطنية والتنموية. اللافت في هذا التطور هو أنه لم يكن استجابة فقط لتطور التكنولوجيا، بل كان مدفوعا أيضا بتغير طبيعة التهديدات: من قراصنة أفراد يسعون للعبث أو الشهرة، إلى مجموعات منظمة تمولها دول، أو تعمل لأهداف أيديولوجية أو اقتصادية. ونتيجة لذلك، أصبح الأمن السيبراني مجالا متعدد الأبعاد: تقني، استراتيجي، قانوني، وحتى أخلاقي كما أرى أن الاعتماد المتزايد على الذكاء الاصطناعي في هذا المجال يحمل فرصًا هائلة، لكنه يفتح الباب أيضا لتعقيد غير مسبوق في نوعية التهديدات، خصوصًا مع التطورات في الذكاء الاصطناعي التوليدي، الذي يمكن أن يستغل لتزوير الهويات، أو إنتاج برمجيات خبيثة أكثر قدرة على التمويه والتخفي..

اما على مستوى الجانب الممارساتي للدول فقد ارتبط ظهور الأمن السيبراني بظهور الهجمات السيبرانية والتي حدثت بسبب عاملين أساسيين:

الأول: باستحداث أجهزة الكمبيوتر في منتصف الخمسينات من القرن المنصرم كأداة لمعالجة وحفظ المعلومات رقميا، رافقه تضافر جهود عدد من الشركات الخاصة والعامة توج بتطوير وحدة المعالجة المركزية، وذلك لتسهيل المهام الموكلة له وقد تطور ذلك بصورة جدرة في العقود اللاحقة، حتى أصبح جهاز الكمبيوتر أساسا في عمل الكثير من المؤسسات الخاصة والعامة، فضلا عن الحياة اليومية.

اما الثاني: فهو ظهور الشبكة العنكبوتية (الانترنت)، الذي أحدث انقلابا مثيرا في حياة البشرية من خلال التواصل ونقل المعلومات بسرعة فائقة، وقد سارعت الدول في وتيرة استخدام الكمبيوتر لتحقيق قفزات نوعية في المجال الأمني والعسكري في مطلع التسعينيات من القرن المنصرم، وذلك حتى البعض أطلق عليها مصطلح الحرب السيبرانية الباردة او سباق التسلح السيبراني[1].

[1]: دحان حيزام، مرجع سابق ص16 ص18

المطلب الثالث: أنواع التهديدات السيبرانية.

أصبحت التهديدات السيبرانية من أبرز التحديات الأمنية المعاصرة التي تواجه الدول والمجتمعات في ظل تعاظم الاعتماد على الفضاء الرقمي في مختلف مجالات الحياة. وتتعدد أشكال هذه التهديدات، من أبرزها:

1. الهجمات على السرية: تشمل سرقة معلومات التعريف الشخصية، والحسابات المصرفية، او معلومات بطاقة الائتمان، حيت يقوم العديد من المهاجرين بسرقة المعلومات، ومن ثم بيعها على شبكة الانترنت المظلمة لكي يشتروها الاخرون، ويستخدموها بشكل غير شرعي

2. الهجمات على التوافر الهدف منها هو منع المستخدمين من الوصول الى بياناتهم الخاصة الى ان يدفعوا رسوما مالية، او فدية معينة.[1]

تتخذ التهديدات السيبرانية أشكالاً متعددة تهدف إلى إلحاق الضرر بالبنية الرقمية للدول أو الأفراد، وتمتد آثارها لتشمل الجوانب الاقتصادية والسياسية والأمنية. من بين أبرز هذه التهديدات

3. **الاحتيال الإلكتروني**: الذي يمارس غالبا عبر تقنيات الهندسة الاجتماعية أو الرسائل المزيفة بهدف الحصول على بيانات مالية أو شخصية، وغالباً ما تستخدم هذه البيانات في تمويل أنشطة غير مشروعة أو التأثير على نزاهة العمليات السياسية. كما يعد اختراق الشبكات من أبرز الأشكال الاستراتيجية للتهديدات السيبرانية، لا سيما عند استهداف الشبكات الحكومية أو الدفاعية، إذ ينظر إليه كأداة في حروب الجيل الخامس. كذلك، يمثل استغلال الثغرات الأمنية مدخلاً خطيرا للهجمات الرقمية، حيث تمكن المخترق من التسلل إلى الأنظمة من خلال نقاط ضعف برمجية، مما يؤدي إلى تسريب وثائق حساسة أو التأثير على قرارات حيوية في قطاعات السياسة والاقتصاد.

4. **ومن التهديدات الشائعة أيضًا برامج الفدية**: حيث تقوم هذه البرمجيات الخبيثة بتشفير ملفات الضحايا وتطالب بفدية مالية مقابل فك التشفير، مما قد يتسبب في أزمات اقتصادية وأمنية، خصوصًا عندما تستهدف مؤسسات حكومية أو بنى تحتية حيوية. وعلى الجانب الاقتصادي الرقمي، يُلاحظ انتشار التعدين غير المشروع للعملات الرقمية، والذي يتم عبر استخدام أجهزة الحاسوب الخاصة دون إذن لاستخراج العملات، وتُستغل أرباح هذه الأنشطة في تمويل منظمات غير قانونية. كما تُعد هجمات إسقاط الخدمة الموزعة (DDoS) من بين أخطر التهديدات، إذ تستهدف تعطيل المواقع الإلكترونية الحكومية أو المصرفية، مما يؤدي إلى زعزعة ثقة المواطنين في المؤسسات الرسمية وزيادة مستويات الاحتقان الداخلي[1].

[1] : دحان حيزام مرجع سابق ص 29

[1]اسراء تريسي ،2021"اسوء الهجمات الالكترونية " تاريخ الزيارة 2025/06/03 من عربي بوست https://arabicpost.net/

5 الهجمات السيبرانية الموجهة: تنفذ هذه الهجمات من قبل دول أو جماعات منظمة ضد أهداف استراتيجية محددة، مثل المؤسسات الأمنية أو شخصيات دبلوماسية، ما يجعلها سلاحاً جديداً في معادلة الصراع الدول

5. **تهديدات أمن الأجهزة المحمولة: بعد** جديد في معادلة الأمن القومي السيبراني في ظل تزايد الاعتماد على الهواتف الذكية في الحياة اليومية، سواء في التواصل أو إدارة البيانات أو حتى العمل الحكومي، برزت تهديدات أمن الأجهزة المحمولة كإحدى أخطر الثغرات التي يمكن أن تُستغل من قبل الفاعلين غير الحكوميين أو حتى الدول ذات الأجندات المعادية.

يمكن للمجرمين السيبرانيين استغلال الثغرات الأمنية في أنظمة تشغيل الهواتف الذكية أو عبر التطبيقات غير الأمنة المثبتة عليها، ما يسمح لهم بالوصول إلى بيانات خاصة مثل المحادثات، الموقع الجغرافي، الصور، وحتى كلمات المرور. وتعد هذه الهواتف هدفاً جذاباً بسبب كثافة المعلومات الشخصية والمهنية المخزنة عليها.

أخطر ما في هذا التهديد هو أنه لا يقتصر على الأفراد فحسب، بل قد يمتد ليطال مسؤولين حكوميين أو دبلوماسيين، مما يعرض أسراراً حساسة للاختراق والتسريب، ويشكل بذلك تهديداً مباشراً للأمن القومي. وتزداد هذه المخاطر في سياقات النزاع أو التوترات الجيوسياسية، حيث يمكن توظيف هذه الاختراقات كوسيلة لجمع المعلومات الاستخباراتية أو شن حملات تشويه أو ابتزاز سياسي.

كما أن تسجيل ضغطات المفاتيح (Keylogging) والتقاط صور الشاشة (Screenshot) باستخدام برمجيات ضارة، قد يؤدي إلى انتهاك مباشر لخصوصية الأفراد والمؤسسات، مما يبرز الحاجة إلى نهج أمني شامل لا يقتصر على الجانب التقني، بل يشمل التوعية الرقمية وصياغة سياسات وقوانين تحمي الأمن السيبراني الوطني.

يتقاطع أمن الأجهزة المحمولة مع مفاهيم السيادة الرقمية والحرب السيبرانية الحديثة، إذ أصبح الهاتف المحمول أداة حساسة يمكن عبرها التأثير على صنع القرار السياسي والأمني. ولذلك، لا بد من تعزيز آليات الرقابة، وتطوير تشريعات وطنية ودولية تنظم أمن الفضاء السيبراني المتعلق بالأجهزة الذكية، خاصة في ظل تسارع تطور التكنولوجيا وتنوع أدوات الاختراق.

في ضوء هذه التهديدات، يتضح أن الفضاء السيبراني أصبح ساحة جديدة للصراع الجيوسياسي، حيث توظف الهجمات الإلكترونية كأداة ضغط واستهداف استراتيجي، وهو ما يفرض على الدول تحديث منظومتها الدفاعية السيبرانية وتفعيل التعاون الدولي في مجال الأمن الرقمي. كما أن هذه التهديدات تثير تساؤلات مهمة

حول سيادة الدول في الفضاء الرقمي، ومشروعية الرد السيبراني، ودور القانون الدولي في تنظيم النزاعات السيبرانية[1].

المبحث الثاني: مفهوم الأمن المجتمعي

لم يعد الأمن في العصر الحديث مفهوماً مقتصراً على حماية الحدود أو المؤسسات، بل اتسع ليشمل أمن الأفراد والمجتمعات، في ظل تهديدات غير تقليدية ترتبط بالعنف الرمزي، والتحولات القيمية، والتفكك الاجتماعي، والتدخلات الخارجية غير المرئية. يندرج مفهوم "الأمن المجتمعي" ضمن هذه المقاربات الجديدة للأمن، ويعكس التوجه نحو مقاربات شاملة تركز على الاستقرار الداخلي والتماسك الاجتماعي. يستعرض هذا المبحث تطور المفهوم، أبعاده النظرية، اختلافه عن الأمن الاجتماعي، ومكوناته الأساسية، مع إبراز علاقته بالأمن الوطني وأهمية تماسك المجتمع في مواجهة التهديدات المعاصرة، خاصة السيبرانية منها.

المطلب الأول: تعريف الأمن المجتمعي واهميته في الاستقرار الوطني

شهد مفهوم الأمن في العلاقات الدولية تحولات جذرية، خصوصا مع الانتقال من المقاربات الواقعية الكلاسيكية إلى المنظورات المعاصرة التي توسّعت في تحليل طبيعة التهديدات. فلطالما ركزت الأدبيات التقليدية على الأمن العسكري، واعتبرت الدولة الفاعل المحوري في النظام الدولي، حيث ربط الأمن بالقدرة على مواجهة التهديدات الخارجية باستخدام أدوات القوة الصلبة، مثل الجيوش والتحالفات العسكرية. وقد ارتبط هذا المفهوم الضيق للسلم والأمن بفترات الحروب والصراعات التي هيمنت على النظام الدولي، لا سيما خلال الحرب الباردة، ما جعل الأمن يُختزل في مبدأ الردع والدفاع الوطني.

غير أن تحولات البيئة الدولية في العقود الأخيرة، وخصوصا بعد نهاية الثنائية القطبية، أدت إلى بروز تهديدات غير تقليدية مثل الإرهاب، التغير المناخي، الأوبئة، الجرائم العابرة للحدود، والتهديدات السيبرانية. هذه التحولات فرضت ضرورة إعادة تعريف الأمن من جديد، ليصبح أكثر شمولية وتعقيدا، فيما يُعرف بالأمن الإنساني أو الأمن متعدد الأبعاد، حيث لم يعد التركيز فقط على حماية الدولة من الهجوم العسكري، بل شمل أيضًا حماية الأفراد وتأمين استقرار المجتمعات.

[1] إبراهيم احمد، "الجريمة الالكترونية في القانون الدولي " مجلة جامعة جيهان أربيل للعلوم الإنسانية و الاجتماعية ،المجلد 6،العدد2، 2022 ص 147

الفرع الأول مفهوم الأمن المجتمعي:

لا يمكن حصر الأمن البشري في تعريف موحد أو مقاربة واحدة، إذ إن فهمه يظل مرهونً بالسياقات الزمنية والمكانية التي ينشأ فيها. فلكل دولة أو منطقة أولوياتها الأمنية الخاصة التي تعكس طبيعة التهديدات التي تواجهها. ففي السياق العربي، وتحديدًا في الجزائر، تبرز قضايا مثل الاستقرار السياسي، ومحاربة الفقر، وتعزيز الوصول إلى الخدمات الأساسية، بوصفها أولويات للأمن البشري. بينما تختلف هذه الأولويات في عدد من الدول الإفريقية، حيث تعد النزاعات الداخلية، والتهجير، وانعدام العدالة الاجتماعية من أبرز التحديات الأمنية التي تهدد الإنسان في حياته اليومية.

ويكشف هذا التعدد في المقاربات أن الأمن البشري ليس مفهومًا جامدا، بل هو إطار مرن يتشكل تبعًا لمحددات داخلية وخارجية، ويخضع لتغيرات البيئة الدولية والمحلية على السواء. وبالتالي، فإن أي مقاربة للأمن البشري لا بد أن تأخذ في الحسبان الخصوصيات الثقافية والسياسية لكل مجتمع، دون السقوط في التعميم أو الإسقاط النظري المجرد[1].

وهذا قد عرف باري بوزان الأمن المجتمعي بأنه القدرة على المحافظة على استمرارية الأنماط التقليدية للغة و الثقافة و الهوية والعادات فالتغيرات الطارئة على مستوى الدولة و المجتمع قد تؤثر سلبا على الخصائص الهوياتية للجماعات بشكل قد يسهم في اختراق خصوصيتها ونسيجها المجتمعي الأصلي و هذه التطورات قد تكون سببا في بروز قيم دخيلة لا تتوافق مع النسيج المجتمعي الذي كان سائدا من قبل وبالنسبة لمفهوم الأمن المجتمعي من منظور الأمن الإنساني فيمكن القول انه شعور الفرد بانتمائه للجماعة او مجتمع محلي او منظمة او جماعة عنصرية او عرقية يمكن ان توفر لأعضائها هوية ثقافية وهذه الجماعة توفر لمساندة العملية له.[2]

يشير "وايفر" إلى أن الأمن المجتمعي بمفهومه الواسع يعني "التقوية الذاتية لهوية الجماعات، والحفاظ على تنوعها وتميزها عبر الزمان والمكان" فالتطورات التكنولوجية وما لها من تأثيرات على الأفراد والمجتمعات قد تنعكس سلبا على الهوية الوطنية والقومية، كما أن بروز النموذج العولمي وتعاظم دوره في مختلف الدول، قد يسهم هو الآخر في طمس وتشويه هويات الأفراد وانتماءاتهم في ظل التأثر بالمد الغربي والقيم الدخيلة، خاصة في ظل تزايد دور وسائل الاعلام والاتصال واستهدافها لقاعدة جماهيرية كبيرة بمختلف الفئات الاجتماعية، وسهولة استخدامها وإمكانية إتاحتها على نطاق أوسع، إلى أن الأمر الذي يستدعي الإشارة اليه هو أنها خاضعة وتابعة للقوى الكبرى، حيث تمتلك هذه الأخيرة سلطة التأثير على وسائل الاتصال الجماهيري، والتي تتيح لها نشر أفكارها وايديولوجيتها والترويج لسياستها وإقناع الرأي العام بها، ما يكسبها تعاطفا وقبول حتى وإن كانت منافية لقيم المجتمع ومخالفة لقواعد القانون الدولي، وهنا تجدر الإشارة إلى أن الولايات

[1] محمد أمين، خديجة عرفة، "الأمن الإنساني: المفهوم والتطبيق في الواقع العربي" الرياض: جامعة نايف العربية للعلوم الأمنية، 2009،ص 45ص46

[2] جميلة علاق، "الأمن المجتمعي: مقاربة في المفهوم والعناصر"، مجلة البحوث السياسية والإدارية، العدد 10 (الجزائر، 2017)، ص 104.

المتحدة الأمريكية ورغم انتهاكها لسيادة بعض الدول وتدخلها في الشؤون الداخلية لها، وارتكابها لجرائم يعاقب عليها القانون، إلى أنها غالبا ما تبرر توجهاتها وسلوكياتها على أنها في إطار مكافحة الإرهاب والحد من أشكال الجريمة المنظمة، وهو ما حدث عند اجتياحها للعراق واتهامها لها على امتلاكها للسالح النووي كذريعة للتدخل، ورغم اتضاح الوضع إلى أنها ظلت في نظر الدول الأخرى كحامي لحقوق الانسان ووحدة فعالة في الساحة الدولية مخول لها بإرساء السلم والأمن.[1]

إن مفهوم الأمن المجتمعي في شقه الواسع أصبح يتضمن مختلف الجوانب المادية والاقتصادية، فالفقر والأوضاع المعيشية وانتشار البطالة والأمراض وتدني الدخل الفردي، كلها أصبحت متغيرات أساسية أسهمت في التحول من التعاريف التقليدية التي تركز على الجوانب المعنوية إلى التحول نحو صياغة مفهوم جديد، بالإضافة إلى البعد العرقي والديني فقد أصبح البعد الاجتماعي يلعب دورا أساسيا في تحقيق الأمن المجتمعي في الدول، لذلك نجد أنه غالبا ما تتراجع مؤشراته في الدول المتخلفة ودول العالم الثالث التي لم تعد قادرة على تلبية حاجات مواطنيها الأساسية، في ظل عجز الدولة على تقديم برامج تنموية لشعوبها، وهو ما يجعل الأفراد والمواطنين في حالة تمرد وعصيان بسبب رفضهما للأوضاع القائمة، وخو ما يدخلهم في صراعات عمودية وأفقية تكون ما بين السلطة الحاكمة والجماعات والأفراد، أو ما بين الجماعات فيما بينهم، ما ينتج عنه معضلة أمنية مجتمعية تكون لها تداعياتها على المستوى الداخلي والخارجي.

الامن المجتمعي والامن الاجتماعي:

هناك فرق بين مفهوم الامن المجتمعي والامن الاجتماعي، اذ لا يمكن ان يكون الأول مرادفا للثاني فالأمن المجتمعي اشمل ويضم عدة ابعاد من بينها الامن الاجتماعي، هذا الأخير الذي ارتبط بإشباع الحاجات الإنسانية ويعرف بانه سلامة الأفراد والجماعات من القتل والاختطاف والاعتداء على الممتلكات بالتخريب او السرقة.

فالأمن الاجتماعي يركز بدرجة أكبر على الرفاهية وتحسين نمط المعيشة وتوفير سبل الراحة من خلال غياب التهديد المادي الذي يقوض امن الفرد داخل المجتمع. كما ويعد الأمن الاجتماعي والهوية الوطنية من العناصر الأساسية للأمن المجتمعي، لذا فهناك علاقة وطيدة بينهما.[1]

الفرع الثاني: أهمية الأمن المجتمعي في الاستقرار الوطني:

يركز مفهوم الأمن الموسع على الترابط والتداخل بين القطاعات الأمنية المختلفة، ومن بينها الأمن المجتمعي ووفقا لمنظور باري بوزان، فإن هذه المجالات الأمنية لا تعد بالضرورة مستقلة عن بعضها البعض، بل غالبا ما تتفاعل وتتشابك بدرجات متفاوتة. ففي بعض الحالات، لا يذكر مصطلح "الأمن المجتمعي" كتصنيف مستقل، بل يُفهم ضمنيًا ضمن إحدى الوحدات الأمنية الخمسة، بحيث تتضمن كل وحدة أنماطًا متنوعة من الأمن (كالأمن العسكري، السياسي، الاقتصادي، البيئي، والمجتمعي). لذلك، يصبح من الضروري

[1] المرجع نفسه، ص105

[1]"المجلة الجزائرية للأمن والتنمية"، جانفي 2023، المجلد12، العدد01، ص166

تحليل طبيعة العلاقة بين الأمن المجتمعي وبقية الأبعاد الأمنية لفهم مدى التداخل والتكامل بينها في السياقات الإقليمية أو القومية.[1]

يعد الأمن السياسي أحد الركائز الأساسية لمفهوم الأمن الموسع، حيث يشير إلى وجود نظام سياسي ديمقراطي يضمن احترام حقوق الإنسان ويحد من ممارسات الاستبداد والتسلط. يرتبط الأمن السياسي ارتباطا وثيقا بأداء هياكل الدولة السياسية، والتي تعد المدخل الأساسي للتأثير على مختلف أبعاد الأمن الأخرى، وفي مقدمتها الأمن المجتمعي.

فالدولة، من خلال أدائها السياسي، تمتلك القدرة على التأثير في فعالية باقي القطاعات الأمنية، بما فيها الاجتماعي والاقتصادي. وتتحقق متطلبات الأمن السياسي عبر مجموعة من العوامل، أبرزها تعزيز "مبادئ الديمقراطية والحكم الرشيد والمساواة بين المواطنين"، لا سيما في الدول ذات التعددية المجتمعية (اللغوية، الدينية، أو العرقية). فالتهميش السياسي لأي مجموعة قد يؤدي إلى اضطرابات أمنية قد تصل إلى حدود المطالبة بالانفصال، خاصة إذا حُرمت هذه الفئة من حقوق تُصنف ضمن الأمن السياسي.

وتشمل هذه الحقوق:

- التمثيل السياسي العادل في المناصب العليا للدولة بما يتناسب مع نسبتها السكانية
- الحق في إنشاء أحزاب سياسية ومنظمات مجتمع مدني تعبّر عن تطلعاتها
- النص الدستوري الصريح على حقوق الأقليات أو المجموعات المجتمعية، بما يضمن ممارستها لحياتها الثقافية والاجتماعية والسياسية بحرية[2].

ويشكل الأمن الاقتصادي أحد الأبعاد المحورية في المنظومة الأمنية الشاملة، إذ يرتبط بقدرة الدولة على توفير الحاجات الأساسية للأفراد والجماعات، بما يضمن استقرارها واستمراريتها. ويقصد بالأمن الاقتصادي التحرر من الخوف والحاجة، أي تأمين حياة المجتمع من مظاهر الفقر والجوع والمرض، وضمان سبل العيش الكريم لكافة المواطنين.

ولا يقتصر هذا المفهوم على مجرد تحسين المؤشرات الاقتصادية، بل يمتد ليشمل العدالة الاجتماعية والتنمية البشرية، من خلال تمكين الإنسان، وحماية كرامته، وصون حقوقه الأساسية. ومن هذا المنطلق، يمثل الأمن الاقتصادي أداة وقائية مبكرة لحماية المنجزات الاقتصادية القائمة والمستهدفة، وذلك عبر خطط تضمن الحياة الكريمة للأجيال القادمة، خصوصًا من خلال:

1.توفير السكن اللائق
2.ضمان فرص العمل المناسبة

[1] منصوري رؤوف، "الهجرة السرية من منظور الامن الإنساني"، (مصر: مكتبة الوفاء القانونية، ط 1، 2016)، ص 18

[2] وليد عبد الحي، "قياس النزعة الانفصالية للأقليات في الوطن العربي"، جدليات الاندماج الاجتماعي، الدوحة: المركز العربي للأبحاث ودراسة السياسات، 2014،ص104ص105

3.تحسين مستوى التعليم

4.وتطوير الخدمات الصحية[1]

ويعد الأمن المجتمعي أساسا محوريا في دعم الأمن العسكري وتحقيق الاستقرار الوطني، إذ لا يمكن تصور قدرة الدولة على حماية حدودها ومصالحها الاستراتيجية ما لم تكن متماسكة داخليا، ويشعر أفراد مجتمعها بالأمان والانتماء والعدالة. فغياب العدالة الاجتماعية، وتفاقم التهميش أو الفقر، وغياب الثقة بين المواطنين ومؤسسات الدولة، كلها عوامل تضعف الجبهة الداخلية، وتقوض فاعلية المنظومة العسكرية مهما بلغت قوتها التقنية..

لذا، فإن بناء مجتمع آمن ومتوازن يعد شرطا أساسيا لتعزيز الأمن العسكري وضمان استقرار الدولة ووحدتها في وجه التحديات الداخلية والخارجية.

[1] سليمان الطفيل، "المعركة الاقتصادية القادمة وضرورة الامن الاقتصادي " 2017 ، دار الفكر الجامعي ص41

المطلب الثاني: مكونات الأمن المجتمعي

الفرع الأول: أنماط الامن المجتمعي وعلاقتها بالنسيج الاجتماعي

يعد الأمن المجتمعي أحد الأبعاد الجوهرية في بناء استقرار الدول والحفاظ على تماسكها الداخلي، إذ يتجاوز المفهوم التقليدي للأمن المرتبط بالمجال العسكري والسياسي، ليشمل أنماطاً أوسع تتعلق بسلامة النسيج الاجتماعي، وضمان استقرار القيم والهوية والثقافة، وتأمين احتياجات المواطنين في محيطهم المحلي. ومن هذا المنطلق، يمكن تحديد أبرز مكونات الأمن المجتمعي في المحاور الآتية:

1.**الأمن الثقافي والفكري:** يتعلق هذا المكون بحماية المجتمع من الغزو الثقافي والفكري الذي يستهدف تفكيك القيم والمرجعيات، من خلال التأثير على منظومته الأخلاقية وهويته الحضارية. ويعد هذا الجانب من أكثر المكونات تعرضًا للتهديدات السيبرانية عبر الحملات الإعلامية المضللة، وترويج الأفكار المتطرفة أو الانهزامية[1].

2.**الأمن الاقتصادي**: مثل الأمن الاقتصادي حجر الأساس في استقرار المجتمعات وتماسكها، إذ أن تلبية الاحتياجات المعيشية الأساسية وضمان توزيع عادل للثروات من شأنه تعزيز الثقة بين الدولة والمواطنين، وتقوية الانتماء الوطني، وتقليص الهشاشة الاجتماعية. ويتجلى الأمن الاقتصادي في تمكين الأفراد من الوصول إلى فرص العمل، والخدمات الأساسية، والحماية من التقلبات الاقتصادية الحادة التي قد تفضي إلى اضطرابات.

في هذا الإطار، تعد التهديدات السيبرانية من أبرز المخاطر المستجدة التي تهدد الأمن الاقتصادي، نتيجة تنامي الاعتماد على الرقمنة والتكنولوجيا في كل من البنوك، الأسواق، نظم التأمين، والجمارك. وتشكل الهجمات الإلكترونية والاحتيال الرقمي والابتزاز عبر الإنترنت أدوات فعالة لزعزعة النظام الاقتصادي للدول، خاصة تلك التي تفتقر إلى استراتيجيات دفاع إلكترونية متطورة[2].

وقد أكدت تقارير دولية أن التهديدات السيبرانية باتت تمثل خطرًا متصاعدًا على الاقتصادات النامية، إذ تُقدّر الخسائر الناجمة عن الهجمات الإلكترونية عالميًا بمليارات الدولارات سنويًا، مما يُلزم الحكومات بوضع سياسات لحماية الاقتصاد الرقمي وتعزيز الوعي المالي الرقمي لدى الأفراد والمؤسسات[3].

3.**الأمن الاجتماعي**: يشكل الأمن الاجتماعي الركيزة الأساسية للحفاظ على الانسجام والاستقرار داخل المجتمع، فهو يُعنى بتحقيق العدالة الاجتماعية، وتعزيز التماسك بين الأفراد والفئات المختلفة، ومنع الانقسامات الطبقية أو العرقية أو الدينية التي قد تُفضي إلى اضطرابات داخلية تهدد النسيج الوطني.

[1] بن حدو محمد، "التهديدات السيبرانية كعامل مؤثر على الاقتصاد الوطني"، مجلة العلوم السياسية والقانون، المجلد 9، العدد 6 (2022):ص 112.

