الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة عباس لغرور – خنشلة –

كلية الحقوق والعلوم السياسية

قسم: العلوم السياسية

نيابة العمادة للدراسات والمسائل

المرتبطة بشؤون الطلبة

الإستراتيجية الوطنية الجزائرية لمواجهة تهديدات الحروب السيبرانية

مذكرة مكملة لنيل شهادة الماستر في

تخصص: دراسات إستراتيجية وأمنية

إعداد الطالبة

خنانو حدة

إشراف الأستاذ:

د/ مومن عواطف

أعضاء لجنة المناقشة

الاسم واللقب	الرتبة العلمية	الجامعة الأصلية	الصفة
أ.د. يحياوي هادية	أستاذ التعليم العالي	جامعة خنشلة	رئيسا
د. مومن عواطف	أستاذ التعليم العالي	جامعة خنشلة	مشرفا ومقررا
أ. طرشي ياسين	أستاذ التعليم العالي	جامعة خنشلة	عضوا مناقشا

السنة الجامعية 2024/2023


بسم الله الرحمن الرحيم

شكر وتقدير

بسم الله الرحمن الرحيم

نتقدم أولا بالحمد والشكر لله تعالى الذي أنار لنا درب العلم
والمعرفة ويسر لنا في إتمام هذا البحث، على الوجه الذي
نرجو أن يرضى به عنا.

كما نتقدم بخالص الشكر وفائق التقدير لأستاذتنا الدكتور المحترم
الفاضلة "**مومن عواطف**" التي تفضلت بالإشراف على مذكرتنا والتي
وجهتنا وشجعتنا على المضي قدما لإستكمال هذا البحث

كما لا يفوتنا أن نتقدم بخالص الشكر والعرفان للجنة المناقشة التي سخرت وقتها
للمناقشة والإطلاع على البحث.

كما لا يفوتنا أن نتقدم بالشكر الجزيل إلى كل من ساعدنا من قريب
أو بعيد، أساتذة، وزملاء في إنجاز هذا البحث.

والذي نتمنى أن يكون إشراقة نافعة في مجال البحث العلمي

كل الشكر والتقدير لطاقم كلية الحقوق

دون إستثناء

إهـــداء

مقدمـــــة

مقدمة:

في ظل التوجه الدولي نحو الحكومة الإلكترونية، أصبحت قضية الأمن المعلوماتي السيبراني من التحديات الكبرى على الصعيدين الإقليمي والعالمي، خاصة مع زيادة التهديدات الأمنية الإلكترونية. تسعى الجزائر، كغيرها من الدول، منذ انتهاجها للإدارة الإلكترونية، إلى حماية منظومتها المعلوماتية من خلال العديد من الأجهزة والخلايا الأمنية، لقد أصبح الأمن المعلوماتي السيبراني ركنًا أساسيًا ضمن المنظومة الأمنية المعاصرة، والتي يجب على الدفاع الوطني، من خلال أجهزته كالدرك الوطني الجزائري، التحقق منه في ظل تنامي الجريمة الرقمية.

يتعين أيضًا التصدي للاستغلال المتنامي للشبكات الإلكترونية لأغراض إجرامية، والتي تؤثر سلبًا على سلامة البنية التحتية للمعلومات الوطنية الحساسة، لاسيما عندما يتعلق الأمر بالمعلومات الشخصية، وفي هذا السياق، يتعين على الجزائر، وغيرها من الدول، تعزيز التعاون الدولي وتبادل الخبرات في مجال الأمن السيبراني لمواجهة هذه التحديات. يجب تطوير استراتيجيات دفاعية فعّالة لحماية البنية التحتية الرقمية الوطنية ومعالجة التهديدات السيبرانية بشكل شامل.

وبالإضافة إلى ذلك، يتعين على الدولة دعم البحث والتطوير في مجال الأمن المعلوماتي وتعزيز التدريب والتوعية لدى المؤسسات والمواطنين حول مخاطر الأمن السيبراني، ومن الضروري أن يلتزم القطاع العام والخاص بتنفيذ أفضل الممارسات والمعايير الدولية في مجال الأمن المعلوماتي، بما يشمل إجراءات الحماية الوقائية والاستجابة للحوادث وإدارة المخاطر. إن تحقيق الأمن السيبراني يشكل تحديًا متزايدًا في ظل تطور التكنولوجيا، ولكن التعاون والتنسيق الدوليين يمكن أن يسهم بشكل كبير في تعزيز الحماية وتعزيز الاستقرار السيبراني للدولة.

أولا: أهمية الموضوع

تظهر أهمية موضوع دراستنا بداية في حداثته، والآثار التي تترتب عن التطور التكنولوجي والمجال المعلوماتي، فقد شهد العالم ميلاد حقبة جديدة أفرزت معها العديد من التحديات المستجدة التي فرضت نفسها بقوة على نمط التفاعلات الدولية وعلى طبيعة الصراعات القائمة مع مطلع القرن 21، وكنتيجة لذلك، فقد بدأت تبرز لنا بوضوح تجليات الفضاء السيبراني في وقتنا الراهن باعتباره رهانا استرتيجيا يتمتع بأولوية قصوى في سياسات الدول، ويؤثر لا محالة على منظوماتها الأمنية والدفاعية.

1 – الأهمية العلمية:

يمثل هذا الموضوع أحد أبرز مواضيع الساعة فالتهديدات السيبرانية أصبحت تحتل صدارة اهتمامات الباحثين والمختصين، ويعد موضوع الأمن السيبراني وإستراتيجيات مواجهة التهديدات السيبرانية من أهم المواضيع في اختصاص الدراسات الإستراتيجية والأمنية.

2 – الأهمية العملية

وتكمن في إعطاء تصور واضح لعلاقة الأمن السيبراني بأمن الدولة وكيف يتحول هذا الجانب لتهديد لا تستطيع الدول مواجهته منفردة بالإضافة إلى دراسة الجزائر ومعرفة أهم التهديدات السيبرانية التي تتعرض لها.

ثانيا: أسباب إختيار الموضوع

هناك العديد من الأسباب التي تبرر اختيار موضوع ما، وموضوع التهديدات السيبرانية من المواضيع الهامة التي أصبحت محل نقاش على مستويات عالمية، فلم يعد التهديد مقتصرا على الجانب العسكري فقط بل تعداه إلى قطاعات أخرى، لذلك فاختيار هذا الموضوع جاء نتيجة عدة عوامل يتمثل أبرزها فيما يلي:

1 - أسباب الموضوعية

الإحاطة بأحد المواضيع المهمة والمتمثل في الأمن والتعمق في أحد قطاعاته والمتمثل في الأمن السيبراني لمحاولة ربطه التهديدات السيبرانية وتأثيرها على الأمن الوطني للدول واخترنا الجزائر كدراسة لنا.

2 - أسباب الذاتية

شكل موضوع الأمن السيبراني اهتماما خاصا للبحث من خلال ما تقدمنا به سابقا، بالإضافة إلى أن الموضوع يعتبر من أحدث المواضيع على الساحة البحثية كون التهديدات السيبرانية تزداد يوما بعد يوم، بالإضافة إلى أن هذا الموضوع يؤثر بشكل كامل على اهتمامنا، واخترنا دراسة حالة الجزائر كونها الدولة التي ننتمي لها ومحاولة منا أن نفيد بهذا البحث ونبرز أهم مكامن الخلل في المنظومة الأمنية السيبرانية الجزائرية، وكذلك لإضافة هذا العمل العلمي لرفوف المكتبات الجامعية الوطنية لإفادة الباحثين والدارسين لهذا الموضوع.

ثالثا: أهداف الدراسة

تهدف دراستنا للموضوع إلى تبيان كل الاستراتيجيات التي اتبعتها الدولة، وكذا سبل التصدي لتهديدات السيبرانية، إلا أن هذا الهدف يتحقق تدريجيًا من خلال الأهداف الجزئية التالي:

- تحديد مفهوم الفضاء والامن السيبراني.
- رصد أهم التهديدات السيبرانية والاستراتيجية المتبعة لتصدي لها.
- الإحاطة بالقوانين التي تم تعديلها، والتي استحدثها المشرع.
- تسليط الضوء على الاتفاقيات التعاون الدولي.

رابعا: إشكالية الدراسة

في العصر الرقمي تزيد مخاطر التهديدات السيبرانية وتتباين أثارها وانعكاساتها على العالم عامة وفي الجزائر خاصة حيث مست هذه التهديدات معظم الدول لتطال عبرها مختلف

القطاعات الاقتصادية والعسكرية والسياسية وأصبحت بذلك تهدد الأمن الوطني للدول بشكل دائم ومستمر.

مما تقدم، يمكن طرح السؤال المركزي التالي:

إلى أي مدى يمكن أن تؤثر التهديدات السيبرانية المعاصرة على الأمن الوطني الجزائري في ظل توجه الدولة الجزائرية نحو تفعيل الحوكمة الإلكترونية لمختلف القطاعات الإستراتيجية للدولة، وماهية الاستراتيجيات والسياسات المنتهجة للتصدي لهذه التهديدات؟

ويتفرع عن هذا السؤال المركزي عديد الأسئلة الفرعية منها:

- ما مفهوم الفضاء والأمن السيبراني وماهي التهديدات السيبرانية؟
- ما هي أبرز وسائل التهديدات السيبرانية؟ وما هي أنجع السبل والإجراءات لمواجهتها؟
- فيما تتمثل أهم أساليب تعامل الجزائر مع التهديدات السيبرانية؟
- فيما تكمن أبرز مرتكزات العقيدة الأمنية الجزائرية؟
- تأثر التهديدات السيبرانية على الأمن الوطني الجزائري؟

خامسا: فرضيات الدراسة.

1- الفرضية الرئيسية: تنطلق الدراسة في فرضية رئيسية كإجابة مؤقتة على الإشكالية المطروحة.

كلما زادت مخاطر التهديدات السيبرانية على الأمن الوطني الجزائري كلما أدى ذلك إلى ضعف المنظومة الأمنية الجزائرية مما يستوجب إعادة ضبط إستراتيجية المواجهة.

2- الفرضيات الجزئية:

- تعدُد مصادر التهديدات السيبرانية ساهم في تطور مستويات وأبعاد الأمن.
- تعتبر الاختراقات السيبرانية بمثابة تهديد للأمن الوطني الجزائري بالنظر لإمكانية المساس بالبنية التحتية الإلكترونية للدولة ومنظومتها الإستراتيجية؛

-إن التعاون والتنسيق بين الدول في الفضاء السيبراني يؤدي حتما إلى التقليل من التهديدات للأمن الوطني.

سادسا: المنهج المتبع

لتمكن من التوصل إلى الإجابة على الإشكالية المطروحة وبلوغ الأهداف المرجوة منها تم الإعتماد على المنهج الوصفي بأداة تحليلية، وهو ما يتلائم مع طبيعة وإشكالية الموضوع من خلال إستعراض مفهوم الامن السيبراني، والتْعرف على أنواع التهديدات السيبرانية وسياسات والاستراتيجيات المتبعة ومضمون النصوص القانونية المتعقلة بهذا الموضوع، وإجراء دراسة معمقة لكل جزئية من جزئيات البحث.

سابعا: الدراسات السابقة

نقصد بها جميع البحوث والدراسات العلمية التي تتشابه مع البحث الراهن أو تقترب منه في جانب ما والتي تأثر بها الباحث في إعداده لهاته الدراسة.

1 – دراسة قامت بها منى الأشقر جبور "جاءت على شكل كتاب بعنوان" السيبرانية هاجس العصر"، تطرقت فيه الباحثة إلى المفاهيم والوسائل التي ترتبط بالأمن السيبراني عبر تحديد مفهومها ورصد أبعادها وتشخيص وقائعها، وكذا التطرق إلى ما تم انجازه حتى اليوم على المستوى الإقليمي والدولي والجهود الدولية والعربية في مجال إرساء الأمن في الفضاء السيبراني والخطوات العملية التي لا تدرك المخاطر السيبرانية.

2– دراسة قام بها الكاتب" فيصل محمد عبد الغفار "جاءت على شكل كتاب بعنوان" الحرب الإلكترونية" عن الدولة :دار الجنادرية للنشر والتوزيع، 2016. اعتبر فيها الكاتب أن ظهور ثورة تكنولوجيا الإلكترونيات واستخدامها في الأغراض العسكرية يعد نقطة تحول كبيرة، سواء في

فن الحرب أوفي إدارة الصراع المسلح ويضيف أن أسلحة القتال الحديثة ووسائله قد اتخذت مكان الصدارة في حسم أي صراع مسلح وخاصة أسلحة الهجوم الجوي الحديثة.

3 – قام بها الدكتور" بارة سليم "في كتابه" :الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائر تكلم فيه على تبني الجزائر كغيرها من الدول" لفكرة الحوكمة الالكترونية "وحمايتها لجهازها المعلوماتي ومنظومتها المعلوماتية من خلال العديد من الأجهزة والخلايا الأمنية وتكلمت عن دور أجهزة الدفاع الوطني في الجزائر لتحقيق الأمن السيبراني وأبرز التحديات الوطنية والعالمية التي يفرضها الفضاء السيبراني حلا مستقبليا.

ثامنا: خطة الدراسة

بناءًا على ما سبق تقع دراسة موضوع المذكرة في مقدمة وثلاث فصول رئيسية وخاتمة:

الفصل الأول: الإطار المفاهيمي والنظري لتهديدات والحروب السيبرانية، يبرز من خلاله

المبحث الأول: مقاربة مفاهيمية للفضاء ولأمن السيبراني.

المبحث الثاني: التهديدات الأمنية السيبرانية.

المبحث الثالث: مفهوم وأبعاد الحرب السيبرانية.

الفصل الثاني: السياسة الأمنية الجزائرية في ظل التطور التكنولوجي، يبرز من خلاله

المبحث الأول: مكانة الأمن السيبراني في السياسة الأمنية للجزائر.

المبحث الثاني: السياسة الأمنية الجزائرية بين العقيدة الأمنية والتطورات التكنولوجية.

المبحث الثالث: تطبيق مبادئ وقواعد القانون الدولي الإنساني بشأن العمليات السيبرانية.

الفصل الثالث: الاستراتيجية الأمنية الجزائرية في مواجهة الحروب السيبرانية، يبرز من خلاله

المبحث الأول: الاستراتيجية الأمنية الجزائرية على المستوى الوطني.

المبحث الثاني: وعلى المستوى الإقليمي.

المبحث الثالث: الرؤية الإستشرافية للأمن السيبراني الجزائري.

الفصل الأول: الإطار المفاهيمي والنظري لتهديدات والحروب السيبرانية

تمهيد

شهد العالم ميلاد حقبة جديدة حملت تغيرات نوعية سريعة لم يشهدها من قبل، خاصة في مجال المعلومات والتكنولوجيا والاتصالات، أفرزت معها العديد من التحديات المستجدة التي فرضت نفسها بقوة على نمط التفاعلات الدولية وعلى طبيعة الصرعات القائمة مع مطلع القرن 21.

وكنتيجة لذلك، فقد برزت لنا بوضوح تجليات الفضاء السيبراني في وقتنا الراهن باعتباره رهانا استراتيجيا يتمتع بأولوية قصوى في سياسات الدول، ويؤثر لا محالة على منظوماتها الأمنية والدفاعية .

ونظرًا لكونه مجالا افتراضيا يصعب مراقبته مقارنة بغيره من الأبعاد التقليدية المتعارف عليها (البر، البحر، الجو والفضاء الخارجي) ، فقد تخللته أنماط جديدة من التهديدات والهجمات السيبرانية الواقعة على أمن الدولة القومي وتماسكها الاجتماعي والسياسي، وهو ما يزيد من حدة تعقيدات آليات مواجهة تلك المخاطر العابرة للحدود التي يطرحها هذا الفضاء الجديد بمعزل عن وعي وإدراك.

وبناءًا على ما تقدم سنقسم هذا الفصل إلى ثلاث مباحث أساسية:

المبحث الأول: مقاربة مفاهيمية للفضاء ولأمن السيبراني.

المبحث الثاني: التهديدات الأمنية السيبرانية.

المبحث الثالث: مفهوم وأبعاد الحرب السيبرانية.

المبحث الأول: مقاربة مفاهيمية للفضاء ولأمن السيبراني

شكلت الثورة الرقمية والمعلوماتية قفزة تكنولوجية، وأصبح الفضاء السيبراني عنصراً مؤثراً في النظام الدولي المعاصر نظراً لما يحمله من أدوات تكنولوجية متطورة، حيث كشف عن محاور جديدة وأضاف مستويات كثيرة من التعقيد للعمليات العسكرية، وبات أكثر تأثيراً في الحسابات الاستراتيجية للدول، والدولة التي لا تملك التكنولوجيا السيبرانية المحصنة أمنياً سيتعرض فضاؤها السيبراني المتضمن للأصول والموارد والمعلومات والخدمات والبنية التحتية الحيوية، بما في ذلك الأمنية والعسكرية والمصرفية والتجارية والتعليمية والصحية والاقتصادية إلى الهجمات السيبرانية التي تسبب دمار هائل فيها.

وقبل البحث في التهديدات والهجمات السيبرانية يجدر بنا التطرق إلى مفهوم السيبرانية والفضاء السيبراني في (المطلب الأول)، أهمية وخصائص الفضاء السيبراني وفواعله الأساسية في (المطلب الثاني)، الامن السيبراني مفهومه وأبعاده_في (المطلب الثالث).

المطلب الأول: مفهوم السيبرانية والفضاء السيبراني

يواجه المجتمع الدولي نوعا جديدا من الحروب تستعمل فيه طرق مستحدثه في القتال بعيدا عن ارض المعركة التقليدية من بينها الحروب السيبرانية، التي جاءت كنتيجة منطقية لتطور وانتشار الأنظمة المعلوماتية والشبكات، وبروز معطيات حيوية كالفضاء السيبراني والأمن السيبراني واحتلالهما لمكانة بالغة الأهمية في مسار حياة الدول، لما يشكلانه من دور أساسي في مجال الحفاظ على أمنها واستقرارها.

الفرع الأول: تعريف السيبرانية.

أولا/ السيبرانية لغة: أُشتق مصطلح السيبرانية "**Cybernetic**" من المصطلح اليوناني "**Kybernetes**" التي وردت بداية في مؤلفات الخيال العلمي، وكان يقصد بها الطيار أو قائد

الدفة أو الحاكم، ويفيد الاشتقاق الحديث بأن كلمة سيبرانية تتضمن آليات تعقيب تتيح وظائف القيادة والتحكم عن بعد في الأنظمة المغلقة [1].

وسيبرانية مأخوذة من كلمة (**سيبر**) وتعني صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الإفتراضي، وتعني (فضاء الأنترنت) [2].

وقد عرفها المعجم الفرنسي "**Le Petit Larousse**" بانها العلم الذي يدرس آليات الإتصال والتحكم في الآلات والكائنات الحية الأخرى [3].

أما قاموس Oxford الإنجليزي فيعرفها على أنها» دراسة فاعلية العمل البشري بمقارنتها بفاعلية الآلات الحاسبة تتصل بسمات وخصائص الحواسيب وتكنولوجيا المعلومات والواقع الإفتراضي [4]، فيما يعرفها قاموس مصطلحات الأمن المعلوماتي بأنها :هجوم الفضاء الإلكتروني يهدف إلى السيطرة على المواقع إلكترونية أو بنية محمية إلكترونيا لتعطيلها أو تدميرها أو الإضرار بها [5].

ويشير قاموس "**المورد**" إلى السيبرانية بأنها علم الضبط ومصدرها (Cybernetics)وهو مصدر يتطابق مع مفهوم الهجمات السيبرانية أي ضبط الأشياء عن بعد والسيطرة عليها [6].

إنّ معظم القواميس المتخصصة في المصطلحات العسكرية، لم ترجع كلمة سايبر إلى مصدرها، بل عرّفت في نطاق استخدامها الفعلي أي العسكري، كقاموس المصطلحات العسكرية

---

[1] – بيتر بي سيل، الكون الرقمي الثورة العالمية في الاتصالات، ترجمة ضياء وارد، مؤسسة هنداويCIC، إنجلترا،2017 ، ص22 .

[2] – أحمد عيسى، نعمة الفتلاوي،" الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم المعاصر"، مجلة المحقق الحليلي، العراق :جامعة الكوفة، كلية القانون،2016، ص05.

[3] – Dictionnaire français Le petit Larousse, (France, Edition, 2001), p104

[4] – English dictionary Oxford dictionaries language, P299.

[5] – أحمد عيسى، نعمة الفتلاوي، المرجع نفشه، نفش الصفحة.

[6] – منير البعلبكي، قاموس المورد دار العلم للملايين، بيروت، 2004، ص243.

الأمريكية إذ يعرفها: "أيّ فعل يستخدم عن طريق شبكات إلكترونية بهدف السيطرة أو التعطيل لبرامج الكترونية أخرى" [1].

أما في اللغة العربية وبالرجوع إلى المختصين فيها، فنجد أن المختصين يواجهون تحديا في الوصول إلى مصطلح مقارب لمصطلح الانجليزي"**Cyber**".

ثانيا/ السيبرانية إصطلاحا: كلمة سيبرانية في مفهومها الحديث استعملت لأول مرة من قبل عالم الرياضيات الأمريكي "**نوربرت وينر**" "**Norbert Winer**" وهو أستاذ الرياضيات في معهد ماساشوستس التقني **MIT** الذي أعطاها مفهومها الإصطلاحي الحديث وكان ذلك عام1948، ومن أجل وصف نظام التغذية الرجعية **Feedback** الإستفادة من مخرجات الأنظمة out puts في ضبط مدخلاتها **in puts** وفي التحكم فيها وإستقرار أدائها، وهي تعني ترابط الحواسيب مع أنظمة أوتوماتيكية، والنظم الإلكترونية المركزية بتنسيق كل الآلات والمعدات التي تُستخدم على نطاق المدينة، والعالم بشكل شامل، لتحقيق أعلى رفاهية للبشر جميعا ويمكن للمرء أن يفكر بهذا كنظام إلكتروني عصبي، لا إداري يمتد في كل مناطق التركيبة الإجتماعية[2].

ورأى "**وينر**" أنه يمكن تطبيق هذا النظام على نطاق واسع في مختلف المجالات ليس العملية فقط بل الإنسانية أيضا [3]، وبالتالي فالمصدر الإصطلاحي الحديث لكلمة سيبرانية هو"علم القيادة والتحكم في الأحياء والآلات ودراسة آليات التواصل".

---

[1] – أحمد عيسى، نعمة الفتلاوي، المرجع السابق، ص04 .

[2] – الموقع الإلكتروني، https://ar-ar.facebook.com/zeitgeist.arabic/posts/cybern/ ماهي" السيبرانية؟ وما دورها في صناعة القرار؟، 7 ماي 2024، 20:31.

[3] – سعد علي الحاج بكري،" الأمن السيبراني ومعضلة حمايته"، الرابط www.alegt.com/article1241506.html ، 07 ماي 2024، 21:03.

الفرع الثاني: تعريف الفضاء السيبراني

الفضاء السيبراني مجال إفتراضي من صنع الإنسان يعتمد على نظم الكمبيوتر وشبكات الانترنيت وكمّ هائل من البيانات والمعلومات والأجهزة هو بيئة إفتراضية تعتمد في بنيتها على التكنولوجية الحديثة في التعامل والتواصل بين العديد من الفواعل سواء كانوا أشخاص أو هيئات حكومية وغير حكومية من خلال شبكة إلكترونية (الحاسوب) لها إستقلاليتها عن وسائل الإتصال، بمعنى أخر أن كل المعلومات والمعاملات المتداولة بقدر ما تسهل عملية الإندماج بين كل أجهزة الإتصالات والقمار الصناعية، والفضاء الإلكتروني، بقدر ما تفتح المجال لعمليات الإختراق[1].

كما يقرر الإتحاد الدولي للإتصالات والوكالة المتحدة المتخصصة في مجال تكنولوجيا المعلومات والإتصالات بأن الفضاء السيبراني هو" الحيز المادي وغير المادي الذي ينشأ أو يتكون من جزء أو من كل العناصر التالية: حواسيب مأجهزة ممكنة وشيكات ومعلومات محوسبة وبرامج ومضامين ومعطيات مرور ورقابة والذين يستخدمون كل ذلك [2].

والفضاء السيبراني هو مجال عالمي داخل بيئة المعلومات تم تشكيله من خلال إستخدام الإلكترونيات وإستغلال المعلومات عبر الشبكات المترابطة والمرتبطة بإستخدام تكنولوجيا المعلومات والإتصالات [3].

---

[1] – عادل عبد الصاد، " الفضاء الإلكتروني والرأي العام :تغير المجتمع والأدوات والتأثير، المركز العربي لبحاث الفضاء الإلكتروني، قضايا استراتيجية، 2013 ، العدد2459

[2] – خالد وليد محمود، الهجمات عبر الإنترنت، ساحة الصراع الإلكتروني الجديدة، سلسلة دراسات ودراسة السياسات، المركز العربي للأبحاث، قطر، 2013 ، ص4 .

[3] – Daniel T–Kuehl, from cyber space to cyber power, defining the problem in cyber power and national security, washing ton, D.C. national Defence up, 2009, P 12.

المطلب الثاني: أهمية وخصائص الفضاء السيبراني وفواعله الأساسية

يواجه المجتمع الدولي نوعًا جديدًا من الحروب تستعمل فيه طرق مستحدثه في القتال بعيدًا عن ارض المعركة التقليدية من بينها الحروب السيبرانية، التي جاءت كنتيجة منطقية لتطور وإنتشار الأنظمة المعلوماتية والشبكات، وبروز معطيات حيوية كالفضاء السيبراني والأمن السيبراني واحتلالهما لمكانة بالغة الأهمية في مسار حياة الدول، لما يشكلانه من دور أساسي في مجال الحفاظ على أمنها واستقرارها.

الفرع الأول: أهمية وخصائص الفضاء السيبراني

أولا/ أهمية الفضاء السيبراني: يعتبر الفضاء السيبراني أحد المقومات الأساسية في مجال تسير الدول الحديثة، فهو مجال حيوي لا يمكن الإستغناء عنه من حيث المزايا التي يوفرها، إلا أن أهميته في المجال العسكري تعتبر إستراتيجية بإعتباره الفضاء الخامس في الشؤون الإستراتيجية، وذلك نظرا لتطور أدوات القتال الشبكي والاستخدام المتزايد لمفاهيم ثورة المعلومات في الحروب الحديثة، وتبرز أهميته من خلال إدارة العمليات الهجومية والدفاعية بواسطة الأنظمة المعلوماتية ضد شبكات العدو، وكذلك إدارة العمليات القيادية التي تجمع بين الهجمات الإلكترونية والتقليدية ضد أنظمة العدو للقيادة بهدف تعطيلها [1].

ثانيا/ خصائص الفضاء السيبراني: يذهب الكثير إلى تشبيه الفضاء السيبراني إلى حد بعيد بالمحيط، فهو بطبيعته مجال إلكتروني يمتاز بالتجانس والمرونة، ولا تحده أي نوع من الحدود، فهو ذلك الفضاء الذي يسمح لأي كان من الولوج إليه دون قيود والتنقل بين حدوده ونطاقه وبلوغ أقصى حدوده في أقصر مدة زمنية معينة، ومن بين أهم خصائصه ثراءه من حيث المعلومات

---

[1] – بوبرطخ نسيم، الفضاء السيبراني مسرح الصراعات الجيوسياسية المعاصرة، مجلة الجيش، العدد 685، 2020، ص ص 24-25.

المخزنة عليه او المتداولة عبره [1].

يعتمد الفضاء السيبراني كمجال إفتراضي على نظم الحواسيب وشبكات الإتصال ومخزون هائل من البيانات بحيث يسمح بالإتصال بالشبكات دون تقييد بالحدود الجغرافية، ومن أبرز خصائصه انه أصبح مكمنًا للتهديدات الإجرامية اللامتناهية من هجمات إلكترونية، وملاذًا للمتطرفين والإرهابيين، ومجالًا حيويًا لتنفيذ سياسات التجسس الإلكتروني وإلحاق الضرر بالغير في صورة الحروب السيبرانية، وذلك راجع أساسًا إلى غياب سلطة عليا تتحكم فيه وآليات تسمح بحصر مجال الخطر الناتج عنه سواء من الناحية القانونية او

الفرع الثاني: فواعل الفضاء السيبراني

يمكن تقسيم الفواعل في الفضاء السيبراني ومن لديهم القدرة على شن الهجمات الالكترونية إلى ما يلي:

أولا/ الدولة: تمثل الخطر الأكثر والفاعل قوة في مجال الفضاء السيبراني، فهي اية عام 2008، استطاعت حوالي 180 دولة أن تمتلك ترسانة من الأسلحة الالكترونية، مما قد يدفع الفواعل من الدول ومن غير الدول للتنافس في السنوات القادمة من أجل تحقيق التفوق الإلكتروني . ونتيجة لما يقدمه الفضاء السيبراني فرض الفواعل لتحقيق مصالحهم، تسعى عديد من الدول إلى تطوير قدرا في هذا المجال، وتنقسم القدرات السيبرانية للدول بشكل عام إلى قدرات دفاعية وأخرى هجومية [3].

ولقد أضاف كل من" **ريتشارد كلارك**" و"**روبرت كناك**"، في كتابيهما عن الحرب الإلكترونية

---

[1] – شلوش نورة، القرصنة الإلكترونية في الفضاء السيبراني التهديد المتصاعد لأمن الدول، مجلة مركز بابل للدراسات الأساسية، المجلد08 ، العدد02 ،2015، ص190.

[2] – Léoutre pierre marie, l'appropriation du cyberespace pour la politique, Revue de la sécurité globale, numero25, 2021, p137.

[3] – نوران شفيق، أثر التهديدات الإلكترونية على العلاقات الدولية، دراسة في أبعاد الأمن الالكتروني، المكتب العربي للمعارف، القاهرة، 2014، ص40 .

باعتبارها الخطر القادم الذي يهدد الأمن القومي للدول، ويعتبر بعدا آخر يرتبط بمدى إعتماد الدول في الفضاء السيبراني لإدارة شؤونها، فقدرة الدولة تزيد كلما زادت قدراتها الهجومية والدفاعية، وقل إعتمادها نسبيا على الفضاء السيبراني مقارنة بغيرها من الفواعل [1].

ثانيا/ الفواعل من غير الدولة: إن تصاعد خطر الفاعلين من غير الدول على الأمن السيبراني في العلاقات الدولية قد أثر بدوره على سيادة الدول، وبخاصة مع بروز دور الشركات التكنولوجية العابرة للحدود الدولية وبروز أخطار القرصنة والجريمة الإلكترونية والجماعات الإرهابية، ومن جهة أخرى فقد فرض ذلك تحدي الحفاظ على الأمن دون إشراك هؤلاء الفاعلين الجدد، في تحمل المسؤولية والعبء في تأمين البنية التحتية المعلوماتية، وبدأ يظهر إتجاه التعددية في الحفاظ على الأمن بين كافة أصحاب المصلحة من الحكومات والمجتمع المدني والقطاع الأكاديمي والتقني والقطاع الخاص ووسائل الإعلام [2].

إن ظهور الأطراف الجدد من غير الدول في تزايد مستمر، فعبور نشاطات هذه الأطراف للحدود جعل التفاعلات الدولية أكثر تعقيدا، حيث أفرزت هذه الأطراف أنماطًا جديدة من المشكلات والمنازعات، فقد ساهمت في خصخصة الحرب وأصبحت تساهم في التدريب والتجنيد والحوار...

ولقد برزت مشكلات الحروب الفضائية التي تمثل الفيروسات بخسائر وصلت إلى حوالي 15مليار دولار، كما أن جماعات الجريمة المنظمة كلفت من خلال إنتهاكات للملكية الفكرية وسرقة البيانات حوالي تريليون دولار في عام 2008، كما أن شبكات التجسس الإلكتروني

---

[1] – نوران شفيق، المرجع السابق، ص40.

[2] – إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائر، مجلة المصداقية، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي، الجزائر، د ن، ص 106.

اقتحمت 1295 حاسوبا في 103 دولة منها 30% اهدافاً حكومية مهمة [1].

ثالثا/ الفرد (القرصنة): أضحى الفرد فاعلا مهما في الفضاء السيبراني، حتى أن له القدرة على إحداث ثورة الرقمية، لتصبح تلك الثورة مجال إستخدام للدولة نفسها، ومثال ذلك ما قام به مارك زوكربارغ" "Mark Zoukberg "عام 2004 ، حين أسس الفيس بوك (Facebook)، لتستقطب أكثر من مليار مستخدم عبر العالم، وغيرها من وسائل التواصل الإجتماعي بمختلف أنواعها، حيث تبقى هذه الوسائل بحرًا لحرية الأفراد الذين يمارسون نوعًا من المعارضة الإفتراضية، إلا أن هذا الجانب من الحرية أعطى الوقت للأفراد على إختلاف توجهاتهم وإنتماءاتهم سواء كانوا رسميون أو غير ذلك، فسحة واسعة لنشر الأفكار والمعلومات سواء كانت سليمة أو ضارة [2].

رابعا/ المجموعات الافتراضية: تتخذ هذه المجموعات سمات متميزة تجعلها فضاءات مثاليا للتواصل، خاصة بالنسبة إلى الأجيال الشابة التي أضحت الثقافة الرقمية المرتكزة على الصورة تشغل حيزا مهما من حياتها بكل ما تحملهم من رموز ودلالات، وقواعد التواصل والتبادل وعلاقات إجتماعية، فالمجموعات الإفتراضية حسب "**هاورد رينغولد**" "Hawrd Rengold هي مجموعات تنشأ من الشبكة حين يستمر أُناس وقت كاف لتشكيل علاقات شخصية في الفضاء السيبراني.

أما" **نديم منصوري** " فيرى أنها مجموعة من الأفراد يتشاركون عبر الأنترنت لفترة زمنية، لتحقيق غاية أو هدف أو هواية، من خلال علاقة إجتماعية إفتراضية تحددها منظومة "**تكنو إجتماعية**"، فتتحقق المجموعات الإفتراضية من خلال بروزها كفاعل أو متفاعل أثناء عمليات التواصل عبر الشبكة، وتختلف هويات هذه المجموعات الى ثلاث هويات حسب "**فاني جورج**"[3]:

---

(1) – إدريس عطية، المرجع السابق، ص 106.

(2) – نفس المرجع، ص107

(3) – كلثوم بيبيمون، السياقات الثقافية الموجهة للهوية الرقمية في ضوء تحديات المجتمع الشبكي من التداول الافتراضي إلى الممارسات الواقعية، مجلة" إضافات"، مركز دراسات الوحدة العربية، العدد23 ، بيروت، 2016، ص 26.

- **الهوية التصريحية** (Identity declarative): تبرز من خلال المعلومات التي يجرى إدخالها من قبل صاحب الحساب.
- **هوية ثنائية القطب** (Diasporiens Bipolaires): تضم أقلية تعبر عن إرتباطها العميق في الوقت ذاته بالوطن الأم والبلد والمستقبل.
- **هوية عالمية** (Les Cosmopolites): تعرض إنفتاحًا على مختلف الثقافات العالمية، وتشير الباحثة إلى أن هذه المجموعات لا تخفي حقيقة التغيرات والممارسات الهوياتية بفعل سهولة التواصل والتفاعل عبر الفضاء السيبراني.

المطلب الثالث: الأمن السيبراني مفهومه وأبعاده.

لقد حازت مسألة الأمن السيبراني على المزيد من الاهتمام، وهذا على جميع المستويات العالمية والإقليمية والوطنية، سواء من جهة إرتفاع عدد الهجمات او التهديدات الناجمة عنها، حيث شهدت الكثير من الدول إختراقات أمنية مقلقة استهدفت المؤسسات والشركات وحتى الأفراد بسرقة البيانات والقرصنة والتجسس والتجنيد والإرهاب الإلكتروني وغيرها.

الفرع الاول: مفهوم الامن السيبراني

أولا/ تعريف الامن السيبراني: ويعرف الأمن السيبراني على أنه عبارة عن مجموعة الوسائل التقنية والتنظيمية والإدارية التي يتم إستخدامها لمنع الإستخدام غير المصرح به، وسوء إستغلال وإستعادة المعلومات الإلكترونية، ونظم الإتصالات والمعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية، وإتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني [1].

والأمن السيبراني هو سلاح استراتيجي بيد الحكومة والأفراد، لاسيما أن الحرب السيبرانية أصبحت جزء لا يتجزأ من التكتيكات الحديثة للحروب والهجمات بين الدول [2].

---

[1] – عنترة بن مرزوق، الأمن السيبراني كبعد جديد من السياسة الجزائرية، محاضرات مقدمة لطلبة جامعة محمد بوضياف، المسيلة، كلية الحقوق والعلوم السياسية، دون سنة، ص 65.

[2] – أوس مجيد غالب العوادي، الأمن المعلوماتي السيبراني، مركز البيان للدراسات والتخطيط، بيروت، 2016، ص 06 .

ثانيا/ مرتكزات وعناصر الأمن السيبراني: يرتكز الأمن السيبراني على مرتكزين أساسين هما:

1- التقنية: تلعب تكنولوجيا المعلومات دورا كبيرا في تحقيق الأمن السيبراني فهي ما يؤمن المعلومات المخزنة والمتداولة.

2- التشريع: يلعب التشريع دور العنصر الذي يستجيب لمتطلبات البيئة الرقمية في مجال التنظيم ووضع الآليات القانونية الكفيلة لضمان الحماية الملائمة للفضاء السيبراني.

أما عناصره فتشمل على:

1- السرية والموثوقية التي يقصد بها التأكد من عدم الكشف عن المعلومات.

2- التكامل وسلامة المحتوى من التلاعب.

3- الإستمرارية والتي يقصد بها ضمان تقديم الخدمة دون إنقطاع.

الفرع الثاني: أبعاد الأمن السيبراني

أولا/ البعد العسكري: تكمن الميزة النسبية للقوة السيبرانية في قدرتها على ربط الوحدات العسكرية ببعضها البعض عبر الشبكات العسكرية في الفضاء الالكتروني، بما يسمح بسهولة تبادل المعلومات وتدفقها، وكذا السرعة وإعطاء الأوامر العسكرية والقدرة على إصالة الأهداف عن بعد وتدميرها، وقد تتحول هذه الميزة إلى نقطة ضعف لا قوة إن لم تكن شبكة الإلكترونية المستخدمة في ذلك مؤمنة جيدا من أي اختراق خارجي، قد ينسب في شن هجمات إلكترونية مضادة على شبكات القوات المسلحة وأجهزة الاستخبارات، ومن ثم تجسس على أمن العسكري للدول، وتعطيل قدرة الدولة على النشر السريع لقدراتها وقواتها، أو قطع أنظمة الاتصال في ما بين الوحدات العسكرية وتعطيل شبكات الكمبيوتر، كما يمكن أن يتم شل وتعطيل عمل أنظمة الدفاع الجوي أو التوجيه الالكتروني فضلا عن إمكانية وفقدان السيطرة على وحدات القيادة[2].

---

[1] – قصعة سعاد، تحديات الأمن المعلوماتي في مواجهة الجرائم الإلكترونية في ظل الإعلام الجديد، مجلة المعيار، المجلد 24، العدد 50، 2020، ص380.

[2] – حمدون تورية، الأمن السيبراني في لبلدان النامية، الاتحاد الدولي للاتصالات، 2006، ص15.

ثانيا/ البعد الاقتصادي: يرتبط الأمن السيبراني إرتباطا وثيقا بالاقتصاد فالتلازم واضح بين إقتصاد المعرفة وتوسيع إستخدام تقنيات المعلومات والإتصالات، بالقيمة التي تمثلها البيانات والمعلومات المتداولة والمخزنة والمستخدمة على كل المستويات، كما تتيح تقنيات المعلومات والاتصالات تعزيز التنمية الاقتصادية لدول كثيرة عبر إفادتها من فرص الإستخدام التي تقدمها الشركات الدولية والشركات الكبرى التي تبحث في إدارة كلفة إنتاجها بأفضل الشروط [1].