[2] Antonio Missiroli, The Future of Cybersecurity in Europe (Paris: EU Institute for Security Studies, 2018), 35.

[3] OECD, The Economic and Social Impact of Cybersecurity Failures (Paris: OECD Publishing, 2020), 23.

ويتجسد الأمن الاجتماعي من خلال مكافحة الفقر، تحسين مستوى المعيشة، الحدّ من التهميش، ومحاربة الظواهر الاجتماعية الخطيرة مثل العنف الأسري، الانحراف، الإدمان، والجريمة المنظمة[1]

4 **الأمن القانوني والمؤسسي:** هو أحد أعمدة الأمن المجتمعي، ويتمثل في ضمان وجود منظومة قانونية عادلة وفعالة، ومؤسسات رسمية تطبق القانون على الجميع دون تمييز، وتحمي الحقوق الأساسية للأفراد مثل الحق في الخصوصية، الأمن الشخصي، حرية التعبير، والعدالة الاجتماعية.

يشمل هذا المكون:

- وجود قوانين واضحة ومستقرة تحكم العلاقات الاجتماعية والاقتصادية والسياسية.
- استقلال القضاء وكفاءة الأجهزة الأمنية والمؤسسات التنفيذية.
- القدرة المؤسسية على تطبيق القانون ومكافحة الجريمة بأشكالها المختلفة، خصوصًا الحديثة منها كالجريمة السيبرانية.
- ثقة المواطن في الدولة ومؤسساتها كضمانة للعدالة والمساواة وحماية الحقوق[2].

الفرع الثاني: التهديدات السيبر انية وتأثيرها على الأمن القانوني والمؤسسي

مع التوسع في الفضاء الرقمي، أصبحت الهجمات السيبرانية تمثل تحديا بالغا للأنظمة القانونية إذ:

- تكشف عن فجوات تشريعية حيث تسبق التكنولوجيا التشريعات في كثير من الأحيان، مما يخلق فراغات قانونية تُستغل من قبل مجرمي الفضاء السيبراني.
- تتطلب تحديثا دائمًا للقوانين وتدريب الكوادر القضائية والأمنية على آليات المواجهة الرقمية.
- تؤثر على مصداقية المؤسسات عندما تعجز عن حماية البيانات أو الاستجابة بفعالية للاختراقات، مما يؤدي إلى فقدان ثقة المواطن.
- في الدول النامية ومنها الجزائر، تتفاقم هذه التحديات بفعل البيروقراطية، نقص الإمكانات التقنية، والتنسيق المحدود بين الجهات.

وتؤثر التهديدات السيبرانية بشكل مباشر على فعالية واستقرار المؤسسات العامة، بما في ذلك الهيئات الحكومية، الإدارات، والمرافق الحيوية:

- تعطيل الخدمات العمومية :مثلما يحصل في هجمات حجب الخدمة أو برمجيات الفدية، والتي قد تؤدي إلى شل خدمات المستشفيات، أنظمة الدفع الإلكتروني، أو إدارة الوثائق الرسمية.

[1] فتحي التريكي، "سوسيولوجيا الأمن: قراءة في مفاهيم التماسك المجتمعي"، مجلة الفكر المعاصر، العدد 12 (2016): ص 88.

[2] د. عبد الحق لخذاري، "مبدأ الامن القانوني ودوره في حماية حقوق الانسان"، كلية الحقوق والعلوم السياسية بجامعة تبسة 2016.ص3

- استهداف البنى التحتية الرقمية للمؤسسات :مما يعرض قواعد البيانات المركزية للضياع أو السرقة، ويؤثر في اتخاذ القرار الإداري المبني على بيانات دقيقة.

- ضرب استقلالية القرار المؤسساتي من خلال التلاعب بالمعطيات الرقمية التي تستند إليها المؤسسات في بلورة السياسات، أو عبر التدخل في عمليات التصويت أو الإحصاء أو التسجيلات الرسمية.

- زعزعة هيبة الدولة فكلما أظهرت مؤسسات الدولة كعاجزة عن حماية نفسها في الفضاء الرقمي، تقلصت هيبتها أمام المواطنين وأمام الفاعلين الدوليين[1].

[1] رغدة البهي، "الردع السيبراني: المفهوم، والإشكاليات، والمتطلبات"، مجلة الدراسات الإعلامية، العدد 12 (2018) ص204 ص205.

المطلب الثالث: التحديات التي تواجه الأمن المجتمعي في الجزائر

الفرع الأول: التحديات القيمية والثقافية

يمثل الأمن المجتمعي أحد أهم ركائز الاستقرار الوطني في الجزائر، كونه يرتبط ارتباطا وثيقا بحماية الأفراد والمجتمع من مختلف التهديدات التي تستهدف وحدته وتماسكه، سواء كانت تهديدات تقليدية مثل الجريمة والانحراف، أو مستجدة كالتطرف الديني، والتحولات الثقافية السلبية، والتهديدات السيبرانية التي باتت تشكل خطرا حقيقيا على النسيج الاجتماعي. غير أن هذا الأمن المجتمعي يواجه اليوم تحديات متعددة، تتطلب تضافر جهود الدولة والمجتمع المدني لمواجهتها.

من أبرز التحديات التي تعترض الأمن المجتمعي في الجزائر هو التحول القيمي والثقافي السريع، خاصة بين أوساط الشباب، نتيجة الانفتاح غير المنضبط على العالم الرقمي، وتنامي تأثير مواقع التواصل الاجتماعي. حيث يُلاحظ تراجع في بعض القيم الجماعية، وصعود لأنماط فردانية تؤثر على مستوى التضامن والانتماء الوطني، ما قد ينعكس سلبًا على مستوى الاستقرار المجتمعي وان الأمن المجتمعي في الجزائر يعاني من هشاشة في المنظومة القيمية، ناجمة عن التأثيرات الخارجية وتراجع دور مؤسسات التنشئة الاجتماعية، وهو ما يهدد الانسجام الاجتماعي ويضعف مناعة المجتمع ضد التحديات الداخلية والخارجية[1]

اضافة إلى ذلك، تعد البطالة والفقر من العوامل الهيكلية التي تساهم في زعزعة الأمن المجتمعي، كونها تدفع بعض الفئات إلى تبني سلوكيات غير قانونية أو الانسياق نحو التطرف أو الهجرة غير الشرعية، ما يشكل ضغطا كبيرا على الاستقرار الداخلي. كما تعد الهشاشة الأمنية في المناطق الحدودية تحديا كبيرا، حيث ترتبط تلك المناطق بأنشطة التهريب والجريمة المنظمة العابرة للحدود، التي تُغذي أحيانا أنماطا من العنف والانفلات الأمني.

من جانب آخر، يبرز التهديد السيبراني كأحد المهددات الحديثة للأمن المجتمعي، حيث باتت شبكات الإنترنت ساحة لنشر خطاب الكراهية، والتضليل الإعلامي، والتحريض على العنف، مما يفرض على الدولة تعزيز أدوات المراقبة السيبرانية، وتحديث التشريعات، مع ضمان عدم المساس بالحريات الأساسية. إلى أن تحقيق الأمن المجتمعي لا يكون فقط من خلال الوسائل الأمنية التقليدية، بل يتطلب استراتيجيات شاملة تتضمن إصلاحات اجتماعية واقتصادية، وترسيخ ثقافة المواطنة، وتعزيز الثقة بين المواطن والدولة

وعليه، فإن مواجهة التحديات المتعددة التي تهدد الأمن المجتمعي في الجزائر تقتضي العمل على إعادة الاعتبار للمدرسة والأسرة كفاعليْن رئيسيَّيْن في التنشئة الاجتماعية، وتفعيل آليات الرقابة المجتمعية، وتعزيز مشاركة الشباب في الحياة العامة، بما يحقق الوقاية من الانحراف ويكرس التماسك الوطني.[2]

[1] عبد الكريم بوسريح،" الأمن المجتمعي في الوطن العربي: مقاربات نظرية ودراسة حالة الجزائر" (طباعة: دار الهدى، 2021)،ص 189.

[2] صالح بوشعير،" الأمن القومي الجزائري بين التهديدات الداخلية والتحولات الإقليمية "(الجزائر: الدار الجامعية، 2019)،ص 143.

كما أن الاستخدام المتزايد لشبكات التواصل الاجتماعي يؤثر في تفاعلات الأفراد مع الأخرين في الواقع بشكل سلبي وتبرز مظاهر هذا الاستخدام على مستوى العديد من المشكلات.

تعد التهديدات السيبرانية من بين أخطر التحديات التي تواجه الدول الحديثة، نظرا لما تسببه من أضرار مباشرة وغير مباشرة على المؤسسات السيادية والبُنى التحتية الحيوية. فهي تستهدف أساسا المعلومات الحساسة والأنظمة الرقمية لمؤسسات الدولة، مما يؤدي إلى زعزعة الثقة العامة وتقويض مصداقية السلطات أمام المواطنين.

وتكمن الخطورة الحقيقية لهذه التهديدات في قدرتها على خلق حالة من الارتباك والشك، سواء عبر نشر معلومات مضللة أو من خلال اختراقات تستهدف الأمن العام والاقتصاد الوطني. وفي ظل الانفتاح التكنولوجي والاعتماد المتزايد على الوسائل الرقمية، أصبحت أدوات الهجوم السيبراني أكثر تطورًا وأقل تكلفة، ما يجعلها متاحة حتى لجهات غير دولية.

ولذلك، فإن إضعاف أمن الدولة السيبراني لا يمس فقط بقدرتها على حماية مصالحها الحيوية، بل يؤثر أيضا على تماسكها الداخلي وقدرتها على الحفاظ على استقرارها السياسي والاجتماعي. وهو ما يستدعي تبني استراتيجيات وطنية شاملة لتعزيز الدفاعات الرقمية، ورفع مستوى الوعي لدى الأفراد والمؤسسات حول طبيعة هذه المخاطر وسبل مواجهتها[1].

الفرع الثاني: الجريمة المنظمة والتطرف كتحديات أمني ومجتمعي

1. الجريمة المنظمة في الجزائر:

تعد الجريمة المنظمة واحدة من التحديات الأمنية الكبرى التي تواجه الجزائر في السنوات الأخيرة، نظرا لتعقيداتها وامتداداتها العابرة للحدود، وتأثيرها المباشر على استقرار الدولة وأمن المجتمع. وهي تشمل مجموعة من الأنشطة غير المشروعة التي تدار من قبل شبكات إجرامية منظمة تسعى لتحقيق أرباح كبيرة، وتتسم بالتخطيط المسبق، التقسيم الوظيفي، والاستمرار الزمني.

أشكال الجريمة المنظمة في الجزائر:

تشمل الجريمة المنظمة في الجزائر عدة مظاهر، أبرزها:

- **تهريب المخدرات** :خاصة من منطقة الساحل عبر الحدود الجنوبية للبلاد.
- **الاتجاربالبشروتهريب المهاجرين** :الجزائر تعد نقطة عبور رئيسية للمهاجرين غير الشرعيين المتجهين نحو أوروبا.
- **تهريب السلع والأسلحة** :خاصة في المناطق الحدودية مع مالي، النيجر، وليبيا.

[1] جهاد بدة، "مفاهيم العلاقات الدولية التخطيط الاستراتيجي لأمن"، القاهرة دار الكتاب،2015الحديث ص662

- **الفساد المالي والإداري** :حيث ترتبط بعض شبكات الجريمة المنظمة بمصالح داخل مؤسسات رسمية، مما يصعب مكافحتها[1].

2. الإرهاب في الجزائر:

تشهد الساحة الأمنية الجزائرية كغيرها من الدول العديد من المخاطر والتهديدات التي فرضتها الثورة التكنولوجية الحديثة، خاصة بعد انتشار وسائل التواصل الاجتماعي والعديد من المواقع الالكترونية التي تحمل أفكارا هدامة تهدد استقرار الوطن ووحدته، وتدعو الى نشر الفوضى والعنف والتطرف والكراهية والانقسام. ومن أهم المخاطر التي تترتب عن استخدام التكنولوجيا الحديثة على الأمن الجزائري الإرهاب الالكتروني .ويقصد به " العدوان أو التخويف أو التهديد ماديا أو معنويا باستخدام الوسائل الإلكترونية الصادر من الدول أو الجماعات أو الأفراد على الإنسان في دينه، أو نفسه، أو ويعتبر أحد عرضه، أو عقله، أو ماله، بغير حق بشتى صنوفه وصور الإفساد في الأرض ."أخطر التهديدات التي تستهدف أمن جميع الدول بما في ذلك الدولة الجزائرية[2]

وهذا ما أكده اللواء مناد نوبة، القائد العام للدرك الوطني الجزائري في كلمة له ألقاها بمناسبة افتتاح الندوة الدولية حول "الأمن السيبراني "، حيث قال: "إن الإرهاب الإلكتروني بات من أخطر الجرائم التي تستهدف الجزائر، من خلال تنامي مظاهر الترويج لكل أشكال العنف والإرهاب والتطرف، باستعمال أحدث التقنيات التكنولوجية خاصة شبكات التواصل الاجتماعي والمنتديات الإلكترونية. "ولذلك دعا إلى إطلاق خلايا أمنية متخصصة هدفها العمل على" تعزيز إجراءات الرقابة لحماية المواطن الجزائري، وخاصة عنصر الشباب، من مثل هذه الجرائم الإلكترونية الخطيرة جداً على استقرار البلاد. "وذلك من خلال قيامها بتعقب وملاحقة كل الأنشطة المتعلقة بالتجنيد للإرهاب والإجرام المنظم العابر للحدود، وتكييفها بالوسائل التكنولوجية العصرية." وذلك يتطلب حسبه ضرورة "التسلح بكل الوسائل التكنولوجية والفعالة لمحاربة إيديولوجيات العنف والتطرف وكل أشكال الجريمة المنظمة والعابرة للأوطان، من خلال اعتماد آليات عملية للتعاون بين كل الشركاء الفاعلين في هذا المجال.[3]

[1] سناء خليل،" الجريمة المنظمة عبر الوطنية، الجهود الدولية ومشكلات الملاحقة القضائية"، المجلة الجنائية القومية، العدد الثاني، 1996، ص 111.

[2] أيسر محمد عطية، "دور الاليات الحديثة للحد من الجرائم المستحدثة الإرهاب الالكتروني وطرق مواجهته" عمان 02 04 سبتمبر 2014 ص09

[3] الخليج اونلاين،" تخصيص خلايا امنية لتعقب الإرهاب الالكتروني في الجزائر" تم التصفح يوم 2025/03/05 https://alkhaleejonline.net/

المبحث الثالث: العلاقة بين الأمن السيبر اني والأمن المجتمعي

في ظل التداخل المتزايد بين الفضاء الرقمي والمجتمع، لم تعد التهديدات السيبرانية تُفهم فقط على أنها مسألة تقنية أو عسكرية، بل أصبح لها تأثيرات مباشرة على الأمن المجتمعي. يسلط هذا المبحث الضوء على الترابط البنيوي بين الأمن السيبراني كآلية حماية رقمية، وبين الأمن المجتمعي باعتباره ضامنًا للسلم الاجتماعي والاستقرار الداخلي. يتم التطرق إلى الأبعاد المختلفة لهذا التفاعل، من خلال تحليل مفاهيم مثل "الهندسة الاجتماعية" وأثرها على سلوك الأفراد، وكذلك دراسة التحديات الناتجة عن اختراق القيم والهويات الثقافية عبر الفضاء السيبراني، باعتبارها عوامل تؤثر مباشرة في التماسك الاجتماعي والثقة المؤسسية.

المطلب الأول: الهندسة الاجتماعية

الفرع الأول: مفهوم الهندسة الاجتماعية

مصطلح" الهندسة الاجتماعية "ليس له تعريف واحد متفق عليه تماما، ومعناه يتطور ويختلف حسب المجال بشكل عام، يمكن فهمه على أنه" الجهود المبذولة للتأثير على سلوكيات الأفراد أو الجماعات"[1] تاريخياً، تم تقديم مصطلح" المهندسين الاجتماعيين "في سياق صناعي عام 1894، حيث كان ينظر إليهم على أنهم متخصصون مطلوبون لمساعدة أصحاب العمل في التعامل مع" مشاكل الإنسان"،وفي عام 1899، ظهر مفهوم "الهندسة الاجتماعية "نفسه في أمريكا كاسم لمهمة المهندس الاجتماعي في هذا المعنى، قبل أن يتطور إلى معنى معياري يستند إلى استعارة للعلاقات الاجتماعية كـ" أجهزة "يمكن التعامل معها بطريقة" هندسية تقنية "[2] بمرور الوقت، اكتسب هذا المصطلح دلالات سلبية، على الرغم من أن القوانين والمراسيم الحكومية التي تسعى للتأثير على السلوك يمكن اعتبارها نوعا من الهندسة الاجتماعية .7في سياق الأمن السيبراني، يشير المصطلح بشكل أساسي إلى" استخدام الحيل والتقنيات لخداع الناس للتخلي عن معلومات سرية أو القيام بعمل ما[3]."

الهندسة الاجتماعية في سياق الأمن السيبراني تشير إلى نوع من الهجمات التي تستغل بشكل أساسي نقاط الضعف البشرية.[4] يعتمد هذا النوع من الهجمات على التفاعل الاجتماعي كوسيلة لتحقيق أهداف المهاجم. الهدف من الهندسة الاجتماعية هو اختراق الأمن السيبراني، والذي قد يتضمن الحصول على

[1] مها عبد القادر، الهندسة الاجتماعية.. نحو مستقبل مشرق، 22-01-2025، اليوم السابع، شوهد بتاريخ.25-05-2025 :
https://bit.ly/4kmqbhr

[2] ماين، إبراهيم. "العلوم الإنسانيَّة والهندسة الاجتماعيَّة ".التنويري 18-07-2024 .شوهد بتاريخ: 25-05-2025 .
https://tinyurl.com/29tr4zg8

[3]

[4] Wang, Zuoguang, Limin Sun, and Hongsong Zhu. "Defining social engineering in cybersecurity." IEEe Access, Vol 8 2020: 85094-85115.

معلومات سرية، أو الوصول غير المصرح به إلى أنظمة الكمبيوتر، أو اختراق الشبكات.[1] يمكن أن تتم هذه الهجمات باستخدام أو بدون استخدام الوسائل التقنية أو استغلال الثغرات التقنية.

تعمل الهندسة الاجتماعية من خلال التلاعب بعلم النفس البشري واستغلال المبادئ النفسية المختلفة. يستغل المهاجمون المهندسون الاجتماعيون مشاعر وسلوكيات بشرية فطرية ونقاط ضعف مثل :الثقة، لخوف، الفضول، الإعجاب أو الميل، الالتزام، المعاملة بالمثل، الشعور بالندرة، السلطة، الإثبات الاجتماعي، الإلهاء، الإقناع، الخداع، التلاعب، استغلال العواطف والمشاعر.[2]

يعتبر العنصر البشري هو الحلقة الأضعف والأكثر تحديا في أمن الأنظمة .هذه الثغرات البشرية متأصلة في طبيعة الإنسان، وهي عالمية ومستمرة. لقد تطورت الهندسة الاجتماعية عبر الزمن، من مجرد أساليب بسيطة مثل انتحال الشخصية أو التظاهر، إلى هجمات معقدة تستخدم التكنولوجيا ووسائل التواصل الاجتماعي والأتمتة .على الرغم من التقدم في الدفاعات التكنولوجية، فإن الهندسة الاجتماعية لا تزال تشكل تهديدا خطيرا وشاملا ومستمرا للأمن السيبراني.

الفرع الثاني :التأثيرات السيبرانية والاجتماعية للهندسة الاجتماعية

لفهم كيفية عمل هجمات الهندسة الاجتماعية وتأثيرها، يمكن النظر إليها من ثلاثة جوانب أساسية مترابطة: أساليب الهجوم المستخدمة، ونقاط الضعف البشرية المستغلة، وآليات التأثير التي تشرح كيفية عمل أساليب الهجوم على نقاط الضعف البشرية لتحقيق نتائج الهجوم.

1.**أساليب الهجوم المستخدمة** :أساليب الهجوم هي الطرق أو الوسائل التي يستخدمها المهاجمون لتنفيذ هجمات الهندسة الاجتماعية .هذه الأساليب هي القوة الدافعة التي تطلق الهجوم وتؤثر بشكل كبير على نجاحه. لقد تطورت هذه الأساليب مع الزمن، من بسيطة إلى معقدة وتكنولوجية. يمكن أن تكون هذه الأساليب تقنية أو غير تقنية .من الأمثلة الرئيسية لأساليب الهجوم :التصيد الاحتيالي، عبر البريد الإلكتروني، الرسائل النصية، أو شبكات التواصل الاجتماعي، والتصيد الصوتي عبر الهاتف .تشمل الأساليب الأخرى التمويه أو الادعاء عن طريق اختلاق سيناريوهات كاذبة، والهندسة الاجتماعية العكسية لجعل الضحية تتفاعل مع المهاجم على أنه جهة موثوقة .[3]

2.**نقاط الضعف البشرية المستغلة** :نقاط الضعف البشرية هي السبب الجذري لكون الضحية تتسبب في عواقب الهجوم .العنصر البشري يعتبر الحلقة الأضعف والأكثر تحدياً في أمن الأنظمة .هذه الثغرات متأصلة في طبيعة الإنسان، وهي عالمية ومستمرة، ولا يمكن القضاء عليها بالكامل حتى مع التدريب الأمني.

[1] Wang, Zuoguang, Hongsong Zhu, and Limin Sun. "Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods." Ieee Access 9 2021: 11895-11910.

[2] Taherdoost, Hamed. "Analyzing Influential Psychological Factors in Social Engineering; Human Psyche and Cybersecurity. " Psychomachina 1 (2023): 1-7.

[3] Taherdoost, Hamed, Opcit.

يعتمد نجاح الهندسة الاجتماعية على استغلال علم النفس البشري ونقاط الضعف النفسية والسلوكية المختلفة. تشمل جوانب نقاط الضعف البشرية التي يستغلها المهاجمون ما يلي[1]:

- **الإدراك والمعرفة** :مثل التفكير القائم على الاستدلالات أو الاختصارات العقلية، التفكير الخامل أو الجامد، القوالب النمطية، التحيز المعرفي، الجهل مثل الوعي الأمني المنخفض، أو الحاجة المنخفضة للإدراك، السذاجة، قلة الخبرة.

- **السلوك والعادة** :مثل الإهمال، عدم التفكير، الكسل، أو أنماط الفعل الثابتة والعادات السلوكية اللاواعي.

- **العواطف والمشاعر** :مثل الخوف، التوتر، الفضول، الإثارة، المفاجأة، الغضب، الاندفاع، السعادة، الحزن، الاشمئزاز، الشعور بالذنب.

- **الطبيعة البشرية** :الخصائص النفسية الأساسية المشتركة عالمياً مثل حب الذات أو النرجسية، الجشع، الشهوة، الشراهة، التعاطف، والميل للمساعدة.

- **سمات الشخصية** :مثل الانبساطية، الوعي بالواجب، الوفاق أو القبول مثل الثقة، الإيثار، الانفتاح على التجربة، أو العصابية مثل القلق، العداء.

- **الخصائص الفردية** :مثل الود، اللطف، الكرم، التواضع، اللباقة، الخجل، اللامبالاة، الغطرسة، أو الحسد.

3.**أساليب الهجوم على نقاط الضعف البشرية لتحقيق نتائج الهجوم** :آليات التأثير هي المبادئ التفسيرية التي توضح كيف تؤثر أساليب الهجوم على نقاط الضعف البشرية .إنها تشرح كيف تستغل أساليب الهجوم نقاط الضعف هذه، ولماذا تؤدي نقاط الضعف إلى عواقب الهجوم، وكيف تحقق الأساليب أهدافها. تعتمد هذه الآليات غالباً على مبادئ نفسية وسلوكية .العديد منها يدفع الأفراد لاستخدام آليات اتخاذ القرار التلقائية بدلاً من التفكير المنطقي العقلاني، تشمل جوانب آليات التأثير:[2]

- **الإقناع** :يتضمن مبادئ مثل التشابه والإعجاب والمساعدة، والمصداقية والطاعة للسلطة t كما أظهرت دراسة ميلغرام، ونموذج الاستجابة المعرفية والمسارات المركزية والمحيطية للإقناع ونموذج احتمالية التفصيل الذي يفسر كيف يؤثر الاهتمام بالرسالة أو الاعتماد على إشارات سطحية في الإقناع.

[1] Wang, Zuoguang, Hongsong Zhu, and Limin Sun, opcit.

[2] Schaab, Peter, Kristian Beckers, and Sebastian Pape. "Social engineering defence mechanisms and counteracting training strategies. " Information & Computer Security 25, no. 2 (2017) : 206-222.

- **التأثير الاجتماعي** :يشمل تأثير المجموعة والمجاراة المجاراة المعيارية والإعلامية، نظرية التبادل الاجتماعي وقاعدة المعاملة بالمثل تقديم خدمة لطلب أكبر لاحقاً، قاعدة المسؤولية الاجتماعية والواجب الأخلاقي استغلال الميل للمساعدة، والكشف عن الذات وبناء العلاقة بناء الثقة والقرب.

- **الإدراك والموقف والسلوك** :يتضمن إدارة الانطباع والتنافر المعرفي والالتزام والاتساق الشعور بالضغط الداخلي والخارجي للتوافق مع الأفعال السابقة، تأثير" القدم في الباب"الامتثال لطلب صغير يزيد احتمالية الامتثال لطلب أكبر، تأثير المتفرج وانتشار المسؤولية وفقدان الهوية عندما يقل الشعور بالمسؤولية الفردية في وجود الآخرين أو في المجموعات، الندرة التي تزيد القيمة المتصورة وتثير المشاعر مثل الخوف، وضغط الوقت وتحميل التفكير الزائد الذي يعيق التفكير المنطقي.

- **الثقة والخداع** :يشمل العلاقة بين الثقة والهندسة الاجتماعية حيث الثقة تزيد احتمالية الوقوع ضحية، العوامل المؤثرة على بناء الثقة مثل ميل الواثق للثقة، وموثوقية الواثق به من حيث القدرة، الإحسان، النزاهة، والعوامل المؤثرة على الخداع واكتشافه مثل التزييف، الإخفاء، والمواربة.

- **اللغة والفكر والقرار** :العلاقة بين اللغة والتفكير واستغلال إدراك اللغة، تأثير التأطير والتحيز المعرفي في التلاعب بالقرارات، التفكير غير المباشر والتعبيرات السلبية، واستخدام اللغة لإثارة الارتباك في التفكير.

- **العواطف واتخاذ القرار** :تأثير العاطفة والشعور على اتخاذ القرار مثل كيف يؤثر الخوف أو الغضب أو السعادة على تقدير المخاطر واتخاذ القرارات، والعلاقة بين العواطف وتعابير الوجه والخداع واكتشافه مثل الميكرو تعابير.

باختصار، فإن أساليب الهجوم مثل التصيد أو الادعاء تستخدم آليات التأثير مثل استغلال السلطة أو الندرة أو الميل للمساعدة لاستهداف واستغلال نقاط الضعف البشرية الكامنة مثل الثقة، الجهل، الخوف، الفضول، أو سمات الشخصية، مما يدفع الضحية لاتخاذ إجراءات مثل الكشف عن كلمة مرور أو النقر على رابط تؤدي إلى اختراق الأمن السيبراني وتحقيق هدف المهاجم.