ثالثا/ البعد السياسي: يتمثل البعد السياسي للأمن السيبراني بشكل أساسي في حق الدولة في حماية نظامها السياسي وكيانها ومصالحها الإقتصادية، التي تعني حقها وواجبها في السعي إلى تحقيق رفاه شعبها في وقت تؤثر موازين القوى داخل المجتمع نفسه، حيث أصبح بإمكان الفرد أن يتحول إلى لاعب أساسي في اللعبة السياسية كما أصبح بإمكانه الإطلاع على خلفيات ومبررات القرارات السياسية التي تتخذها حكومته عبر الكم الهائل من المعلومات التي يمكنه الوصول إليها [2].

وبالمقابل لا يتوانى العاملون في الشأن السياسي من الإستفادة مما تقدمه هذه التقنيات للوصول إلى أكبر شريحة ممكنة من الأفراد والترويج لسياساتهم في العالم، ومدى التأثير الذي يتركه هذا الأمر بغض النظر عن صحة السياسات والمبادئ والمواقف التي تروج لها، فقد استخدم "أوباما "مثلا الشبكات الاجتماعية بشكل مكثف خلال حملته الإنتخابية كما تركت التسريبات لآلاف الوثائق الدبلوماسية السرية عبر الويكي ليكس أثرا سلبيا على العلاقات بين الدول [3].

---

[1] – منى أشقر جبور، **مرجع سابق**، ص31 .

[2] – **المرجع نفسه**، ص29.

[3] – نوران شفيق، المرجع السابق، ص 40.

رابعا/ البعد الاجتماعي: تساهم شبكات التواصل الإجتماعي بشكل خاص في فتح المجال للأفراد للتعبير عن تطلعاتهم السياسية وطموحاتهم الإجتماعية بأشكالها المختلفة، وكذلك تشكل مشاركة جميع شرائح المجتمع ومكوناته وسيلة لتطوير المجتمع مما يتيح الفرصة للإطلاع على الأفكار والمعلومات وبما تكونه من حاجة لدى المجتمع في الحفاظ على إستقرار الفضاء الإلكتروني والمجتمع الذي يرتكز إليه، كما أن إنفتاح مجتمع ما على المجتمعات الأخرى يؤسس لتبادل خبرات وأفكار وتكوين آفاق للتعاون والتكامل [1].

خامسا/ البعد القانوني: تعد العلاقة بين القانون والتكنولوجيات علاقة تبادلية فالتطورات التكنولوجية المختلفة تفرض مواكبة التشريعات القانونية لها، من خلال وضع أطر وتشريعات للأعمال القانونية وغير القانونية منها ولكن بصورة عامة تفتقد الجريمة السيبرانية في الوقت الحالي للأطر القانونية الصارمة للتعامل معها، ولعل ذلك يعود لعوامل مثل طبيعة الجريمة الإلكترونية في حد ذاتها وصعوبة تحديد هوية مرتكبي تلك الجرائم ومرونة التعريفات المرتبطة بتكنولوجيا المعلومات، إلى جانب ذلك فإن الجرائم السيبرانية غير مقيدة بحدود الدول، الأمر الذي يقتضي تفعيل التعاون الدولي المشترك لمكافحتها [2].

المبحث الثاني: التهديدات الأمنية السيبرانية.

أصبحت التهديدات السيبرانية إحدى التحديات الرئيسية التي يتحتم على الدول مواجهتها خلال الفترة الحالية، ومع تزايد الإعتماد على الإنترنت خاصة في المجالات التي تتعلق بالأمن القومي مثل الشبكات العسكرية والبيانات المالية والمصرفية وتزايد الحديث عن أهمية مواجهة هذه التهديدات.

---

[1] – محمد مختار، هل يمكن تجنب الدولة مخاطر الهجمات الإلكترونية؟، مجلة مفاهيم المستقبل، العدد06 ، بيوت، لبنان، 2015، ص 7.

[2] – قصعة سعاد، المرجع السابق، ص381.

المبحث الثاني: التهديدات الأمنية السيبرانية.

أصبحت التهديدات السيبرانية إحدى التحديات الرئيسية التي يتحتم على الدول مواجهتها خلال الفترة الحالية، ومع تزايد الإعتماد على الإنترنت خاصة في المجالات التي تتعلق بالأمن القومي مثل الشبكات العسكرية والبيانات المالية والمصرفية وتزايد الحديث عن أهمية مواجهة هذه التهديدات.

وفي هذا المبحث سيتم التعرض إلى ماهية التهديدات السيبرانية التي يمكن أن تتعرض لها الدول، وسيتم توضيح ذلك فيما يلي:

المطلب الأول: مفهوم التهديد السيبراني.

سيتوجب التطرق إلى موضوع التهديدات السيبرانية توظيف بعض المفاهيم الأساسية التي لابد من التدقيق في استعمالها ومعرفة فحواها، ومن بين هذه المفاهيم مفهوم التهديد. ومن أبرز التعريفات التي قدمت لهذا المصطلح نذكر ما يلي:

الفرع الأول :تعريف التهديد الأمني.

أُشتقت كلمة تهديد من الناحية اللغوية من لفظ" هدد "ويقصد به محاولة إلحاق الضرر والأذى بشيء معين قصد الإخلال بالأمن [1].

ويرى "**بيتري دبيل**" أن التهديد عمل نشط وفعال تقوم به دولة معينة للتأثير على سلوك دولة أخرى ويشترط نجاحه توفر عدة عوامل أبرزها الصداقة والجدية والقدرات التي تتناسب مع التهديد. وهناك ثلاث سمات وهي درجة الخطورة ومدى احتمالية وقوع التهديد وعنصر الوقت [2] .

---

[1] – جارش عادل،" مقاربة معرفية حول الإرهاب السيبراني"، مجلة المستقبل العربي، العدد 20 ، بيروت، لبنان، 2000 ، ص73.

[2] – نفس المرجع، نفس ص.

الفرع الثاني: تعريف التهديدات السيبرانية.

التهديدات السيبرانية هي التي تهدد أمن المجتمع وأمن الإقتصاد الوطني والجانب الأمني والعسكري للدول، كما أن للتهديدات السيبرانية أهداف مسطّرة، حيث تمس كلا من الجانب المعنوي والجانب المادي وعلى جميع الأصعدة [1].

ويُعَرف قاموس " أوكسفورد" التهديدات السيبرانية على أنها إمكانية محاولة إلحاق الضرر عن قصد وبنية سيئة أو تعطيل عمل شبكات الكمبيوتر أو النظام .[2]

ومن الناحية الاصطلاحية يمكن تقديم تعريف أكثر شمولا يرتبط بنقطة ضمان الحكومات بأنها: أي ظرف أو حدث ينطوي على إمكانية التأثير سلبا على العمليات التنظيمية أو الأفراد من خلال نظام معلومات عن طريق الدخول غير المصرح به أو التدمير أو الكشف أو تعديل الحكومات والخدمات .

وبالتالي فالتهديدات السيبرانية هي: أي فعل ضار الذي يحاول الوصول إلى شبكات الحاسوب بدون ترخيص أو إذن من أصحابها [3].

المطلب الثاني: أنماط التهديدات السيبرانية.

تتعدد أشكال التهديدات السيبرانية وتختلف من حيث الطبيعية والمصادر والأهداف كالتجسس وسرقة المعلومات وشن الحروب وبالتالي بات العديد من الفواعل الدوليين يلجئون الى آليات الكترونية لتحقيقها، وعلى الرغم من تعدد صور وأشكال الهجمات الإلكترونية، غير أنه من الممكن تقسيمها الى المجموعات رئيسية التالية:

---

[1] – حسن بن أحمد الشهري، الأنظمة الالكترونية الرقمية المطورة لحفظ وحماية سرية المعلومات من التجسس، مركز النور للأبحاث الإلكترونية، 2010، ص 11 .

[2] –**What is cyber threat how to explain cyber threat your CEO**, Date de visite 15/05/2024, www.threatcomment.com/bloghowtoexplainwahtisacyberthreat.

[3] –www.threatcomment.com Op cit, Date de visite 15/05/2024, P 15.

أولا/ القرصنة الالكترونية: القرصنة الإلكترونية أو المعلوماتية هي عملية إختراق لأجهزة الحاسوب تتم عبر شبكة الإنترنت غالبا، إلا أن أغلب حواسيب العالم مرتبطة عبر هذه الشبكة، أو حتى عبر شبكات داخلية يرتبط فيها أكثر من جهاز حاسوب، ويقوم بهذه العملية شخص أو عدة أشخاص متمكنين في برامج الحاسوب وطرق إدارتها، أي إنهم مبرمجون ذو مستوى عال يستطيعون بواسطة برامج مساعدة إختراق حاسوب معين والتعرف على محتوياته ومن خلالها يتم إختراق باقي الأجهزة المرتبطة معها في نفس الشبكة وهم [1]:

1- **الهواة (الهاكرز- Hackers):** يعتمد الهواة على برامج التجسس الجاهزة والمتاحة في كل مكان سواء عن طريق الشراء أو التحميل من شبكة الإنترنت، ويقوم الهاكرز بزرع ملفات التجسس (Patches & Trojans) في حواسيب الضحايا عن طريق البريد الإلكتروني أو ثغرات الويندوز التي يكشفها البرنامج .هذا الصنف من الهاكرز أهدافه طفولية؛ حيث يسعى لإثبات نجاحه في إستخدام هذه البرامج وانضمامه إلى قائمة الهاكرز، بهدف التفاخر بين الأصحاب كشخص يمتلك مواهب يفتقدها بعضهم.

2- **المحترفون (الكراكرز -Crackers):** أما المحترفون فهم الفريق الأخطر لأنهم يعلمون ماذا يريدون وماذا يفعلون، وكيفية الوصول إلى أهدافهم بإستخدام ما لديهم من علم يطورونه بإستمرار، بالإضافة إلى إستخدام البرامج الجاهزة المتطورة، إلا أنهم يعتمدون على خبرتهم في لغات البرمجة والتشغيل، وتصميم وتحليل وتشغيل البرامج بسرعة، كما أن هوايتهم الأساسية معروفة كيفية عمل البرامج لا تشغيلها، إن أهداف هذا الفريق أكبر وأخطر من الفريق السابق، فأهدافهم المصارف وسحب الأموال من حساب العملاء، أو الولوج إلى أخطر المواقع وأكثرها حساسية والتلاعب ببياناتها أو تدميرها[2].

---

[1]- كريم حميد، "القرصنة الإلكترونية ، / https://www.alakah.net/culturel/052639 ، 20ماي2024، 10:43.

[2]- نفس المرجع

ثانيا/ الإرهاب السيبراني: يعرف الإرهاب السيبراني أيضا على أنه الفعل المتعمد الذي تقوم به جهات فاعلة في الأنترنت قصد تدمير أو تخريب أو تعديل البيانات أو تدفق المعلومات، أو نظم المعلومات الحيوية للدولة أو الشركات، بحيث أن الغرض من إحداث الضرر يكون للأسباب سياسية أو دينية أو إيديولوجية [1].

والإرهاب السيبراني هو أحد الأنماط المستخدمة للإرهاب الذي يعبر عن تكيف الجماعات الإرهابية مع تكنولوجيا المعلومات وشبكة الإنترنت، وبالتالي أنتج لنا ما يسمى الإرهاب السيبراني، هو مصطلح يعبر عن استخدام الجماعات الإرهابية لتكنولوجيا المعلومات لشن هجمات ضد أجهزة الكمبيوتر والبنى التحتية للدولة والأفراد بغرض تحقيق أهداف سياسية .ويطلق عليه أيضا الإرهاب الإلكتروني أو الإرهاب الصامت أو الناعم، ومن وسائلهالبريد الإلكتروني، شبكات التواصل الاجتماعي Social networks، الفيس بوكFacebook ، تويتر Tweter، المواقع الإلكترونية Web sites.

ثالثا/ الحرب السيبرانية: وهي تعني في إحدى تعريفاتها أن تقوم دولة أو كيان ما بشن هجوم إلكتروني، وذلك في إطار متبادل، أو حتى من طرف واحد، وعلى الرغم من إنتشار مصطلح" الحرب الإلكترونية "على نطاق واسع على المستوى الإعلامي، فإن المصطلح ذاته يعد قديما، خصوصا باقترانه مع رصد حالات التشويش على أنظمة الاتصال، والرادار، وأجهزة الإنذار المعروف إبان حروب القرن العشرين، أما في الوقت الراهن فإنه يرتكز على تفاعلات الفضاء الإلكتروني، مع دخول شبكات الاتصال والمعلومات الرقمية إلى المجال العسكري، وسوف نتطرق الي دراسة ماهية الحرب السيبرانية في المبحث الثالث من هذا الفصل.

---

[1]– جارش عادل، المرجع السابق، ص 76.

المطلب الثالث: تأثير التهديد السيبراني على الأمن القومي.

تبلورت المصالح الوطنية للدول في الفضاء السيبراني، إثر تزايد الإعتماد على ربط البنى التحتية لها، بذلك الفضاء في بيئة عمل تشابكية واحدة، تعرف بالبنية التحتية الوطنية للمعلومات (NTI)، فأي هجوم أو تهديد محتمل على تلك المصالح قد يشكل حدوث عدم توازن إستراتيجي، وهو ما يكشف عن نمط جديد من التهديدات للأمن القومي للدول، وأبرزها [1]:

- تزايد إرتباط العالم الفضائي السيبراني، الأمر الذي اتسع معه خطر البنية التحتية الكونية للهجمات السيبرانية.
- تراجع دور الدولة في ظل العولمة وإنسحابها من بعض القطاعات الإستراتيجية لمصلحة القطاع الخاص.
- نشوء نمط جديد من الضرر على خلفية الهجمات السيبرانية، يمكن تسببه دولة لدولة ثانية دون الحاجة للدخول المادي إلى أراضيها.
- تحول الحروب السيبرانية إلى إحدى أدوات التأثير في المعلومات في مستويات مراحل الصراع المختلفة.
- توظيف الفضاء الإلكتروني في تعظيم قوة الدول، من خلال إيجاد ميزة أو تفوق أو تأثير في البيئات المختلفة، وبالتالي ظهر ما يسمى **بالاستراتيجية السيبرانية** للدول.
- إتساع نطاق مخاطر الأنشطة العدائية التي يمارسها الفاعلون، سواءً الدول أو من غير الدول.

تفرض طبيعة المجال الذي يتعرض له الأمن القومي للمخاطر السيبرانية، إجراءات وأساليب مناسبة يمكنها الحفاظ عليه، فالأسلحة التقليدية منها المتطورة، وحتى النووية، عاجزة عن حماية الفضاء السيبراني بل أن القواعد العسكرية، وأجهزة الإتصال وغيره، يمكن أن تكون هي نفسها

---

[1] – محمد علي قطب، الجرائم المعلومات وطرق مواجهتها، مركز الاعلام الأمني، الأكاديمية الملكية للشرطة، 2009، ص11.

هدفا لمقتحمي الأنظمة المعلوماتية والمواقع، لكن ذلك لا يمنع أوجه التشابه بين سياسات الأمن، كما لا يمنع إعتماد بعض المبادئ في سياسة وإستراتيجية الدفاع والحماية [1].

وعلى خطٍّ موازٍ يشمل الأمن الوطني، أمن المعلومات ليس فقط بالمعنى المادي، أي ضمان عدم تخريبها، أو تشويهها، والقضاء عليها أو سرقتها، بل أيضا ضمان سرّيتها، وعدم إطلاع الآخرين عليها ومصداقيتها وصحبتها، ومن أهم سمات المخاطر السيبرانية التي لها تأثير على الأمن القومي ما يلي [2]:

- **السرعة الفائقة** :هناك فجوة في السرعة بين الدول المتقدمة والنامية، ومن أمثلة هذا التسارع تنامي معدل المعاملات الإلكترونية العالمية عبر شبكات الأنترنت.
- **اللامحدودية (إنهيار الفواصل الجغرافية)**: يحقق النظام الدولي للمعلومات الفرصة للجميع من أجل الخروج إلى العالمية، فوق كل الحدود، وفوق كل الفواصل، ويخلق ما يسمى الفضاء اللامتناهي يتسابق فيه الجميع نحو تلك العالمية.
- **الازمنية (التنافس في الوقت)**: يتسم النظام الدولي المعلوماتي بالعمل في الزمن الحقيقي، حيث تعمل كل المواقع والخدمات بلا توقف في جميع أنحاء العالم 24 سا، 7 /7 بالرغم من الفواصل الزمنية.
- **اللامادية (تضاؤل قيمة المكونات المادية)**: تضاءلت قيمة المكونات المادية إلى 30 % من قيمة المنتج، فإنها قد وصلت إلى حوالي 10 % سنة 2011 [3].

---

[1] – جمال محمد غيطاس، الأمن المعلوماتي والجرائم الالكترونية، أدوات جديدة للصراع، مركز الجزيرة للدراسات، القاهرة، 2012، ص06 .

[2] – زهوة خلوط، التسويق الابتكاري وأثره على بناء ولاء الزبائن، دراسة حالة :مؤسسة اتصالات الجزائر، رسالة ماجيستير، جامعة امحمد بوقرة، بومرداس، كلية العلوم الاقتصادية تجارة وعلوم التسيير، 2014 – 2013

[3] – نعيمة برنيس، الوظيفة الإعلامية لشبكة الأنترنت في عصر ثورة المعلومات، رسالة ماجستير، جامعة منثوري قسنطينة، كلية العلوم الإنسانية والإجتماعية، فرع :صحافة مكتوبة وسمعية بصري، 2009–2010، ص 101.

فبما أن المخاطر السيبرانية ترقى إلى مستوى الأمن الوطني ككل، فإن وسائل المواجهة والحماية لا بد وأن تظللها منظومة الأمن الوطني، لأنه من الخطأ أن تكون الأخطار والتهديدات شاملة وربما منسقة ومخططة أحيانا، ثم تأتي سبل وسائل مواجهتها جزئية وعفوية وخالية من التخطيط وتفتقر للتنسيق والرشد، فإدارة التهديدات السيبرانية داخل البنية المعلوماتية الوطنية يتطلب بيئتين للأمن الوطني (بيئة داخلية وبيئة خارجية) [1].

البيئة الداخلية للأمن الوطني: إدارة التهديدات المتداولة داخل البيئة المعلوماتية الداخلية يتطلب فهما ورؤية جديدة لأساليب ومناهج وأدوات تداول المعلومات بين الدولة الواحدة أو بينها وبين أفرادها، ومجتمعاتها ومؤسساتها الحكومية وغير الحكومية.

البيئة الخارجية للأمن الوطني: إدارة التهديدات يتطلب مناهج وأدوات وأساليب بين الدولة وباقي الدول الأخرى والفواعل الرسمية وغير الرسمية.

المبحث الثالث: مفهوم وأبعاد الحرب السيبرانية.

لقد أفرزت العولمة مجموعة من التطورات وتحديدا على الصعيد التكنولوجي، فتم الدمج بين الفضاء السيبراني والأساليب المستخدمة في مجال الصراعات الدولية، فأصبحت بذلك حرب المعلومات عمليات عسكرية تدور في ميدان تكنولوجي رفيع المستوى في صورة حرب سيبرانية بين القيادات الصديقة والمعادية.

---

(1) – باديس لونيس، جمهور الطلبة الجزائريين والأنترنت، دراسة في استخدامات إشباعات طلبة جامعة منتوري قسنطينة، رسالة ماجستير، جامعة منتوري –قسنطينة، كلية العلوم الإنسانية والعلوم الإجتماعية، قسم علوم الإعلام والاتصال 2007،2008 ، ص6 .

ارتبطت ثورة المعلومات بالمجال العسكري أثناء الحرب الباردة، نظرا لشدة التنافس بين القطبين لذا بدأ التفكير في تطوير مجالات البحث التقنية ودخلت التكنولوجيا في صناعة الاسلحة التقليدية، لتصبح إحدى أهم العناصر المكونة لمنظومة المن الشامل " **القوة الصلبة** + **القوة الناعمة**"، وأصبحت السرعة والدقة في تنفيذ العمليات تتجه نحو القطاعات الحساسة باستهداف أجهزة الانترنت والحواسيب، ومن بين العمليات نذكر، الحرب الإلكترونية التقليدية، القرصنة الإلكترونية وحرب المعلومات الاقتصادية [1].