المطلب الثاني: الاثار المتبادلة بين المجالين

مع تطور التكنولوجيا وازدياد الاعتماد على الفضاء الرقمي في مختلف مناحي الحياة، برزت التهديدات السيبرانية كأحد أخطر التحديات الأمنية التي لا تقتصر على المؤسسات الحكومية أو القطاعات الاقتصادية فحسب، بل تمتد تأثيراتها لتشمل الأفراد والمجتمعات. من هذا المنطلق، أصبح من الضروري النظر إلى الأمن السيبراني كجزء لا يتجزأ من الأمن المجتمعي، نظرا لما يربط بينهما من تفاعل وتأثير متبادل حيث نذكر منها:

الفرع الأول: تهديد الهوية والقيم المجتمعية:

نقلت التكنولوجيا العالم الى مرحلة جديدة من مراحل تطور الاتصال الاجتماعي لها أبعادها الاجتماعية والثقافية والاقتصادية التي لا يمكن تجاهل سلبياتها وتأثيراتها المختلفة، وبذلك فقد عبر أنطوني جيدنز Gidnes Anthony عن سمات الثقافة الجديدة في للمجتمع المعاصر على أنها ثقافة ذات خصائص مشوشة ومضطربة[1]

كما أنها تؤثر سلبا على التفاعلات الاجتماعية بين الأفراد وتؤدي الى العزلة الاجتماعية والانجذاب الى العالم الافتراض ي مما يشجع على الاستخدام غير المناسب لهذه المواقع وجعلها منصات لنشر خطاب الكراهية.[2]

كما أكد العديد من الباحثين بأن المجتمعات الافتراضية تسمح للفرد بأن يضع هويته محل استكشاف وتجريب وأطلق بعض العلماء على العالم الافتراضي اسم "ورشات الهوية " وذكر الكاتب محمد عابد الجابري "أن الهوية أصبحت تركيبا بين معطيات العالم الواقعي والعالم الافتراض ي الذي يشكل جزء كبير من العالم الواقعي، وهو ما من شأنه أن يؤدي الى انقسام على صعيد الهوية[3]"

تغريب الانسان المسلم وعزله عن قضاياه:

وذلك من خلال التشكيك في جميع قناعاته الدينية وهويته الثقافية وقلب منظومة القيم لديهم، حيث أصبح يقضي أوقاته من خلال الاستخدام اللاعقلاني لأجهزة الهواتف النقالة والأنترنت من خلال السعي الى إقامة عالقات مع مختلف الاجناس عبر تطبيقات وبرامج متعددة تتيحها الانترنت وتسمح بتبادل فيديوهات ومقاطع وأفلام غير أخلاقية ومدمرة للذات الإنسانية مما أدى الى انتشار ظاهرة الشذوذ والتخنث والعلاقات

[1] خضر حلمي ساري.2008." تأثير الاتصال عبر الانترنت في العلاقات الاجتماعية دراسة ميدانية للمجتمع القطري". مجلة جامعة دمشق العدد03 ص23

[2] ناصر الرحامنة. 2018"خطاب الكراهية في شبكة الفيسبوك في الأردن" دراسة مسحية.. قسم الصحافة، الشرق الاوسط: كلية الاعلام ص26

[3] وليدة حدادي .2018" الفضاء السيبراني وأزمة القيم الأخلاقية في المجتمعات العربية ": الشبكات الاجتماعية نموذجا، مجلة الحقيقة ص17

المحرمة بين متماثلي الجنس وإشاعة ثقافة العنف التي من شأنها خلق جيل يؤمن بالعنف كظاهرة عادية في الحياة اليومية مما ينتج عن ذلك انتشار الرذيلة والجريمة في مجتمعاتنا.[1]

الفرع الثاني: التحريض على العنف وخطابات الكراهية:

سهلت هذه الوسائط الى الدعوة لممارسة العنف الرمزي الذي يستهدف إلحاق الضرر بالأخرين كونه خفي وغير واضح، ويعتبر الفيسبوك فضاءا تعبيريا لجملة من الرموز

التي تندرج ضمن اشكال العنف الرمزي منها الكلمات الاستفزازية المنتشرة في تعليقات البعض والتي القت رواجا كبير وانتشارا واسعا بسبب عدم وجود سلطة رادعة تقيد حرية التعبير. وبذلك فان العولمة الثقافية التي تسعى من خلالها الولايات المتحدة الأمريكية الى أمركة مختلف شعوب العالم أثرت بشكل سلبي على المجتمع الجزائري من خلال فقدانه لخصوصيته وهويته الثقافية، ولم يعد يقتصر تأثيرها على الهوية الثقافية للمجتمع فحسب بل أثر بشكل جلي على مختلف البنى والأنساق الثقافية والاجتماعية وهذا ما أشار اليه المجلس الاوروبي للثقافة سنة 1998 بالقول "ان زمن العولمة هو زمن تهديدات الهويات والثقافات[2]"

و أصبحت وسائل التواصل الاجتماعي وسيلة للتأثير في الأحداث الاجتماعية والسياسية، ووسيلة فعالة في تشكيل الرأي العام وتعبئة الجماهير وتنظيم الاحتجاجات والمظاهرات التي يصعب تحقيقها أحيانا في ظل وسائل الأعلام التقليدية، وتختلف درجة تأثير شبكات التواصل الاجتماعي على الرأي العام باختلاف قوة تأثيرها على الأفراد ودرجة تغلغلها في حياتهم بإضافة إلى سهولة المادة الإعلامية التي تقدمها لهم، ويجتمع الباحثون على أن الرأي العام ينشأ دائما حول قضية محددة ويزول بزوال أسبابها، ولكي تكون القضية محل اهتمام الرأي العام لابد أن تكون معاصرة وجدية، تتضارب الآراء بشأنها وتختلف حولها وجهات النظر فعلى سبيل المثال عرفت حادثة سقوط الشاب الجزائري عياش محجوبي في البئر الارتوازي بولاية المسيلة متابعة وتغطية إعلامية واسعة سواء عبر شبكات التواصل الاجتماعي أو عبر وسائل الاتصال الجماهيري، حيث عرفت هذه الحادثة التفافا كبيرا من قبل الشباب حول القضية في شبكات التواصل الاجتماعي في محاولة لتغطية الوضع بالمنطقة والعمل على تشكيل أو صناعة الرأي العام عن طريق خلق مجتمعات افتراضية تعمل على تعبئة الجماهير والانتقال من الحشد الافتراضي إلى الحشد الواقعي بغية التفاعل مع الضحية وعائلته.[3]

تشكل التهديدات السيبرانية تحديا متزايدا للأمن المجتمعي، حيث تؤثر على ثقة المواطنين في المؤسسات، وتنشر الفوضى المعلوماتية، وتؤدي إلى تهديد الاستقرار الاجتماعي والثقافي. وفي المقابل، فإن قوة الأمن المجتمعي من خلال الوعي الرقمي، والتماسك الاجتماعي، والتعاون مع الجهات الأمنية تعد عاملا حاسما في

[1] هناء عاشور. ديسمبر, 2017 "تأثيرالعولمة على القيم الثقافية السائدة في المجتمع دراسة تحليلية" (مجلة العلوم الإنسانية) 8 ص104

[2] فيصل لكحل2017." إثر مواقع التواصل الاجتماعي على المجتمع الجزائري المعاصر". مجلة العلوم الاجتماعيةالعدد .26. صفحة 220

[3] نعيم بوعموشة، وهشام بوبكر. 2019 "دور شبكات التواصل الاجتماعي في صناعة الرأي العام لدى المواطن الجزائري". مجلة البحوث والدراسات الإنسانية، العدد13 ، ص 09

مواجهة هذه التهديدات والتقليل من آثارها. بالتالي، هناك علاقة تفاعلية: كلما زادت التهديدات الإلكترونية تراجع الأمن المجتمعي، وكلما تعزز الأمن المجتمعي ضعفت فعالية هذه التهديدات.

الفصل الثاني: تأثير التهديدات السيبرانية على الأمن المجتمعي الجزائري

تمهيد

بعد تأسيس الإطار المفاهيمي في الفصل الأول، ينتقل هذا الفصل لتسليط الضوء على التأثيرات المتعددة الأبعاد للتهديدات السيبرانية على الأمن المجتمعي في الحالة الجزائرية .لم تكن الجزائر بمنأى عن تصاعد وتيرة هذه التهديدات، خاصة في فترات الاضطراب السياسي أو النقاشات المجتمعية الحادة، فخلال السنوات الأخيرة، عرفت البلاد تصاعداً في وتيرة التهديدات السيبرانية، خاصة في فترات الاضطراب السياسي أو النقاشات المجتمعية الحادة، حيث تم استغلال الفضاء الرقمي لبث حملات تضليل إعلامي، ونشر أخبار كاذبة، فضلاً عن محاولات اختراق قواعد بيانات حساسة تابعة لمؤسسات حكومية. إن خطورة هذه التهديدات تكمن في كونها لا تستهدف فقط البنى المادية، بل تتجاوز ذلك إلى المساس بالأمن الثقافي والفكري، وتوجيه الرأي العام، وخلق فجوات مجتمعية تهدد التماسك الداخلي. سيتناول الفصل بالتحليل كيف تتجاوز آثار التهديدات السيبرانية البنى المادية لتصل إلى المساس بالأمن الثقافي والفكري، توجيه الرأي العام، وخلق فجواتٍ مجتمعية تهدد التماسك الداخلي. كما سيركز على كيفية تأثير هذه التهديدات على الأبعاد السياسية والاقتصادية والاجتماعية والثقافية للأمن المجتمعي. سيتم تفصيل الآثار على النظام السياسي من خلال التدخلات الخارجية وحملات التضليل الإعلامي والتلاعب بالرأي العام، وتأثيرها على البنية الاقتصادية من خلال الجرائم المالية السيبرانية وتداعياتها على المؤسسات والثقة العامة. بالإضافة إلى ذلك، سيبحث الفصل في كيفية استهداف القيم والمعتقدات المجتمعية عبر الفضاء الرقمي، وتأثير ذلك على النسيج الاجتماعي. تكتسي دراسة موضوع "تأثير التهديدات السيبرانية على الأمن المجتمعي الجزائري" أهمية قصوى، بالنظر إلى تزايد ارتباط الأمن القومي، بالأمن المجتمعي، بالمجال السيبراني. يهدف هذا الفصل إلى كشف مدى انكشاف المجتمع الجزائري على الفضاء السيبراني وكيفية انعكاس التهديدات الرقمية على استقراره ووحدته.

المبحث الأول: اثار التهديدات السيبرانية على الاستقرار السياسي والاجتماعي

تشهد الجزائر في السنوات الأخيرة تصاعدًا ملحوظا في الهجمات السيبرانية، استهدفت مؤسسات حكومية، بنوكا، وقطاعات حيوية، بالإضافة إلى استغلال الفضاء الرقمي في بث خطاب الكراهية والتضليل. وفي هذا المبحث، سنتطرق إلى أبرز مظاهر هذه التهديدات، وخصائصها التقنية والاجتماعية، إضافة إلى الإحصائيات المتوفرة حولها.

المطلب الأول: التأثير على النظام السياسي

الفرع الأول التدخلات الخارجية:

منذ الاستقلال، سعى النظام السياسي الجزائري إلى الحفاظ على سيادته واستقلال قراره السياسي، خاصة في ظل الإرث الاستعماري الثقيل والتجاذبات الجيوسياسية الإقليمية والدولية. إلا أن الجزائر، كغيرها من الدول النامية ذات الأهمية الاستراتيجية، لم تسلم من محاولات التدخل الخارجي المباشر وغير المباشر، سواء عبر الضغوط الدبلوماسية أو الاقتصادية أو من خلال أدوات "القوة الناعمة" والرقمية.

أولاً: اختراق الوكالة الوطنية للأنباء

تعد وكالة الأنباء الجزائرية المنصة الرسمية الأساسية التي تنقل الأخبار والمواقف الرسمية للدولة. ومن هذا المنطلق، فإن محاولة اختراقها لا يعد حدثا عابرا، بل هو عمل عدائي سيبراني موجه يمس صميم السيادة الوطنية .إذ إن قواعد بيانات الوكالة قد تحتوي على:

- مراسلات رسمية مع مؤسسات حكومية وسياسية،
- مواقف دبلوماسية لم تعلن بعد،
- مخططات إعلامية متصلة بالأمن الداخلي والخارجي.

وفي حال تمكن المخترقون من الوصول إلى هذه البيانات أو نشر أخبار مزيفة، فإن الضرر قد يمتد إلى افتعال أزمات دبلوماسية، كما حدث في أزمة اختراق وكالة الأنباء القطرية "قنا" سنة 2017، حيث أدت تصريحات مفبركة نسبت لأمير قطر إلى اندلاع أزمة الخليج، وحصار سياسي واقتصادي لقطر من طرف السعودية والإمارات والبحرين.[1]

ثانيا: اختراق حساب وزارة العدل

حادثة اختراق حساب وزارة العدل الجزائرية على "تويتر" من طرف قراصنة مغاربة حملت أبعادا جيوسياسية خطيرة. فقيام القراصنة بنشر عبارات مؤيدة للحرب الروسية على أوكرانيا اعتبر من طرف السفارة الأوكرانية في الجزائر تصريحا رسميا قد يستدعي ردا دبلوماسيا .ومثل هذا التصرف يظهر أن السيطرة

[1] البلاد، "الموقع الالكتروني لوكالة الانباء الجزائرية يتعرض لسلسلة من الهجمات السيبرانية الحادة" تم التصفح يوم01 /2025/06

على وسائط التواصل الرسمية للدول قد تستخدم كأدوات استفزاز واستفحال التوترات الدولية، لا سيما عندما يكون البلد المستهدف في موقع الحياد أو التوازن.

وأكدت فضيحة "بيغاسوس" التي استخدم فيها المخزن وأجهزته الاستخبارية نظام برمجيات NSO الإسرائيلية للتجسس "بيغاسوس (Pegasus) "الصهيوني، للتجسس على سياسيين وإعلاميين جزائريين، وغيرهم من السياسيين والناشطين والإعلاميين داخل المغرب أيضا وفي أوروبا، وهو ما كشفت عنه التسريبات التي نشرتها 17 مؤسسة إعلامية دولية بتعاون مع مؤسسة"Forbidden Stories" ، وأكدت أن الجهة الأكثر استهدافا بهذا البرنامج الخبيث كانت الجزائر وأجهزتها الرسمية.

وبذلك يشكل المغرب ودولة الكيان أسوأ أنواع التحالفات خاصة في المجال السيبراني، حيث سبق للرباط أن وقعت مع تل أبيب على اتفاقية تعاون في مجال الحرب الإلكترونية، وأن الاتفاقية تقضي بإقامة تعاون في "البحث والتطوير ومجالات عملياتية في السايبر"، والمستهدف الأول بطبيعة الحال هي الجزائر بالدرجة الأولى.

ويضاف إلى هذا الثنائي، طرف ثالث لا يمكن أن تأمن الجزائر شره، وهو الطرف الفرنسي، الذي أثبت مؤخرا من خلال عملية تهريب بوراوي، التي أعقبها مباشرة الهجوم السيبراني على وكالة الأنباء الجزائرية، أنه بأجهزته الاستخبارية يشكل الضلع الثالث من معادلة الشر التي تستهدف الجزائر، حتى وإن حاول إخفاء ذلك حماية لمصالحه الاقتصادية والثقافية عندنا.

وأمام هذه التهديدات المتزايدة في مجال الحرب السيبرانية التي تستهدف الجزائر بضراوة ووحشية، أكدت الدولة الجزائرية عبر عديد المناسبات إدراكها لحجم التحديات التي يفرضها مثل هذا النوع من الحروب الحديثة، وقد أعدت لها عدتها باعتبارها جزءا أساسيا من استراتيجية الدفاع الوطني الشامل.

وكان الرئيس عبد المجيد تبون قد أكد في أكتوبر من العام 2021، بمناسبة اليوم الوطني للصحافة، أن الجزائر تواجه "حربا سيبرانية مسعورة" للتشويش على البناء الوطني، موجها تحيته للإعلاميين وكل من يقوم بالتصدي "للحرب السيبرانية المسعورة، التي ينفذها بالأصالة أو بالوكالة محترفو الأكاذيب حقدا على الجزائر

الفرع الثاني: اختراق البيانات الحكومية الجزائرية

في العصر الرقمي الذي نعيشه، أصبحت البيانات الحكومية تمثل أحد أعمدة السيادة الوطنية، وأي اختراق لها لم يعد مجرد مسألة أمن معلوماتي، بل تهديدا مباشرا للنظام السياسي واستقراره. وتشكل الهجمات السيبرانية على قواعد بيانات الوزارات والمؤسسات الرسمية الجزائرية أحد أبرز مظاهر هذا الخطر، إذ تسعى جهات خارجية أو تنظيمات غير شرعية إلى زعزعة الثقة بين الدولة والمواطن، أو إحراج السلطات أمام الرأي العام الدولي، أو حتى تعطيل عمل المؤسسات السيادية.

ففي 25 ماي 2025، أعلنت السلطات الجزائرية عن إعفاء المدير العام لشركة "صيدال" الحكومية، عبد الواحد غريمس، وذلك عقب حادثة اختراق سيبراني كبيرة استهدفت قاعدة بيانات وزارة الصناعة الصيدلانية. وتعود هذه الهجمة إلى مجموعة قرصنة مغربية تدعىMOR_H4X ، والتي تمكنت من الوصول إلى

أكثر من 34 جيجابايت من البيانات السرية المتعلقة بالواردات الدوائية والصفقات التجارية الممتدة بين عامي 2019 وأبريل 2024.

الحادثة التي وصفت بأنها الأخطر في تاريخ البنية السيبرانية لقطاع الصحة والصناعة الدوائية في الجزائر، دفعت إلى موجة من ردود الفعل الرسمية، خاصة بعد أن عمدت المجموعة إلى نشر الوثائق المسروقة على المنصات الرقمية، مما تسبب في حرج دبلوماسي واقتصادي واسع النطاق. وتسبب في زعزعة الثقة في المؤسسات الرسمية وإقالة المدير العام لصيدال لم تكن مجرد إجراء إداري، بل إشارة سياسية إلى تحميل المسؤوليات حول القصور في الحوكمة السيبرانية فالاختراق لم يصب فقط شركة دوائية، بل كشف عن:

- ضعف في منظومة الأمن المعلوماتي بالقطاع الوزاري ككل.
- غياب استراتيجيات استباقية للتعامل مع الهجمات السيبرانية.
- هشاشة التنسيق بين مؤسسات الدولة في إدارة البيانات الحساسة.

المطلب الثاني: التأثيرعلى السلم الاجتماعي

في ظل الثورة الرقمية التي يشهدها العالم، أصبحت وسائل التواصل الاجتماعي أداة مركزية في تشكيل الرأي العام والتأثير في اتجاهاته، متجاوزة بذلك الوسائط التقليدية في سرعة الانتشار وقوة التأثير. وقد أدى هذا التحول إلى بروز ظواهر جديدة، من بينها التلاعب بالرأي العام وبث الشائعات، التي باتت تمثل تهديدا حقيقيا للاستقرار المجتمعي، خاصة في الدول التي تشهد تحولات سياسية واقتصادية متسارعة، على غرار الجزائر.

لقد تحولت بعض المنصات الرقمية إلى فضاءات مفتوحة لنشر معلومات مضللة وشائعات مغرضة، تستهدف النسيج الاجتماعي والثقة العامة بين المواطنين ومؤسسات الدولة. وغالبا ما يتم توظيف هذه الحملات لأغراض سياسية أو أيديولوجية أو حتى إجرامية، بما يهدد السلم الأهلي ويغذي النزاعات والانقسامات داخل المجتمع.

الفرع الأول: التلاعب بالرأي العام

يعد مفهوم الرأي العام من بين المفاهيم التي حظيت باهتمام واسع في الأدبيات الأكاديمية، إذ تم التطرق إليه باعتباره ظاهرة اجتماعية لها تأثير مباشر على السياسات العامة وتوجهات صانعي القرار. ويعود هذا الاهتمام إلى رغبة الأنظمة السياسية في فهم اتجاهات شعوبها ومواقفها تجاه قضايا مصيرية أو آنية. فالرأي العام ليس ظاهرة حديثة، بل هو مرتبط بوجود الجماعات البشرية وتطور المجتمعات، ويُعَدّ تجليا واضحا للحياة الاجتماعية. وقد وعى الإنسان منذ القدم بأهمية الرأي العام وطاقته التأثيرية، فسعى إلى توظيفه لتحقيق أهدافه المختلفة، مبتكرًا في ذلك وسائل وأساليب متعددة للتأثير فيه أو توجيهه بما يخدم مصالحه[1].

فالرأي العام في الأصل مصطلحا ذا جذور غربية، شاع استخدامه في الأوساط السياسية الغربية، لا سيما في الأنظمة الديمقراطية التي كانت تولي أهمية كبرى للرأي العام، باعتباره أداة لتعزيز شرعية تلك الأنظمة والتأكيد على تمثيلها لإرادة الأغلبية. ويمكن إرجاع بداية استخدام هذا المفهوم بشكل واضح إلى القرن الثامن عشر، رغم وجود مفاهيم مشابهة له من حيث المضمون في فترات سابقة. وقد ظهر هذا المفهوم بشكل خاص في الكتابات الفلسفية التي تناولت القضايا السياسية والاقتصادية والاجتماعية في ذلك العصر[2].

اما التلاعب فانه يكون عن طريق بث الشائعات والتي هي سلوك مخطط ومدبر تقوم به جهة أو شخص لنشر معلومات أو أفكار غير دقيقة ومجهولة المصدر وتوحي بالتصديق، وتتضمن جزء ضئيل من الحقيقة،

[1] عدي إبراهيم المناوي، "التيارات السياسية العلمانية وصناعة الرأي العام": دراسة حالة العراق بعد 2003، عمان: دار زهران للنشر، ط 1، 2014، ص 53.

[2] ضرغام الدباغ." محاضرات في الإعلام والرأي العام،" الأكاديميون للنشر والتوزيع، عمان، ط ،1،2016 ص .140

وتتعلق بالأحداث الراهنة وباهتمام الجمهور الموجهة إليهم في وقت محدد وعبر وسائل الاتصال الممكنة، وذلك لتدمير معنى أو تشويه صورة أو للتأثير في شخص أو في الرأي العام تحقيقا لأهداف جهة المنشأ[1] .

وتعرف أيضا بأنها أقوال وأفعال مجهولة المصدر غير مصحوبة بدليل على صدقها، بتناقلها للأفراد وتدور حول موضوعات هامة بالنسبة لهم وتتصف بالغموض والاهمية لدى الجمهور، ولها وسائل تقليدية والكترونية مختلفة لنقلها وتهدف لتحقيق غايات معينة [2].

الفرع الثاني: تأثيرهما على السلم الاجتماعي:

لعب الرأي العام دورا أساسيا في الحياة السياسية " كلما كانت المشاركة الشعبية في الحكم أكثر وأوسع ،كان الرأي العام ذا معنى أعمق وحقيقة شاخصة لا يمكن أن ينكر وجودها أحد ، حيث أن ميزة التغير في المجتمعات من الميزات الرئيسية فإن ظاهرة الرأي العام تتغير بأشكال وصور مختلفة تبعا لهذا التغيير ،وتزداد أهمية الرأي العام ودوره سواء في النظم الديمقراطية أو غيرها ،مع زيادة أهمية المواطن العادي في عملية صنع السياسة ،إذ أن المجتمع السياسي في الواقع المعاصر ،وبصرف النظر عن طبيعة نظامه السياسي ،يحاول أن يرضي بل وان يتملق هذا الرجل العادي ،مما يجعل هذا الأخير أحد عناصر (مدخلات) عملية صنع السياسة ولو في الأمد القصير.[3]

ويعد التلاعب بالرأي العام إحدى أبرز الأدوات المعاصرة التي تستخدم في توجيه السلوك الجماهيري والتأثير على الإدراك الجماعي داخل المجتمع. وفي السياق الجزائري، برز هذا التهديد بشكل ملحوظ خاصة مع الانتشار الواسع لاستخدام شبكات التواصل الاجتماعي، التي تحولت إلى منصات رئيسية لنشر المعلومات، ولكن أيضا لترويج الشائعات، وصناعة خطاب تحريضي يهدد الأمن المجتمعي.

لقد عرفت الجزائر خلال السنوات الأخيرة عدة حالات تم فيها توظيف وسائل الإعلام الرقمي في بث أخبار زائفة، وتحريف الوقائع، بهدف خلق حالة من الفوضى أو زرع الفتنة بين فئات المجتمع

نذكر على سبيل المثال:

• حادثة سقوط الشاب "عياش محجوبي" في بئر ارتوازي سنة 2018 بولاية المسيلة، حيث عرفت الحادثة تضخيما إعلاميًا كبيرا على شبكات التواصل، رافقته حملات تشكيك في قدرات الدولة ومؤسسات الإنقاذ، مما أدى إلى احتقان شعبي واسع. وعلى الرغم من التضامن الكبير، إلا أن طريقة تغطية الحدث على فيسبوك ويوتيوب أدّت إلى تأجيج مشاعر الغضب، وهو ما يمثل حالة نموذجية للتأثير العاطفي السلبي للرأي العام في لحظات الأزمات

[1] مصطفى، حسام الدين، 2007."استخدام تكنولوجيا الاتصال في انتشار الشائعات"، دراسة حالة على مستخدمي الانترنت والهاتف بكلية دراسات الحاسبات الالية "كمبيوتر مان"، جامعة أم درمان السالمية، الخرطوم، السودان. ص09

[2] سلمان احمد ،2017 "شبكات التواصل الاجتماعي ودورها في نشر الشائعات من وجهة نظر أعضاء هيئة التدريس في جامعة ديالى"، رسالة ماجستير، جامعة الشرق الاوسط، عمان، الأردن ص19

[3] إسماعيل على سعد، "الاتصال والرأي العام مبحث في القوة والأيديولوجيا"، دار المعرفة الجامعية، الاسكندرية ،1989، ص111

• كما شهدت فترة الحراك الشعبي (2019-2020) محاولات متكررة للتأثير على توجهات المواطنين عبر الأخبار الكاذبة والصفحات المجهولة الهوية، التي روجت لمعلومات مضللة حول قرارات حكومية أو تصريحات مزعومة لمسؤولين، ما أسهم في تغذية الشكوك وزيادة الانقسام بين فئات الشعب.

هذا النوع من التلاعب يسهم في إضعاف الثقة بين المواطن ومؤسسات الدولة، ويؤدي إلى تفكك الوحدة الوطنية، وانتشار الهلع والريبة، وهو ما يضعف مناعة المجتمع تجاه الأزمات الطارئة. كما أن الاستخدام الممنهج للإشاعة والتضليل قد يفتح المجال لتدخلات خارجية تسعى لزعزعة استقرار الدولة من خلال التأثير في توجهات الرأي العام الداخلي.

فكما الاشخاص عرضة للشائعات وقد تلحق بهم الاذى النفسي كذلك الحال لأمن القومي والوطني فقد يتعرض الأمن الوطني للشائعات بقصد زعزعة الأمن والاستقرار واثارة الفوضى والبلبلة كالشائعات المضللة عن أعمال تخريبية مثال والتي تثير اهتمام العامة من الناس ما يضر بأمن المجتمع.[1]

ويعتبر المجتمع الذي تنتشر فيه الاشاعة مجتمع معرض ليكون ثورة لانتشار وتدني المعنويات ومناخ مربك للجمهور وذلك بفتح المجال لانتشار الاكاذيب والاخبار ذات النيات السيئة والدوافع غير البريئة مما يحول المجتمع الى بيئة لتفشي الكذب والامراض الاجتماعية والفساد وانتشار الفوضى التي تهدم العلاقات الاجتماعية وتنشر الفتن بين الجماعات إضافة إلى انتشار الامراض النفسية كالقلق والتوتر والارهاق والشرود.[2]

وقد تطرق المشرع إلى هذه الجريمة في القسم الاول من الفصل الخامس 5 والذي عنون بالجنايات التي يرتكبها الاشخاص ضد النظام العمومي وذلك في القانون رقم6_23

والقانون رقم 11_14 حيث جرم المشرع الاهانة ضمن المادة 144 محددا من خلال هذه المواد الفئات المستهدفة الجهات القضائية، الجيش الوطني الشعبي، او أي هيئة نظامية عمومية أخرى المشرع من خلال هذا النص كأنه قصد حماية مؤسسات الدولة وهيبتها من إساءة قد تمس بوجودها وكيانها كهيئة نظامية تمثل الدولة وسمعتها اما الوسيلة المستعملة فقد حدد المشرع الوسائل التي ترتكب من خلالها هذه الجريمة فيما يلي

1. الكلام أو الكتابة أو الرسم
2. اليات بث الصورة أو الصوت
3. أية وسيلة الكترونية أو معلوماتية أو إعلامية[3].