من هذا المنطلق، أصبح السباق نحو التفوق في القدرات العسكرية من اجل السيطرة على العالم بواسطة التكنولوجية المعلوماتية العصب الرئيسي الذي حاول توظيفه أكثر من فاعل في الساحة الدولية خلال القرن الواحد والعشرون، وبذلك أصبحت التقنيات المستعملة خاصة الانترنت من اهم الوسائل في النشاط العسكري والأمني للضغط والتجسس على الدول.

ومن هذا المنطلق قمنا بتقسيم هذا المبحث الى ثلاث مطالب تناولنا في اولهم مفهوم الحرب السيبرانية أما المطلب الثاني فقد خصصناه لطبيعة الحرب السيبرانية ودوافعها والمطلب الثالث تحت عنوان خصائص وأنواع الحرب السيبرانية.

المطلب الأول: مفهوم الحرب السيبرانية.

تغيرت الحروب ولم تعد تعتمد على جيوش عسكرية واسلحة قتالية، بل أصبحت الحروب السيبرانية بديلا لتلك الحروب التقليدية، وذلك لسرعتها ودقتها في تنفيذ العمليات العسكرية وتعتبر من أدوات الحرب الشاملة.

---

[1] – ذيب بن عايض القحطاني، أمن المعلومات، مدينة الملك عبد العزيز للتعليم والتقنية، الرياض، المملكة العربية السعودية، 2015، ص58

الفرع الأول: تعريف الحرب السيبرانية.

تعني الحرب الإلكترونية الأفعال التي تقوم بها الدول القومية لاختراق الأنظمة والشبكات المعلوماتية للدول الأخرى بغاية إحداث الضرر والتخريب ويعرفها هيرش (herch) بأنها إختراق للشبكات الأجنبية من اجل تخريب أو تفكيك تلك الشبكات وجعلها غير قابلة للعمل [1].

وتعرف كذلك بأنها كل فعل فردي أو جماعي مخطط له يهدف إلى المساس بوحدة وسلامة النظام المعلوماتي لمؤسسة أو منظمة أو دولة معينة، بإستخدام كل أو جزء من شبكة الإتصالات سواء الإنترنت أو أنواع من الشبكات الإتصالية الرقمية، بحيث تؤدي إلى حدوث أضرار توازي ما قد ينجم عن إستخدام القوة العسكرية المسلحة وقد صنفتها وزارة الدفاع الأمريكية إلى ثلاث 03 أصناف وهي حرب سيبرانية هجومية وأخرى دفاعية والثالثة إستخباراتية [2].

الفرع الثاني: التعريف الاجرائي.

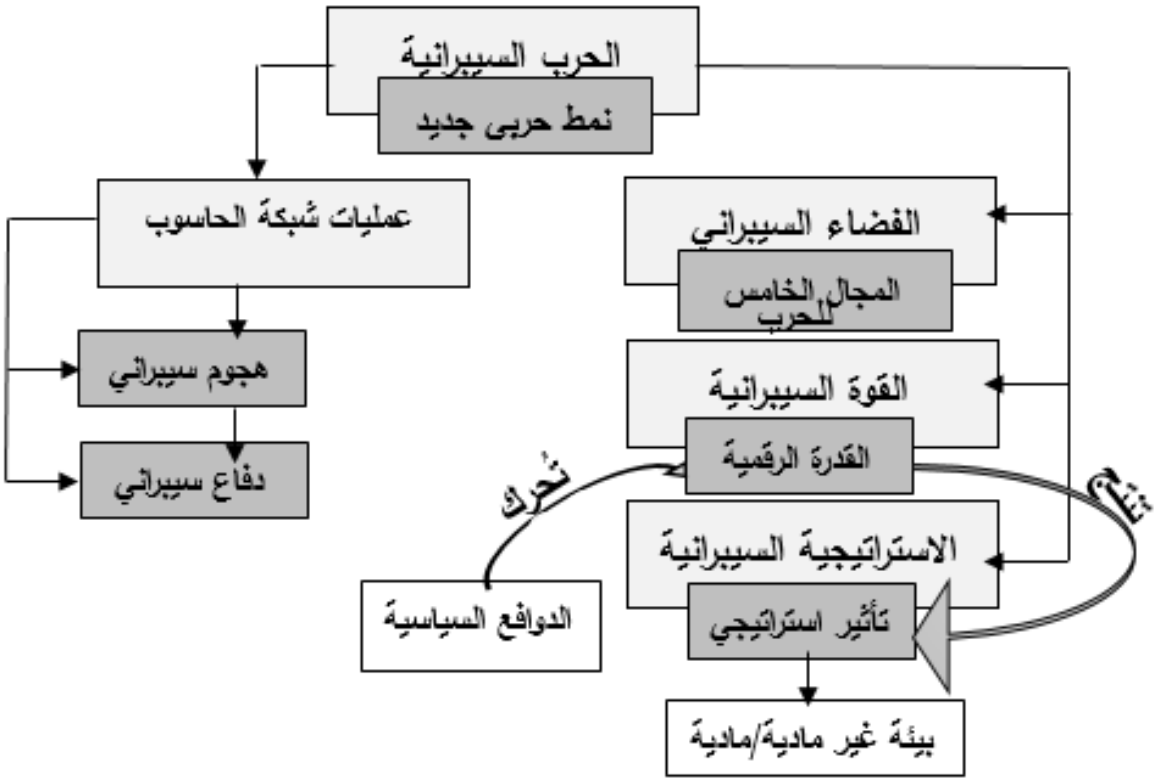
الحرب السيبرانية هي حرب نشأة في الفضاء السيبراني، تستخدم التأثير الرقمي الذي تحركه دوافع سياسية، لإجبار الخصم على تنفيذ إرادة الطرف المهاجم، وتعرف أيضا أنها نزاع عسكري في الفضاء السيبراني الذي يمثل مجالا جديدا للحروب.

---

[1] – بوبرطخ نسيم، الفضاء السيبراني مسرح الصراعات الجيوسياسية المعاصرة، مجلة الجيش، العدد685 ، ص25.

[2] – عسكري محمد، مرجع سابق، ص 275.

الشكل رقم (01): مخطط تعريف الحرب السيبرانية.



المطلب الثاني: طبيعة الحرب السيبرانية ودوافعها.

الفرع الأول: طبيعتها.

تختلف الحروب السيبرانية من حيث طبيعتها لان الصراع داخل الفضاء السيبراني غير مضمون النتائج المتوقعة والمسطرة، فهي حروب تهدد وتستهدف النظام والأمن العام بصفة مباشرة من خلال محاولات شل وتعطيل الأنظمة المعلوماتية المتعلقة بالمسائل الحيوية للدولة المستهدفة، كما انها ديناميكية ودائمة لأنها خفية فالدول في ظلها وقيادتها العسكرية إما في حالة هجوم او دفاع دائم [1].

---

[1] – غريب، صفحة113

كما أنها تتسم من حيث طبيعتها العملياتية:

- عدم وضوح الخطوة الفاصلة بين الحرب والسياسة وبين المقاتلين والمدنيين.
- غياب التسلسل الهرمي للقيادات كما أنها لا تستند إلى قيادة وطنية.
- تستهدف جمع المعلومات الاستخباراتية والمتعلقة بالبنية الإستراتيجية.
- تستهدف تفكيك البنية النفسية والانسجام داخل مجتمع العدو[1].

الفرع الثاني: دوافعها.

أما من حيث دوافعها فيمكن ذكر إلى جانب واقع تزايد إرتباط العالم بالفضاء الرقمي وتراجع دور الدول في الرقابة والتحكم في الفضاء السيبراني وقلة تكلفة الحروب السيبرانية:

- ظهور قواعد البيانات Big Data حيث أدى الاعتماد على الأنظمة المعلوماتية في مجال اتخاذ القرارات العسكرية منها خصوصا وتسيرها إلى توفير كم هائل من المعلومات التي تستخدم في مجال تسيير المعارك وتنمية الكفاءات القتالية، وهوما جعل منها هدفا لمختلف الهجمات الإلكترونية بغرض الاستيلاء عليها.
- غيان الطابع الهجومي على الدفاعي بحيث تميل الكفة في مجال الحروب السيبرانية للهجمات الإلكترونية أكثر من الأحزمة الدفاعية وهوما جعل الكل إما عنصرا مهاجما او مدافعا بشكل إجباري في ظل عدما اعتراف الهجمات الإلكترونية بالحدود لا المكانية ولا الزمانية [2].

---

[1] – بوبرطخ، المرجع السابق، ص 25.

[2] – ربيعي حسين وسمر محمود، الحروب السيبرانية :المخاطر واستراتيجيات تحقيق الأمن السيبراني الدولي والداخلي، المجلة الجزائرية للأمن الإنساني، جامعة الأخوة منتوري قسنطينة1 ، المجلد 07، العدد 2، جويلية 2022، ص ص177-178.

المطلب الثالث: خصائص وأنواع الحرب السيبرانية.

الفرع الأول: خصائص الهجمات السيبرانية

تتسم الهجمات السيبرانية التي توجه من خلال الفضاء السيبراني بخصائص تميزها عن غيرها من الهجمات العادية ومن أبرزها ما يلي:

- الهجمات السيبرانية هي هجمات تقنية متطورة، عكست قمة التطور الذي وصلت إليه ثورة المعلومات [1].
- التكلفة المتدنية نسبيًا للهجمات السيبرانية، فلا تحتاج الدول إلى تخصيص ميزانيات ضخمة لإنتاج أسلحتها السيبرانية على خلاف الأسلحة المستخدمة في النزاعات العنيفة التقليدية ذات الكلفة العالية جداً كحاملات الطائرات والمقاتلات المتطورة [2].
- الهجوم السيبراني قد يحدث في أي وقت وفي مدة قصيرة من الزمن، سواء في السلم، أو في الحرب [3].
- يتمتع المهاجم بميزة واضحة في الهجمات **السيبرانية** على المدافع، لأن هذه الهجمات تتميز بالسرعة والمرونة والمراوغة، فمن غير المرجح أن تنجح عقلية التحصن لوحدها، لأن التحصين في هذا الاتجاه سيجعل الجانب الآخر عرضة لمزيد من محاولات الاختراق، وبالتالي المزيد من الضغط.
- لا تعرف الهجمات **السيبرانية** الحدود الجغرافية فهي متنوعة ومتطورة بوسائلها المرتبطة بأكثر المجالات التقنية تطوراً وتغيراً في الحياة المعاصرة للدول، وهي علاوة على ذلك

---

[1] – موقع الموسوعة الجزائرية للدراسات السياسية والاستراتيجية، الحرب السيبرانية وتداعياتها على الأمن العالمي، متاح على الرابط https://cutt.ly/uh5Gq3D، 05/16 2204، 14:06.

[2] – نفس المرجع، نفس الموضوع

[3] – نفس المرجع، نفس الموضوع

غير محدودة الأهداف والنتائج، إذ قد تتعدى مخاطرها ميادين القتال التقليدية لتصل بدمارها إلى أكثر المواقع السيادية والحساسة تحصيناً وبعداً عن دائرة القتال.

- صعوبة تحديد موقع وشخصية القائم بالهجمات السيبرانية ذات التأثير العالي لكونها لا تترك أثر أو دليل على حصولها، إذ إن معظم الهجمات السيبرانية يتم اكتشافها بالصدفة، وبعد فترة طويلة وبمساعدة المهارات الفنية عالية المستوى لإكتشاف مصدر الهجوم.
- كذلك تتميز الهجمات السيبرانية بأن بها تدمير لا تصاحبه دماء وأشلاء بالضرورة، وبسبب انتشار الفضاء السيبراني وسهولة الوصول إليه يمكن أن يزيد عدد المهاجمين وكذلك توسع دائرة المواقع المستهدفة، ولتدور تلك الهجمات المتبادلة على نحو من الكر والفر ليعبر عن حالة صراع مطولة مرتبطة بالطبيعة المتنوعة للفضاء السيبراني [1].

الفرع الثاني: أنواع الحروب السيبرانية.

تتعدد وتتنوع الحروب **السيبرانية** بحسب أهدافها وتأثيراتها، ولكنها لا تخرج عما يأتي:

- **حرب سيبرانية هجومية:** تستهدف هذه النوعية من الحروب إفساد وتخريب أو التشكيك في دقة المعلومات ومن أمثلة ذلك عمليات التنصت الإلكتروني، والقرصنة الالكترونية والهجمات الإرهابية الإلكترونية، ومن أهم أسلحة هذه الحرب الفيروسات بأنواعها Logic Doors و Back Doors وعمليات الر Chipping وكذلك الإختراقات الإلكترونية(E. Penitration.

-**حرب سيبرانية دفاعية:** وتشمل إستخدام كافة التقنيات، والوسائل التكنولوجية الوقائية لتجنب أو التقليل من مخاطر وتهديد الحروب السيبرانية الهجومية المعادية من الدول أو الفاعلين من غير الدول، فالحروب **السيبرانية** حروب حقيقية مسرحها المباشر الشبكات والتقنيات الرقمية، وأهدافها الأساسية نفسية معنوية للتأثير على الخصوم في كافة المجالات*

---

[1] – العبودي، علي عبد الرحيم، هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين، المجلة العلمية الأكاديمية العراقية، العدد57 ، جامعة برداد، كلية العلوم السياسية،2019 ، ص ص 118 – 89 .

خلاصة الفصل

يستنتج من خلال ما سبق أن العالم اليوم يشهد مجموعة من التغيرات في الدراسات الأمنية أثرت على مختلف المفاهيم وتطويرها إلى مفاهيم جديدة مواكبة للعصر، ومن أهم هذه المفاهيم نجد الفضاء السيبراني وهو عبارة عن ساحة عالمية عابرة لحدود الدول، هذا المجال الكبير الذي أنتج مفهوم" **الأمن السيبراني** "في ظل" **تهديدات جديدة سيبرانية** "خلفت تحولا كبيرا في استخدامات القوة من قوة صلبة وناعمة إلى قوة" **ذكية سيبرانية** "مما جعل ظهور" **فواعل سيبرانية**" أخرى جديدة لها تأثير على العلاقات الدولية وعلى الأمن والوطني ككل وأمن الأفراد أيضا، كما فرضت الثورة التكنولوجية مجموعة من التحديات والتهديدات الأمنية الجديدة والتي تسمى بالحروب السيبرانية.

وعليه فالأمن السيبراني في الدراسات الأمنية والعلاقات الدولية، هو مسألة الحاضر كما أنه موضوع المستقبل أيضا.

الفصل الثاني: السياسة الأمنية الجزائرية في ظل التطور التكنولوجي

تمهيد

في ظل التوجه الدولي نحو الحكومة الإلكترونية، أصبحت قضية الأمن المعلوماتي السيبراني من التحديات الكبرى على الصعيدين الإقليمي والعالمي، خاصة مع زيادة التهديدات الأمنية الإلكترونية، الجزائر كغيرها من الدول، تسعى منذ إنتهاجها للإدارة الإلكترونية، إلى حماية منظومتها المعلوماتية من خلال العديد من الأجهزة والخلايا الأمنية، وتهدف السياسة العامة للأمن السيبراني في الجزائر إلى ضمان الحماية والأمان للبنية التحتية السيبرانية في البلاد والتصدي للتهديدات الإلكترونية والهجمات السيبرانية.

تعتبر الحكومة الجزائرية الأمن السيبراني أمرًا ذا أولوية عالية وتعمل على تنفيذ إجراءات وسياسات لحماية البيانات الحكومية والمعلومات الحساسة والأنظمة الحيوية، تعمل جاهدة على وضع تشريعات وقوانين قوية تنظم مجال الأمن السيبراني وتعاقب على الجرائم الإلكترونية والاختراقات السيبرانية، وتعمل أيضًا على تطوير القدرات القانونية لمكافحة الجرائم السيبرانية، وتعزيز التعاون الدولي في مجال الأمن السيبراني من خلال التعاون مع الدول الأخرى والمؤسسات الدولية ذات الصلة.

المبحث الأول: مكانة الأمن السيبراني في السياسة الأمنية للجزائر.

لقد وضعت الجزائر الأمن السيبراني أحد أولوياتها على غرار باقي دول العالم التي سارعت إلى مراجعة سياساتها الأمنية، وإدراجها الآليات وميكانزمات جديدة تعني بهذه المسائل، بالمؤازرة مع تطوير البنيات الأساسية المتعلقة بتكنولوجيات العالم الرقمي، ويفرض مطالب الأمن مضاعفة أنظمة الرقابة التي قد تشكل تهديدا ممكنا للحريات الفردية.

لقد أصبح الأمن السيبراني ركن أساسي ضمن العقيدة الأمنية الجزائرية المعاصرة، والتي يجب على الدفاع الوطني من خلال أجهزتها المختلفة، ولا ننسى كذلك الجانب القانوني والمشرع الجزائري وكيف قام بمواجهة هذه الجرائم والاعتداءات الأمنية وتشير الإحصائيات المسجلة في الجزائر أن الجريمة الإلكترونية أخذت منحا تصاعديا في الآونة الأخيرة، ولهذا فإن السلطات الجزائرية ملزمة باتخاذ الاحتياطات الأمنية اللازمة لتفادي أي نوع من الجرائم السيبرانية.

المطلب الأول: السياسات العامة السيبرانية.

تختلف السياسات العامة السيبرانية عن غيرها من السياسات العامة ويرجع ذلك إلى إختلاف بيئتها وكذا الفاعلين المساهمين فيها.

الفرع الأول: مفهوم السياسة العامة والسياسة العامة السيبرانية.

أولا/ السياسة العامة: تشكل السياسة العامة أحد المفاهيم المستحدثة في دراسات العلوم السياسية– النظم السياسية بشكل خاص– والإدارة العامة، والتي أصبحت اليوم أحد أخصب المواضيع وأعقدها، حيث لقيت إهتمامًا بالغا وتداولا واسعا من لدن الباحثين والمتخصصين في علم الإدارة العامة وعلماء السياسة، إذا فهي فكرة مائعة ومضمون لزج يستجلب الكثير من المعاني كالحكومة، الإدارة العامة والمصالح الوطنية ... .

وقد تتعدد تعريفات هذا المصطلح شأنه شأن غيره من المصطلحات في نطاق العلوم الاجتماعية.

فالسياسة هي برنامج عمل يحمل أهدافا متنوعة، تعمل مختلف تكوينات المؤسسات السياسية الرسمية نحو تحقيقها بما يضمن القدر الكافي من التوافق والانسجام، وبما يحقق تناغما كافيا أو نسبيا مع مختلف التأثيرات البيئوية، وهناك من يؤكد أن الصراع والقوة والسياسة والسياسة العامة هي العناصر التحليلية في تعريف السياسة [1].

فالسياسة العامة بهذا المعنى وصفها البعض بأنها: ذلك الممر الحلزوني المؤطر والغير مؤطر أحيانا يجد المارون منه أنفسهم مجبرين على المرور منه، صناعاً ومستفيدين ومنفذين وهناك تعاريف أخرى متعددة ومتباينة لكلمة " **سياسة** " فقد عرفت بأنها: "برنامج معد للقيم المستهدفة والممارسات، وهي وضع وصياغة وتطبيق التحديات والمطالب والتوقعات فيما يخص مستقبل علاقات الذات مع الغير , وقد أكد البعض على عنصر الإكراه , فوضعت السياسة بأنها الإكراه المخطط عمدا، أو أقوال تحدد غرض ووسائل وموضوع أشياء ممارسة الإكراه داخل سياق علاقة القوة في المنظمات ، وأشار البعض إلى مخرج لأي صانع قرار وأشار البعض إلى تعلقها بالمدى الطويل والبعض إلى جوانب التوجه نحو الهدف"[2].

ثانيا/ السياسة العامة السيبرانية: غرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بتوثيق متطلبات الأمن السيبراني والتزام جامعة الحدود الشمالية بها، لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية

---

[1] – وصال نجيب العزاوي، مبادئ السياسة العامة، الأردن، دار أسامة للنشر والتوزيع، 2003، ص 14.

[2] – كمال المنوفي، السياسة العامة وأداء النظام السياسي، القاهرة، مكتبة النهضة المصرية، 1988، ص15.

والخارجية، ويتم ذلك من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأعمال التنظيمية الخاصة بجامعة الحدود الشمالية، والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم 1-3-1 من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

وفي ابسط تعريفاتها تعتبر السياسات العامة السيبرانية، السياسات التي تمكن الدولة من تعظيم الإستفادة من الشبكة المعلوماتية وتفادي مخاطرها، كما تعرف على أنها مجمل القوانين والسياسات والأدوات والنصوص والمفاهيم وميكانزمات الأمن وطرق تسيير الأخطار، والممارسات التكنولوجية المتعلقة بتكنولوجيا المعلومات والإتصالات، لحماية الدول والمنظمات والأشخاص.