[1] سيرين أسامة جرادات، "محمد أحمد القضاة، "المسؤولية الجنائية لمروجي الشائعات عبر شبكات التواصل الاجتماعي"، مجلة جرش للدراسات والبحوث، العدد1، ص81

[2] غانم عبد الوهاب، "بلعباس نادية .دور وسائل الإعلام في نشر الإشاعة وكيفية الحد من آثارها السلبية": دراسة في طرق النشر ودور السياق والفاعل الاجتماعي .رسالة ماجستير، جامعة مستغانم، الجزائر، ص 32

[3] محمد توجي-عثماني عبد القادر. 2019."الاشاعة وأثرها على الفرد والمجتمع"، مجلة البحث العلمي في االاداب العدد 20ص10

وقد برز هذا التأثير بوضوح خلال فترات الأزمات، مثل أزمة كورونا، حيث انتشرت معلومات مغلوطة حول أعداد الإصابات وفعالية اللقاحات، مما أحدث نوعا من البلبلة والهلع في أوساط المواطنين. كما استخدمت الشائعات بشكل خطير في تضخيم بعض الأحداث الأمنية أو تشويه صورة مؤسسات الدولة، وهو ما يؤثر سلبًا على الثقة المتبادلة بين المواطن والدولة، ويغذي الشعور بالهشاشة والشك.

وتؤكد دراسات أكاديمية، منها ما أشار إليه محمد أحمد القضاة، أن الشائعات عبر شبكات التواصل الاجتماعي يمكن أن تشكل تهديدا مباشرا للسلم الأهلي إذا لم يتم التصدي لها عبر التوعية والمحاسبة القانونية.

المبحث الثاني: الاثار الاقتصادية للتهديدات السيبرانية

استكمالاً لبحث تأثير التهديدات السيبرانية على الأمن المجتمعي بأبعاده السياسية والاجتماعية، يتجه هذا المبحث نحو تحليل الانعكاسات الاقتصادية لهذه التهديدات .تعد الجرائم المالية والاحتيال الإلكتروني، التي تتم باستخدام آليات شبكات الإنترنت وأجهزة الحاسوب، من أبرز التحديات السيبرانية التي تواجه الدول والمؤسسات والأفراد في العصر الرقمي. فمع تزايد الاعتماد على التكنولوجيا الرقمية، أصبحت المجتمعات عرضة لهجمات إلكترونية تستهدف البنى التحتية الحيوية والمؤسسات، وتؤثر سلباً على الثقة في المؤسسات والنظام المالي والاقتصادي. سيبحث هذا المبحث في طبيعة الجرائم المالية السيبرانية وأساليب الاحتيال الإلكتروني وخصائصها، وتداعياتها الاقتصادية المباشرة وغير المباشرة على الدولة والمؤسسات، مع التركيز على تأثير هذه الهجمات على قطاعات حيوية مثل البنوك والشركات الكبرى في الجزائر.

المطلب الأول: الجرائم المالية والاحتيال الالكتروني

الفرع الأول ماهية الجرائم المالية والاحتيال الالكتروني:

تشير الجرائم المالية إلى الأفعال غير المشروعة التي تهدف إلى تحقيق مكاسب مالية غير قانونية، سواء من خلال التزوير، الاختلاس، الرشوة، أو غسل الأموال. وغالباً ما ترتكب هذه الجرائم في المؤسسات الاقتصادية، المالية أو حتى عبر الفضاء الرقمي، خاصة مع تطور وسائل الدفع الإلكترونية والتعاملات الافتراضية.

تعرف الجرائم المالية بأنها: "كل سلوك إجرامي يتم عن قصد بهدف تحقيق منافع مالية غير مشروعة، ويمس مصالح الأفراد أو الكيانات الاقتصادية أو المالية.[1]

الاحتيال الإلكتروني هو نوع من الجرائم السيبرانية يعتمد على خداع الأفراد أو المؤسسات باستخدام تقنيات رقمية، بهدف الحصول على معلومات أو أموال بطرق غير قانونية. من أبرز صوره: التصيد الاحتيالي (Phishing)، انتحال الهوية، اختراق الحسابات المصرفية، التزوير الرقمي، وبرمجيات الفدية.

ويعرف بأنه: "كل سلوك ينطوي على استخدام وسائل إلكترونية أو معلوماتية لخداع الضحية وسرقة بياناته أو أمواله، سواء عبر البريد الإلكتروني أو المواقع المزيفة أو التطبيقات المخترقة[2]"

وبالرجوع للمشرع الجزائري وكعادته لم يعرف جريمة الاحتيال في قانون العقوبات، بل اكتفى بتوضيح الأفعال المكونة والظروف المشددة له لهذه الجريمة من خلال نص المادة 372 من قانون العقوبات.[3]

---

[1] دربال امال،" النصب في التأمينات"، مذكرة ماجستير في قانون الاعمال المقارن، جامعة وهران، الجزائر،2012ص 15

[2] محمد هشام صالح عبد الفتاح،" جريمة الاحتيال "دراسة مقارنة ، رسالة ماجستير في القانون العام، جامعة النجاح، نابلس فلسطين 2008 ص 5

[3] علواش ايمان، ليلى كراش، "الاحتيال على شركات التامين البحري"، المجلة الجزائرية للحقوق والسياسية، المجلد 07، العدد01 ،2022 ص 354

1. اساليب الاحتيال الإلكتروني:

يعد الاحتيال الإلكتروني من أبرز التهديدات السيبرانية التي تواجه الأفراد والمؤسسات في البيئة الرقمية، حيث تتنوع أساليبه ودوافعه تبعًا لهدف المهاجمين. ومن أبرز الأسباب التي تدفع الأفراد للانخراط في ممارسات الاحتيال الإلكتروني، الرغبة في التحدي التقني، أو تحقيق مكاسب مادية، أو إثبات الذات داخل مجتمعات القرصنة.

أ. انتحال الشخصية:

يُعدّ هذا الأسلوب من أكثر الطرق شيوعًا في عمليات الاحتيال الإلكتروني، حيث يقوم المهاجم بانتحال هوية شخص حقيقي أو اعتباري عبر الوسائط الرقمية، باستخدام رسائل بريد إلكتروني مزيفة أو صفحات إلكترونية مقلّدة. ويهدف ذلك إلى خداع الضحية وسرقة معلوماته الحساسة، مثل البيانات البنكية أو كلمات المرور، من خلال تقنيات تعرف باسم الهندسة الاجتماعية.

ويستغل بعض المهاجمين مهاراتهم في البرمجة لإنشاء برمجيات خبيثة أو أدوات اختراق، يتم توجيهها إلى أهداف محددة بغرض جمع المعلومات، أو تنفيذ هجمات احتيالية، أو الوصول إلى أنظمة معلوماتية حساسة، خصوصا في المؤسسات المالية أو الحكومية. يعد هذا النوع من الانتحال أحد أكثر أشكال الاحتيال خطرا، لما له من تداعيات مباشرة على الأمن المعلوماتي للأفراد والدولة[1].

ب. الاعتداء على المعطيات:

يمثل الاعتداء على المعطيات أحد أخطر صور الاحتيال والتهديدات السيبرانية، ويتم في الغالب من خلال عمليات الاختراق المعروفة باسم الهاكينغ .(Hacking) وتستهدف هذه الهجمات بشكل مباشر البيانات الرقمية الحساسة، سواء كانت معلومات شخصية، أو وثائق سرّية، أو ملفات ذات طابع خاص تتعلق بالحياة الفردية للمستخدمين.

وتستخدم في هذه الاعتداءات أدوات رقمية متقدمة تعتمد على التحايل والاختراق، أو التزوير، أو إدخال برمجيات خبيثة أو بيانات مزيفة إلى النظام المستهدف. ويكون الهدف منها إما تعطيل النظام، أو التلاعب بالمحتوى، أو سرقة بيانات خاصة مثل الهوية، الحسابات البنكية، الصور، الوثائق، وغيرها من المعلومات الشخصية.

تنعكس خطورة هذا النوع من الهجمات في أنها لا تستهدف الأفراد فقط، بل تمتد لتشمل المؤسسات الإعلامية، والمنصات الاجتماعية، والمواقع الحكومية، وحتى الأجهزة الأمنية، مما يجعل الأفراد والمجتمعات عرضة للابتزاز والتشويه والتضليل .كما تؤدي هذه الاعتداءات إلى إضعاف الثقة في الفضاء الرقمي، وتدفع

[1] هيثم حمود الشلبي،" إدارة مخاطر الاحتيال في قطاع الاتصالات"2009، دار الصفاء للنشر والتوزيع طبعة 28 ص 197

المستخدمين نحو زيادة الحذر والانكماش الرقمي، وهو ما يشكل تحديا للأمن المجتمعي والسيبراني على حد سواء[1].

خصائصه:

1 الاحتيال الإلكتروني جريمة عابرة للحدود: تعد جريمة الاحتيال الإلكتروني من الجرائم الحديثة التي تتجاوز الحدود الجغرافية للدول، إذ يمكن تنفيذها من دولة بينما يقع ضحاياها في دولة أخرى، دون أن توجد بالضرورة علاقة إقليمية مباشرة بين الجاني والضحية. ويعزى ذلك إلى الطبيعة الرقمية لهذه الجريمة، التي تنفذ عبر الشبكة العنكبوتية العالمية، مما يجعل الحدود التقليدية للسيادة الوطنية غير فعالة في الحد منها أو متابعتها قضائيًا.

وتتجلى خطورة هذه الخاصية في أن العديد من الدول قد تواجه صعوبات كبيرة في ملاحقة مرتكبي هذه الجرائم، خصوصا في حال غياب الاتفاقيات الدولية أو عدم وجود إطار قانوني للتعاون القضائي في المجال السيبراني. وهذا ما يجعل جريمة الاحتيال الإلكتروني تحديا أمام منظومة العدالة الجنائية الدولية، ويستدعي ضرورة تطوير آليات التعاون القانوني والتقني عبر الحدود، إلى جانب تعزيز قدرات الأجهزة الأمنية والقضائية لمواجهة هذا النوع من التهديدات.

وقد أولت العديد من المنظمات الدولية اهتماما كبيرا بهذه الجريمة، مثل الاتحاد الأوروبي والانتربول والاتحاد الدولي للاتصالات، ودعت إلى ضرورة تبني تشريعات وطنية متوافقة مع المعايير الدولية، وإنشاء شبكات اتصال وتنسيق لتبادل المعلومات بشكل سريع وفعال[2].

2 لاحتيال الإلكتروني من الجرائم التي يصعب اكتشافها: تعد جريمة الاحتيال الإلكتروني من الجرائم التي يصعب اكتشافها وتتبعها، ويعود ذلك إلى طبيعتها غير المادية وارتكازها على بيئة افتراضية رقمية لا تترك في الغالب آثارًا مادية ملموسة، مما يعقد من مهام جهات التحقيق والمتابعة. فالمجرم الإلكتروني غالبا ما يستعين بوسائل تقنية متقدمة، كاستخدام برامج تشفير، أو تقنيات "إخفاء الهوية(Anonymization) "، أو الشبكات الخاصة الافتراضية(VPN) ، التي تمكنه من تنفيذ الجريمة دون أن يكشف موقعه أو هويته الحقيقية.

ويزداد تعقيد الاكتشاف عندما يلجأ الجاني إلى تقنيات التمويه السيبراني، مثل انتحال هويات رقمية أو استعمال خوادم متعددة وعابرة للدول، ما يؤدي إلى تضليل أجهزة الأمن السيبراني وتأخير الوصول إلى المجرم.

[1] خليل العمر" الجرائم المستحدثة"، دار وائل للنشر، عمان، الأردن 2012ص 225

[2] عبيد علي ناصر، "ماهية جريمة الاحتيال الالكتروني"، مجلة كلية القانون للعلوم القانونية والسياسية، كلية الحقوق جامعة تكريت، بغداد، ص 340

كما أن بعض الضحايا لا يدركون في البداية أنهم تعرضوا للاحتيال، مما يؤدي إلى تأخر الإبلاغ عن الجريمة، وبالتالي ضياع الكثير من الأدلة الرقمية التي قد تكون حاسمة في التحقيق[1].

3 الاحتيال الإلكتروني من الجرائم التي لا تقوم على العنف:

تتميز جريمة الاحتيال الإلكتروني بكونها لا تعتمد في تنفيذها على استخدام العنف الجسدي أو الإكراه المادي كما هو الحال في العديد من الجرائم التقليدية، وإنما تستند إلى وسائل خداعية نفسية وتكنولوجية. إذ يقوم الجاني باستغلال الثغرات المعرفية والسلوكية لدى الضحية باستخدام أدوات مثل الهندسة الاجتماعية، الرسائل الاحتيالية، والمواقع المزيفة، لتحقيق أهدافه دون أي تفاعل مادي مباشر.

ويعرف هذا النمط من الجرائم بـ "الجرائم الهادئة (Silent Crimes) "لأنها تنفذ غالبا خلف شاشات الحاسوب وفي بيئة افتراضية، مما يجعلها غير محسوسة على المستوى الآني، وغير مرتبطة بمظاهر عنف جسدي أو صراع صريح. ومع ذلك، فإن النتائج النفسية والاقتصادية المترتبة على الضحية قد تكون مدمرة، مثل فقدان الثقة، الإحباط، وضياع الأموال أو البيانات الحساسة[2].

الفرع الثاني: التأثيرات الاقتصادية للجرائم المالية

تعد الجرائم المالية والاحتيال الإلكتروني من أبرز التحديات التي تهدد استقرار الاقتصاد الوطني، إذ تتسبب بخسائر مالية مباشرة للدولة والمؤسسات والأفراد، وتؤثر سلبا على مناخ الاستثمار، وتضعف من ثقة المتعاملين في النظام المالي والمصرفي. فالاحتيال الإلكتروني، الذي يشمل عمليات النصب عبر الإنترنت، واختراق الحسابات البنكية، وسرقة البيانات المالية، قد أدى إلى تحويل غير مشروع لرؤوس الأموال، وتدفقها نحو أنشطة إجرامية مثل غسيل الأموال أو تمويل الإرهاب. وتؤكد دربال أمال في دراستها حول "النصب في التأمينات" أن هذا النوع من الجرائم لا يقتصر على الأثر المالي المباشر فحسب، بل يمتد إلى تهديد الأمن الاقتصادي من خلال تقويض الثقة في مؤسسات حيوية مثل شركات التأمين، التي تعد من دعائم الاقتصاد العصري، إذ يعرقل تكرار عمليات النصب والاحتيال قدرتها على الاستمرار والتوسع، ويؤدي إلى رفع تكاليف التشغيل نتيجة زيادة إجراءات المراقبة والتأمين[3]

وشهدت الجزائر خلال السنوات الأخيرة ارتفاعًا ملحوظا في الجرائم المالية والاحتيال الإلكتروني، سواء على مستوى الأفراد أو المؤسسات، مما أثر بشكل مباشر على البنية الاقتصادية، وعلى ثقة المواطنين في المنظومة الرقمية والمالية.

1.**قضية اختراق الحسابات البنكية عبر الإنترنت:** كشفت تقارير صادرة عن المديرية العامة للأمن الوطني في الجزائر عن تفكيك عدة شبكات إجرامية كانت تستخدم بطاقات دفع إلكتروني مزيفة لشراء سلع

[1] عبد المؤمن بن الصغير،" الطبيعة الخاصة للجريمة المرتكبة عبر الانترنت في التشريع الجزائري والتشريع المقارن"، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة ،2015، ص 350

[2] عبيد علي، مرجع سابق 349

[3] دربال أمال" .النصب في التأمينات" مرجع سابق ص 103.

وخدمات عبر الإنترنت، واستهدفت بشكل خاص الشركات التجارية الكبرى ومواقع التسوق الإلكتروني المحلية. وقد أدى ذلك إلى خسائر مباشرة قدرت بملايين الدنانير، وأجبر العديد من المنصات على تعليق خدمات الدفع الإلكتروني مؤقتا، مما أثر سلبًا على توسع التجارة الإلكترونية الناشئة في البلاد.[1]

2.**جرائم غسيل الأموال عبر العملات الرقمية:** أشارت تقارير صادرة عن البنك المركزي الجزائري إلى رصد معاملات مالية غير مشروعة مرتبطة بمنصات العملات الرقمية، مثل البيتكوين، تستخدم لتحويل الأموال إلى الخارج دون رقابة. هذه الظاهرة تهدد الأمن المالي للدولة، وتساهم في نزيف العملة الصعبة، ما يؤدي إلى تقويض الاحتياطات النقدية وزيادة التضخم على المدى البعيد.[2]

وبالتالي فان التهديدات السيبرانية من أبرز المخاطر التي تهدد الاقتصاد الوطني والعالمي على حد سواء. فعلى الصعيد العالمي، تقدر الخسائر الناتجة عن الهجمات الإلكترونية بمليارات الدولارات سنويا، وتشمل تعطيل الخدمات، وسرقة البيانات، وابتزاز الشركات، وانخفاض ثقة المستثمرين. أما في الجزائر، فقد بدأت هذه التهديدات تؤثر بشكل واضح على المؤسسات المالية، والشركات الخاصة، وحتى الإدارات الحكومية، مما يعرقل التحول الرقمي ويزيد من كلفة التأمين الإلكتروني. كما أن ضعف البنية التحتية الرقمية وغياب ثقافة الأمن السيبراني يزيد من الهشاشة الاقتصادية، ويحد من القدرة على جذب الاستثمارات الرقمية.

[1] المديرية العامة للأمن الوطني، "تقرير حول مكافحة الجرائم السيبرانية"، الجزائر، 2021.

[2] بنك الجزائر، "تقرير السياسة النقدية 2022"، الجزائر: بنك الجزائر، ص 33

المطلب الثاني: تأثير الهجمات السيبرانية على البنوك والشركات الكبرى

تعد الهجمات السيبرانية من أخطر التهديدات التي تواجه البنوك والمؤسسات المالية والشركات الكبرى في العصر الرقمي، نظرا لما لها من تأثيرات عميقة تمتد إلى الجوانب التقنية، والمالية، والأمنية، بل وحتى السمعة المؤسسية.

في الولايات المتحدة سنة 2012وفقًا لما نشرته صحيفة نيويورك تايمز، فقد أدى هجوم إلكتروني في عام 2012 إلى إحباط شديد لدى عملاء عدد من أكبر البنوك الأمريكية، مثل: بنك أوف أمريكا (Bank of America)، جي بي مورغان تشيس(JPMorgan Chase) ، سيتي بنك(Citigroup) ، يو إس بنك(U.S. Bank) ، ويلز فارجو(Wells Fargo) ، وبي إن سي.(PNC)

هؤلاء العملاء لم يتمكنوا من الوصول إلى حساباتهم المصرفية أو دفع فواتيرهم عبر الإنترنت، مما تسبب في استيائهم الشديد، خاصةً مع غياب التوضيح الكافي من البنوك بشأن ما كان يحدث بالفعل.

وقد صرح براين موينيهان، الرئيس التنفيذي لبنك أوف أمريكا، للمحللين أن البنك ينفق "مئات الملايين من الدولارات سنويا" على الأمن السيبراني، وذلك بهدف حماية بيانات العملاء من الاختراقات والهجمات.

الجدير بالذكر أن هدف المهاجمين لم يكن سرقة الأموال أو تحقيق مكاسب مالية مباشرة، بل كان الهدف إرباك العملاء وإحباطهم من خلال تعطيل خدمات البنوك الإلكترونية. وهذا من شأنه أن يلحق ضررا غير مباشرا بالبنوك من خلال فقدان ثقة العملاء، وبالتالي خسائر مالية محتملة.

كما أوضحت شبكة CNNأن الهجمات كانت من نوع "هجمات حجب الخدمة – Denial of Service) " (DoS، وهي أداة فعالة لكنها بسيطة من حيث التنفيذ، ولا تتضمن أي اختراق مباشر للأنظمة أو سرقة بيانات. لم تُسرق أي معلومات من البنوك، كما لم تتأثر أنظمتها الأساسية مثل شبكات الصراف الآلي. وكان الهدف الوحيد من الهجوم هو إسقاط المواقع العامة للبنوك (مواقع الإنترنت) بشكل مؤقت، أي المواقع التي يستخدمها العملاء للوصول إلى الخدمات المصرفية[1].

في افريقيا سنة 2016وفقًا لتقرير شركة Serianu، "قام مجرمو الإنترنت بتنفيذ هجوم إلكتروني معقد للغاية استهدف 10 مؤسسات تعمل في قطاعات البنوك، التأمين، الخدمات العامة، والحكومة في ثلاث دول إفريقية".

ووفقًا لنفس التقرير، فإن القطاع المصرفي والخدمات المالية كان الأكثر تضررا من هذه الهجمات السيبرانية، حيث بلغت الخسائر الناتجة عنها ما يقارب 206مليون دولار أمريكي في عام 2016 وحده. كما أشار التقرير إلى

[1] Goldman D (2018) CNN Money. http://money.cnn.com/2012/09/27/technology/bank-cyberattacks/index.html

أن ما لا يقل عن 19 مؤسسة في كينيا تأثرت بفيروس فدية (ransomware) ضمن حملة قرصنة عالمية كانت مستمرة في ذلك الوقت[1].

هذا ما ينتج عنه:

1 خسائر مالية مباشرة وكبيرة

الهجمات على البنوك والمؤسسات المالية تعد من أخطر التهديدات لأنها تستهدف أموال العملاء والأصول الوطنية. في حالة عام 2016، بلغت الخسائر في القطاع البنكي وحده 206 مليون دولار، وهو رقم كبير نسبيا بالنظر لحجم الاقتصادات الإفريقية الناشئة.

2 زعزعة الثقة في النظام المالي

عندما تتعرض البنوك لهجمات متكررة دون قدرة فعالة على الردع أو الحماية، يفقد العملاء الثقة في المؤسسات المصرفية، ما يؤدي إلى سحب الودائع، انخفاض الاستثمار، واعتماد الناس أكثر على الأنظمة النقدية غير الرسمية.

3 تأثير سلبي على مناخ الاستثمار

المستثمرون الأجانب يبحثون عن بيئة آمنة ومستقرة تكنولوجيا. ضعف الأمن السيبراني يرسل إشارات سلبية عن قدرة الدولة على حماية البيانات والمعاملات المالية

وفي أوروبا سنة2015 كشفت مجموعة "آر بي إس" المصرفية (RBS) أنها تعرضت لهجوم سيبراني استهدف خدماتها الإلكترونية، ما أدى إلى صعوبة دخول العملاء إلى حساباتهم لما يقارب الساعة، وذلك بالتزامن مع وقت تحويل الرواتب الشهرية إلى الحسابات، مما تسبب في حالة من الإرباك والانزعاج بين العملاء.[2]

وفي أواخر عام 2015، وقعت عدة حوادث لهجمات سيبرانية استهدفت أنظمة التداول الإلكتروني، كما ذكرت "ناسداك". ومن أبرزها ما حدث مع شركة FXCM Inc.، وهي مزود لخدمات تداول العملات الأجنبية عبر الإنترنت. ففي الأول من أكتوبر، أكدت الشركة أن قراصنة تمكنوا من الوصول غير المصرح به إلى بيانات العملاء، وتم تنفيذ بعض التحويلات المالية من حسابات معينة[3].

[1] Nairobi (2017) WannaCry ransomware virus hits 19 Kenyan firms. The Indian Express. http://indianexpress.com/article/technology/tech-news-technology/wannacry-ransomware-virus-hits-19-kenyan-firms-4665265/

[2] Collinson (2015) Business. The Guardian. https://www.theguardian.com/business/2015/jul/31/rbs-and-natwest-customers-complain-of-online-problems

[3] Research Zacks Equity (2015) 5 Cyber security stocks to change how we protect our data.http://www.nasdaq.com/article/5-cyber-security-stocks-to-change-how-we-protect-our-data-cm531047

وسنة 2016في تقرير آخر صادر عن موقع Crime Russia، جاء أن "القراصنة من مجموعة Lurk، التي طورت برنامجًا خبيثًا (تروجان) يحمل نفس الاسم، تمكنوا من سرقة أكثر من 1.7 مليار روبل روسي (ما يعادل حوالي 28.3 مليون دولار أمريكي) من حسابات البنوك الروسية، قبل أن يتم اعتقالهم من قبل وزارة الداخلية وجهاز الأمن الفيدرالي الروسي (FSB) في يونيو 2016.[1]

كما أشار التقرير إلى حالة بنك Energobank، حيث تسبب هجوم باستخدام برنامج Metelفي أضرار بلغت 244 مليون روبل (حوالي 3.7 مليون دولار أمريكي). وبحسب ما كتبته شركة Kasperskyفي مدونة لها: "بشكل أو بآخر، قام المجرمون بسرقة مبالغ تراوحت بين 2.5 مليون و10 ملايين دولار أمريكي من كل بنك ضحية – وهي مبالغ كبيرة حتى عند النظر إليها بشكل منفرد."

أما هجوم Buhtrapفهو نوع آخر من الهجمات السيبرانية، حيث "قدّر الخبراء أن أقل مبلغ سُرق من أحد البنوك الروسية بلغ 370,000 دولار أمريكي (ما يعادل 25 مليون روبل)، بينما وصل أعلى مبلغ مسروق إلى نحو 9 ملايين دولار (600 مليون روبل).[2]

[1] High Profile Cases (2017) Hackers of Russian group cobalt attacked 250 companies around the world

[2] Kovacs E (2016) Buhtrap gang steals millions from russian banks cybercrime. http://www.securityweek.com/buhtrap-gang-steals-millions-russian-banks

المبحث الثالث: الاثار الثقافية والفكرية للتهديدات السيبر انية

بعد تناول الآثار السياسية والاجتماعية والاقتصادية للتهديدات السيبرانية، ينتقل هذا المبحث إلى البعد الثقافي والفكري لتأثيرات هذه التهديدات على الأمن المجتمعي .لم تعد التهديدات السيبرانية مقتصرة على الجوانب التقنية أو المادية، بل تتجاوز ذلك إلى المساس بالأمن الثقافي والفكري. لقد أدت الثورة الرقمية وتوسع استخدام وسائل التواصل الاجتماعي إلى تحولات في أنماط الاتصال والتفاعل، مما فتح المجال لبروز ظواهر مثل حملات التضليل الإعلامي والتلاعب بالقيم والمعتقدات المجتمعية. سيتناول هذا المبحث كيف يتم توظيف الفضاء الرقمي لبث حملات تضليل إعلامي ونشر أخبار كاذبة تستهدف الوعي الجماعي وثقة المواطنين في المؤسسات، وكيف يؤثر التلاعب بالقيم والمعتقدات من خلال الإنترنت ووسائل الإعلام الرقمية على النسيج الاجتماعي والهوية الثقافية، بالإضافة إلى قضايا مثل انتهاك الخصوصية وتأثيرها على الأفراد والمجتمع.

المطلب الأول: الحملات الاعلامية المظللة

الفرع الأول مفهوم الحملات الإعلامية المظللة

"مجموعة من الأنشطة الإعلامية المخططة والمنظمة التي تهدف إلى نشر معلومات زائفة أو مغلوطة أو مجتزاه، بشكل متعمد ومنهجي، بغرض التأثير على الرأي العام، وتوجيهه أو تضليله، أو إرباكه، أو زعزعة ثقته بمؤسسات الدولة، أو دعم أجندات معينة".

أبرزسمات الحملات الإعلامية المضللة:

1.**التحكم في المحتوى والمصادر** :استخدام معلومات مضللة، إحصائيات خاطئة، صور مفبركة أو خارجة عن السياق.

2.**الانتشار المكثف والمنسق** :غالباً ما تستخدم حسابات وهمية، منصات رقمية متعددة (فيسبوك، تويتر، يوتيوب).

3.**البعد النفسي والسياسي** :تستغل الأزمات، التوترات الاجتماعية أو القضايا الهوياتية لإثارة الانقسام أو التشويش.

4.**السرعة والاختراق** :تعتمد على سرعة النشر لخلق بلبلة قبل التحقق من المعلومة، ما يصعب مواجهتها فورياً[1].

الفرع الثاني: تأثيرها الثقافي والفكري:

تعد الحملات الإعلامية المضللة إحدى أخطر الأدوات التي توظفها التهديدات السيبرانية للتأثير على الوعي الجماعي والثقافة العامة للمجتمعات، حيث تعتمد هذه الحملات على نشر معلومات كاذبة أو محرفة

[1] محمود رمضان دياب ."استراتيجيات الحملات الإعلامية" .الإسكندرية مؤسسة شباب الجامعة، 2019.ص 10

عبر الفضاء الرقمي، مستهدفة تشكيل الرأي العام وفق أجندات خفية، قد تكون سياسية أو أيديولوجية أو اقتصادية. وغالبا ما يتم تنفيذ هذه الحملات عبر وسائل التواصل الاجتماعي، مستفيدة من خوارزميات الانتشار الواسع وسرعة التفاعل، بما يؤدي إلى خلق "فقاعات معرفية" تعيق الوصول إلى الحقائق وتعزز الانقسام داخل المجتمع.

تتجلى خطورة هذا النوع من الهجمات في قدرته على إضعاف ثقة المواطنين بالمؤسسات، ونشر خطاب الكراهية، والتأثير على العمليات الانتخابية وصناعة القرار، بل وتغيير السلوكيات والقيم الثقافية من خلال بث رسائل مضادة للثقافة المحلية أو الرموز الوطنية.

ويلاحظ أن الدول ذات المناعة الرقمية الضعيفة تصبح أهدافا مفضلة لهذه الحملات، إذ تفتقر إلى الوعي الإعلامي الرقمي لدى شرائح واسعة من السكان، ما يجعل من السهل اختراق وعيهم المجتمعي وبث الأفكار الزائفة التي قد تؤدي إلى زعزعة الاستقرار الثقافي والاجتماعي[1].

وتشكل الحملات الإعلامية المضللة أحد أبرز تجليات التهديدات السيبرانية، نظرا لما تسببه من آثار عميقة في البنية الفكرية والثقافية للمجتمع، حيث تستهدف هذه الحملات تفكيك الوعي الجمعي، وبث الشكوك، وإحداث انقسامات داخل النسيج الاجتماعي من خلال بث معلومات مغلوطة أو مضللة عبر الفضاء الرقمي.

وتتجلى خطورة هذه الحملات في قدرتها على النفاذ السريع إلى شرائح واسعة من المجتمع عبر وسائل التواصل الاجتماعي، خصوصا في البيئات التي تعاني من هشاشة إعلامية أو انخفاض في منسوب الوعي الرقمي. في هذا السياق، يشير الباحث عبد الله محمد سيد إلى أن "التهديدات السيبرانية لم تعد مقتصرة على البنية التحتية التقنية، بل تطورت لتشمل عمليات تضليلية منهجية تؤثر في الرأي العام، وتستهدف إدراك الأفراد واتجاهاتهم حيال قضايا وطنية وسياسية.[2]

تستخدم هذه الحملات أحيانا كأدوات لحرب نفسية ناعمة، إذ لا تحتاج إلى أسلحة تقليدية بل تعتمد على التأثير النفسي والثقافي والتلاعب بالإدراك الجمعي، الأمر الذي يضعف ثقة المواطنين في مؤسساتهم الرسمية، ويغذي الشعور بالاغتراب والشك. وكما أوضح محمود رمضان دياب، فإن "استراتيجيات الحملات الإعلامية تبنى على تحليل البيئة النفسية والاجتماعية للمجتمع المستهدف، ما يجعلها قادرة على اختراقه ثقافيًا وإحداث التصدع الداخلي عبر منصات رقمية.[3]

أما في السياق الدولي، فيُظهر تحليل صدر عن معهد ستراتفور الأمريكي أن الحملات التضليلية أصبحت أداة رئيسية في الحرب السيبرانية الحديثة، حيث تُستغل الثغرات السيكولوجية والثقافية لنشر خطاب الكراهية، وتضخيم الانقسامات السياسية والعرقية[3]. ويشير Thomas Rid، الخبير في الحروب المعلوماتية،

[1] عبد الكريم حسام،" التحولات الرقمية وأمن المعلومات "عمّان: دار الصفاء للنشر والتوزيع، 2021 ص، 91.

[2] عبد الله محمد. "الأمن السيبراني: التهديدات والتحديات في البيئة الرقمية المعاصرة." القاهرة: مكتبة الأنجلو المصرية، 2020.ص 19

[3] محمود رمضان دياب ."استراتيجيات الحملات الإعلامية" .الإسكندرية: مؤسسة شباب الجامعة، 2019.ص 81

إلى أن "أثر المعلومات الزائفة لا يكمن فقط فيما تقوله، بل في قدرتها على زرع الشك في كل شيء، وبالتالي تقويض أسس الحقيقة ذاتها.[1]

وعلى ضوء ذلك، فإن الأثر البعيد المدى لهذه الحملات لا يقتصر على التضليل المؤقت، بل يمتد ليؤسس لحالة **"فوضى معرفية "**تعطل وظيفة الإعلام النزيه، وتعرقل آليات اتخاذ القرار داخل المجتمعات، بما يهدد الأمن المجتمعي في أبعاده الثقافية، والسياسية، والسلم الأهلي.

[1] Stratfor. Disinformation and Cyber Threats: A Global Strategic Report, Stratfor Global Intelligence, 2021

المطلب الثاني: التلاعب بالقيم والمعتقدات عبر الانترنت

الفرع الأول: مفهوم الانترنت

تعد الإنترنت من أبرز مظاهر الثورة التكنولوجية في العصر الحديث، وقد غيّرت بشكل جذري أنماط التواصل، والمعرفة، والتفاعل الاقتصادي والسياسي والثقافي. وبالرغم من استخدامها الواسع، إلا أن وضع تعريف جامع مانع لها يُعد أمرًا صعبًا بسبب تشعّب وظائفها وتعدد الحقول التي ترتبط بها، سواء على الصعيد التقني، الاجتماعي، أو القانوني.

قد عرفها الباحث طارق طه بأنها:

"شبكة دولية واسعة النظام غير خاضعة لأي تحكم مركزي، تضم بداخلها مجموعة شبكات لحاسبات آلية خاصة وعامة منتشرة في جميع أنحاء العالم.[1]

ثانيًا – تعريف القيم

أ- المعنى اللغوي:

تُشتق كلمة "القيم" من الجذر اللغوي(**ق-و-م**)، والذي يفيد معنى القيام والاستقامة والاعتدال .وقد ورد في قوله تعالى" :فاستقيموا إليه"، أي التوجه إلى الله دون غيره من الآلهة، دلالة على الالتزام والانضباط الأخلاقي. كما يُقال: "قوّمت الشيء"، أي جعلته قويما ومستقيما، أي على الطريق السوي والصحيح.[2]

الفرع الثاني: تأثير الانترنت ووسائل الاعلام على القيم والمعتقدات الاجتماعية:

لقد أصبحت الانترنت ووسائل الإعلام أدوات أساسية تلعب دورها في عملية التطبيع والتنشئة الاجتماعية. إذ يتعرض الفرد منا إلى ساعات طويلة أمامها وهناك اتفاق عام على هذه الوسائط التي تزودنا بمعلومات، آراء ومواقف تساعد إلى حد كبير على تكوين تصورنا للعالم الذي نعيش فيه .أن الانترنت ووسائل الإعلام تحدث آثار على الاتجاهات والقيم. أما الفترة اللازمة لإحداث هذا الأثر فما زالت محل جدل، إذ تشير بعض الدراسات إلى انها تقوم بدور ملموس في تكوين آرائنا أكثر من تغييرها.[3]

ومن بين الآثار السلبية الخطيرة التي يمكن أن تحدثها وسائل الإعلام – خاصة الترفيهية منها – هو تحييد القيم، ويُقصد بذلك إقصاء القيم الأخلاقية والدينية والإنسانية من المحتوى الإعلامي، أو تهميشها لدرجة تصبح فيها غير فعالة في تشكيل الوعي العام. وتتمثل هذه العملية في تغييب القيم من المضامين، ضمن ما يعرف بدائرة "العرض والطلب الثقافي"، حيث تسعى وسائل الإعلام إلى تقديم ما يرغب فيه الجمهور، بينما يقبل الجمهور بدوره على الوسائط التي تشبع رغباته، ما يخلق بيئة تفضي إلى انتشار مضامين العنف،

[1] درمان، الذناني عبد المالك، 2008، "تكنولوجيا الاتصال وعولمة المعلومات"، المكتب الجامعي الحديث. ص 208

[2] نصير بوعلي، "الاعلام والقيم"، دار الهدى، عين مليلة الجزائر، 2005، ص.133

[3] خليل صابات، "وسائل الإعلام نشأة وتطورها"، مكتبة الانجلو مصرية، القاهرة، 1972، ص. .169

الجنس، والممارسات الهابطة، خصوصًا في الإنتاجات ذات الطبيعة التجارية كالدراما والمسلسلات والألعاب الرقمية.

وقد أسهم هذا الاتجاه بشكل ملحوظ في تآكل البنية القيمية للمجتمع، خاصة في ظل سيطرة المنصات الرقمية ذات الطابع العابر للحدود، حيث أصبحت الثقافة المحلية مهددة بالتهميش أو الاستبدال بقيم مستوردة لا تتلاءم دائما مع خصوصيات المجتمعات العربية، ومنها الجزائر.

1. جمهرة الثقافة: بين التبسيط والتشويه

تعد جمهرة الثقافة من أبرز التحولات التي أحدثتها الوسائط الرقمية الحديثة، حيث تسعى وسائل الإعلام إلى جذب أكبر عدد ممكن من الجمهور، وهو ما يتحقق غالبا من خلال تبسيط المحتوى وتقديمه في قالب ترفيهي سطحي .في هذا السياق، يتم التضحية بالعمق والجودة لصالح الانتشار الجماهيري، ما يؤدي إلى تشويه المفاهيم الثقافية وتحويل الثقافة من عملية تنويرية إلى مجرد سلعة إعلامية.

وتعرف هذه الظاهرة أحيانا بـ**"الثقافة الجماهيرية"**، وهي ثقافة تنتجها وسائل الإعلام (كالإعلانات، المسلسلات، الأفلام) وتُوجَّه لأوسع جمهور ممكن، دون اعتبار للقيم أو الأبعاد الفكرية العميقة. هذه الثقافة لا تسعى إلى الارتقاء بالذوق العام، بل إلى التأثير الدعائي وخلق احتياجات استهلاكية وهمية أو حقيقية، مما يسهم في تشويه الوعي الجمعي، وإضعاف الحس النقدي، لا سيما بين الفئات الشابة، ويهدد القيم الثقافية الأصلية للمجتمعات.

وفي ظل الفضاء السيبراني، تتسارع هذه الظاهرة بشكل أكبر، إذ تتيح المنصات الرقمية العالمية بث هذه الثقافة على نطاق غير مسبوق، مما يجعلها واحدة من أبرز التهديدات السيبرانية الثقافية التي تمس الأمن المجتمعي[1].

2. اضعاف نسيج الاتصال الاجتماعي

من بين أبرز الآثار الاجتماعية التي تفرزها الوسائط الرقمية الحديثة، تَبرز ظاهرة تفكك النسيج الاجتماعي كنتيجة مباشرة لتغير أنماط الاتصال والتفاعل. فقد أدّى الاعتماد المفرط على وسائل الاتصال الحديثة، مثل الهواتف الذكية والحواسيب المتصلة بالإنترنت، إلى تقليص الزمن الاجتماعي الذي يُفترض أن يقضى في تفاعل مباشر داخل الأسرة أو المجتمع.

ويرى بعض الباحثين أن وسائل الإعلام، رغم كونها لا تسعى عمدا إلى تقويض العلاقات الاجتماعية، تمارس بشكل غير مباشر عملية تفكيك اجتماعي، لأن الوقت الذي يمضيه الفرد في استخدام هذه الوسائل يكون دائمًا على حساب التفاعل الإنساني الواقعي. ومع تزايد مدة البث وتعدد قنوات الإعلام، صارت الأسرة

[1] عزي عبد الرحمن، السعيد بومعيزة، نصير بوعلي، "نظرية الحتمية القيمية في الإعلام، جامعة الأمير عبد القادر للعلوم الإسلامية"، قسنطينة، 2009، ص 116

محرومة من أوقات الحوار والتشاور وتبادل الرأي، ما يُضعف الروابط العاطفية والاجتماعية داخلها، ويفتح المجال أمام العزلة الفردية والانطواء.

وتعزز هذه الظاهرة الطابع الفردي في استخدام وسائل الاتصال، إذ لم تعد الأجهزة كالحاسوب والهاتف تُستخدم بشكل جماعي داخل الأسرة، بل أصبحت أدوات شخصية تعمق من الانفصال داخل الوحدة الاجتماعية، الأمر الذي يشكل تهديدًا مباشرًا لركائز الأمن المجتمعي من الداخل، لا سيما في ظل الانتشار الواسع للمنصات السيبرانية[1].

3. المعيارية والاستهلاكية:

تشير المعيارية في السياق الإعلامي والثقافي إلى تلك العملية التي يتم فيها قولبة المضمون الثقافي في شكل بضائع رمزية متجانسة قابلة للتسويق الجماهيري، حيث تقصى أو تهمش العناصر الثقافية التي لا تتوافق مع ما يُعتبر سائدا أو مقبولًا وفق معايير السوق أو الثقافة المهيمنة. وتصبح بذلك وسائل الإعلام الرقمية عاملاً فاعلا في إعادة تشكيل الثقافة الجماهيرية من خلال فرض نماذج محددة من القيم، السلوكيات، والأنماط الاجتماعية.

أما الاستهلاكية، فتتجلى في الدور الذي تلعبه هذه الوسائل في تعزيز النزعة المادية، وذلك من خلال الإعلانات المباشرة أو عبر الترويج غير المباشر لأنماط الحياة التي تسوقها المسلسلات والأفلام، والتي غالبا ما تصور النجاح والسعادة كمحصلة للامتلاك والاستهلاك. يؤدي هذا الترويج إلى تغيير في أنماط التفكير والسلوك داخل المجتمعات، حيث يربط الرفاه بالسلوك الاستهلاكي، يصبح الفرد أكثر عرضة للتأثير من خلال المعايير المادية بدلا من القيم الأخلاقية أو الثقافية.

هذا النمط الثقافي يهدد الأمن الثقافي للمجتمعات، خصوصا في الدول النامية، من خلال تفريغ الثقافة من محتواها القيمي واستبدالها بمضامين تجارية تفتقر إلى العمق والهوية. كما تسهم هذه العملية في إضعاف التنوع الثقافي وتعزيز الهيمنة الثقافية الرقمية ذات الطابع الغربي في الغالب.[2]

4. انتهاك الخصوصية:

أصبحت الأنترنت مجال خصبا للاعتداء على الحياة الخاصة خاصة بعد انتشار مواقع الدردشة وشبكات التواصل الاجتماعي وغزوها لمجتمعاتنا مثل space my, twitter, YouTube وارتفاع عدد مستخدميها الذين يقومون بوضع معلومات عن أنفسهم تكون متاحة للجميع كوضع صورهم وأصدقائهم وعائلاتهم ومقاطع فيديو عن مناسبات خاصة بهم، مما يجعلهم عرضة للمساس بخصوصياتهم من قبل المتطفلين أو الهاكرز أو حتى محترفي الاجرام الالكتروني، والأسوأ استخدام المراهقين والأطفال لهذه المواقع والشبكات ووضعهم لكثير من المعلومات الخاصة بهم دون رقيب أو حسيب مما يجعلهم في كثير من الأحيان-لقمة سائغة لابتزاز- تارة

[1] عزي عبد الرحمن، مرجع سبق ذكره ص 117

[2] عزي عبد الرحمن، مرجع سيق ذكر ص119 ص120

والتهديد والتعزير بهم تارة أخرى من قبل مجرمي الانترنت الذين استغلوا المعلومات الخاصة بهؤلاء المراهقين الذين وضعوها بكل براءة وقلة ادراك اهميتها من خلال اشتراكهم في غرف الدردشة أو مواقعها أو شبكات التواصل الاجتماعي.[1]

أدى هذا الانتشار الواسع للإنترنت ووسائل التواصل الاجتماعي إلى فتح المجال أمام حملات رقمية تستهدف التأثير في القيم والمعتقدات الفردية والجماعية، خاصة في المجتمعات النامية. وتستخدم أدوات إعلامية رقمية موجهة لنشر معلومات مضللة، وترويج أنماط سلوكية وثقافية غريبة عن البيئة المحلية، مما يهدد التماسك الاجتماعي ويغذي الانقسام الثقافي والفكري. هذا التلاعب غالبا ما يكون منظما ومدعوما من جهات داخلية أو خارجية تهدف إلى زعزعة الهوية الثقافية، والتأثير على الرأي العام، وتوجيهه بما يخدم مصالح معينة، سواء كانت سياسية أو أيديولوجية أو اقتصادية.

[1] سوزان عدنان، وصفاء اوتاني. 2013 "انتهاك الحياة الخاصة عبر الانترنت" دراسة مقارنة. مجلة جامعة دمشق للعلوم الاقتصادية والقانونية العدد03 ص29

الفصل الثالث: استراتيجيات مواجهة التهديدات السيبرانية وتعزيز الأمن المجتمعي

تمهيد

استكمالا للفصل الثاني الذي بحث في تأثيرات التهديدات السيبرانية على الأمن المجتمعي، يتجه هذا الفصل نحو استعراض وتحليل الاستراتيجيات والآليات المتبعة وطنيا ودوليا لمواجهة هذه التحديات المتزايدة وتعزيز الأمن المجتمعي في وجهها .إدراكاً لخطورة هذه التهديدات، التي تستهدف مؤسسات الدولة وبناها التحتية الحيوية والمواطنين، أصبحت معالجتها تقتضي مقاربة شاملة تأخذ بعين الاعتبار الجوانب التكنولوجية، القانونية، السياسية، والاجتماعية، وتحلل انعكاساتها على السلم المجتمعي. يستوجب البحث الوقوف على الاستراتيجية الجزائرية لمواجهة هذه التهديدات، والتحديات التي تعترض جهودها في هذا المجال، في ظل ضعف البنية الرقمية الوطنية، وقصور الوعي السيبراني لدى فئات واسعة من المجتمع. سيبحث هذا الفصل في جهود الجزائر الوطنية في التصدي لمخاطر الفضاء السيبراني، بما في ذلك تطوير البنية الرقمية، وسن التشريعات القانونية لمكافحة الجريمة السيبرانية، وتعزيز الوعي السيبراني لدى فئات المجتمع. كما سيتناول دور المؤسسات الحكومية المتخصصة في حماية البنية التحتية السيبرانية. إلى جانب الجهود الوطنية، سيسلط الفصل الضوء على أهمية التعاون الدولي، واستعراض بعض التجارب الدولية الناجحة في هذا المجال. يهدف هذا الفصل إلى تقييم مدى فعالية الاستجابات الحالية وكشف التحديات التي لا تزال تعترض بناء منظومة حماية سيبرانية فعالة تعزز الأمن المجتمعي الوطني.

المبحث الأول: السياسات الوطنية لمواجهة التهديدات السيبرانية

في سياق البحث عن سبل مواجهة التحديات التي تفرضها التهديدات السيبرانية على الأمن المجتمعي الجزائري، يركز هذا المبحث على تحليل السياسات والاستراتيجيات التي تبنتها الدولة الجزائرية على المستوى الوطني .لقد أدركت الجزائر، كغيرها من دول العالم، حجم الخطر الذي تمثله الجرائم السيبرانية والاختراقات الرقمية على سيادتها واستقرار مؤسساتها وأمن مواطنيها. لم تكن هذه المواجهة سهلة، خاصة في ظل هشاشة البنية التحتية الرقمية الوطنية، وقصور الوعي السيبراني لدى فئات واسعة من المجتمع، فضلاً عن الموقع الجيوسياسي الحساس الذي يجعلها هدفاً لمحاولات اختراق ممنهجة. سيتناول هذا المبحث بالتحليل الجهود التشريعية والمؤسساتية التي قامت بها الجزائر للتصدي لهذه التهديدات، وتقييم مدى فعاليتها في بناء منظومة وطنية للأمن السيبراني.

المطلب الأول: التشريعات والقوانين المتعلقة بالأمن السيبراني في الجزائر

يشهد العالم المعاصر تحولات نوعية غير مسبوقة، خاصة في مجال التكنولوجيا الرقمية، حيث ساهمت الثورة المعلوماتية في إعادة تشكيل مفهوم التواصل والاقتصاد والخدمات العامة، كما مكنت الإنسان من تجاوز الحيز الجغرافي والزماني، عبر بيئة افتراضية باتت تتحكم في جوانب كثيرة من الحياة اليومية. وقد أصبح من الممكن، بفعل هذه التطورات، إنجاز الأعمال وتسيير المؤسسات عن طريق شبكات إلكترونية، وعلى رأسها شبكة الإنترنت، ما عزز من فعالية الأداء وسرعة التفاعل، لكنه في المقابل أفرز تحديات أمنية جديدة.

الفرع الأول: التدابير التقنية والأمنية:

رغم الإيجابيات المتعددة التي أفرزها التقدم التكنولوجي، إلا أن الفضاء السيبراني تحول إلى ساحة نزاع جديدة، تهدد الأفراد والدول على حد سواء. فقد تنامت في السنوات الأخيرة الهجمات السيبرانية التي تستهدف البيانات الشخصية والمؤسسات السيادية والمالية، وتعددت أشكال الجرائم الإلكترونية، من الاحتيال المصرفي إلى القرصنة والتجسس، وصولا إلى الإرهاب السيبراني الذي بات يهدد الأمن القومي للدول واستقرارها الداخلي. وتكمن خطورة هذا النوع من التهديدات في كونه غير تقليدي، عابر للحدود، ويصعب رصده في الوقت المناسب.

في السياق الجزائري، لم تكن الدولة بمعزل عن هذه التهديدات، فقد عرفت مؤسساتها، لا سيما الوطنية منها، محاولات اختراق متكررة، لعل أبرزها ما تم الكشف عنه بشأن برمجية التجسس الإسرائيلية "بيغاسوس"، ما كشف عن هشاشة البنية الرقمية في مواجهة الهجمات المتطورة. كما عرفت البلاد تزايدًا ملحوظا في جرائم الاحتيال والنصب الإلكتروني، خاصة عبر شبكات التواصل الاجتماعي، والتي استغلت لتضليل المستخدمين واختراق حساباتهم، مما جعل الأفراد والمؤسسات أهدافا سهلة للاعتداءات الإلكترونية.

ويرتبط تصاعد هذه التهديدات السيبرانية بشكل مباشر بالموقع الجيوسياسي الحساس للجزائر، مما جعلها عرضة لمحاولات اختراق ممنهجة من أطراف دولية وجهات غير حكومية. وعليه، فقد كان من الضروري أن تعيد الجزائر النظر في مقاربتها الأمنية، وأن تعطي الأمن السيبراني أولوية ضمن استراتيجيتها الوطنية، عبر

تبني آليات تشريعية وتقنية فعالة، وتطوير قدرات الاستجابة السريعة، ورفع مستوى الوعي الرقمي لدى المستخدمين، لضمان سيادة الدولة وحماية أمنها القومي في ظل التحديات الرقمية المتسارعة..

أدركت الدولة الجزائرية في السنوات الأخيرة حجم التهديد الذي تمثله الجرائم السيبرانية على أمنها الوطني، خاصة مع تنامي الاعتماد على تكنولوجيا المعلومات والاتصال في مختلف القطاعات. وقد جاء هذا الوعي في سياق دولي يتسم بتعاظم دور الفضاء السيبراني كساحة جديدة للصراعات الجيوسياسية، حيث باتت الحروب الحديثة تعتمد بشكل متزايد على الهجمات الإلكترونية إلى جانب الأدوات التقليدية.

وفي هذا الإطار، تحرك المشرع الجزائري لتدارك النقص القانوني والمؤسساتي، من خلال إطلاق سلسلة من الإصلاحات التشريعية الهادفة إلى تجريم الأفعال التي تمس بأنظمة المعالجة الآلية للمعطيات .وقد بدأت هذه الإصلاحات بتعديل قانون العقوبات بموجب القانون 15-04 [1]الذي أدرج فصولاً جديدة تجرم المساس بالأنظمة الإلكترونية وقرصنتها. كما تعززت هذه الإجراءات لاحقًا بإصدار القانون 22-06 [2]المعدل لقانون الإجراءات الجزائية، والذي جاء بمقتضيات جديدة تتيح تتبع الجرائم المرتبطة بتكنولوجيا المعلومات والتحقيق فيها بكفاءة أعلى.

إلى جانب ذلك، أقر القانون 04-09 [3]المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ليشكل بذلك دعامة تشريعية أساسية في استراتيجية الدولة لمكافحة التهديدات الرقمية.

لم يعد من الكافي أن تكون الملاحقة الفعالة للمجرمين السيبرانيين مقتصرة فقط على القواعد القانونية الموضوعية ذات الطبيعة العقابية، بل من الضروري أن تصاحبها قواعد إجرائية وقائية وردعية وتنظيفية، تسمح بالكشف المبكر عن الجرائم الإلكترونية أو على الأقل الحد منها، وتسهم في منع وقوعها من خلال إجراءات احترازية فعالة.

وقد أدرك المشرع الجزائري هذه الضرورة، ما دفعه إلى إدراج نصوص قانونية تنظم الإجراءات الإلكترونية ضمن قانون الإجراءات الجزائية، لاسيما من خلال القانون رقم 06-22. فقد نص هذا القانون على تدابير إجرائية محددة تتعلق بالتحقيق في الجرائم الإلكترونية، والتي تشمل مراقبة الاتصالات الإلكترونية وتسجيلها واعتراضها[4].

[1] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم15 04، لمؤرخ في 01 فيفري 2015، المتضمن القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، الجريدة الرسمية، العدد06

[2] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 06/ 22، المؤرخ في 20 ديسمبر2006، المتضمن قانون الإجراءات الجزائية، الصادر في الج. ج ج، العدد37

[3] الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 09/ 04، المؤرخ في 2009، المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال مكافحتها، الجريدة الرسمية العدد 47

ويقصد بهذه التدابير تسجيل أو نسخ أو اعتراض المراسلات الصادرة أو الواردة عبر الوسائل الإلكترونية، سواء كانت تلك المراسلات عبارة عن بيانات قابلة للتخزين أو التوزيع أو العرض، وتم نقلها عبر قنوات الاتصال السلكية أو اللاسلكية. ويتم ذلك في إطار البحث والتحري عن الجريمة السيبرانية، وضمانًا لجمع الأدلة المتعلقة بها.