غير أن هاته السياسة ليست مثل باقي السياسات العامة الأخرى أو السياسات القطاعية من حيث وضوح الفاعلين ومجال عملهم، وذلك راجع للفضاء السيبراني الذي يتجاوز الجغرافيا، واضعا الحكومة في مشكلة أساسية هي الحماية والعقاب، أي حماية المنشآت وعقاب المجرمين الذين لا يمكن تحديد أماكنهم دائما ما يجعل الأمن السيبراني يمثل يحديا صعبا بالنسبة للحكومات [3].

---

[3] – بورياح سليمة، السياسات العامة الجزائرية في مجال السيبرانية، الواقع والتحديات، مجلة دفاتر السياسة والقانون، جامعة امحمد بوقرة ، بومرداس، الجزائر،المجلد15، العدد 01، 2023، ص 276.

الفرع الثاني: السياسات العامة الجزائرية والدولية في مجال الأمن السيبراني.

اولا/ السياسات العامة الجزائرية: السياسة العامة للأمن السيبراني في الجزائر تهدف إلى ضمان الحماية والأمان للبنية التحتية السيبرانية في البلاد والتصدي للتهديدات الإلكترونية والهجمات السيبرانية. تعتبر الحكومة الجزائرية الأمن السيبراني أمرًا ذا أولوية عالية وتعمل على تنفيذ إجراءات وسياسات لحماية البيانات الحكومية والمعلومات الحساسة والأنظمة الحيوية.

تعمل الحكومة على وضع تشريعات وقوانين قوية تنظم مجال الأمن السيبراني وتعاقب على الجرائم الإلكترونية والاختراقات السيبرانية. وتعمل أيضًا على تطوير القدرات القانونية لمكافحة الجرائم السيبرانية، تعزيز التعاون الدولي في مجال الأمن السيبراني من خلال التعاون مع الدول الأخرى والمؤسسات الدولية ذات الصلة. تتمثّل هذه التعاونيات في تبادل المعلومات والخبرات والتدريب وتنظيم الفعاليات المشتركة لمكافحة التهديدات السيبرانية. تعمل السياسة العامة للأمن السيبراني في الجزائر إلى زيادة الوعي والتثقيف حول أهمية الأمن السيبراني وكيفية التصدي للتهديدات السيبرانية تتضمن هذه الجهود توعية المستخدمين بأفضل الممارسات الأمنية وتقديم المشورة [1].

ثانيا/ السياسات العامة الدولية: يرجع بداية التعاون الدولي في المجال السيبراني إلى عام 2000 حيث تعهد رؤساء الدول في قمة الأرض بتحقيق الأهداف الإنمائية للألفية، ففي المجال السيبراني دعا الهدف الثامن إلى تعاون الدول مع القطاع الخاص من اجل إتاحة فوائد تكنولوجيا المعلومات والإتصالات للذين لديهم فرص قليلة في الوصول أليها [2].

---

[2] – بورياح سليمة، المرجع السابق، ص ص 277-278.

ففي عام 2004 تضمن الإعلان الصادر عن القمة العالمية لمجتمع المعلومات المنعقدة بجنيف، الرغبة في بناء مجتمع معلومات محوره الانسان وغايته تحقيق التنمية بناءا على مبادئ ميثاق الأمم المتحدة واحترام الإعلان العالمي لحقوق الانسان.

وفي عام 2005 وضع الإتحاد الدولي للإتصالات الأهداف المتوخاة لسياسات الأمن السيبراني، وهي تعزيز التعاون بين الحكومات في الأمم المتحدة وكل أصحاب المصلحة، والقطاع الخاص ورفع مستوى الوعي وتشجيع التعليم وتثقيف المواطنين.

أما في 2007 أطلق الأمين العام للاتحاد الدولي للإتصالات، جدول أعمال الأمن السيبراني العالمي، من أجل تقديم إطار عمل يمكن من خلاله الاستجابة للتحديات المتنامية للأمت السيبراني، من خلال إشراك كل أصحاب المصلحة من حكومات وقطاع خاص ومجتمع مدني ومنظمات دولية.

وفي عام 2015 نشرت منظمة التعاون الاقتصادي والتنمية، توصية حول إدارة مخاطر الأمن الرقمي، لتحقيق الازدهار الاقتصادي والاجتماعي من أجل توفير المعلومات اللازمة لتطوير الاستراتيجيات الوطنية التي تهدف لإدارة الامن القومي ولتحسين الفوائد الإقتصادية والاجتماعية المتوقعة من الإنفتاح الرقمي.

المطلب الثاني: التحولات في مفهوم الأمن والتقنيات المستخدمة:

عملت الجزائر منذ بداية القرن الخالي على مواكبة التغيرات العالمية في مجال الامن السيبراني والسياسات العامة السيبرانية بدءاً بتكثيف تشريعياتها وقوانينها بما يتماشى مع المعاهدات

---

[1] – بورياح سليمة، المرجع السابق، ص 275.

[2] – المرجع نفسه، ص ص 277-278.

والاتفاقيات الدولية وأيضا التطورات التكنولوجية، كما أنشأت العديد من المؤسسات إلى جانب تعزيز التعاون الدولي في مجال الأمن السيبراني وهذا ما سنراه في هذا المطلب.

الفرع الأول: تحولات في مفهوم الأمن.

أولا/ مفهوم الامن: لقد توسع نطاق مفهوم الأمن من المعنى التقليدي العسكري، والذي يركز على إحتياجات البقاء الوطني وحماية الدولة والحدود والشعب والنظم والقيم وضد العدوان الخارجي، إلى المعنى العالمي الذي يشمل قطاعات أخرى غير العسكرية، تتمثل في الأمن المجتمعي وأمن البشر والأمن البيئي والأمن الصحي وغيرها [1]، فقد تم الإقرار بالحاجة إلى تطبيق سياسات غير عسكرية والذي أصطلح عليه بالأمن الناعم، الذي تندرج في إطاره كل التحديات غير العسكرية التي تواجه الدولة كالعنف الإجرامي، والجوع، الأوبئة، الإرهاب وغيرها [2].

فالأمن وإن كان نسبيا في الحصول عليه وفقا لطبيعة النظام السياسي السائد ومدى التهديدات المنبثقة عنه وضده، فإنه يتم عن طريق ظرف خاص تبعا لما خلفه من تطور أو تراجع، أخذا بعين الإعتبار على دول الجوار أو تأثيرا على الدولة المعنية [3]. فأصبح" **مفهوم الأمن** "مختلفا في سياق متطلبات المجتمع ككل، وهو أمن يتسع ليشمل نواح كثيرة، ففي الزمن الأخير لم تقتصر الدفاعات للمصالح والأوطان على الأعمال العسكرية فقط، بل تعداها إلى مفاهيم ووقائع أخرى.

---

[1]– ذياب موسى البداينة،"الأمن الوطني في عصر العولمة"، الرياض، جامعة نايف العربية للعلوم الأمنية، 2011، ص22.

[2]– حنان بن عبد الرزاق،"تأثير المأزق الأمني الاثني على الاستقرار الداخلي لدولة، د راسة للنموذج الاسباني" أطروحة دكتورا، جامعة محمد خيضر، بسكرة، كلية العلوم السياسية، تخصص :علاقات دولية ود راسات استراتيجية،2017، ص19

[3]– ميلود عامر الحاج،"الأمن القومي العربي وتحدياته المستقبلة ، المملكة العربية السعودية، مركز الدراسات والبحوث، ص21

ثانيا/ أسباب تحول مفهوم الأمن: شكلت نهاية الثمانينيات وبداية التسعينيات من القرن الماضي، بداية التحول في ميدان الدارسات الأمنية، إذ بدأ الحديث عن إعادة النظر في مسألة توسيع" **مفهوم الأمن** "وعدم حصره في الإطار العسكري فقط، وذلك بتوسيع قائمة التهديدات إلى مجالات أخرى غير عسكرية، ولم يكن ممكنا حدوث تغيير في المناهج الأمنية لو لم تتغير التهديدات المحددة لمفهوم الأمن، والجزائر وكغيرها من باقي الدول كانت تعاني من أنماط تلك التهديدات التي أثرت على العالم بأسره [1].

ثالثا/ الأمن السيبراني الجزائري: في ظل التوجه الدولي نحو الحكومة الإلكترونية أصبحت قضية الأمن المعلوماتي السيبراني من التحديات الكبرى على الصعيدين الإقليمي والعالمي، لا سيما مع تزايد التهديدات الأمنية الإلكترونية، والجزائر كغيرها من الدول سعت منذ انتهاجها للإدارة الإلكترونية حماية منظومتها المعلوماتية من خلال العديد من الأجهزة والخلايا الأمنية .لقد أصبح الأمن المعلوماتي السيبراني ركن أساسي ضمن المنظومة الأمنية المعاصرة، والتي يجب على الدفاع الوطني من خلال أجهزته كالدرك الوطني الجزائري باعتباره مسؤول أمني داخلي تحقيقه في ظل تنامي الجريمة الرقمية، وكذا نظرا للاستغلال المتنامي للشبكات الالكترونية لأهداف إجرامية، والتي تؤثر سلباً على سلامة البنى التحتية للمعلومات الوطنية الحساسة لا سيما على المعلومات الشخصية.

الفرع الثاني: التقنيات المستخدمة.

توجد العديد من تقنيات الحماية المستخدمة في مجال الأمن السيبراني، وتتنوع حسب

---

[1] – سالم المعوش،"مجتمع المعرفة وتعزيز الأمن القومي، المشهد العالمي الجديد"، لبنان، مركز الأبحاث العلمية، 2011، ص18.

الاحتياجات والتحديات الفردية، وإليك بعض التقنيات الرئيسية [1]:

أولا/ برامج مكافحة البرمجيات الخبيثة: تساعد تكنولوجيا مكافحة البرمجيات الخبيثة في اكتشاف وإزالة البرامج الضارة والفيروسات من الأنظمة.

ثانيا/ جدران الحماية: تراقب حركة المرور بين الشبكة الداخلية والشبكة الخارجية، مما يساعد في حماية الأنظمة من التسلل.

ثالثا/ التحديثات: يساعد تحديث البرمجيات والأنظمة بانتظام في سد الثغرات الأمنية وتعزيز الأمان.

رابعا/ أنظمة الكشف عن التسلل: تراقب هذه الأنظمة حركة المرور عبر الشبكة وتحاول اكتشاف ومنع التسلل غير المرغوب فيه.

خامسا/ تقنيات التشفير: تساعد في تأمين البيانات عند نقلها عبر الشبكة، مما يحميها من التجسس والاستخدام غير المصرح به.

المطلب الثالث: محددات السياسات السيبرانية الجزائرية والتهديدات المتطورة.

لا شك في أن الأمن السيبراني يمثل الدرع الرقمي الذي يحمي عالمنا المتصل بالإنترنت. وفي عصر تكنولوجيا المعلومات حيث تتداخل حياتنا مع الشبكة العنكبوتية، يصبح الأمن السيبراني أمرا حيويا للحفاظ على خصوصيتنا وأمان بياناتنا، ويشمل الأمن السيبراني مجموعة من السياسات والتقنيات التي تستهدف الوقاية من الهجمات وتحددها منظومات معينة للحفاظ على سلامة

---

[1]– أحمد عنتر، تقنيات الأمن السيبراني والتحديات المستقبلية مقال منشور على الانترنت بتاريخ 2023/12/04، https://www.aljazeera.net/tech/2023/12/4/، تاريخ التصفح 2024/05/05، 20:50.

الأنظمة الرقمية، وبناء حاجز ضد التهديدات السيبرانية المتزايدة والمتطورة.

الفرع الأول: محددات السياسات السيبرانية الجزائرية

أولا/ المنظومة القانونية: في أطار مراجعة قوانين الجمهورية لتكييفها مع التطورات التكنولوجية العالمية وأيضا مع المعاهدات والإتفاقيات الدولية التي أبرمتها الجزائر، ومن أجل مواكبة عصر المعلومات راجعت الجزائر بعض القوانين منها، القانون 09-04 والقانون 03/15 والقانون 18-04 و18-05...[1].

ثانيا/ المنظومة المؤسساتية: بتفحص المؤسسات القائمة على الأمن السيبراني بشكل عام نجد في المقدمة المؤسسات التابعة لوزارة الدفاع التي كانت سباقة في انشاء مؤسسات تعنى بحماية الأمن السيبراني الجزائري التركيز أولا على مكافحة الجريمة ثم وضع الاستراتيجيات الدفاعية لتأمين المنشآت الوطنية الرقمية نذكر منها على سبيل المثال ما يلي [2]:

- مركز الوقاية من جرائم الإعلام الالي وجرائم المعلوماتية للدرك الوطني.
- المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني.
- المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني.
- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.
- مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة.
- المركز الوطني للإشارة والحروب الإلكترونية.

ثالثا/ المنظومة الاستراتيجية: التحديات الراهنة للجزائر تستوجب بناء وإرساء بنية تحتية رقمية قوية للإندماج في البيئة العالمية في ظل تحديات ترافق هاته الخدمة مثل: معايير أمن المعلومات، وانقطاع الانترنت أو ضعف خدماتها، والعقود التي تفرضها الشريكات المُوردة للخدمات والتي

---

[1] – انظر بورياح سلمة، المرجع السابق، ص ص 280-281.

[2] – انظر المرجع نفسه، ص ص 282-284.

تتسبب في إعاقة حركة البيانات والخدمات، وهذا لا يتأتى إلا بوضع استراتيجية شاملة لكل القطاعات، ويندرج كل هذا في المجالات التالية [1]:

- في مجال الأمن والدفاع الوطني.
- في مجال تعزيز القوات.
- في مجال التعاون الدولي.
- في مجال التدابير التقنية.

الفرع الثاني: تطور التهديدات السيبرانية.

من المتوقع أن تستمر التهديدات السيبرانية في التطور والتقدم في السنوات القادمة مع تقدم التكنولوجيا، ويشير خبراء الأمن إلى إمكانية ظهور تحديات وتهديدات جديدة في المستقبل، ومن هذه التهديدات المحتملة [2]:

أولا/ الذكاء الاصطناعي: يعد الذكاء الاصطناعي تقنية سريعة التطور ويمكن استخدامها لإنشاء هجمات سيبرانية أكثر تعقيدا وقوة، مما يجعل من الصعب اكتشافها والتصدي لها، حيث يمكن استخدام الذكاء الاصطناعي لإنشاء برامج ضارة أكثر ذكاء يمكنها التهرب من تقنيات الأمان التقليدية، كما يمكن أيضا استخدام الذكاء الاصطناعي لإنشاء هجمات تستهدف البنية التحتية الحيوية، مثل شبكات الطاقة أو نظم النقل.

ثانيا/ إنترنت الأشياء: وتُستخدم أجهزة إنترنت الأشياء من أجل إنشاء هجمات حجب الخدمة الموزعة (DDoS) أو سرقة البيانات أو حتى السيطرة على الأجهزة، وقد يزداد التركيز على استهدافها للوصول إلى بيانات المستخدمين أو التحكم في الأنظمة المتصلة.

---

[1] – انظر بورباح سلمة، المرجع السابق، ص 285.

[2] - احمد عنتر، المرجع السابق.

ثالثا/ الهجمات الهجينة: وتَستخدم الهجمات الهجينة مزيجا من الأساليب التقليدية وغير التقليدية، وتتميز بأنها أكثر تعقيدا وصعوبة في الاكتشاف والحماية منها مقارنة بالهجمات التقليدية.

رابعا/ هجمات الحواسيب الكمومية: قد تظهر هجمات تعتمد على الحوسبة الكمومية من أجل كسر أنظمة التشفير الحالية، حيث تتميز الحواسيب الكمومية بقدرتها على إجراء العمليات الحسابية بشكل أسرع بكثير من الحواسيب التقليدية، وهذا يجعلها قادرة على كسر أنظمة التشفير الحالية.

خامسا/ الهجمات على الذكاء الاصطناعي: قد تُستهدف نظم الذكاء الاصطناعي بشكل مباشر لتشويه البيانات أو النتائج، وقد تتسبب هذه الهجمات بتعطيل الأنظمة أو سرقة البيانات أو حتى تعديل البيانات أو إتلافها.

سادسا/ التهديدات السيبرانية للصحة الرقمية: قد تستهدف أجهزة الرعاية الصحية أو نظم السجلات الطبية، وذلك لأنها حساسة للغاية ويمكن استخدامها لأغراض ضارة، مثل الابتزاز أو التجسس أو حتى إلحاق الضرر الجسدي.

سابعا/ هجمات التحكم في الطائرات المسيرة: أصبح استهداف الطائرات المسيرة أو أنظمة التحكم فيها محط اهتمام متزايد، وقد تتسبب هذه الهجمات بأضرار جسيمة، بما في ذلك تعطيل لطائرات أو سرقة البيانات أو حتى إسقاطها.

المبحث الثاني: السياسة الأمنية الجزائرية بين العقيدة الأمنية والتطورات التكنولوجية.

تكتسي العقيدة الأمنية أهميتها من اعتبارها دليلا موجها انطلاقا من المصالح الجيوسياسية للدولة، وذلك من خلال تحديد الأوليات والتحديات البارزة والكامنة التي تواجه أمنها في ظل ما

يشهده العالم من تطور سريع وظهور أنواع جديدة من التهديد، أصبح لازما دراستها والتصدي لها، وهو ما سيتم توضيحه في المطالب الآتي:

المطلب الأول: العقيدة الأمنية الجزائرية ومرتكزاتها، المطلب الثاني: مراحل تطوير العقيدة الأمنية الجزائرية، المطلب الثالث: الاهتمامات الأمنية للجزائر.

المطلب الأول: العقيدة الأمنية الجزائرية ومرتكزاتها.

إن العقيدة الأمنية للدولة يقصد بها مجموعة الآراء والاعتقادات والمبادئ التي تشكل نظاما فكريا لمسألة الأمن في الدولة، وتتبنى الدول هذه العقيدة عندما يتعلق الأمر بتعاطيها مع التحديات والقضايا التي تواجهها، والجزائر تواجه تهديدا بالغ التطور والصعوبة والمتمثل في التهديدات السيبرانية، فالجزائر تحاول دائما أن تطور أنواع دفاعاتها ومواجهته هذه التحديات بإعادة صياغة قوانين تتماشى مع الواقع والتطور الحاصل.

الفرع الأول: العقيدة الأمنية الجزائرية:

العقيدة الأمنية تمثل تصورا أمنيا يحدد المنهجية التي تقارب بها الدولة أمنها، كما يحدد كذلك أفضل السبل لتحقيقه، وعليه عادة ما تكون مرجعية هذه العقيدة عبارة عن أطروحات نظرية تتبناها الدولة وصناع القرار فيها كما يمكن أن تأخذ صيغة إيديولوجية إذ وصلت حد النظام الفكري المتجانس والمتناغم الذي يوفر تفسيرات معينة للواقع، ويترتب على ذلك تبني القوى النافذة في المجال الأمني لهذه التفسيرات والرؤى [1].

العقيدة الأمنية :هي مجموعة القواعد والمبادئ والنظم العقائدية المنظمة والمرتبطة، التي توجه سلوك الدولة الأمني (تعاوني /غير تعاوني) وقرارا تاما على المستوى المحلي والدولي، وتعمل على كيفية استخدام القادة للقوة (العسكرية، الاقتصادية، السياسية...) من أجل الوصول

---

[1] – صالح زياني،" مرتكزات عقيدة الأمن القومي الجزائري بين الثبات والتحول"، محاضرة مقدمة لطلبة جامعة باتنة، كلية الحقوق والعلوم السياسية، د.س، ص3 .

للأهداف الإستراتيجية للدولة.

وبالرجوع إلى العقيدة الأمنية الجزائرية يمكن القول أن هناك تعدد وتنوع في المرتكزات والعوامل التي ساهمت في تحديد طبيعة العقيدة الأمنية الجزائرية منذ الأيام الأولى لإستقلال الجزائر فجملة التهديدات والمخاطر، قد لعبت دور كبير في تحديد طبيعة هذه العقيدة، وأدت إلى إعتماد على مفهوم الأمن بشقيه الصلب واللين [1].