وقد أشار المشرع الجزائري في المادة 65 مكرر 5 من قانون الإجراءات الجزائية إلى الشروط والظروف التي تجيز اللجوء إلى هذا النوع من الإجراءات. يُسمح بذلك للسلطات القضائية المختصة إذا اقتضت ضرورة التحقيق في جريمة إلكترونية ذلك، سواء تعلق الأمر بمراسلات سلكية أو لاسلكية، تسجيلا أو اعتراضا، أو تسجيل الأصوات والصور والمحادثات، وحتى التعرف على بيانات الطاقة.

ويشترط لذلك توفر الوسائل التقنية المناسبة للقيام بهذه العمليات، بهدف الكشف عن الجريمة والمشتبه فيهم، وذلك دون المساس بمبدأ الحصول على إذن قضائي في إطار التفتيش أو الضبط وفقًا للمادة 20 من القانون نفسه[1].

مع ذلك، فإن المشرع الجزائري لم يمنح هذا الإجراء صلاحية مطلقة، بل أحاطه بجملة من الضمانات القانونية التي تهدف إلى الحد من تعسف السلطات في استعمال وسائل التحري، والحفاظ على الحقوق والحريات العامة والفردية، بما يضمن التوازن بين مقتضيات الأمن وحماية الحريات.

الفرع الثاني: التدابير القانونية والتعاون الدولي

إدراكا منها للطبيعة العابرة للحدود للجرائم السيبرانية، عملت الجزائر على تعزيز البنية المؤسسية للأمن السيبراني، من خلال إنشاء هياكل متخصصة داخل الأجهزة الأمنية والقضائية. كما أولت أهمية كبيرة لتكثيف التعاون الدولي، سواء في إطار التعاون الثنائي أو عبر الانخراط في المبادرات الدولية المتعلقة بمكافحة الجرائم الرقمية، وذلك في سياق مواجهة التحديات التي تفرضها العولمة الأمنية واختراقات الفضاء السيبراني لسيادة الدول.[2]

تأثرت الجزائر، على غرار العديد من الدول، بالتحولات الكبرى التي أفرزتها الثورة المعلوماتية، والتي أدت إلى بروز أنماط جديدة من الإجرام لم تعهدها المجتمعات البشرية من قبل، خاصة ما بات يعرف بـ "الجرائم السيبرانية". وقد دفعت هذه التحديات المشرع الجزائري إلى التدخل لتقنين الظاهرة، عبر إدراج مجموعة من التعديلات التشريعية في قانون العقوبات، لمواكبة المستجدات الرقمية والحد من انعكاساتها الأمنية.

في هذا السياق، أصدر المشرع القانون رقم 15-04 الذي عدل بموجبه الأمر رقم 66-156 المتضمن قانون العقوبات، حيث أدرج قسما جديدا تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات"، وشمل المواد

1اسمهان بوضياف، "الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد03، العدد 03، ص 364

[2] محمد احمد سليمان عيسى، "التعاون الدولي لمواجهة الجرائم الالكترونية"، المجلة الاكاديمية للبحث القانوني، كلية العلوم والدراسات الإنسانية، المجلد14، العدد02 2016 ص61

من 394مكرر إلى 394 مكرر 7، وهو ما مثل أول تقنين صريح للجرائم المعلوماتية في التشريع الجزائري. وقد نُص في هذا القسم على جملة من الأفعال المجرّمة التي تمس بسرّية وسلامة المعطيات الرقمية، سواءً من خلال الاختراق أو التعديل أو الإتلاف أو القرصنة.

ولم يتوقف التطوير القانوني عند هذا الحد، بل عزز لاحقا من خلال إصدار القانون رقم 23-06 لسنة 2006، والذي جاء ليشدد العقوبات المتعلقة بالجرائم السيبرانية دون أن يمس بالبنية الأساسية للنصوص التجريمية السابقة. ويفهم من هذا التعديل أن المشرع الجزائري قد بات أكثر وعيا بخطورة هذا النمط من الجريمة، خصوصا لما له من تأثير مباشر على الاقتصاد الوطني والاستقرار المؤسسي، إضافة إلى اتساع نطاق ارتكابه وانتشاره.

وفي عام 2016، تواصل هذا المسار التشريعي بإصدار القانون رقم 16-02[1]، الذي عدل قانون العقوبات مرة أخرى، مضيفاً مادتين هامتين هما 87مكرر 11 و 394مكرر 8 .وقد استخدمت في المادة الأولى مصطلحات حديثة مثل "تكنولوجيات الإعلام والاتصال"، بينما تم في الثانية إدراج مفاهيم ترتبط بالبنية التحتية للفضاء السيبراني، مثل "مقدمي خدمات الإنترنت"، مما يعكس تطورا في اللغة القانونية نفسها لمواكبة البيئة الرقمية.[2]

[1] الجمهورية الجزائرية الديمقراطية الشعبية، القانون 02/ 16، المؤرخ في 19 جوان 2016، المتضمن تعديل قانون العقوبات، الجريدة الرسمية. العدد 37

[2] مراد مشوش، الجريمة المعلوماتية في ظل قانون العقوبات وقانون الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، مجلة القانون المجلد 09، العدد01 2020 ص 112

المطلب الثاني: دور المؤسسات الحكومية في حماية البنية التحتية السيبرانية

أدركت الجزائر في ظل التحديات التي تفرضها الجرائم السيبرانية والتهديدات الرقمية المتزايدة، ضرورة تطوير منظومة وطنية للأمن السيبراني تهدف إلى حماية البنى التحتية الرقمية الحيوية وضمان أمن المعلومات. وقد تجسدت هذه الرؤية عبر إنشاء وتفعيل مؤسسات وهيئات حكومية متخصصة، تعمل على مواجهة المخاطر السيبرانية وفق إطار تشريعي وتنظيمي يتماشى مع التحولات التكنولوجية.

1. **مركز الوقاية من جرائم الاعلام الالي والجرائم المعلوماتية للدرك الوطني:** أنشئ في 2008 ويعتبر الجهاز الوحيد المختص بهذا الصدد في الجزائر ويهدف الى تامين منظومة المعلومات لخدمة الأمن العمومي، واعتبر بمثابة مركز توثيق ومقره يوجد ببئر مراد رايس، هذا المركز يعكف على تحليل معطيات وبيانات الجرائم المعلوماتية المرتكبة، وتحديد هوية أصحابها سواء كانوا اشخاص فرادى او عصابات، وهذا كله من اجل تامين الأنظمة المعلوماتية والحفاظ عليها، لا سيما تلك المستعملة في المؤسسات الرسمية والبنوك والبيوت.
2. **وزارة الدفاع الوطني ومركز الإشراف السيبراني:** تلعب وزارة الدفاع الوطني دورا محوريا في مجال الأمن السيبراني، لا سيما عبر مديرياتها التقنية والاستخباراتية، التي تعنى برصد التهديدات الخارجية المحتملة التي تستهدف البنى التحتية الرقمية للدولة، خصوصًا تلك ذات الطابع الاستراتيجي (الطاقة، الاتصالات، النقل...).

كما عملت الوزارة على تطوير مركز إشراف سيبراني يتولى مراقبة الفضاء الرقمي الوطني، واكتشاف محاولات الاختراق والهجمات الإلكترونية في الزمن الحقيقي، مع العمل على تعزيز قدرات الحماية والرد السيبراني.

3. **وزارة الرقمنة والإحصائيات:** تشرف وزارة الرقمنة والإحصائيات على وضع الأطر التكنولوجية والإدارية المتعلقة بتسيير أنظمة المعلومات الحكومية، وهي الجهة المسؤولة عن تنسيق مشاريع الرقمنة على المستوى الوطني، بما في ذلك:

- تطوير منصات حكومية مؤمنة
- تشجيع تبني المعايير الدولية في الأمن السيبراني
- دعم المؤسسات العمومية في عملية التحول الرقمي مع مراعاة الجوانب الأمنية[1].

4. **التنسيق مع الهيئات الدولية:** ضمن البعد التعاوني، تسعى الجزائر إلى الانخراط في أطر إقليمية لمواجهة التهديدات الرقمية، من خلال

- التعاون مع الاتحاد الإفريقي في إطار "الاتفاقية النموذجية حول الأمن السيبراني" (مالابو 2014)

[1] إلهام غازي، "الوقاية ومكافحة الجريمة المعلوماتية في التشريع الجزائري"، مجلة الجيش. العدد،630 :جانفي ،2016 ص.44ص.45

- التنسيق مع الجامعة العربية والأمم المتحدة في إعداد استراتيجيات مشتركة للتصدي للتهديدات العابرة للحدود

- يظهر استعراض دور المؤسسات الحكومية الجزائرية في حماية البنية التحتية السيبرانية أن الجزائر تسير بخطى متسارعة، وإن كانت متفاوتة، نحو ترسيخ ثقافة الأمن السيبراني كأولوية وطنية .ويتضح من خلال الإطار التشريعي والتنظيمي أن الدولة الجزائرية أصبحت واعية بكون الأمن السيبراني لم يعد مسألة تقنية فحسب، بل يمثل بُعدًا من أبعاد الأمن القومي الشامل، بالنظر إلى التهديدات السيبرانية المتزايدة التي تمس استقرار الدولة، وسلامة مؤسساتها، وثقة المواطنين في الخدمات العامة.

- على الصعيد المؤسساتي، يبدو أن الجزائر تتبنى مقاربة أمنية دفاعية تقليدية، حيث لا يزال العبء الأكبر في مكافحة التهديدات السيبرانية يقع على عاتق المؤسسات العسكرية وشبه العسكرية، مثل وزارة الدفاع ومديرية الأمن الداخلي، في حين أن المقاربة الشاملة للأمن السيبراني، التي تستند إلى إشراك المجتمع المدني، القطاع الخاص، والمؤسسات البحثية، ما زالت في طور التشكل. هذا يعكس تحديا في الانتقال من سياسة حماية إلى سياسة صمود سيبراني شامل.

5. **المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني :** استجابة لمطلب الأمن المعلوماتي ومحاربة التهديدات الأمنية الناجمة عن الجرائم الالكترونية قامت مصالح الأمن بأنشاء المصلحة المركزية للجريمة الالكترونية التي عملت على تكييف التشكيل الأمني لمديرية الشرطة القضائية، والتي كانت عبارة عن فضيلة شكلت النواة الأولى لتشكيل امني خاص لمحاربة الجريمة الالكترونية على مستوى المديرية العامة للأمن الوطني والتي أنشئت سنة2011ليتم بعدها انشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال بقرار من المدير العام للأمن الوطني و اضيف الهيكل التنظيمي لمديرية الشرطة القضائية في جانفي 2015.[1]

[1] http://www.essalamonline.com/ara/permalink/52564.html#ixzz4UVGdiFR1.

جدول 1: يوضح عدد القضايا المعالجة من طرف مركز الوقاية من جرائم المعلوماتية ومكافحتها

السنة	عدد القضايا المعالجة	طبيعة القضايا
2009	18	– التهديد – جرائم المساس بالنظام العام – الإرهاب – جرائم المساس بأنظمة المعالجة الالية للمعطيات (الاختراق) – تحريض القسر على الفسق والدعارة – إهانة هيئة نظامية – إهانة رموز الدولة – النصب والاحتيال
2010	22	
2011	24	
2012	30	
2013	46	
2014	102	
2015	240	

المصدر: عز الدين عز الدين، "الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها " قيادة الدرك الوطني، مداخلة بالملتقى الوطني حول: الجريمة المعلوماتية بين الوقاية والمكافحة، جامعة محمد خيضر بسكرة، 16 نوفمبر 2015، ص 30

جدول 2: يوضح عدد القضايا المعالجة من طرف المديرية العامة للأمن الوطني

السنة	عدد القضايا المعالجة	عدد الأشخاص المتورطين
2007	31	31
2008	06	10
2009	29	21
2014	245	/
2015	409	347

المصدر: حملاوي عبد الرحمان، دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية، المديرية الولائية للأمن الوطني بسكرة، مداخلة بالملتقى الوطني حول: الجريمة المعلوماتية بين الوقاية والمكافحة، جامعة محمد خيضر بسكرة، 2015/9/16، ص10

المبحث الثاني: التعاون الدولي في مواجهة التهديدات السيبرانية

استكمالا لبحث الاستراتيجيات المتبعة لمواجهة التهديدات السيبرانية، ينتقل هذا المبحث إلى تناول دور التعاون الدولي في التصدي لهذه الظاهرة العابرة للحدود .نظرا للطبيعة العالمية للفضاء السيبراني وقدرة الهجمات على اختراق الحدود الجغرافية والسيادية، لم يعد بمقدور أي دولة، مهما بلغت قدراتها التقنية، مواجهة هذه التحديات بمعزل عن باقي الفاعلين الدوليين. لقد أصبحت التهديدات السيبرانية قضية أمن دولي تتطلب جهوداً منسقة على مستويات متعددة، تشمل الاتفاقيات الدولية، دور المنظمات المتخصصة، الدبلوماسية السيبرانية، وتبادل الخبرات وبناء القدرات بين الدول. سيبحث هذا المبحث في أهمية التعاون الدولي في مجال الأمن السيبراني، ويستعرض أبرز الأطر الدولية والإقليمية لمكافحة الجريمة السيبرانية، مع الإشارة إلى بعض التجارب الدولية الناجحة في هذا المجال للاستفادة منها.

المطلب الأول: أهمية التعاون الدولي في مجال الأمن السيبراني

يعد الأمن السيبراني من أبرز التحديات الأمنية العابرة للحدود التي تواجه المجتمع الدولي في القرن الواحد والعشرين. ومع تعاظم التهديدات الرقمية التي تطال البنى التحتية الحيوية، والمؤسسات السيادية، والشبكات الاقتصادية والمالية، تبرز الحاجة الماسة إلى تعاون دولي فعال ومنسق، كخيار استراتيجي لا غنى عنه لضمان الاستقرار السيبراني العالمي.

1.**الاتفاقيات الدولية والإقليمية:** من أبرز الاتفاقيات في هذا المجال، "اتفاقية بودابست بشأن الجريمة السيبرانية" لعام 2001، التي تعد أول اتفاقية دولية ملزمة تسعى إلى توحيد الجهود القانونية في مكافحة الجرائم المرتبطة بالفضاء السيبراني، كما ساهمت في خلق إطار قانوني مشترك بين الدول الموقعة.

2.**المنظمات الدولية والإقليمية:** تلعب مؤسسات كالإنتربول، ومكتب الأمم المتحدة المعني بالمخدرات والجريمة(UNODC) ، والاتحاد الدولي للاتصالات، دورا محوريا في تناسي الجهود بين الدول، وبناء قدرات الدول النامية، وتوفير قواعد بيانات مشتركة للمجرمين السيبرانيين، ومساعدة السلطات الوطنية على التحقيق والاستجابة.

3.**الدبلوماسية السيبرانية:** برزت في السنوات الأخيرة "الدبلوماسية السيبرانية" كأداة جديدة في العلاقات الدولية، تقوم على التفاوض حول قواعد وضوابط السلوك في الفضاء الإلكتروني، وتبادل الخبرات الأمنية، وتفادي النزاعات الإلكترونية بين الدول، مثل ما يجري ضمن الأمم المتحدة في إطار "المجموعة الحكومية المفتوحة العضوية" المعنية بأمن المعلومات.

4.**بناء القدرات وتبادل الخبرات:** تسعى الدول المتقدمة ومؤسسات المجتمع الدولي إلى دعم الدول النامية في بناء منظوماتها السيبرانية، عبر تقديم الدعم التقني والتدريب وتطوير الأطر القانونية، كجزء من استراتيجيات الأمن الجماعي في الفضاء الرقمي.

5.**اتفاقية الجامعة العربية لمكافحة الجريمة السيبرانية:** في إطار تزايد التهديدات السيبرانية واستخدام الفضاء الرقمي في تنفيذ أنشطة إجرامية وإرهابية، أصدرت جامعة الدول العربية "الاتفاقية العربية لمكافحة الجرائم المعلوماتية"، والتي تم توقيعها في 21ديسمبر 2010 .تهدف هذه الاتفاقية إلى تعزيز التعاون بين الدول العربية من أجل مكافحة الجرائم السيبرانية، والحفاظ على أمن المجتمعات وسلامتها من المخاطر الرقمية المتنامية.

وقد صادق مجلس وزراء الداخلية العرب على هذه الاتفاقية، حيث أوصى الدول الأعضاء باتخاذ الإجراءات التشريعية والتنظيمية اللازمة لمواءمة قوانينها مع أحكام الاتفاقية. وتغطي الاتفاقية صورا متعددة من الجرائم الإلكترونية، من بينها استخدام الإنترنت لأغراض إرهابية، والتحريض على العنف أو تمويل الأنشطة الإرهابية، وكذلك استغلال التكنولوجيا الحديثة لأغراض التخطيط أو الدعم اللوجستي. كما دعت الاتفاقية إلى تعزيز التعاون مع المنظمات الإقليمية والدولية لمواجهة كافة أشكال الجرائم الإلكترونية، خاصة

تلك العابرة للحدود. وأكد مجلس وزراء الداخلية العرب على أهمية بناء القدرات الوطنية اللازمة لمواجهة هذه التهديدات، والتعاون مع المنظمات الدولية المتخصصة لتأمين المطارات والموانئ والحدود من محاولات استغلالها في الأعمال الإجرامية المنظمة[1].

ومن الناحية النظرية، قد يتطلب الردع السيبراني الفعال مخططا واسع النطاق من القدرات السيبرانية الدفاعية والهجومية، مدعومة بإطار قانوني دولي قوي، وكذلك القدرة على عزو الهجوم إلى مهاجم دون أدنى شك. إن تصميم القدرات السيبرانية الدفاعية وتصميم أفضل الأدوات القانونية غير متنازع عليها نسبيا. فالعديد من المنظمات والهيئات الدولية اتخذت خطوات لرفع مستوى الوعي، وتأسيس شراكات دولية، والاتفاق على قواعد وممارسات مشتركة. وإحدى القضايا الرئيسية للتنسيق القانوني هي تسهيل محاكمة مرتكبي الجرائم الإلكترونية.

وبينما هناك اتفاق واسع على ماهية الخطوات الضرورية لمعالجة الجرائم الإلكترونية الدولية، فإن الدول غير راغبة في التخلي تماما عن العدوانية والهجومية في استخدام الفضاء الإلكتروني. ونتيجة لهذا، وبشكل متزايد، منذ اكتشاف ستاكسنت، كانت الجهود جارية للسيطرة على الاستخدام/الاستغلال العسكري للكمبيوتر عن طريق الحد من التسلح أو معايير السلوك المتعدد الأطراف، والاتفاقيات التي قد تتعلق بتطوير وتوزيع ونشر الأسلحة السيبرانية، أو لاستخدامها. ومع ذلك، من الواضح أن اتفاقيات الحد من قدرات التسلح التقليدية ليست ذات فائدة كبيرة، ويرجع ذلك أساسا إلى استحالة التحقق من القيود على القدرات التقنية للفاعلين، ولاسيما الفاعلين من غير الدول. إن السبل المتاحة للحد من التسلح في هذا المجال هي تبادل المعلومات وبناء المعايير في المقام الأول، في حين أن الاقترابات والمحاولات الهيكلية لحظر وسائل الحرب الإلكترونية تماما أو تقييد توافرها مستحيلة إلى حد كبير بسبب الوجود في كل مكان والاستخدامات ذات الطبيعة المزدوجة لتقنية المعلومات.

إن الفضاء السيبراني يتطلب تصورا جديدا للردع الأمني لا يستند إلى القوة الصلبة فقط، بل إلى منظومة متعددة الأبعاد من التعاون، القوانين، والدبلوماسية السيبرانية .ورغم صعوبة حظر الأسلحة السيبرانية بشكل فعلي، فإن تقنين استخدامها، وتكريس مبادئ "الامتناع عن الهجوم" و"احترام البنية التحتية المدنية الرقمية"، تعد خطوات واقعية أكثر قابلية للتطبيق.

[1] محمد عبد الجواد، اميرة عبد العظيم ،2020، "المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام"، مجلة الشريعة والقانون العدد35، ص 499

المطلب الثاني: التجارب الدولية الناجحة في مكافحة التهديدات السيبرانية

عرفت العديد من الدول المتقدمة خطوات ناجحة وفاعلة في مجال مكافحة التهديدات السيبرانية، وذلك من خلال وضع إستراتيجيات وطنية متكاملة، وتنمية قدرات دفاعية وهجومية، وتعزيز التنسيق المؤسساتي، بالإضافة إلى توسيع التعاون الدولي

الفرع الأول: جهود الأمم المتحدة في مجال مكافحة الجريمة السيبرانية

اتخذ المجلس الاقتصادي والاجتماعي التابع للأمم المتحدة توصية بأن تأخذ المنظمة الدولية على عاتقها دورا رئيسيا في رسم سياسة منع الجريمة وتحقيق العدالة الجنائية الدولية. وقد تحقق ذلك فعلياً بموافقة الجمعية العامة للأمم المتحدة على هذه التوصية في عام 1950، والتي بموجبها تم إنشاء اللجنة الاستشارية للخبراء في منع الجريمة ومعاملة المجرمين. وقد أُنيط بهذه اللجنة مهمة مكافحة الجريمة، وتقديم المشورة للأمين العام، وإيجاد البرامج، ووضع الخطط، ورسم السياسات المتعلقة بتدابير دولية في مجال منع الجريمة ومعاملة المجرمين.

وبعد انعقاد مؤتمر الأمم المتحدة لمنع الجريمة ومعاملة المجرمين في كيوتو باليابان عام 1970، تم استبدال اللجنة الاستشارية بلجنة منع الجريمة ومكافحتها، بناءً على توصية المجلس الاقتصادي والاجتماعي في عام 1971. وتهدف مؤتمرات الأمم المتحدة المعنية بمنع الجريمة ومعاملة المجرمين، والتي تعقد كل خمس سنوات، إلى تعزيز تبادل المعرفة والخبرات بين الدول الأعضاء و الاخصائيين من مختلف الدول والى تدعيم التعاون الدولي و الاقليمي في مكافحة الجريمة ،و هي بذلك تشكل محفلا رئيسيا للتعاون الدولي والذي يعنينا في هذه الدراسة هو جهود الأمم المتحدة من خلال مؤتمراتها الخاصة بمنع الجريمة ومعاملة المجرمين المتعلقة بالجرائم التقنية او جرائم الحاسب الالي و هنا تشير الى ان مؤتمر الأمم المتحدة السابع لمنع الجريمة ومعاملة المجرمين الذي تم انعقاده في مدينة ميلانو بإيطاليا في عام1985 ، انبثقت عنه مجموعة من القواعد التوجيهية و التي اكتملت صياغتها في المؤتمر الثامن الذي أجاز هذه المبادئ و الذي عقد في هافانا بكوبا في العام 1990م.[1]

[1] عبابنة،2009، مرجع سابق، ص156 ص157

الفرع الثاني: جهود المنظمات الدولية في مجال مكافحة الجريمة السيبرانية:

اتخذت العديد من المنظمات الدولية مبادرات في مجال مكافحة الجريمة ونذكر من بينها:

أولا: منظمة التعاون الاقتصادي والتنمية:

تهدف هذه المنظمة إلى تحقيق أعلى مستويات النمو الاقتصادي، وتناغم التطور الاقتصادي مع التنمية الاجتماعية. وقد بدأت منظمة التعاون الاقتصادي والتنمية الاهتمام بالجريمة السيبرانية منذ عام 1978، حيث وضعت مجموعة من الأدلة والقواعد الإرشادية المتعلقة بتقنية المعلومات. ويعد الدليل المتعلق بحماية الخصوصية وقواعد نقل البيانات من أوائل الأدلة التي تبناها مجلس المنظمة في عام 1980، مع التوصية للدول الأعضاء بالالتزام بها.

وفي عام 1983، أصدرت المنظمة تقريرا بعنوان "الجرائم المرتبطة بالحاسوب وتحليل السياسة القانونية الجنائية"، حيث استعرض التقرير السياسات الجنائية القائمة والمقترحات الخاصة بعدد من الدول الأعضاء، وتضمن التقرير الحد الأدنى من أفعال سوء استخدام الحاسوب والتي على الدول تجريمها مثل:

- الاستخدام أو الدخول إلى أنظمة ومصادر الحاسب بشكل غير مصرح به،
- النسخ أو الإتلاف أو التخريب غير المشروع للمعلومات المعالجة آليًا،
- الإفشاء غير المصرح به لما تحتويه هذه المعلومات من بيانات وبرامج،
- الإعاقة غير المشروعة للوصول إلى مصادر الحاسب، من خلال منع أو تعطيل استخدام الحاسب أو برامجه أو البيانات المخزنة فيه.

وفي عام 1992، وضعت المنظمة مجموعة من التوصيات والإرشادات الخاصة بأنظمة المعلومات، وأوصت بضرورة أن تتضمن التشريعات الجنائية للدول الأعضاء مبادئ عامة، من أبرزها:

1. **حدود التجميع** :ضرورة فرض قيود على تجميع البيانات.
2. **نوعية البيانات** :يجب أن تكون البيانات ذات صلة بالغرض الذي ستستخدم من أجله.
3. **تعيين الغرض** :يجب تحديد الغرض من استخدام البيانات الشخصية بشكل واضح ومسبق.
4. **حدود الاستخدام** :الالتزام بعدم إفشاء البيانات الشخصية أو نشرها لغير المصرح لهم بذلك.
5. **الوقاية الأمنية** :اتخاذ تدابير وإجراءات أمنية ملائمة وصارمة لحماية البيانات[1].

ثانيا: الاتحاد الدولي للاتصالات

اعتمد المؤتمر العالمي لتنمية الاتصالات في عام 2006 القرار رقم (45)، الذي دعا فيه مدير مكتب تنمية الاتصالات إلى تنظيم اجتماع بشأن الأمن المعلوماتي ومكافحة الرسائل الاقتحامية(Spam) ، وتقديم تقرير

[1] مراد مشوش، 2019،" الجهود الدولية لمكافحة الاجرام السيبراني"، مجلة الواحات للبحوث والدراسات، المجلد12 العدد 01 ،ص709 ص710

يتضمن نتائج الاجتماع إلى مؤتمر المندوبين المفوضين في العام نفسه. وقد تم تبني مجموعة من التوصيات في مجال الأمن المعلوماتي والحد من الرسائل الاقتحامية.

وفي 2007، أطلق الأمين العام للاتحاد جدول أعمال الأمن المعلوماتي العالم، بهدف وضع إطار شامل لمواجهة التهديدات السيبرانية وتعزيز حماية الفضاء الرقمي على المستوى الدولي و جاء إطلاق جدول أعمال الأمن المعلوماتي العالمي في إطار الاستجابة للتحديات المتزايدة لأمن الإنترنت، وسعيًا لإيجاد حلول تعزز الثقة والأمن في مجتمع المعلومات وفي أكتوبر 2008 تم إنشاء فريق الخبراء رفيعي المستوى(HLEG) ضمّ أكثر من مائة خبير من مختلف الدول وقد قدم الفريق تقاريره وتوصياته في 2008، وتم نشر **الاستراتيجية العالمية للأمن السيبراني** في 12 نوفمبر 2008[1].

ومن بين اهم التجارب الدولية الناجحة في مكافحة التهديدات الاقتحامين السيبرانية:

. **أولًا: تجربة إستونيا – الريادة في الأمن السيبراني**

في عام 2007، تعرضت إستونيا لهجوم سيبراني منظم أدى إلى شلل شبه كامل في مواقع حكومية، ومصارف، ومؤسسات إعلامية. اعتُبر هذا الهجوم أحد أولى نماذج الحروب السيبرانية الحديثة.

عناصر النجاح:

1.**إنشاء بنية تحتية رقمية مؤمنة:**

طورت إستونيا نظاما متكاملًا قائمًا على الهوية الرقمية، والتوقيع الإلكتروني، ونظام حماية البيانات باستخدام تقنيات التشفير المتقدمة.

2.**الاستجابة المؤسساتية:**

أنشأت مركز الدفاع السيبراني التعاوني التابع لحلف الناتو(CCDCOE) ، الذي أصبح مركزا للبحث والتدريب وتبادل الخبرات في الأمن السيبراني.

3.**الاعتماد على "الحوكمة الإلكترونية:"**

أصبحت إستونيا من أوائل الدول التي وفرت خدمات حكومية رقمية شاملة للمواطنين، ما تطلب بنية سيبرانية آمنة لضمان الثقة العامة.

4.**التعاون الدولي:**

سعت إستونيا إلى عقد شراكات استراتيجية مع الاتحاد الأوروبي والناتو في مجال الحماية والتخطيط للطوارئ السيبرانية.

[1] عبد الاله نوايسية، 2017،" جرائم تكنولوجيا المعلومات شرح الاحكام الموضوعية" دار وائل للنشر والتوزيع، ص150

أصبحت إستونيا نموذجا عالميا في الأمن السيبراني، وغالبا ما تستشهد تجربتها كدراسة حالة في المنتديات الدولية المتخصصة.

ثانيا: تجربة سنغافورة – الدولة الذكية في مواجهة الجرائم السيبرانية

مع سعي سنغافورة للتحول إلى "أمة ذكية"، واجهت تحديات متزايدة في حماية بنيتها التحتية الرقمية، خاصة في قطاعات مثل النقل، والصحة، والخدمات المالية.

عناصر النجاح:

1. **تأسيس وكالة الأمن السيبراني:(CSA)**

أُنشئت في عام 2015 كهيئة مركزية مسؤولة عن تنسيق جهود الأمن السيبراني على المستوى الوطني، مع صلاحيات واسعة في التشريع والمراقبة.

2. **الاستراتيجية الوطنية للأمن السيبراني:(2016)**

تضمنت أربعة محاور رئيسية: حماية البنية التحتية الحرجة، تعزيز القدرات الوطنية، تطوير قطاع الأمن السيبراني، وتعزيز التعاون الدولي.

3. **نظام إنذارواستجابة وطني:**

يضمن هذا النظام الاستجابة الفورية للهجمات، وتحليلها في الوقت الفعلي، وتوفير الدعم الفني للجهات المتضررة.

4. **تدريب وبناء القدرات:**

استثمرت الحكومة في برامج تعليمية ومهنية متقدمة في الجامعات والمعاهد المتخصصة لتكوين جيل من الخبراء المحليين.

5. **شراكات مع القطاع الخاص:**

تعمل سنغافورة على إشراك الشركات في حماية البيانات، وتشارك معها التهديدات وتحذيرات الأمن السيبراني.

تصنف سنغافورة ضمن الدول الأكثر أمانا إلكترونيا عالميًا، وتستضيف مؤتمرات دولية كبرى في هذا المجال مثلCyberTech Asia"

فتجربة سنغافورة في مواجهة الهجمات السيبرانية تعتبر نموذجا ملهما للدول التي تسعى لتعزيز امنها الرقمي بعد تعرضها لهجوم سيبراني كبير في عام2018 استهدف السجلات الصحية لنحو 1.5مليون شخص بما في ذلك السجلات الخاصة برئيس الوزراء.[1]

ثالثا: التجربة الأمريكية – نموذج القيادة والشراكة

بحكم موقعها كقوة اقتصادية وعسكرية عالمية، تتعرض الولايات المتحدة لهجمات سيبرانية مستمرة من جهات حكومية وغير حكومية.

عناصر النجاح:

1.**إنشاء مؤسسات متخصصة مثل:CISA** الوكالة الأمريكية للأمن السيبراني وأمن البنية التحتية (CISA)تعد الجهة المركزية للتنسيق والاستجابة للهجمات السيبرانية على المستوى الوطني.

2.**الشراكة مع القطاع الخاص:** بسبب امتلاك القطاع الخاص لمعظم البنية التحتية الرقمية، أنشأت الدولة قنوات تواصل وتعاون لحماية البيانات والشبكات.

3.**التشريعات الصارمة:** وضعت الدولة قوانين مثل قانون أمن المعلومات الفيدرالي (FISMA) وقانون حماية البيانات الصحية(HIPAA) ، لضمان التزام الجهات العامة والخاصة بالمعايير الأمنية.

4.**برامج التدريب والمحاكاة:** تنظم الحكومة تمارين أمنية دورية لمحاكاة الهجمات، بمشاركة الوكالات الحكومية والشركات، مثل تمرين."Cyber Storm"

5.**الردع السيبراني:** تبنت أمريكا مفهوم "الردع السيبراني"، حيث تلمح إلى استعدادها للرد على الهجمات الرقمية بوسائل دبلوماسية أو حتى عسكرية.

رغم التحديات، تتمتع الولايات المتحدة بقدرات عالية في الرصد والرد السيبراني، وتعتبر فاعلا رئيسيا في وضع المعايير الدولية للأمن السيبراني[2].

رابعًا: تجربة الاتحاد الأوروبي – سياسة أمن رقمي موحدة

في ظل تزايد الهجمات على دول الاتحاد الأوروبي، أصبح من الضروري وضع إطار أمني رقمي موحد لحماية السوق الأوروبية الموحدة ومواطنيها.

عناصر النجاح:

[1] نبيلة رجب، "الامن السيبراني وتحدي حماية بياناتنا في عصر الهواتف الذكية " 2024 تم التصفح يوم 2025/06/02 -https://akhbar /alkhaleej.com

[2] مهوب وسام،" نموذج الولايات السيبراني: بين المتحدة الامريكية في مجال الامن السيبراني: بين ضرورة الهجوم وإمكانات الدفاع" المجلد 08 العدد02 ص 130 ص131

1.**اللائحة العامة لحماية البيانات:(GDPR)** تُعد من أقوى التشريعات العالمية في حماية البيانات الشخصية، وتلزم الشركات والمؤسسات بإجراءات صارمة في معالجة البيانات.

2.**الاستراتيجية الأوروبية للأمن السيبراني:(2020)** تهدف إلى تحقيق "المرونة الرقمية" وتوسيع قدرة الاتحاد الأوروبي على الوقاية والاستجابة للهجمات.

3.**وكالة ENISA للأمن السيبراني:** تُعنى هذه الوكالة بتطوير المعايير وتقديم الدعم التقني والتدريب للدول الأعضاء.

4.**مركز الأمن السيبراني الأوروبي:(ECCC)** أُنشئ حديثًا لتعزيز القدرات الصناعية والبحثية في المجال، وتحقيق السيادة الرقمية الأوروبية.

5.**التعاون السيادي بين الدول الأعضاء:** يعمل الاتحاد على تنسيق جهود الاستجابة، وتبادل الإنذارات السيبرانية بشكل فوري، عبر آليات موحدة.

أصبح الاتحاد الأوروبي نموذجا ناجحا في خلق توازن بين الأمن السيبراني وحماية الحقوق الرقمية للمواطنين[1]

المبحث الثالث: تعزيز الأمن المجتمعي من خلال التعليم والتوعية

بعد استعراض الاستراتيجيات الوطنية وأطر التعاون الدولي لمواجهة التهديدات السيبرانية، يتجه هذا المبحث إلى تسليط الضوء على الركيزة المجتمعية في بناء الأمن السيبراني، المتمثلة في التعليم والتوعية .لم تعد حماية الفضاء الرقمي والبنى التحتية الحيوية كافية دون بناء مناعة بشرية ومجتمعية قوية قادرة على إدراك المخاطر السيبرانية والتعامل معها بوعي وحذر. إن العامل البشري غالباً ما يمثل الحلقة الأضعف في منظومة الأمن السيبراني، مما يجعل التثقيف والتدريب ضرورة حتمية لتمكين الأفراد والمؤسسات من مقاومة أساليب الهجمات السيبرانية، خاصة تلك التي تعتمد على الهندسة الاجتماعية والتضليل الإعلامي. سيبحث هذا المبحث في دور التعليم، بمختلف مراحله، في رفع مستوى الوعي السيبراني، وأهمية برامج التدريب في تطوير المهارات التقنية، ودور المؤسسات التعليمية والمجتمع في بناء ثقافة رقمية آمنة.

[1] Union C. o., Report on the Implementation of the European Security Strategy - Providing Security in a Changing World -, 2008, p. 05

المطلب الأول: دور التعليم في رفع مستوى الوعي السيبراني

الفرع الأول: أهمية التعليم في تعزيز الوعي السيبراني

يعد التعليم أحد الركائز الأساسية في بناء وعي مجتمعي فاعل لمواجهة التهديدات السيبرانية المتزايدة، لا سيما مع الانتشار الواسع لتكنولوجيا المعلومات والاتصالات في مختلف مناحي الحياة. فالتحديات السيبرانية لم تعد مقتصرة على الجانب التقني فحسب، بل أصبحت قضية أمن وطني تستدعي إشراك المجتمع بأكمله، بدءًا من المدارس وصولًا إلى الجامعات ومراكز البحث.

إن إدراج مفاهيم الأمن السيبراني ضمن المناهج التعليمية، منذ المراحل الأساسية وحتى الجامعية، من شأنه أن يُسهم في تعزيز ثقافة الحذر الرقمي، ويقلل من السلوكيات الإلكترونية الخاطئة التي قد تستغل من قبل المهاجمين. وتشير الدراسات إلى أن غياب التوعية التعليمية يُعد أحد أبرز أسباب نجاح الهجمات السيبرانية، خصوصًا تلك التي تعتمد على الهندسة الاجتماعية والخداع الإلكتروني.

ومع تطور البيئة الرقمية، وتزايد التهديدات السيبرانية التي تستهدف الأفراد والمؤسسات والدول، أصبح من الضروري التركيز على بناء وعي سيبراني شامل لدى مختلف شرائح المجتمع، وهو ما لا يتحقق إلا من خلال التعليم المنظم والتكوين المستمر .فالثغرات السيبرانية غالبا ما تكون نتيجة سلوك بشري غير مدرك للمخاطر، أكثر من كونها مجرد قصور تقني، ما يجعل من التعليم حجر الأساس في منظومة الأمن السيبراني الوطني.

الفرع الثاني: دور التعليم في الوقاية من التهديدات الرقمية

يسهم التعليم في تعزيز الوعي السيبراني من خلال ما يلي:

1. **غرس الثقافة الأمنية الرقمية منذ سن مبكرة:** إدماج مفاهيم الأمن الرقمي والسلامة الإلكترونية ضمن المناهج التربوية يساعد على تكوين أجيال أكثر إدراكا للمخاطر الرقمية، وأكثر قدرة على التعامل الآمن مع التكنولوجيا.

تمكين العاملين في القطاعات الحساسة من مهارات الحماية الرقمية: التدريب المستمر للموظفين في الإدارات العمومية والقطاعات الحيوية يقلل من أخطاء السلوك البشري كفتح روابط خبيثة أو تسريب معلومات عن غير قصد.

2. **تعزيز التفكير النقدي تجاه المعلومات والأخبار الرقمية:** يسهم التعليم في مكافحة الشائعات وخطاب الكراهية والتضليل المعلوماتي، عبر تمكين الأفراد من مهارات التحقق من المصادر والتعامل الواعي مع وسائل التواصل الاجتماعي.

3. **تكوين كوادر متخصصة في الأمن السيبراني:** الجامعات والمعاهد العليا تشكل المصدر الرئيسي لإعداد خبراء قادرين على تصميم الأنظمة الدفاعية، ورصد الهجمات، وتحليل البرمجيات الخبيثة، والرد عليها تقنيا وقانونيا:

4. **تعليم** الطلاب **مهارات التفكيرالنقدي:** يجب على المؤسسات التعليمية تعليم الطلاب مهارات التفكير النقدي، مما يساعدهم على تحديد المعلومات الموثوقة من غير الموثوقة، وتجنب الوقوع ضحية للمعلومات الكاذبة أو الاحتيال.

5. **إعطاء الطلاب القدرة على تحليل المعلومات:** يجب تعليم الطلاب كيفية تحليل المعلومات التي يجدونها على الإنترنت، مما يساعدهم على اتخاذ قرارات مستنيرة حول كيفية استخدام هذه المعلومات.

6. **المشاركة في برامج التوعية بالأمان السيبراني:** يجب على الأفراد المشاركة في برامج التوعية بالأمان السيبراني التي تقدمها المؤسسات التعليمية أو الحكومة[1]

وان للجامعة الجزائرية والمعاهد الوطنية المتخصصة دورا "محوريا" و"بالغ الأهمية" في تطوير منظومة الأمن السيبراني الوطنية. وقد أشار المشاركون إلى أن الإشكال القائم حاليًا لا يتعلق بغياب الكفاءات أو الرؤية، بل بضعف التنسيق والربط بين الجهات المستفيدة من الأمن السيبراني، كالمؤسسات الحكومية المنتجة للمعلومات، والمؤسسات الأكاديمية المسؤولة عن التكوين والبحث.

وفي هذا السياق، صرح البروفيسور رياحلة محمد الأمين، أخصائي في الأمن السيبراني بجامعة بومرداس، بأن الجامعة الجزائرية تسعى حاليا إلى لعب دور فاعل في مرافقة المؤسسات الوطنية من خلال توفير الكفاءات، وتكوين الأخصائيين، واقتراح الحلول التقنية المناسبة لمواجهة التحديات السيبرانية، وفقا لاحتياجات كل قطاع.

من جهته، أشار كل من البروفيسور محمد بوليف من جامعة الجزائر والبروفيسور حمزة صدوق من جامعة تلمسان إلى أن وزارة التعليم العالي والبحث العلمي بدأت فعليا في تنفيذ خارطة طريق وطنية لرقمنة قطاع التعليم العالي .وتتمثل المرحلة الأولى من هذا المخطط في التحول من نظام المعاملات الورقية إلى النظام الرقمي ("صفر ورق")، تمهيدا للانتقال إلى مراحل أكثر تقدمًا في المعالجة الرقمية للمعلومات.

وأكد المتخصصون أن المراحل اللاحقة من هذا المخطط تشمل تطوير آليات ذكية للتعامل مع الكم الهائل من المعطيات الإلكترونية، بما فيها المعطيات الشخصية، والعمل على تنظيمها ومعالجتها وتأمينها باستخدام تقنيات الذكاء الاصطناعي، مع التوجه نحو إنشاء بيئة متكاملة لحماية البيانات وتطوير منظومة وطنية فعالة للأمن السيبراني.

[1] الحبيب ماجد،2022،" درجة الوعي بالامن السيبراني لدى طلاب وطالبات الدراسات العليا بكلية التربية بجامعة الامام محمد بن سعود الإسلامية وسبل تعزيزه من وجهة نظرهم " ص 229

وتجدر الإشارة إلى أن تنظيم هذا المؤتمر العلمي جاء تتويجا لجهود استمرت لعامين، تم خلالها تنظيم مسابقة وطنية للالتحاق ببرنامج دكتوراه في مجالات الرقمنة والأمن السيبراني. وأسفرت هذه المبادرة عن تأطير ومرافقة 12 طالبا باحثا في خمس تخصصات تقنية دقيقة، مما يعكس سعي الجامعات الجزائرية إلى تعزيز حضورها البحثي والتكويني في هذا المجال الحساس[1].

المطلب الثاني: برامج التدريب وتطوير المهارات التقنية للأفراد

في ظل تزايد حجم وخطورة التهديدات السيبرانية لم تعد حماية الفضاء الرقمي مسؤولية المؤسسات التقنية فقط، بل أصبحت الحاجة ملحّة لتأهيل الأفراد وتمكينهم من المهارات اللازمة للتعامل مع هذه التهديدات بشكل فعال. فبرامج التدريب السيبراني تهدف إلى رفع مستوى الوعي الأمني لدى المستخدمين وتعليمهم كيفية التعرف على المخاطر الإلكترونية مثل التصيد الاحتيالي، والبرمجيات الخبيثة، والهندسة الاجتماعية. كما تشمل هذه البرامج تطوير المهارات التقنية المتقدمة لموظفي تكنولوجيا المعلومات، من خلال التدريب على تحليل الثغرات، والاستجابة للحوادث، وحماية البنية التحتية المعلوماتية. وتعد هذه الجهود جزءا أساسيا من استراتيجية الأمن السيبراني الوطنية، حيث أن بناء قدرات بشرية مؤهلة يعتبر جدار الصد الأول ضد أي اختراق محتمل.

تعد حماية البنية التحتية الرقمية من التهديدات السيبرانية أحد الأولويات الاستراتيجية التي ينبغي أن تعتمدها المؤسسات والشركات المعاصرة، لاسيما في ظل تصاعد وتيرة الهجمات الإلكترونية وتنوع أساليبها. وفي هذا السياق، تلعب برامج الأمن السيبراني دورا محوريًا في تعزيز منظومة الحماية، حيث توفر أدوات متقدمة لمراقبة الأنظمة، واكتشاف التهديدات، والاستجابة الفورية للحوادث، مما يقلل من احتمالات الاختراق والضرر المؤسساتي.

الفرع الأول: أبرز برامج الحماية المستخدمة عالميا

أبرز هذه البرامج المستخدمة عالميا والتي توفر حماية متكاملة ما يلي:

• برنامج :Log360 يعد من أبرز أدوات الأمان السحابية التي توفر حماية ضد برامج الفدية وإزالة الفيروسات. يمتاز بإمكانية التكامل مع أنظمة أمنية متعددة، ويستخدم على نطاق واسع في مراقبة وتحليل سجلات الدخول والأنشطة المشبوهة.

• برنامج :Palo Alto Networks NGFW يوفر جدران حماية متقدمة تعتمد على الذكاء الاصطناعي، ويمنح المؤسسات إمكانيات تحليلية متقدمة لرصد التهديدات القادمة من داخل وخارج الشبكة، مع تعزيز الحماية ضد البرمجيات الخبيثة.

[1] وكالة الانباء الجزائرية، "الجامعة الجزائرية تمتلك المؤهلات في مجال الرقمنة وتوفير الامن السيراني"2022، تم التصفح يوم 2025/06/03 https://www.aps.dz/ar/

• برنامج :Symantec Endpoint Security متخصص في حماية نقاط النهاية، ويعتمد على تقنيات الذكاء الاصطناعي لاكتشاف التهديدات غير المعروفة. يوفر حماية شاملة ضد الفيروسات والبرمجيات الضارة، مما يجعله مثاليًا للشركات ذات الأنظمة الموزعة.

• برنامج :Kaspersky Endpoint Security يستخدم على نطاق واسع في المؤسسات الحكومية والخاصة، ويتميز بكفاءته العالية في رصد التهديدات وتقديم حلول حماية متعددة الطبقات.

• برنامج :Fortinet FortiGate من البرامج المتقدمة التي تدمج بين الحماية من البرمجيات الخبيثة والتحكم في حركة مرور الشبكة، ويستعين بالذكاء الاصطناعي لتحليل البيانات وتأمين البريد الإلكتروني بشكل فعال.

• برنامج :Proofpoint Email Protection يستخدم لحماية البريد الإلكتروني من هجمات التصيد الاحتيالي، حيث يقوم بتحليل محتوى الرسائل إلكترونيا وتصفية الرسائل المشبوهة تلقائيا.

• برنامج :Mimecast يوفر حماية متعددة المستويات للبريد الإلكتروني، ويعمل على فحص الرسائل بحثًا عن المحتوى الضار والبرمجيات الخبيثة والتصيد الاحتيالي، مما يرفع مستوى الأمان المعلوماتي داخل المؤسسات.

• برنامج :LastPass Enterprise متخصص في إدارة كلمات المرور بشكل آمن، حيث يتيح تخزينها وتشفيرها تلقائيًا، وإنشاء كلمات مرور قوية، كما يمكن من إعداد تقارير تحليلية حول استخدام الأذونات وتحديد المخاطر المحتملة.

• برنامج :Total AV Cyber Security يعتبر من الحلول الشاملة للأمن السيبراني، إذ يوفر جدار حماية متقدما، وحماية في الوقت الحقيقي ضد التهديدات، إضافة إلى قدرات لحظر المواقع الضارة والكشف عن محاولات التصيد، إلى جانب تحسين أداء النظام[1].

الفرع الثاني: أبرز البرامج المستخدمة في الجزائر

في ظل التزايد الملحوظ في حجم التهديدات السيبرانية التي تواجه الجزائر، ظهرت مبادرات ميدانية نوعية تهدف إلى تعزيز الوعي الأمني الرقمي، وتمتين مناعة المجتمع والمؤسسات ضد الهجمات الإلكترونية. ومن أبرز هذه المبادرات، تنظيم شركة كاسبرسكي (Kaspersky) الرائدة عالميًا في مجال الأمن السيبراني، لورشة توعوية حول ما يعرف بـ "النظافة السيبرانية(Cyber Hygiene) "، وذلك في العاصمة الجزائرية، بمشاركة مسؤولين كبار من الشركة، على رأسهم غلاديس سالموت، مسؤولة التواصل المؤسسي لمنطقتي شمال وغرب إفريقيا، وتوفيق سيد أحمد، مسؤول مبيعات B2B في الجزائر.

تمثل هذه الورشة نموذجا متقدمًا لمبادرات التوعية المجتمعية حول الأمن السيبراني، حيث تم خلالها استعراض أحدث التهديدات الإلكترونية المسجلة في الجزائر خلال عام 2024، والتي شهدت تصاعدا كبيرا

[1]" برامج الامن السيبراني"، تم تصفح الموقع يوم 2025 /06/04 https://short-link.me/13Cow

مقارنة بسنة 2023. فقد كشفت الشركة، استنادا إلى بياناتها الداخلية، عن تسجيل أكثر من 70 مليون محاولة هجوم إلكتروني استهدفت الأجهزة والشبكات في الجزائر خلال العام الجاري.

وقد تمكنت شركة كاسبرسكي من التصدي لأغلب هذه التهديدات بفضل ما تملكه من تقنيات رصد ذكية وحلول حماية متقدمة تعتمد على الذكاء الاصطناعي والتحليل السلوكي، مما ساهم في تقليص الأضرار المحتملة على المؤسسات الحكومية والخاصة.

وتكمن أهمية هذه الورشة في تأكيدها على الدور المحوري للعنصر البشري في منظومة الحماية السيبرانية، حيث شددت المتحدثة الرسمية غلاديس سالموت على أن رفع الوعي الرقمي لدى الأفراد يمثل "الركيزة الأساسية" لنجاح أي استراتيجية أمنية، وهو ما يستدعي دعما مؤسساتيا مستمرا لتعزيز ثقافة حماية البيانات واستخدام الأدوات الرقمية بشكل آمن.

كما أشارت الورشة إلى أن تزايد الاعتماد على التكنولوجيا في الجزائر، خاصة في قطاعات التعليم، الإدارة الحكومية، والمعاملات الاقتصادية، يفرض على الفاعلين في الدولة الاستثمار في برامج تدريبية، وبناء قدرات وطنية في مجال الحماية الرقمية، فضلا عن اعتماد حلول تقنية حديثة تتماشى مع التحديات المتسارعة.

وبذلك، تعد ورشة كاسبرسكي مثالا واقعيا على أهمية الشراكة بين القطاع الخاص والدولة في بناء منظومة دفاع سيبراني وطني فعالة، وهو ما يعزز السيادة الرقمية ويقلل من مخاطر الاختراقات والابتزازات الإلكترونية التي باتت تهدد استقرار الأنظمة السياسية والاقتصادية والاجتماعية الحديثة[1].

إن ورشة كاسبرسكي تمثل خطوة نموذجية ضمن توجه وطني متصاعد نحو حماية الأمن السيبراني، لكنها أيضا تكشف عن حجم التحديات التي تواجهها الجزائر في هذا المجال، مما يتطلب رؤية شمولية، واستثمارا طويل الأمد في العنصر البشري والتكنولوجيا، وتنسيقا أكبر بين الدولة والقطاع الخاص والمجتمع الأكاديمي.

إن أهمية هذه البرامج لا تقتصر على وظيفتها التقنية فقط، بل تشمل أيضا أبعادا أمنية، اقتصادية، سيادية واستراتيجية، مما يجعل من تبنيها أمرا حتميا لكل الدول والمؤسسات التي تسعى إلى حماية منظومتها الرقمية ومكانتها الدولية. وفي السياق الجزائري، تمثل هذه البرامج رادعا وقائيا ضروريا في ظل التحديات المتزايدة والموجهة للبنى التحتية الوطنية الحيوية

[1] الإخبارية، " كاسبرسكي تتصدى ل 70هجوم الكتروني في الجزائر" 2024، تم التصفح يوم 2025/06/04 /https://elikhbaria.dz

الخاتمة

في خضم التحولات العميقة التي يشهدها العالم في عصر الرقمنة المتسارعة والثورات التكنولوجية المتلاحقة، برز الأمن السيبراني كأحد المفاهيم المركزية في أدبيات العلاقات الدولية والدراسات الأمنية المعاصرة، نظرا لما يفرضه من تحديات مركبة ومتداخلة تهدد سيادة الدول واستقرار مؤسساتها ومجتمعاتها. لذلك فان التهديدات السيبرانية باعتبارها ظاهرة أمنية معقدة متعددة الأبعاد، لا تمس فقط البنى التحتية الحيوية للدول، وإنما تتعدى ذلك لتطال أبعاد الأمن السياسي، القانوني، المؤسساتي، الثقافي، والاقتصادي، بل وتهدد تماسك المجتمعات واستقرار الأنظمة السياسية. من خلال الأمثلة الوطنية والدولية، أن التهديدات السيبرانية لم تعد مجرد اختراقات فردية أو عبث إلكتروني، بل أصبحت أدوات استراتيجية في يد دول وفاعلين غير حكوميين، توظفها في سياقات صراعية وتنافسية لا تقل أهمية عن أدوات الردع العسكري أو الاقتصادي، ما يؤكد الانتقال من الصراعات التقليدية إلى حروب الجيل الخامس(5G Wars) ، حيث المعلومة والسيرفرات ومراكز البيانات تحل محل الدبابات والطائرات.

وفي السياق الجزائري، فان واقعا حساسا يتمثل في تعرض عدد من المؤسسات الوطنية الحيوية إلى اختراقات خطيرة، كشفت هشاشة البنية الرقمية، وضعف الثقافة السيبرانية، وغياب إطار قانوني شامل ومتكامل يواكب تحديات العصر الرقمي. كما برزت عدة حالات واقعية، من بينها اختراق مواقع رسمية كوكالة الأنباء الجزائرية، ووزارة العدل، وشركة "صيدال"، ما يعكس مدى تنامي الخطر السيبراني وتأثيره المباشر على السيادة الوطنية والاستقرار السياسي.

وعلاوة على ذلك، هناك ترابط الجوهري بين الأمن السيبراني والأمن المجتمعي، حيث تؤدي الهجمات الإلكترونية إلى زعزعة ثقة المواطنين في مؤسسات الدولة، وتغذية خطاب الكراهية، والتلاعب بالرأي العام، ما يهدد الأمن النفسي والاجتماعي للمجتمع، ويسهم في خلق بيئة خصبة لعدم الاستقرار. وفي هذا الإطار، تبين أن الرهان الحقيقي يكمن في تحقيق أمن شامل ومندمج، يضع الأمن السيبراني كجزء لا يتجزأ من هندسة الأمن القومي المعاصر.