الفرع الثاني: مرتكزات العقيدة الأمنية الجزائرية:

بهدف توضيح أهم المرتكزات التي تقوم عليها العقيدة الأمنية الجزائرية، سوف نحاول أن نذكرها في النقاط التالية:

-احترام سيادة الدول وعدم التدخل في شؤونها الداخلية كمبدأ أساسي.

-الحل السلمي للنزاعات الدولية والإقليمية بالطرق المباشرة وغير المباشرة بين الأطراف المتنازعة.

-التركيز على مفهوم الأمن بشقيه (الصلب، اللين) للحفاظ على السلم والاستقرار وفض النزاعات.

ينطلق مبدأ عدم التدخل في الشؤون الداخلية من العامل التاريخي حيث تعتبر الجزائر من بين الدول التي كافحت من أجل نيل استقلالها، فبعد نهاية الثورة اتبع القادة السياسيين سياسة الاعتماد على نفس المبدأ في بناء دولة الجزائر الحديثة ورسم سياستها المستقبلية، لذلك تم إتخاذه كمبدأ يصون ويدافع عن سيادة الدولة خاصة في الساحة الإقليمية التي تتواجد بها، وعدم التدخل في شؤونها سواء على الصعيدين السياسي والعسكري، وهو ما يفسر عدم إبرامها لأي معاهدات

---

[1] – عبد النور بن عنتر،" عقيدة الجزائر الأمنية :ضغوطات البيئة الإقليمية ومقتضيات المصالح الأمنية"، من الرابط: http://studies.aljazeera.net/ar/reports/2018/05/180502110656159.html.2019-05-تاريخ التصفح:17/05/19،2024، 15:24.

أو اتفاقيات دفاعية مع القوى الأجنبية لأنها لا تتناسب مع الخطاب الرسمي والتوجهات السياسية لإستقلالية البلاد [1].

فمن أجل الحفاظ على أمنها ورغبة منها لمباشرة العديد من الإصلاحات سواء كانت سياسية أو إقتصادية وحتى على مستوى الإحتراف داخل المؤسسة العسكرية، حدث تحولا هاما في هذه العقيدة لتتلاءم وعملية التحول المرن نحو الديمقراطية، وتزامنت عملية إعادة صياغة بعض المبادئ التي تقوم عليها العقيدة الأمنية للجزائر لتواكب السياسة الجديدة.

وتشكل الأزمات السياسية والإقتصادية الحادة تهديدا حقيقيا للأمن القومي الجزائري، وهو ما استلزم بلورة عقيدة أمنية تؤخذ في الحسبان كلا من جانبي الأمن الصلب والناعم، وساهمت بعض الظواهر المعقدة كظاهرة الإرهاب والجريمة المنظمة وتجارة واستهلاك المخدرات في إعادة تشكيل هذه العقيدة الأمنية.

وبذلك يمكن القول أن العوامل والمرتكزات التي ساهمت في تحديد طبيعة العقيدة الأمنية للجزائر كانت متنوعة وكل عامل كان له تأثير معين على جانب من جوانب اهتماماتها الأمنية، فبرغم من تنوع العوامل المؤثرة والمحركة للعقيدة الأمنية للجزائر، فإن المبادئ الكبرى لهذه العقيدة لم تتغير بل يتم في كل مرة تكيف هذه المبادئ لتتماشى مع التحولات الداخلية والدولية [2].

---

[1] – عبد النور بن عنتر،" البعد المتوسطي للأمن الجزائري :الجزائر، أوربا، الحلف الأطلسي"، الجزائر :مكتبة العصر للطبع والنشر والتوزيع، 2005، ص120.

[2] – صالح زياني، مرجع سابق، ص6.

المبحث الثالث: تطبيق مبادئ وقواعد القانون الدولي الإنساني بشأن العمليات السيبرانية.

إذا كنا فيما سبق تطرقنا إلى مفهوم الحرب السيبرانية، بالرغم مما يثيره ذلك المفهوم من غموض، فأننا في هذا المقام سوف نتناول استخدام الهجمات السيبرانية في إطار النزاعات المسلحة، تلك النزاعات التي لا يحتمل بشأنها الخلاف، في انها النزاعات التي يستخدم أو من المرجح أن يستخدم فيها السلاح من قبل كل الاطراف أو بعضهم، وحسبنا في ذلك أن نشير إلى النطاق المادي لتطبيق القانون الدولي الإنساني، انما هو زمن النزاعات المسلحة، سواء اكانت تلك مسلحة دولية، أو مسلحة غير ذي طابع دولي، كل ذلك لمعرفة مدى اتساق قواعد ذلك القانون ومدى امكانية تطبيقها بشأن العمليات السيبرانية.

المطلب الأول: شمولية مبادئ وقواعد القانون الدولي الإنساني

إذا كنا نتفق بأن قواعد القانون الدولي الإنساني لم تشير على وجه الخصوص للعمليات السيبرانية، غير أن غياب اشارات محددة في ذلك القانون لا يعني عدم خضوع هذه العمليات لقواعد القانون الدولي الإنساني، وذلك من خلال قواعده العامة التي تنظم جميع اساليب الحرب ووسائلها بما فيها استخدام الاسلحة، حيث جاءت تلك القواعد لتشتمل على كافة التطورات ذات الصلة، حيث يمكن أن نشير إلى ما تضمنه البروتوكول الاضافي الأول الملحق باتفاقيات جنيف الاربعة لعام 1977 اذ نص على ما يلي :

يلتزم أي طرف سام متعاقد عند دراسة أو تطوير أو اقتناء سلاح جديد أو أداة للحرب أو اتباع اسلوب للحرب، بأن يتحقق مما إذا كان ذلك محظورا في جميع الأحوال أو في بعضها بمقتضى هذا الملحق أو أية قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها الطرف السامي المتعاقد [*].

---

[*]– المادة (39) من البروتوكول الاضافي الأول الملحق باتفاقيات جنيف لسنة 1977.

ووفقاً للنص السابق وإذا ما تم تكييف التكنولوجيا الجديدة بأنها سلاح للحرب أو أداة لها أو اسلوب من اساليب الحرب، فعلى الاطراف التحقق في مدى مشروعية استخدامها وفقاً لقواعد البروتوكول أو أية قاعدة أخرى من قواعد القانون الدولي، ويمكن الاستناد ايضاً إلى المبادئ الأساسية للقانون الدولي الإنساني لمعرفة مدة امكانية تطبيقها بشأن ما اطلقنا عليها الحرب السيبرانية.

المطلب الثاني: خصوصية الهجمات السيبرانية وأثرها في تطبيق مبادئ وقواعد القانون الدولي الإنساني.

إذا كنا قد تطرقنا إلى شمولية مبادئ وقواعد القانون الدولي الإنساني، إلا أن ذلك لا يعني انكار حقيقة التغيرات التي شهدتها طبيعة الحروب منذ اعتماد اتفاقية جنيف الأصلية قبل ما يقارب مائة وخمسون عاماً، حيث اصبحت وسائل واساليب الحروب متطورة إلى درجة لم يكن يتصورها واضعي تلك الاتفاقية، ولعل الاستخدام المتزايد للفضاء السيبراني للأغراض العسكرية احد أهم الأسباب التي تدعو إلى إعادة النظر في القواعد التي تنظم سير النزاعات المسلحة وصياغتها بالشكل الذي يتلائم مع طبيعة هذه الاستخدامات [1].

وقد يثير تطبيق مبدأ التناسب على الهجمات السيبرانية بعض الصعوبات، ذلك أن الأضرار العرضية أمر لا محال بسبب عدم وجود الفاصل في كثير من الاحيان بين الفضاء السيبراني موضع استخدام المدنيين وبين ذلك الفضاء الذي يستخدم من قبل القوات والجماعات المسلحة والمدنيين المشاركين في العمل العدائي.

وبالرغم من الصعوبة العملية المشار إليها إلا أن دليل تالين بشأن القانون المطبق على

---

[1] – احمد عبيس نعمة الفتلاوي، مصدر سابق، ص9 .

الحروب السيبرانية، تضمن وجوب الالتزام بمبدأ التناسب، من حيث حظر الهجمات السيبرانية التي من شأنها أن تسبب الخسارة في ارواح المدنيين أو أصابتهم أو الأضرار بالأعيان المدنية أو مزيجاً منهما، والتي تكون مفرطة مقارنة بالميزة العسكرية الملموسة والمباشرة التي يتوقع من الهجوم الحصول عليها.

وبخصوص تطبيق مبدأ الإنسانية والتي قد يكون عدم التسبب بالآلام لا مبرر لها جزء منها، فيمكن القول أن تطبيق هذا المبدأ على الهجمات السيبرانية قد لا يختلف عن جميع صور واساليب الحرب الاخرى من حيث ضرورة عدم التسبب بأضرار أو الآلام لا مبرر لها.

المطلب الثالث: الجهود الدولية المباشرة للتنظيم القانوني للهجمات السيبرانة.

إن الاهتمام المتزايد لمعالجة الهجمات السيبرانية من خلال أطراف قانونية مشتركة، جعل اغلب المنظمات الدولية تسعى إلى وضع تنظيم قانوني يحكم الهجمات، السيبرانية وسوف نبين ذلك فيما يلي:

الفرع الأول: الأمم المتحدة.

لقد سعت الأمم المتحدة إلى تلأمين سلامة استخدام التكنولوجيا، والشبكات المعلوماتية بشكل عام، وتشارك كل من الجمعية العامة ومجلس الامن ومكتب مكافحة الإرهاب التابع للأمم المتحدة في مختلف المفاوضات لإجاد توافق في الآراء من أجل وضع معايير توفير الحماية لشبكات الانترنت [1].

---

[1] – لبكي، جورج، المعاهدات الدولية للأنترنت، حقائق وتحديات، مجلة الدفاع الوطني، بيروت، العدد83 ، 2013، متاح على الرابط https://cutt.ly/nh5HelI، 2024/06/04، 23:32.

الفرع الثاني: حلف شمال الأطلسي (الناتو).

أدت تداعيات الهجمات السيبرانية التي استهدفت البنية التحتية الرقمية لإستونيا عام 2007، وأيضاً الهجمات السيبرانية ضد جورجيا خلال نزاعها المسلح م روسيا عام 2008 ، إلى سعي حلب شمال الأطلسي(**الناتو**) للتصدي للهجمات السيبرانية ، فقد عمد إلى إنشاء مركز الدفاع الإلكتروني التعاوني للتميز .

وفي الفترة ما بين سنتي 2009 و 2012 ، وبطلب من مركز الدفاع الإلكتروني التعاوني للتميز، قامت مجموعة من الخبراء والباحثين القانونيين بتقييم إمكانية تطبيق المبادئ القانونية على الهجمات السيبرانية ، وتم تتويج هذه الجهود بنشر دليل يعرف باسم" **دليل تالين** "وهو وثيقة قانونية غير ملزمة، تنظم قواعد الاشتباك عبر الانترنت.

الفرع الثالث :مجلس أوروبا.

يعد مجلس أوربا أول من اتخذ خطوات جدية ومباشرة لتنظيم جزء من الأمن السيبراني لأي منظمة دولية أو إقليمية أخرى، فقد قام بإنشاء اتفاقية بودابست المتعلقة بالجريمة السيبرانية وتعد هذه الاتفاقية أولى المعاهدات الدولية التي سعت إلى معالجة الجرائم السيبرانية من خلال تنسيق القوانين الوطنية، وزيادة التعاون بين الدول في محاربة هذي الجرائم وتمت في العاصمة المجرية بودابست في 2001/11/23،

ويعهد التوقيع على تلك المعاهدة الدولية الخطوة الأولى في مجال تكوين التضامن الدولي ضد تلك الجرائم التي تتم عبر شبكة الانترنت والاستخدام السيء لها [1].

---

[1] – الزهراني، شيخة حسين، التعاون الدولي في مواجهة الهجوم السيبراني"، مجلة جامعة الشارقة للعلوم القانونية، المجلد 17، العدد 1 ، كلية القانون، الامرات العربية المتحدة، 2020 ، ص ص 772 – 740 .

الفرع الرابع: مبادرات منظمة شنغهاي للتعاون.

اتخذت منظمة شنغهاي للتعاون، خطوات أولية مهمة نحو التعاون في مجال الأمن السيبراني ففي:

-عام 2006 وقع رؤساء الدول الأعضاء إعلاناً حول أمن المعلومات الدولية.

-عام 2009 تم صدور" إعلان يكاترينبورغ "وذلك في قمة منظمة شنغهاي للتعاون التي عقدت في روسيا وقد أظهرت المنظمة من خلاله التعاون والالتزام تهدف منع الحروب والهجمات السيبرانية، والحاجة الملحة للرد على التهديدات السيبرانية واعتبر أمن المعلومات على نفس أهمية السيادة الوطنية، والأمن الوطني، والإستقرار الاجتماعي والاقتصادي.

خلاصة الفصل الثاني:

السياسة العامة للأمن السيبراني في الجزائر تهدف إلى ضمان الحماية والأمان للبنية التحتية السيبرانية في البلاد والتصدي للتهديدات الإلكترونية والهجمات السيبرانية، وتعتبر الحكومة الجزائرية الأمن السيبراني أمرًا ذا أولوية عالية وتعمل على تنفيذ إجراءات وسياسات لحماية البيانات الحكومية والمعلومات الحساسة والأنظمة الحيوية.

تعمل الحكومة على وضع تشريعات وقوانين قوية تنظم مجال الأمن السيبراني وتعاقب على الجرائم الإلكترونية والاختراقات السيبرانية، وأيضًا على تطوير القدرات القانونية لمكافحة الجرائم السيبرانية، وتعزيز التعاون الدولي في مجال الأمن السيبراني من خلال التعاون مع الدول الأخرى والمؤسسات الدولية ذات الصلة، التي تتمثّل في تبادل المعلومات والخبرات والتدريب وتنظيم الفعاليات المشتركة لمكافحة التهديدات السيبرانية.

كما تعمل السياسة العامة للأمن السيبراني في الجزائر إلى زيادة الوعي والتثقيف حول أهمية الأمن السيبراني وكيفية التصدي للتهديدات السيبراني، تتضمن هذه الجهود توعية المستخدمين بأفضل الممارسات الأمنية وتقديم المشورة والتوجيه للجمهور والقطاع العام والخاص.

الفصل الثالث: الاستراتيجية الأمنية الجزائرية في مواجهة الحروب السيبرانية

تمهيد:

تعتمد الدول في مكافحتها لأفة الجريمة السيبرانية الماسة بالأمن، الاستقرار، القيم الاجتماعية والثقافية إلى تفعيل الاليات القانونية وتكليف كل السلطات (المؤسسة العسكرية، القضائية، المنية) بالتنفيذ الصارم للإجراءات للحد من خطورة الجريمة، كما تلتزم الدول في هذا الإطار إلى مراعاة الشرعية الدولية للاستفادة في إطار التعاون من الخبرات في المجال، لأن مثل هذه الجرائم لا تعترف بالحدود ولا الهوية ولا يستطيع مواجهتها إلا من له القدرة في التحكم في تكنولوجيا المعلومات.

من هذا المنطلق، وفي إطار رسم السياسة المنية العامة طرح صناع القرار في الجزائر مخططا وطنيا لتفادي الوقوع في مأزق أمني جديد (إختراق أنظمة المعلومات الحساسة لرئاسة الجمهورية، وزارة الدفاع الوطني، وأجهزة الأمن) ، أخذين بعين الاعتبار من جهة، الأزمة الأمنية التي تحاصر البلاد في شقها المتوسطي، والمغاربي والساحل الافريقي، ومن جهة ثانية الحفاظ على الحقوق الشخصية والحريات الفردية وفق ما تضمنته المواثيق الدولية والقوانين الوطنية.

وسوف نقوم في هذا الفصل بدراسة، الاستراتيجية الأمنية الجزائرية على المستوى الوطني في المبحث الأول، وعلى المستوى الإقليمي في المبحث الثاني، اما المبحث الثالث نتناول فيه الرؤية الإستشرافية للأمن السيبراني الجزائري.

المبحث الأول: على المستوى الوطني.

أدرجت الجزائر الأمن السيبراني كإحدى الأولويات في برنامج المواجهة ضد الجريمة الالكترونية والارهاب الالكتروني، بل أصبح يشكل جزءاً لا يتجزأ من إستراتيجيات الدفاع، لأن الدروس المستخلصة من الدول التي لها تجربة في هذا المجال، أثبتت أن النجاعة في التطبيق وفعالية المعايير والوسائل المستعملة لا يمكن لها أن تتجسد ما لم يكن هناك تخطيط محكم وتنسيق بين الفاعلين في الميدان، وعليه توجهت الجزائر إلى رسم استراتيجيتها مركزة على النقاط التالية:

-تحديد المخاطر، - اتخاذ التدابير اللازمة، - تحديد الهيئات المكلفة بإدارة الأمن، - تحديد الهيئات المكلفة بالتنسيق، - تحديد الهيئة المكلفة بالجانب التقني للبحث عن الثغرات وتوجيه التحقيق، ليبقى الهدف في الأخير، زيادة قدرات الأمن السيبراني لحماية الأنظمة المعلوماتية وتعزيز سبل المواجهة الوقائية والمواجهة الردعية [1].

المطلب الأول: من الناحية القانونية والعملية.

سنتطرق في هذا المطلب الى دراسة الإستراتيجية الأمنية الجزائرية من الناحية القانونية في الفرع الأول ومن الناحية العملية في الفرع الثاني.

الفرع الأول: من الناحية القانونية.

لقد أخص المشرع الجزائري تنظيم الجرائم الإلكترونية بقوانين عامة وخاصة حيث تمثلت القوانين العامة في:

---

[1] - جمال بوازدية، الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية، التحديات والافاق المستقبلية، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 01، ص ص 1277-1278.

أولا/ الدستور الجزائري: كفل دستور 1996 وكذا التعديل الطارئ عليه 2016 حماية الحقوق الأساسية والحريات الفردية وذلك عن طريق أهم المبادئ الدستورية في مواده:

المادة 38: الحريات الأساسية وحقوق الإنسان والمواطن مضمونة.

المادة 44: حرية الإبتكار الفكري والفني والعلمي مضمونة [1].

ثانيا/ قانون العقوبات: لقد إستدرك المشرع الجزائري في السنوات الأخيرة الفراغ القانوني في مجال الجريمة الإلكترونية نسبيا، بإستحداث القسم السابع مكرر ضمن الفصل الثالث من الباب الثاني من الكتاب الثالث عنوانه المساس بأنظمة المعالجة الآلية للمعطيات[2]، وفي عام 2006أدخل المشرع تعديل بموجب قانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 ، ليصدر في 2009 القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من جرائم تكنولوجيا الإعلام والإتصال ومكافحتها.

ثالثا/ قانون الإجراءات الجزائية: تتابع الجريمة الإلكترونية بنفس إجراءات تتبع الجريمة التقليدية (التفتيش، المعاينة، الإستجواب، الضبط، التسرب، الشهادة، الخبرة ...)، مع زيادة تمديد الإختصاص المحلي لوكيل الجمهورية في الجرائم الإلكترونية في المادة37 من قانون الإجراءات الجزائية.

وتكمن القوانين التي أقرها المشرع الجزائري للجريمة الإلكترونية:

1- **قانون البريد والإتصالات السلكية واللاسلكية:** حيث نصت عدة مواد منه فيما يخص المجال السيبراني، المادة 87 ، والتي نصت على سهولة إجراء التحويلات المالية إلكترونيا،

---

[1] – يوسف بوغرارة ، الأمن السيبراني، الإستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبيري، دراسة منشورة مجلة الدراسات الأفريقية وحوض النيل، المركز الديموقراطي العربي، العدد الثالث، 2018، ص 109.

[2] – أمحمدي بوزينة آمنة، وسائل وأساليب التحري في مجال مكافحة الجرائم الإلكترونية، دراسة تحليلية لأحكام قانون العقوبات، كلية الحقوق والعلوم السياسية، جامعة حسيبة بن بوعلي، الشلف، ص 02.