ولعل الدور المحوري يجب أن تضطلع به الجامعة الجزائرية والمؤسسات الأكاديمية، إلى جانب أهمية التعليم والتكوين المستمر في ترسيخ الوعي السيبراني لدى الأفراد والمؤسسات. وفي هذا السياق، تبين أن الاستثمار في العنصر البشري المتخصص، وتبني سياسات رقمية فعالة، وتطوير الكفاءات التقنية والقانونية، هو السبيل الأمثل لضمان سيادة رقمية وطنية تستجيب لتحديات القرن 21.

وبناء على فرضيات الدراسة فإن ضعف البنية التحتية الرقمية الوطنية في الجزائر، إلى جانب تزايد اعتماد البلاد على الفضاء السيبراني، يجعلها عرضة بشكل خاص لهجمات سيبرانية معقدة ومتصاعدة .هذه

الهجمات، التي شهدت تزايدًا ملحوظًا خاصة في فترات الاضطراب السياسي والنقاشات المجتمعية الحادة، لا تستهدف فقط البنى التحتية الحيوية والمؤسسات السيادية للدولة، بل تتجاوز ذلك لتمس قواعد البيانات الحكومية الحساسة، كما يتضح من محاولات اختراق وكالة الأنباء الجزائرية ووزارة العدل، وحادثة اختراق شركة صيدال التي كشفت عن بيانات سرية. هذا النوع من الاختراقات لا يقتصر تأثيره على الجانب التقني أو المادي فحسب، بل يؤثر سلباً بشكل مباشر على استقرار الدولة ويزعزع الثقة العامة بين المواطنين ومؤسساتهم، مما يقلل من هيبة السلطات أمام الرأي العام والفاعلين الدوليين.

يؤدي الاستغلال المتزايد للمنصات الرقمية في الجزائر لنشر المعلومات المضللة، الشائعات، وخطاب الكراهية، خاصة خلال الفترات التي تشهد تحولات سياسية واقتصادية متسارعة، إلى تآكل النسيج الاجتماعي وتقويض الأمن الثقافي والفكري للبلاد .هذه الظاهرة، التي تستغل طبيعة الفضاء الرقمي في سرعة الانتشار وقوة التأثير، تهدف إلى إحداث البلبلة وزرع الفتنة بين فئات المجتمع، مما يهدد تماسك الوحدة الوطنية الجزائرية ويغذي الانقسامات الداخلية. فالتهديدات السيبرانية، من هذا المنظور، تتجاوز الجوانب المادية لتصل إلى المساس بالوعي الجماعي وقيم المجتمع، وقد تؤدي إلى استبدال الثقافة المحلية بمضامين تجارية أو قيم وافدة لا تتوافق مع الخصوصيات الجزائرية، مما يجعلها تهديدًا وجوديًا للهوية الوطنية.

على الرغم من الجهود التشريعية والمؤسساتية التي تبذلها الجزائر لمواجهة التهديدات السيبرانية، والتي تمثلت في تعديل قوانين العقوبات وإنشاء مراكز متخصصة لمكافحة الجرائم المعلوماتية داخل أجهزة الأمن والدفاع، فإن فعالية استراتيجيتها الوطنية تظل محدودة .هذا القصور يعزى بشكل كبير إلى ضعف الوعي السيبراني العام لدى فئات واسعة من المواطنين، مما يجعلهم الحلقة الأضعف في منظومة الأمن السيبراني وعرضة لأساليب الهندسة الاجتماعية والخداع الإلكتروني. كما تشير المصادر إلى وجود فجوات في الكفاءات التقنية المتخصصة داخل مؤسسات الدولة، وضعف التنسيق بين الجهات المستفيدة من الأمن السيبراني والمؤسسات الأكاديمية المسؤولة عن التكوين والبحث .بالتالي، فإن الاستراتيجية الحالية تبدو أقرب إلى المقاربة الدفاعية التقليدية، مما يعرقل بناء منظومة حماية سيبرانية شاملة تتطلب إشراك المجتمع والقطاع الخاص، والانتقال من سياسة الحماية إلى سياسة الصمود السيبراني الشامل.

وختاما، يمكن القول إن التهديدات السيبرانية أصبحت تمثل تحديا استراتيجيا وجوديا لا يمكن التعامل معه إلا من خلال مقاربة شاملة متداخلة الأبعاد، تتجاوز الحلول الأمنية التقنية إلى إرساء أسس حوكمة رقمية رشيدة، وتعزيز التعاون الدولي والإقليمي، ومراجعة الأطر القانونية، وبناء منظومة وطنية للردع السيبراني قائمة على الحوكمة، الذكاء الاصطناعي، والتحليل الاستباقي للتهديدات.

إن مستقبل الأمن القومي الاجتماعي، كغيره من الدول، سيتوقف بدرجة كبيرة على قدرته في التكيف مع الواقع الرقمي الجديد، وعلى استعداده لتطوير بنيته المؤسساتية والتشريعية لمواجهة أخطر تهديد غير تقليدي عرفته الدول في العصر الحديث. ومن هذا المنطلق، تدعو هذه الدراسة إلى بلورة استراتيجية وطنية

متكاملة للأمن السيبراني، تبنى على مبدأ السيادة الرقمية، والتحصين المؤسساتي، والشراكة المجتمعية، والتعاون الدولي متعدد الأطراف.

قائمة المراجع

قائمة المراجع

المصادر:

القوانين

1. الجمهورية الجزائرية الديمقراطية الشعبية، القانون 02/ 16، المؤرخ في 19 جوان 2016، المتضمن تعديل قانون العقوبات، الجريدة الرسمية. العدد 37
2. الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 06/ 22، المؤرخ في 20 ديسمبر2006، المتضمن قانون الإجراءات الجزائية، الصادر في الج. ج ج، العدد37
3. الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم 09/ 04، المؤرخ في 2009، المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال مكافحتها، الجريدة الرسمية العدد 47
4. الجمهورية الجزائرية الديمقراطية الشعبية، القانون رقم15 04، لمؤرخ في 01 فيفري 2015، المتضمن القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، الجريدة الرسمية، العدد06

المراجع:

الكتب

5. إسماعيل على سعد، "الاتصال والرأي العام مبحث في القوة والأيديولوجيا"، دار المعرفة الجامعية، الاسكندرية ،1989.
6. جبور الأشقر،" السيبرانية: هاجس العصر "بيروت: المركز العربي للبحوث القانونية والقضائية.2016
7. جهاد بدة، "مفاهيم العلاقات الدولية التخطيط الاستراتيجي لأمن". القاهرة دار الكتاب الحديث 2015
8. خليل العمر،" الجرائم المستحدثة"، دار وائل للنشر، عمان، الأردن 2012.
9. خليل صابات، "وسائل الإعلام نشأة وتطورها"، مكتبة الانجلو مصرية، القاهرة، 1972.
10. دحان حيزام القريطي، "الامن السيبراني وحماية امن المعلومات ". دار الفكر الجامعي، الاسكندرية2022
11. سليمان الطفيل، "المعركة الاقتصادية القادمة وضرورة الامن الاقتصادي " دار الفكر الجامعي2017
12. صالح بوشعير، "الأمن القومي الجزائري بين التهديدات الداخلية والتحولات الإقليمية" الجزائر: الدار الجامعية، 201..
13. ضرغام الدباغ،"محاضرات في الإعلام والرأي العام "، الأكاديميون للنشر والتوزيع، عمان، ط ،2016،1
14. عادل عبد الصادق، "أسلحة الفضاء الالكتروني في ضوء القانون الدولي الإنساني" القاهرة، المركز العربي لأبحاث الفضاء الالكتروني، 2016

15. عبد الاله نوايسية، "جرائم تكنولوجيا المعلومات شرح الاحكام الموضوعية" دار وائل للنشر والتوزيع 2017،
16. عبد الكريم بوسريح، "الأمن المجتمعي في الوطن العربي" مقاربات نظرية ودراسة حالة الجزائر طباعة: دار الهدى، 2021،
17. عبد الكريم حسام، "التحولات الرقمية وأمن المعلومات" عمان: دار الصفاء للنشر والتوزيع، 2021.
18. عبد الكريم حسام،" التحولات الرقمية وأمن المعلومات "عمّان: دار الصفاء للنشر والتوزيع، 2021.
19. عبد الله محمد." الأمن السيبراني: التهديدات والتحديات في البيئة الرقمية المعاصرة ."القاهرة: مكتبة الأنجلو المصرية، 2020.
20. عدي إبراهيم المناوي،" التيارات السياسية العلمانية وصناعة الرأي العام": دراسة حالة العراق بعد 2003، عمان: دار زهران للنشر، ط 1، 2014.
21. محمود رمضان دياب.." استراتيجيات الحملات الإعلامية " الإسكندرية: مؤسسة شباب الجامعة، 2019.
22. محمود رمضان دياب، "استراتيجيات الحملات الإعلامية." الإسكندرية: مؤسسة شباب الجامعة، 2019.
23. منصوري رؤوف، "الهجرة السرية من منظور الامن الإنساني"، مصر: مكتبة الوفاء القانونية، ط 1، 2016،
24. نصير بوعلي، "الاعلام والقيم"، دار الهدى، عين مليلة الجزائر، 2005.
25. هيثم حمود الشلبي، إدارة مخاطر الاحتيال في قطاع الاتصالات، دار الصفاء للنشر والتوزيع طبعة 28 2009،
26. وليد عبد الحي، "قياس النزعة الانفصالية للأقليات في الوطن العربي"، جدليات الاندماج الاجتماعي، الدوحة: المركز العربي للأبحاث ودراسة السياسات، 2014

الرسائل الجامعية

27. الحبيب ماجد،2022،" درجة الوعي بالأمن السيبراني لدى طلاب وطالبات الدراسات العليا بكلية التربية بجامعة الامام محمد بن سعود الإسلامية وسبل تعزيزه من وجهة نظرهم "
28. دربال امال، "النصب في التأمينات"، مذكرة ماجستير في قانون الاعمال المقارن، جامعة وهران، الجزائر،2012
29. درمان، الذناني عبد المالك، 2008،"تكنولوجيا الاتصال وعولمة المعلومات"، المكتب الجامعي الحديث.
30. سلمان احمد، 2017" شبكات التواصل الاجتماعي ودورها في نشر الشائعات من وجهة نظر أعضاء هيئة التدريس" في جامعة ديالى، رسالة ماجستير، جامعة الشرق الاوسط، عمان، الأردن
31. صلاح حيدر عبد الواحد،"حروب الفضاء الالكتروني، دراسة في مفهومها وخصائصها وسبل مواجهتها" عمان.2021

32. عبد المؤمن بن الصغير، "الطبيعة الخاصة للجريمة المرتكبة عبر الانترنت في التشريع الجزائري والتشريع المقارن"، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة 2015.

33. عزي عبد الرحمن، السعيد بومعيزة، نصير بوعلي، "نظرية الحتمية القيمية في الإعلام "جامعة الأمير عبد القادر للعلوم الإسلامية، قسنطينة، ،2009

34. غانم عبد الوهاب، بلعباس نادية،" *دور وسائل الإعلام في نشر الإشاعة وكيفية الحد من آثارها السلبية" دراسة في طرق النشر ودور السياق والفاعل الاجتماعي* .رسالة ماجستير، جامعة مستغانم، الجزائر2015

35. محمد أمين، خديجة عرفة،" *الأمن الإنساني: المفهوم والتطبيق في الواقع العربي"* الرياض: جامعة نايف العربية للعلوم الأمنية، 2009

36. محمد هشام صالح عبد الفتاح، "جريمة الاحتيال دراسة مقارنة "، رسالة ماجستير في القانون العام، جامعة النجاح، نابلس فلسطين 2008

37. مصطفى حسام الدين،2007" استخدام تكنولوجيا الاتصال في انتشار الشائعات"، دراسة حالة على مستخدمي الانترنت والهاتف بكلية دراسات الحاسبات الالية "كمبيوتر مان"، جامعة أم درمان السالمية، الخرطوم، السودان.

38. ناصر الرحامنة، 2018 "خطاب الكراهية في شبكة الفيسبوك في الأردن": دراسة مسحية.. قسم الصحافة، الشرق الأوسط كلية الاعلام

المقالات العلمية:

39. اسمهان بوضياف، 2018"الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد03، العدد 03 ص 364

40. إلهام غازي، "الوقاية ومكافحة الجريمة المعلوماتية في التشريع الجزائري"، مجلة الجيش. العدد،630 : جانفي ،2016 ص.44ص45

41. بن حدو محمد، "التهديدات السيبرانية كعامل مؤثر على الاقتصاد الوطني"، مجلة العلوم السياسية والقانون، المجلد 9، العدد 6 (2022) ص 112.

42. بن صابر، بلقاسم، وحيدرة محمد. "الهجمات السيبرانية ومواجهتها في ضوء القانون الدولي المعاصر ". مجلة حقوق الإنسان والحريات العامة، جامعة مستغانم، المجلد 2، العدد 4 (2017)

43. جميلة علاق، "الأمن المجتمعي: مقاربة في المفهوم والعناصر"، مجلة البحوث السياسية والإدارية، العدد 10 (الجزائر، 2017)، ص 104

44. خضر حلمي ساري، "تأثير الاتصال عبر الانترنت في العلاقات الاجتماعية دراسة ميدانية للمجتمع القطري". مجلة جامعة دمشق، عدد03، ص،23 2008

45. د. عبد الحق لخذاري،2016" مبدأ الامن القانوني ودوره في حماية حقوق الانسان"، كلية الحقوق والعلوم السياسية بجامعة تبسة، العدد 37.ص3

46. رغدة البهي، "الردع السيبراني: المفهوم، الإشكاليات، والمتطلبات"، مجلة الدراسات الإعلامية، العدد 5 (2018): 209.

47. رغدة البهي، "الردع السيبراني: المفهوم، والإشكاليات، والمتطلبات"، مجلة الدراسات الإعلامية، العدد 12 (2018): ص 205 ص204

48. سناء خليل،" الجريمة المنظمة عبر الوطنية، الجهود الدولية ومشكلات الملاحقة القضائية"، المجلة الجنائية القومية، العدد الثاني، ،1996 ص111

49. سوزان عدنان، وصفاء اوتاني. 2013 "انتهاك الحياة الخاصة عبر الانترنت دراسة مقارنة". مجلة جامعة دمشق للعلوم الاقتصادية والقانونية العدد03، ص29.

50. سيرين أسامة جرادات، محمد أحمد القضاة، "المسؤولية الجنائية لمروجي الشائعات عبر شبكات التواصل الاجتماعي"، مجلة جرش للدراسات والبحوث، المجلد، 20، العدد1، ص81، 2019

51. عبد الله جعفري، "التهديدات السيبرانية وتأثيرها على الأمن القومي الجزائري"، المجلة الإفريقية للدراسات القانونية والسياسية، العدد 8 (2022): 247.

52. عبد الله محمد سيد، الأمن السيبراني: التهديدات والتحديات في البيئة الرقمية المعاصرة (القاهرة: مكتبة الأنجلو المصرية، 2020) العدد35 ص104.

53. عبيد علي ناصر،"ماهية جريمة الاحتيال الالكتروني"، مجلة كلية القانون للعلوم القانونية والسياسية كلية الحقوق جامعة تكريت، بغداد، العدد 03ص 340.

54. علواش ايمان، ليلى كراش، "الاحتيال على شركات التامين البحري"، المجلة الجزائرية للحقوق والسياسية، المجلد 07، العدد01 ،2022 ص 354

55. فتحي التريكي، "سوسيولوجيا الأمن: قراءة في مفاهيم التماسك المجتمعي" مجلة الفكر المعاصر، العدد 12 (2016) ص 88.

56. فيصل لكحل2017. "إثر مواقع التواصل الاجتماعي على المجتمع الجزائري المعاصر". مجلة العلوم الاجتماعية العدد26.صفحة 220

57. محمد احمد سليمان عيسى، "التعاون الدولي لمواجهة الجرائم الالكترونية"، المجلة الاكاديمية للبحث القانوني، كلية العلوم والدراسات الإنسانية، المجلد14، العدد02 2016 ص61

58. محمد توجي-عثماني عبد القادر". 2019.الاشاعة وأثرها على الفرد والمجتمع"، مجلة البحث العلمي في الآداب العدد 20، ص10

59. محمد عبد الجواد، اميرة عبد العظيم ،2020،" المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام"، مجلة الشريعة والقانون، العدد ،35 ص 99

60. مراد مشوش، "الجريمة المعلوماتية في ظل قانون العقوبات وقانون الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال"، مجلة القانون المجلد 09، العدد01، 2020، ص 112

61. مراد مشوش، 2019،" الجهود الدولية لمكافحة الاجرام السيبراني"، مجلة الواحات للبحوث والدراسات، العدد 703 المجلد12 ص709 ص710
62. مهوب وسام ،2023" نموذج الولايات والدراسات، المتحدة الامريكية في مجال الامن السيبراني: بين ضرورة الهجوم وإمكانات الدفاع" المجلد 08 العدد02 ص 130 ص131
63. نعيمم بوعموشة، وهشام بوبكر. 2019 "دور شبكات التواصل الاجتماعي في صناعة الرأي العام لدى المواطن الجزائري"، العدد 13، مجلة البحوث والدراسات الانسانية، ص 09
64. هناء عاشور. " تأثير العولمة على القيم الثقافية السائدة في المجتمع " دراسة تحليلية (مجلة العلوم الإنسانية) العدد 8 ص104، 2017
65. وليدة حدادي،" الفضاء السيبراني وأزمة القيم الأخلاقية في المجتمعات العربية: الشبكات الاجتماعية نموذجاً". مجلة الحقيقة العدد 01 ،2018 ص17

المو اقع الالكترونية:

1. الإخبارية،" كاسبرسكي تتصدى ل 70هجوم الكتروني في الجزائر" 2024، تم التصفح يوم 2025/06/04 https://elikhbaria.dz/
2. اسراء تريسي، 2021"اسوء الهجمات الالكترونية " تاريخ الزيارة 2025/06/03 من عربي بوست /https://arabicpost.net
3. أيسر محمد عطية، "دور الاليات الحديثة للحد من الجرائم المستحدثة الإرهاب الالكتروني وطرق مواجهته" عمان 02 04 سبتمبر 2014 ص09
4. برامج الامن السيبراني، تم تصفح الموقع يوم 2025 /06/04 https://short-link.me/13Cow
5. البلاد، "الموقع الالكتروني لوكالة الانباء الجزائرية يتعرض لسلسلة من الهجمات السيبرانية الحادة" تم التصفح يوم2025/06/01
6. الخليج اونلاين،" تخصيص خلايا امنية لتعقب الإرهاب الالكتروني في الجزائر" تم التصفح يوم 2025/03/09 /https://alkhaleejonline.net
7. الخليج اونلاين،" تخصيص خلايا امنية لتعقب الإرهاب الالكتروني في الجزائر" /https://alkhaleejonline.net
8. ماين، إبراهيم. "العلوم الإنسانيَّة والهندسة الاجتماعيَّة ".التنويري 18-07-2024 .شوهد بتاريخ: 25-05-2025 . https://tinyurl.com/29tr4zg8
9. مها عبد القادر، "الهندسة الاجتماعية نحو مستقبل مشرق"، 22-01-2025، اليوم السابع، شوهد بتاريخ : 25-05-2025. https://bit.ly/4kmqbhr
10. نبيلة رجب، "الامن السيبراني وتحدي حماية بياناتنا في عصر الهواتف الذكية " 2024 تم التصفح يوم 2025/06/02 /https://akhbar-alkhaleej.com

11. وكالة الانباء الجزائرية، "الجامعة الجزائرية تمتلك المؤهلات في مجال الرقمنة وتوفير الامن السيراني"2022، تم التصفح يوم 2025/06/03

التقارير:

1. المديرية العامة للأمن الوطني، "تقرير حول مكافحة الجرائم السيبرانية"، الجزائر، 2021.
2. بنك الجزائر، "تقرير السياسة النقدية 2022"، الجزائر: بنك الجزائر

قائمة المراجع باللغة الأجنبية

1. Antonio Missiroli, *The Future of Cybersecurity in Europe* (Paris: EU Institute for Security Studies, 2018),
2. CNN Money. http://money.cnn.com/2012/09/27/technology/bank-cyberattacks/index.html
3. Collinson (2015) Business. The Guardian. https://www.theguardian.com/business/2015/jul/31/rbs-and-natwest-customers-complain-of-online-problems
4. High Profile Cases (2017) Hackers of Russian group cobalt attacked 250 companies around the world
5. Kovacs E (2016) Buhtrap gang steals millions from Russian banks cybercrime. http://www.securityweek.com/buhtrap-gang-steals-millions-russian-banks
6. Nairobi (2017) WannaCry ransomware virus hits 19 Kenyan firms. The Indian Express. http://indianexpress.com/article/technology/tech-news-technology/wannacry-ransomware-virus-hits-19-kenyan-firms-4665265/
7. OECD, *The Economic and Social Impact of Cybersecurity Failures* (Paris: OECD Publishing, 2020)
8. Research Zacks Equity (2015) 5 Cyber security stocks to change how we protect our data.http://www.nasdaq.com/article/5-cyber-security-stocks-to-change-how-we-protect-our-data-cm531047

9. Schaab, Peter, Kristian Beckers, and Sebastian Pape. "Social engineering defence mechanisms and counteracting training strategies. " Information & Computer Security 25, no. 2 (2017): 206-222.
10. Stratfor. *Disinformation and Cyber Threats: A Global Strategic Report*, Stratfor Global Intelligence, 2021
11. Taherdoost, Hamed. "Analyzing Influential Psychological Factors in Social Engineering; Human Psyche and Cybersecurity. " Psychomachina 1 (2023): 1-7.
12. Wang, Zuoguang, Hong song Zhu, and Limin Sun. "Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods." IEEe Access 9 2021: 11895-11910.
13. Wang, Zuoguang, Limin Sun, and Hong song Zhu. "Defining social engineering in cybersecurity." IEEe Access, Vol 8 2020: 85094-85115.

قائمة المحتويات

الملخص 5

مقدمة..... 6

1. المشكلة البحثية 8

2. مجالات الدراسة 9

3. اهمية الدراسة 9

4. أهداف الدراسة..... 9

5. أسباب اختيار الموضوع 10

6. مناهج الدراسة: 10

الفصل الأول: الإطار النظري لمفهوم التهديدات السيبرانية والأمن المجتمعي..... 14

تمهيد..... 15

المبحث الأول: مفهوم التهديدات السيبرانية 16

المطلب الأول: الإطار النظري للأمن السيبراني 16

الفرع الأول: مفهوم الامن السيبراني..... 16

الفرع الثاني: المفاهيم المرتبطة بالأمن السيبراني..... 18

المطلب الثاني: تطور الأمن السيبراني 19

الفرع الأول: نشأة الأمن السيبراني..... 19

الفرع الثاني: الامن السيبراني كحقل معرفي..... 20

المطلب الثالث: أنواع التهديدات السيبرانية. 22

المبحث الثاني: مفهوم الأمن المجتمعي..... 24

المطلب الأول: تعريف الأمن المجتمعي واهميته في الاستقرار الوطني 24

الفرع الأول مفهوم الأمن المجتمعي: 25

الفرع الثاني: أهمية الأمن المجتمعي في الاستقرار الوطني:..... 26

قائمة المحتويات

المطلب الثاني: مكونات الأمن المجتمعي 29

الفرع الأول: أنماط الامن المجتمعي وعلاقتها بالنسيج الاجتماعي..... 29

الفرع الثاني: التهديدات السيبرانية وتأثيرها على الأمن القانوني والمؤسسي..... 30

المطلب الثالث: التحديات التي تواجه الأمن المجتمعي في الجزائر 32

الفرع الأول: التحديات القيمية والثقافية 32

الفرع الثاني: الجريمة المنظمة والتطرف كتحديات أمني ومجتمعي 33

المبحث الثالث: العلاقة بين الأمن السيبراني والأمن المجتمعي..... 35

المطلب الأول: الهندسة الاجتماعية 35

الفرع الأول: مفهوم الهندسة الاجتماعية 35

الفرع الثاني :التأثيرات السيبرانية والاجتماعية للهندسة الاجتماعية 36

المطلب الثاني: الاثار المتبادلة بين المجالين..... 39

الفرع الأول: تهديد الهوية والقيم المجتمعية:..... 39

الفرع الثاني: التحريض على العنف وخطابات الكراهية: 40

الفصل الثاني: تأثير التهديدات السيبرانية على الأمن المجتمعي الجزائري..... 42

تمهيد..... 43

المبحث الأول: اثار التهديدات السيبرانية على الاستقرار السياسي والاجتماعي..... 44

المطلب الأول: التأثير على النظام السياسي 44

الفرع الأول التدخلات الخارجية: 44

الفرع الثاني: اختراق البيانات الحكومية الجزائرية..... 45

المطلب الثاني: التأثير على السلم الاجتماعي 47

الفرع الأول: التلاعب بالرأي العام 47

الفرع الثاني: تأثيرهما على السلم الاجتماعي:..... 48

المبحث الثاني: الاثار الاقتصادية للتهديدات السيبرانية 51

المطلب الأول: الجرائم المالية والاحتيال الالكتروني 51

الفرع الأول ماهية الجرائم المالية والاحتيال الالكتروني: 51

الفرع الثاني: التأثيرات الاقتصادية للجرائم المالية..... 54

قائمة المحتويات

المطلب الثاني: تأثير الهجمات السيبرانية على البنوك والشركات الكبرى 56
المبحث الثالث: الاثار الثقافية والفكرية للتهديدات السيبرانية..... 59
المطلب الأول: الحملات الاعلامية المظللة 59
الفرع الأول مفهوم الحملات الإعلامية المظللة 59
الفرع الثاني: تأثيرها الثقافي والفكري: 59
المطلب الثاني: التلاعب بالقيم والمعتقدات عبر الانترنت 62
الفرع الأول: مفهوم الانترنت 62
الفرع الثاني: تأثير الانترنت ووسائل الاعلام على القيم والمعتقدات الاجتماعية:..... 62
الفصل الثالث: استراتيجيات مواجهة التهديدات السيبرانية وتعزيز الأمن المجتمعي..... 66
تمهيد..... 67
المبحث الأول: السياسات الوطنية لمواجهة التهديدات السيبرانية..... 68
المطلب الأول: التشريعات والقوانين المتعلقة بالأمن السيبراني في الجزائر..... 68
الفرع الأول: التدابير التقنية والأمنية: 68
الفرع الثاني: التدابير القانونية والتعاون الدولي 70
المطلب الثاني: دور المؤسسات الحكومية في حماية البنية التحتية السيبرانية 72
المبحث الثاني: التعاون الدولي في مواجهة التهديدات السيبرانية 75
المطلب الأول: أهمية التعاون الدولي في مجال الأمن السيبراني 76
المطلب الثاني: التجارب الدولية الناجحة في مكافحة التهديدات السيبرانية..... 78
الفرع الأول: جهود الأمم المتحدة في مجال مكافحة الجريمة السيبرانية 78
الفرع الثاني: جهود المنظمات الدولية في مجال مكافحة الجريمة السيبرانية: 79
المبحث الثالث: تعزيز الأمن المجتمعي من خلال التعليم والتوعية 83
المطلب الأول: دور التعليم في رفع مستوى الوعي السيبراني 83
الفرع الأول: أهمية التعليم في تعزيز الوعي السيبراني 84
الفرع الثاني: دور التعليم في الوقاية من التهديدات الرقمية 84
المطلب الثاني: برامج التدريب وتطوير المهارات التقنية للأفراد..... 86
الفرع الأول: أبرز برامج الحماية المستخدمة عالميا 86

الفرع الثاني: أبرز البرامج المستخدمة في الجزائر 87

خاتمة 89

قائمة المراجع 93

قائمة المحتويات 101