والمادة 2/84 على إستعمال حوالات الدفع العادية والإلكترونية أما المادة 127 بخصوص جزاء كل من يفتح أو يخرب بريد

2- **قانون التأمينات:** وقد نص هذا القانون على تنظيم الجريمة الإلكترونية من خلال مؤسسات وهيئات الضمان الإجتماعي، وذلك من عدة نصوص تخص البطاقة الذهبية.

3- **القانون الخاص:** بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها جاء منظما للجرائم المتصلة بالمعلوماتية [1].

الفرع الثاني: من الناحية العملية.

لضمان التنفيذ الفعلي والجدي لمختلف التدابير الهادفة لتحقيق الأمن السيبراني، أوكلت السلطات العليا للدولة هذه المهمة إلى هيئات متخصصة ضمن أسلاك الأمن، وأوصت باحترام الحريات في إطار الشرعية الدستورية والمواثيق الدولية، من بين الهيئات، نذكر ما يلي:

أولا/ مركز الوقاية من جرائم الإعلام الآلي وجرائم المعلوماتية للدرك الوطني: يعتبر هذ المركز الذي أنشئ سنة" 2008 **ببئر مراد رايس** "جهازا يهدف إلى تأثير تأمين منظومة المعلومات لخدمة الأمن العمومي، ويعكف على تحليل معطيات وبيانات الجرائم المعلوماتية، المرتكبة وكذا تحديد هويه أصحابها سواء كانو أشخاص فرادى أو عصابات أو غيرها [2].

ثانيا/ المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني:

يعتبر المعهد أحد المشاريع المنجزة في إطار تطوير سلك الدرك الوطني" **ببوشاوي**"، حيث تم إنشاءه بموجب مرسوم رئاسي 04-133 المؤرخ في 26 جوان 2004 ، ودخل حيز

---

[1] – يوسف بوغرارة، مرجع سابق، ص109.

[2] – سمير بارة، لدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائر، الدور والتحديات، جامعة قاصدي مرباح، ورقلة، ص445.

الخدمة إبتداءًا من الفاتح جانفي 2009، أما الفترة الممتدة بين 2004 و 2009 كرست لتكوين المورد البشري وإقتناء المعدات العلمية والتقنية الضرورية، ويقوم المعهد بالعديد من المهام التي من شأنها تلبية الطلبات الواردة من السلطة القضائية، ضباط الشرطة القضائية والسلطات المؤهلة ، قانونيا خاصة أثناء معالجة القضايا المعقدة [1].

ثالثا/ المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني:

إستجابةً لمطلب الأمن المعلوماتي ومحاربة التهديدات الأمنية الناجمة عن الجرائم الإلكترونية قامت مصالح الأمن بإنشاء المصلحة المركزية للجريمة الإلكترونية التي عملت على تكييف التشكيل الأمني لمديرية الشرطة القضائية، والتي كانت عبارة عن فصيلة شكلت النواة الأولى لتشكيل أمني خاص لمحاربة الجريمة الإلكترونية وعلى مستوى المديرية العامة للأمن الوطني والتي أُنشئت سنة 2011 ليتم بعدها إنشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال بقرار من المدير العام للأمن الوطني وأضيف للهيكل التنظيمي لمديرية الشرطة القضائية في جانفي 2015[2].

المطلب الثاني: من الناحية الإدارية والتقنية.

لتفادي الوقوع في تداخل الصلاحيات بين مختلف الاجهزة الفاعلة في مسائل الأمن والدفاع الوطني، حرص المشرع الجزائري على وضع ضوابط لاحترام الإطار الإداري المنظم لصلاحيات

الهيئات المدنية والعسكرية والتقنية في إدارة الاستراتيجية الجزائرية للأمن السيبراني، ويمكن تقسيم

---

[1] – نسيمة سحواذ، الطموح لتوسيع دائرة الاعتماد المتبادل بإدراج طرق تحليلية لفائدة مخابر أخرى،www.Dikanews.com ، تاريخ التصفح، 18 ماي 2024، 15:06.

[2] – إلياس شاهد، الحاج عرابة، عبد النعيم دفرو، تقييم تجربة تطبيق الحكومة الإلكترونية في الجزائر، المجلة الجزائرية للدراسات المحاسبية والمالية، العدد الثالث،2016 ، ص 130.

المطلب إلى فرعين أساسيين هما: الفرع الأول: من الناحية الإدارية والفرع الثاني: من الناحية التقنية.

الفرع الأول/ من الناحية الإدارية:

أولا/ الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات العلام والاتصال ومكافحتها: التي أنشئت سنة 2009، ووضعت تحت السلطة المباشرة لوزير العدل حافظ الاختام، ولم تدخل حيز التنفيذ إلا بعد صدور المرسوم الرئاسي رقم 261-15 المؤرّخ في 2015.10.08 ، من أبرز المهام المنوطة بها:

– استغلال المعطيات المتوفرة بطريقة تسمح بمتابعة كل ما يجري في الفضاء السيبراني من نشاطات غير شرعية وبالتالي توجيه القدرات البشرية والمالية للحد من الثغرات.

– تعزيز التنسيق بين مختلف الفاعلين في الميدان والتشديد على ضرورة التعاون بين القطاعين العام والخاص والمجتمع المدني، من أجل نشر ثقافة المواجهة لكل الممارسات التي تخالف القانون في الفضاء السيبراني وحماية الحقوق والحريات السياسية [1].

– العمل من أجل خلق إطار مركزي للمعلوماتية على شاكلة وحدة بحث، يتم من خلالها جمع المعطيات والاحصائيات في هذا المجال من أجل التحليل المستمر للتهديدات واقتراح الحلول المناسبة.

– التنسيق والتعاون بين مختلف الأجهزة الأمنية والمالية والإدارية التي لها علاقة مباشرة بأنشطة تكنولوجيا الاعلام، من اجل تحديد المسؤوليات لفرض مراقبة صارمة بعد حصر المجالات المستهدفة من طرف محترفي الجريمة الالكترونية [2].

---

[1] – الندوة الافريقية، حوكمة النترنت CAGI، www.lemaghrebdz.com ، 11 ماي 2024، 16:07.

[2] – أستاذ شريف بسام، واقع الحوكمة الالكترونية في الدول العربية، مجلة العلوم الاجتماعية والإنسانية، جامعة الجزائر3، العدد 06، 2016، ص157 .

– اقتراح الرضية اللازمة لتجسيد الاستراتيجية الوطنية للوقاية ومحاربة الجرائم الالكترونية، حسبما جاء في المادة الرابعة من المرسوم أعلاه، وتعتبر هذه الخطوة من الصلاحيات الدالة على أهمية إدارة الأمن السيبراني بالنسبة للدولة.

ثانيا/ قطاع الدفاع الوطني: أستحدث بتاريخ 2015.06.11، على مستوى دائرة الاستعمال والتحضير لركان الجيش الوطني الشعبي " مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة"، وأوكلت لها مهمة، حماية المنظومات والمنشآت الحيوية للبلاد ضد كل أنواع الجريمة السيبرانية، ومن بين المحاور التي تناولتها الأرضية العملياتية لهذه المصلحة، نذكر ما يلي[1]:

– توجيه وتنفيذ وتأطير الأعمال في هذا المجال لا يجب أن يتعدى الإطار الوظيفي أو التنظيمي.

– تطوير وتعزيز المنظومة القانونية لتفادي التجاوزات أثناء إستخدام التكنولوجيا وضمان حماية منظومات الإعلام.

– إعتماد التكوين التقني والعلمي لنتاج الكفاءات والمهارات القادرة على خلق نظام الدفاع السيبراني في كافة أنشطة المؤسسة العسكرية وبالتالي تفادي الأخطار الإجرامية.

– غرس ثقافة الإستعمال الكيفي لهذا العنصر الحيوي " تكنولوجيات الإعلام والإتصال "من خلال حملات تحسيسية لكافة مستخدمي المؤسسة، بغض النظر عن الرتبة أو الوظيفة.

– الإعتماد وبطريقة مستمرة على البحث العلمي لتطوير وسائل الدفاع إستجابة للتطورات الحاصلة في مجال التكنولوجيا.

---

[1]– ب . بوعلام، الجيش الوطني الشعبي ورهانات تداول المعلومة عبر شبكات التواصل الاجتماعي، مجلة الجيش، العدد 603، جانفي 2016.

– فتح مجال التعاون الدولي مع المؤسسات العسكرية الأجنبية، خاصة تلك التي لها رصيد في المجال، لتبادل الخبرات والإستفادة من تجاربهم في هذا المجال.

الفرع الثاني/ من الناحية التقنية:

الجزائر حسب المؤشر، لم تصل إلى مرحلة آمنة في مؤشرات الأمن السيبراني للدولة، بإستثناء الجانب التشريعي والمؤسساتي اللذين وصلت إلى مرحلة مقبولة فيهما وهذا راجع للإجراءات التي إتخذتها الدولة، غير أنها ليست في مجال بناء القدرات، خاصة في تنظيم الدورات التدريبية المحترفة وصناعة المواطنة والبرامج التعليمية، فهي بحاجة إلى بذل المجهودات.

وفيما يتعلق بالإجراءات التنظيمية لا تزال غير كافية لوضع إستراتيجية واضحة المعالم وخطة شاملة للتنفيذ، تراعي الأحتياجات التي تتطلبها حماية البنى التحتية للمعلومات على الصعيد الوطني، وبخصوص الشراكة بين مؤسسات القطاع العام فيما بينها وبين القطاع العام والقطاع الخاص، فإنها تحتاج للمزيد من الجهود لتطويرها [1].

بناءا على ما سبق يمكن القول أن الأمن السيبراني لم يدخل بعد في صلب العديد من الاستراتيجيات التكنولوجية الوطنية والصناعية، حتى وإن تعددت جهود الدولة إلا أنها عامة تتسم بالانتقائية والتشتت، فسياسة عامة قوية في مجال الامن السيبراني تتطلب تكامل جهود العديد من القطاعات العدل، والمؤسسات التعليمية والوزارات وشركات القطاع الخاص ومطوري التكنولوجيا، وكذا الشراكات بين القطاع العام والخاص ضمن الدولة نفسها [2].

---

[1] – بوكبشة محمد، الأمن والدفاع السيبراني أولوية قصوى، مجلة الجيش، وزارة الدفاع الوطني، الجزائر، العدد 651، 2017، ص ص 32–37.

[2] – بورابحة سليمة، السياسات العامة الجزائرية في مجال السيبرانية: الواقع والتحديات، مجلة دفاتر السياسة والقانون، المجلد 15، العدد 01، 2023، ص ص 286– 287.

كما يتطلب إشراك المجتمع المدني وحملات التوعية للمواطنين، فقد أظهرت إحصائيات عالمية أن أغلب الهجمات السيبرانية الناجحة تدخل ضمن تسمية " الهندسة الاجتماعية" التي تشتغل نقائص مردها السلوكات البشرية.

المطلب الثالث: من الناحية العلمية.

حتى تتمكن الهيئات من السيطرة على مختلف الجوانب المتعلقة بعملية تحقيق الأمن السيبراني وفق ما تم ترسيمه في الاستراتيجية الوطنية، توجهت المؤسسات السيادية (رئاسة الجمهورية، وزارة الدفاع، المؤسسات الأمنية، الوزرات) إلى تنظيم دورات تكوينية وسخرت لها كافة الوسائل المادية والبشرية، كما استنجدت الجزائر بخبراء دوليين لتمكين الإطارات الناشطة في المجال من جميع الاسلاك لمعرفة أفضل الممارسات في تكنولوجيا الأمن والسياسات العامة للأعمال الالكترونية المعمول بها في الخارج، كما تم إرسال بعثات للحضور والمشاركة في المؤتمرات الدولية للاستفادة من الخبرات التي تهدف إلى إصدار التوصيات المناسبة لأمن وسلامة المعلومات في الفضاء السيبراني[1].

كما ساهمت الجامعات ومؤسسات البحث العلمي من خلال تنظيم أيام دراسية وملتقيات الأكاديمية.

---

[1] – الملتقى الدولي، الدفاع السيبراني مكون اساسي للأمن والدفاع الوطني، المنظم من طرف قيادة الاركان للجيش الوطني الشعبي، بتاريخ 15-2017/05/16.

وكذلك الندوة الدولية، الخدمات الالكترونية والأمن العمومي، المنظمة من طرف قيادة الدرك الوطني، 2017/03/28، في طبعتها الثانية.

المبحث الثاني: على المستوى الإقليمي.

سارعت الجزائر لإيجاد حلول التهديدات الأمنية السيبرانية لكنها لم تستطع وحدها وانتقلت الى التعاون الإقليمي والدولي مع بقية الدول الصديقة والتي لا تستخدم التكنولوجيا للتهديد.

سايرت الجزائر مختلف الجهود الدولية والإقليمية والمبادرات ذات الطابع الدولي والاقليمي لمواجهة التحديات السيبرانية سواء من حيث التصدي لها قبل وقوعها أو التنسيق الدولي مع الأخذ بعين الاعتبار الإمكانيات والأطر التشريعية المحلية.

وهذا ما سنقوم بتطرق اليه من خلال المبحث الثاني، نقوم بدراسة الاستراتيجية الأمنية على المستوى **العربي في المطلب الأول**، على المستوى الأوروبي في المطلب الثاني، وفي المطلب الثالث نخصصه للاستراتيجية الأمنية على المستوى الدولي.

المطلب الأول: المستوى العربي.

من خلال الدراسات الاكاديمية وتحليل المعطيات المستقاة من المؤسسات المتخصصة في الأمن السيبراني المتضمنة النقائص والثغرات في حماية النظم المعلوماتية للدول العربية، المعلن عليها خلال اللقاءات، يتضح أن المقاومات البشرية والمادية المتوفرة والقادرة على تفادي المخاطر لم تجدي نفعا، والدليل أن السلبيات التي أصبحت تشكل نسبة كبيرة من المخاطر لا تزال تطرح نفسها بشدة، ومن بينها نذكر ما يلي [*]:

- المنظومة التشريعية والتنظيمية العربية تشهد حركة بطيئة، مما يجعلها غير جامعة للعديد من الجوانب الحساسة في الفضاء السيبراني، بحيث يلاحظ أن معالجة العديد من حالات التهديد تتم من خلال تفعيل الجانب العقابي سواء بإدراج مواد جديدة أو تعديل القوانين السابقة وهذا ما يتعارض والتوجيهات العالمية.

---

[*]– في قراءة للاتفاقية العربية لمكافحة جرائم تقنية المعلومات المبرمة في 2010.120.21 ، يتضح ان التهديدات الخطيرة التي تسببها الجرائم الالكترونية للمساس بالمن والاستقرار، اصبحت تشكل إحدى أهم الاهتمامات لدى صناع القرار للدول العربية.

- عدم توازن المعادلة في الموارد البشرية بين ما هو موجود (افتقار وعجز الكفاءات المؤهلة لتغطية النقائص) وما يجب أن يكون (مواكبة التحديات المترتبة عن التطور السريع للتكنولوجيا) .
- الآليات الموظفة لتنفيذ الإجراءات المنية في عالم التكنولوجيا ميدانيا غير ملائمة وغير مطابقة للمواصفات العالمية، والاحصائيات المتوفرة لدى الاتحاد الدولي للاتصالات تبقى شاهدا بدون منازع على ما تقدم من طرح.

الفرع الأول: تبادل المعلومات.

مع إنتشار وتصاعد النشاط الاجرامي الالكتروني ونظرا لتعقيدات التحكم في هذا المجال، سارعت الجزائر إلى تفعيل الاحكام المتعلقة بتبادل المعلومات والمساعدة التقنية التي تعتبر من المبادئ العامة التي اعتمدتها العديد من الصكوك الدولية، وأوصى بها مؤتمر الأمم المتحدة السادس لمنع الجريمة ومعاملة المجرمين، وتعتبر هذه الوسيلة(المعلومة)من الجانب الوقائي عنصرا جوهريا وقاعدة أساسية لمتابعة الجريمة الالكترونية، أما من الجانب العقابي فإن المصالح الخاصة بمكافحة الجريمة والأجهزة القضائية يستندون عليها كإحدى الدعائم الموثوقة لتنفيذ القوانين في كافة المجالات*

الفرع الثاني: تبادل الخبرات والمساعدة التقنية.

في نفس الإطار وبغية تحقيق التكامل بين المؤسسات المنية والقضائية العربية، وسعت الدولة من دائرة التقارب لتشمل تبادل الزيارات الميدانية، الدورات التكوينية واللقاءات التشاورية في المجالات التي شملتها السياسة الجنائية لمكافحة الاجرام عامة والاستفادة من خبرات بعض

* – من بين الاتفاقيات المتعددة الأطراف (اتفاقية الرياض العربية للتعاون القضائي) التي وافق عليها مجلس وزراء العدل العرب في المؤتمر العربي الاول بتاريخ أفريل 1983 ، التي قضت في المادة الاولى على ضرورة تبادل المعلومات بين الدول الاطراف فيما يتعلق بالنصوص التشريعية والتنسيق بين المنظمة القضائية كما قضت المادة الخامسة منها بأن ترسل وزارة العدل في الدول الاطراف أخر بيانات الاحكام القضائية النهائية الصادرة ضد المواطنين أو الاشخاص المولودين أو المقيمين في إقليميا.

الدول العربية والتعرف على البيئة التشريعية التي ينشطون فيها وكذا الاليات التقنية المستعملة في مواجهة الفضاء السيبراني والقدرات البشرية المسخرة لهذه المهمة[1].

كما تشمل هذه الخطوة، العمل الميداني المتضمن المساعدة التقنية الثنائية والمتعددة الطراف التي تخص النيابة القضائية وتسليم المجرمين(حالات تستدعي تشريعا خاصا للإحاطة بكافة الضمانات القانونية من الجوانب الموضوعية والإجرائية) ، ورغم الصعوبات التي تواجهها العديد من الدول في تحقيق التسليم، ونظرا لارتباط إجراءاته بالسيادة الوطنية من جهة، وعدم التزام بعض الدول المطالبة بالتسليم بالتنفيذ حجة حقوق النسان من جهة ثانية، إلا أن الدول استطاعت أن تتخطي هذه العقبات، وأبرمت اتفاقيات تعاون قضائية خاصة في إطار ثنائي ومتعدد الطراف[2].

الفرع الثالث: مبادرة مركز البحوث والدراسات القانونية والقضائية.

مع التطور المذهل لثورة المعلومات وتزايد نسبة الجرائم السيبرانية، سارعت الجزائر كذلك إلى توقيع العديد من الاتفاقيات الثنائية والمتعددة الاطراف مع الدول العربية في إطار الاتفاقية العربية لمكافحة الارهاب لسنة 1998، والاتفاقية العالمية لمكافحة الجريمة المنظمة العابرة للحدود لسنة 2000، وتعزيز التعاون بين الدوائر المختصة لوضع مقاييس ومعايير مطابقة لبرامج الأمن والسلامة المعلوماتية العالمي لضمان الأمن السيبراني الوطني من جهة وتحضير الأرضية لسن تشريع خاص بالجرائم السيبرانية[3].

كما دعمت كل المبادرات المطروحة لمواجهة الظواهر الاجرامية عامة والجريمة الالكترونية خاصة، ومن بين الإسهامات المحسوبة للجزائر المشاركة بفريق من خبراء القانون

---

[1] – جمال بوازدية، مرجع سابق، ص 1285.

[2] – أبو المعالي محمد عيسى، الحاجة إلى تحديث أليات التعاون الدولي في مجال مكافحة الجريمة المعلوماتية"، مداخلة في المؤتمر المغاربي الاول حول (المعلوماتية والقانون) ، طرابلس، ليبيا، 2009/10/28.

[3] – جمال بوازدية، المرجع السابق، ص 1286.

في العديد من الدورات، لشغال مركز البحوث التابع للجامعة العربية لمناقشة مشاريع القوانين والاتفاقيات المطروحة للتكيف مع التطورات المتسارعة، لا سيما في المجال التكنولوجي ومن بين المشاريع المنجزة الاتفاقية عربية لضمان أمن وسلامة الفضاء السيبراني [1].

❖ المحاور الكبرىّ التي تناولتها الاتفاقية:

-بناء الثقة في الفضاء السيبراني، يعتبر الهدف الساس ي للاتفاقية.

-تسخير طاقات تقنيات المعلومات والاتصالات لخدمة النمو والتطوير الإنساني.

-حماية أمن المجتمعات العربية في العصر الرقمي، من خلال التعاون بين الحكومات العربية، وإقرارها للأطر التشريعية والتنظيمية الملائمة والمنسجمة، التي تتضمن تبادل المعلومات بين الأجهزة المعنية، وتظافر جهود السلطات القضائية لمكافحة الجريمة السيبرانية [2].

المطلب الثاني: على المستوى الأوروبي.

لتجسيد مبدأ الشراكة الاورو متوسطية الذي وقعت عليه الجزائر مع الدول الاعضاء في الوحدة الاوروبية بتاريخ 2002.04.22 المتضمن التعاون في المجال المني والقضائي لمحاربة مختلف الجرائم، وكذا الاتفاق المبرم مع فرنسا بتاريخ 2003.10.25 المتضمن التعاون في مجال المن ومكافحة الاجرام المنظم، انطلقت الجزائر في خطوة جديدة بعنوان" التعاون لمواجهة الجرائم السيبرانية في الضفة الجنوبية" ، للاستفادة من التجربة الاوروبية، وعقدت في هذا الشأن، عدة لقاءات في الجزائر جمعت فريق من الخبراء من مختلف المؤسسات الفاعلة في هذا المجال وخبراء اجانب، وانتهت المشاورات بمجموعة من التوصيات، من بينها[3]:

---

[1] – أنظر محتوى الاتفاقية العربية لبناء الثقة في الفضاء السيبراني، وكذلك التوصيات الصادرة عن المؤتمر الرابع للمتخصصين في الأمن وسلامة الفضاء السيبراني، المنعقد في مقر المركز العربي للبحوث القانونية، الجامعة العربية، بيروت، لبنان، 2015/08/19.

[2] – منى الشقر جبور، الأمن السيبراني، التحديات ومستلزمات المواجهة"، اللقاء السنوي الاول للمختصين في امن وسلامة الفضاء السيبراني، بيروت ، لبنان، 2012.08.28 ، ص 24 .

[3] – جمال بوازدية، مرجع سابق، ص 1286.

– تعزيز المنظومة القانونية ومطابقتها للتشريعات الدولية) اتفاقية بودابست* للرد على تحديات الاجرام السيبراني سواء على المستوى الوطني، الجهوي أو الدولي مع احترام مبدأ السيادة الوطنية وحقوق الإنسان.

– تعزيز الامكانيات المادية والبشرية للمؤسسات المنية المكلفة بمواجهة الاجرام السيب راني، وكذا التنسيق بين ذات المصالح والهيئات المشرفة.

– استعمال الدليل الالكتروني كمعيار للقيام بالإجراءات القضائية الصحيحة.

– الديمومة في تكوين الإطارات المنية والقضائية وفق المناهج العلمية المعتمدة دوليا لتسهيل عملية التأقلم مع التطورات الحاصلة في الميدان.

– الإسراع في رسم استراتيجية فعالة تتضمن كل الجوانب التنظيمية، العملية والتقنية لتدارك الخطار الناجمة عن هذه الجرائم

المطلب الثالث: على المستوى الدولي.

أما على المستوى الدولي فقد نصت المادة 16 من ق/و على أنه في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة ذا القانون وكشف مرتكبيها، يمكن السلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني من أجل تبادل المعلومات بين الدول في الخارج بشأن الجريمة والتعرف على الفاعلين وتحديد مكان تواجدهم.

تقوم الهيئة الجزائرية بمشاركة الأعمال التحضيرية الضرورية مع الهيئات الدولية المماثلة لها دف البحث والتعرف على الجرائم المعلوماتية ومرتكبيها وتحديد مكان تواجدهم.

---

*– اتفاقية بيدابيست الاوروبية حول الاجرام المعلوماتي المصادق عليها من طرف المجلس الاوروبي بتاريخ 2001.11.23 ، دخلت حيز التنفيذ سنة 2004 ، تعتبر بمثابة الارضية القانونية التي اعطت دفعا للدول الاوروبية خاصة ودول العالم عامة، للإسراع في سن قوانين وفرض إجراءات قانونية وإدارية لمحاصرة الاجرام السيبراني، خاصة وان اهم معضلة تواجه التعاون الدولي تسليم المجرمين والنيابة القضائية)، قد تم الفصل فيها.

تسعى الجزائر لتبادل المعلومات بين الدول وتركز على المنظمة الدولية للشرطة الجنائية لأ نها أهم جهاز دولي في مجال مكافحة الإجرام بما فيها الجرائم المعلوماتية، كما تعمل على تشجيع التعاون الدولي بين أجهزة الشرطة من خلال وضع قائمة تضم ضباط مختصين في مجال البحث والتحري بشان الإجرام المعلوماتي والذين يمكن الاستعانة بهم من طرف الدول كما تسهل الإجراءات القضائية المتعلقة بتسليم المجرمين وتنفيذ الإنابات القضائية الدولية وكذا نشر أوامر القبض الدولية للمبحوث عنهم والمطالبة بتسليمهم [1].

ومع الإنفتاح الذي عرفه العالم بعد الحرب الباردة، أضحت كل المعاملات تخضع إلى مبدأ الحرية في التنقل لأي نقطة في العالم بأقل تكلفة وذلك من خلال ما توفره التكنولوجيا من وسائل اتصال، ومع مرور الزمن أصبحت هذه الوسيلة في متناول الجميع، بالمقابل تزايد النشاط الاجرامي الالكتروني، مما استدعى من المجتمع الدولي التحرك للحد من هذه التهديدات التي باتت تشكل خطرا على الحريات الفردية والسلامة الجماعية.

من هذا المنطلق وأمام تصاعد الاهتمام العالمي بهذا العالم الافتراضي، توجهت الهيئات المتخصصة سواء على المستوى الدولي (الشركات المتعددة الجنسيات)، أو على المستوى الأممي (الاتحاد الدولي للاتصالات) بوضع مقاييس وضوابط لحماية البيانات، سلامة التحويلات الالكترونية في جميع المجالات، (حوكمة النترنت) ، كما تم وضع مناهج وأليات للحماية من الجريمة السيبرانية وتداعياتها المستقبلية [2]، ومن بين الخطوات المسجلة نذكر ما يلي:

---

[1] – إيمان بن سالم، جريمة التجنيد الالكتروني للإرهاب وفقا لقانون العقوبات الجزائري، برلين، المركز الديمقراطي العربي لدراسات الاستراتيجية والسياسية والإقتصادية، 2008، ص 85.

[2] – دليل الأمن السيبراني للبلدان النامية، الاتحاد الدولي للاتصالات ، 2017.

1- أوكلت مهمة متابعة قضايا التنمية من أجل تحسين الخدمة في ضل المرونة التي توفرها تكنولوجيا الاتصالات عامة والأنترنت خاصة إلى المجلس الاقتصادي الاجتماعي التابع لهيئة الامم المتحدة.

2- نفس المهمة أوكلت إلى اللجنة الخاصة المكلفة بالعدالة الجنائية ومنع الجريمة لمتابعة الجهود الدولية في مكافحة ومنع الجرائم الوطنية والعابرة للحدود (الجرائم الالكترونية.)

3- تم التوقيع على مذكرة تفاهم بين المكتب الاممي المكلف بالمخدرات والجريمة والاتحاد الدولي للاتصالات للاستفادة من خبرة هذا الاخير لمساعدة الدول لاتباع الاجراءات الملائمة للحد من المخاطر التي تشكلها الجريمة السيبرانية [1].

4- توجت المجهودات الدولية بصدور سنة 2000 من جامعة ستات فورد الولايات المتحدة الامريكية، على مسودة اتفاق عالمي حول مكافحة الإرهاب الالكتروني والتي بفضلها تم فتح مجال جديد لتجسيد التعاون دولي لمواجهة الجرائم السيبرانية.

5- أصدرت الأمم المتحدة 2002 العديد من القرارات المتضمنة إرساء ثقافة الأمن في الفضاء السيبراني من خلال التحسيس الدول على تكثيف التعاون لحماية البنية التحتية للمعلومات وتفعيل سياسات موجهة الارهاب الإلكتروني.

6- تم إنشاء سنة 2004 مجموعة الخبراء الحكومية GCE وفريق دولي بهدف مناقشة الأخطار القائمة والمحتملة في مجال أمن المعلومات الدولي والإجراءات الممكنة لوضع الأسس الدولية التي تهدف إلى تقوية أمن نظم الاتصالات والمعلومات العالمية [2].

---

[1] – نوران شفيق، مرجع سابق، ص 108 .

[2] – رائد العدوان، المعالجة الدولية لقضايا الارهاب الالكتروني، توظيف شبكات التواصل الاجتماعي في مكافحة الارهاب"، محاضرة القيت في دورة تدريبية بالرياض، السعودية،2016 ،ص ص 09-10.

7- حثت الهيئة الأممية المختصين بالجرام المرتبط بالأنظمة المعلوماتية في المؤسسات العمومية والخاصة للبحث من أجل تحديد الإطار العقابي لهذه الجرائم، وجاءت هذه التوصيات خلال المؤتمر الحادي عشر حول الوقاية من الجريمة والعدالة الجنائية.

8- سياسة التحسيس التي اعتمدها المجتمع الدولي للوقاية من أخطار هذه الجريمة، انتهت إلى إصدار قوانين أو عقد اتفاقيات لمكافحة الإجرام، تبادل المعلومات والمساعدة الفنية بين العديد من الدول.

هذه الخطوات وغيرها كان لها أثر إيجابي ومباشر على الإستراتيجية الجزائرية التي تفاعلت مع كل صور التعاون الدولي بمختلف مظاهره خاصة وأن معدل الإختراقات على الشبكة العالمية للمعلومات، وعلى الأنظمة المعلوماتية الوطنية بلغ درجات من الخطورة المهددة للأمن الوطني، القومي والعالمي.

المبحث الثالث: رؤية إستشرافية للأمن السيبراني.

سنتطرق في دراسة هذا الفصل إلى معرفة أوجه القوة السيبرانية في الجزائر كمطلب أول، ثم في المطلب الثاني أوجه ضعف الأمن السيبراني في الجزائر، يليه المطلب الثالث تحت عنوان معيقات ومستقبل الأمن السيبراني في الجزائر.

المطلب الأول: أوجه القوة السيبرانية في الجزائر.

الفرع الأول: مقارنة بين الجزائر ودول أخرى.

تجتهد الجزائر في سبيل أجهزتها الأمنية، حيث أشرف خبراء تكونية سنة 2010 وكانت حول مكافحة الجريمة المعلوماتية لفائدة ضباط الشرطة القضائية والقضاة، وغيرها من الأجهزة الأمنية الأخرى، حيث تهدف هذه الأخيرة إلى إطلاعهم على آخر التكنولوجيات لمحاربة الجريمة وكيفية استخدام الأدلة الالكترونية في التحقيق والمقاضاة، وقد شارك في الاشراف على الورشة

التدريبة خبراء في الجرائم الحاسوبية والملكية الفكرية، وقسم الجريمة المنظمة وإبتزاز الأموال التابعة لوزارة العدل الأمريكية، وقد نصب التدريب على الجانب النظري والتطبيقي معا.

كما تم التعرف على تقنيات إجراء التحري وإقامة الدليل على الجرائم المعلوماتية وكيفية إستغلال الأنترنت والبريد الالكتروني، وكذا التعاون في هذا المجال [1].

[1] – عبد الحليم بوقرين، حتمية إنشاء ضبطية خاصة بالجرائم الإلكترونية، مجلة العلوم القانونية والسياسية، المجلد 05 ، العدد 02، 2016، ص158.

الولايات المتحدة الأمريكية	فرنسا	الجزائر
في مجال الدرك الوطني		
	-إنشاء قسم أنترنت تابع للمصلحة التقنية للبحوث القانونية سنة 1998 يتكون من 13 دركيا من بين مهندسين وتقنيين ويتولى هذا القسم مهمة معالجة المعلومات -إنشاء قسم معلوماتي تابع لمعهد البحوث الجنائية في الدرك الوطني سنة1992 مهمته تقديم المساعدة التقنية على شكل خبرة	-إنشاء مركز الوقاية من الجرام الاعلام الالي سنة 2008 ببئر مراد رايس -إنشاء المعهد الوطني للأدلة الجنائية وعلم الاجرام الوطني ببوشاي بموجب مرسوم رئاسي رقم 133-04 في جوان 2004 ودخل حيز الخدمة في جانفي 2009
في مجال الشرطة		
-إنشاء مكتب مركزي لمكافحة الجريمة المعلوماتية سنة 1991، ووصل عدد أعضائه إلى20 وكيل نيابي سنة2000	-إنشاء مكتب مركزي لمكافحة الاجرام المعلوماتي سنة 2000 ويتواجد على مستوى المديرية المركزية للشرطة القضائية	-إنشاء ورشة تكوينية سنة 2001حول مكافحة الجريمة المعلوماتية لفائدة الشرطة القضائية وتطويرها بالتعاون مع خبراء من الاستخبارات الأمريكية
في مجال الهيئة	الوطنية للوقاية من الجرائم المتصلة	الاعلام والاتصال بتكنولوجيا
	-إنشاء مكتب مركزي لمكافحة الجريمة المعلوماتية على مستوى مديرية للشرطة القضائية	-إنشاء هيئة متعلق بالوقاية من الجرائم المعلوماتية

جدول يوضح مقارنة بين الجزائر ودول أخرى للأجهزة الأمنية المختصة في الأمن السيبراني

نشر الاتحاد الدول للاتصال (ITU) التقرير السنوي لتصنيف دول العالم في مجال الأمن السيبراني ويقيس المؤشر التزام الدول في جميع أنحاء العالم بتفعيل وتطوير مختلف تقنيات الامن السيبراني ،ووفقا للاتحاد الدولي للاتصالات ،فإن حوالي نصف بلدان العالم لديها استراتيجية النظر في السياسات الوطنية الرامية إلى الحماية من الجرائم المعلوماتية والالكترونية ، وأظهر التقرير أن هناك مجالا للمزيد من التحسينات والتعاون على كافة المستويات وفقا لما جاء في التقرير الذي يدعو إلى تشجيع الحكومات على الاهتمام بالسياسات الوطنية التي تأخذ في تأخذ في الاعتبار الأمن السيبراني، وكذلك زيادة وعي المواطنين حول استعمال الأنترنت[1].

وتم تقسم الدول إلى ثلاث فئات في مجال الامن السيبرانيي، المتخلفة – الناضجة – المتقدمة .

المرتبة	الدول العربية
01	عمان – عالميا 04
02	مصر – عالميا 14
03	قطر – عالميا 25
04	تونس – عالميا 40
05	المملكة العربية السعودية – عالميا 46
06	الامارات العربية المتحدة – عالميا 47
07	المغرب – عالميا 49
08	البحرين – عالميا 65
09	الجزائر – عالميا 68
10	الأردن – عالميا 93

[1]. – أماني جهاد، تصنيف الدول الغربية والعربية في مجال الأمن السيبراني، WWW.3ARABINSIDEE.COM ، 23 ماي 2024، 20:43.

الفرع الثاني: البنية الأساسية لتكنولوجيا المعلومات ولاتصالات.

شهدت البنية الأساسية في المنطقة العربية تطورا سريعا مع ظهور الأجيال الجديدة من الشبكات النقالة وسرعة الاتصال بالأنترنت عبر الشبكات الثابتة والنقالة على سواء، حيث إحتلت الجزائر المرتبة الثانية بعد الأردن تحت مسؤولية سلطة الضبط للبريد والموصلات السلكية واللاسلكية[1].

1 – الأردن (الهيئة التنظيم قطاع الاتصالات)

2 – الجزائر (سلطة الضبط للبريد والمواصلات السلكية واللاسلكية)

3 – تونس (الهيئة الوطنية للاتصالات)

4 – البحرين (هيئة تنظيم الاتصالات)

5 – الإمارات العربية المتحدة (هيئة تنظيم الاتصالات)

6 – سوريا (الهيئة الناظمة لقطاع الاتصالات)

الفرع الثالث: مؤشر الاستعداد التكنولوجي

أصدر مؤتمر الأمم المتحدة للتجارة والتنمية قراراً تحت عنوان "التكنولوجيا والابتكار 2023"، يوضح من خلاله أن موجة التغيير التكنولوجي التي أطلقتها التقنيات المتجددة وغيرها من التقنيات الخضراء، تفتح نوافذ جديدة من الفرص لبناء القدرة على الصمود ضد التهديدات، وتنمية اقتصادات أقوى وأكثر تنوعًا، والانتقال إلى مسارات تنمية أفضل مع اقتصادات أقل عبئًا على البيئة.

وضم التقرير مؤشر الاستعداد التكنولوجي الرائد 2023، حيث صنفت 166 دولة على مستوى استعدادها لبدء استخدام التقنيات الرائدة مع المؤشرات الخمسة التالية: تكنولوجيا المعلومات والاتصالات والمهارات والصناعة والبحث والتطوير والتمويل [2].

---

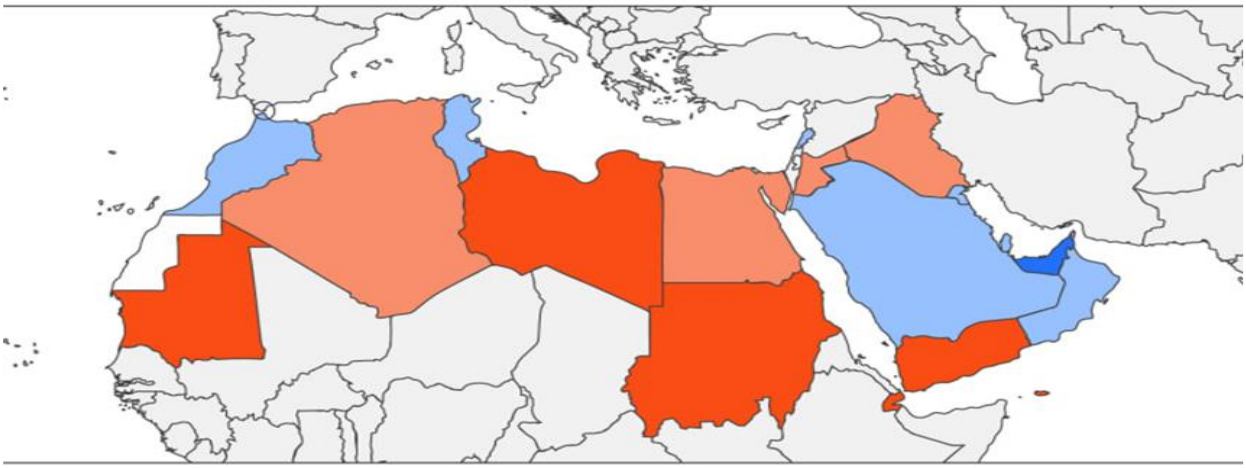
[1] – الاسكوا، تقرير الملامح الإقليمية لمجتمع المعلومات في المنطقة العربية، اللجنة الإقتصادية والإجتماعية لغربي آسيا، بيروت، لبنان،(2016) ، ص 23.

[2] – مقال على الانترنيت، ما ترتيب الدول العربية على مؤشر الاستعداد التكنولوجي لعام 2023، https://arabic.cnn.com/middle-east/article/2023/04/29

مؤشر الاستعداد التكنولوجي الرائد لعام 2023

تقييم الدول العربية وفقًا لمجموع النقاط في المؤشر

مرتفع
متوسط مرتفع
متوسط منخفض
منخفض



ترتيب الدول العربية العالمي ضمن المؤشر

37	الإمارات	
47	السعودية	
51	الكويت	
60	البحرين	
64	سلطنة عُمان	
66	تونس	
67	قطر	
77	لبنان	
80	الأردن	
83	مصر	
97	الجزائر	
107	العراق	
122	ليبيا	
150	جيبوتي	
153	موريتانيا	
156	جزر القمر	
163	السودان	

المصدر: مؤتمر الأمم المتحدة للتجارة والتنمية

المطلب الثاني: أوجه الضعف للأمن السيبراني في الجزائر.

الفرع الأول: سياسات واستراتيجية تكنولوجيا المعلومات والاتصالات.

دفعت القمة العالمية لمجتمع المعلومات عددا من الدول العربية إلى سياسات وإستراتيجيات، لبناء مجتمع المعلومات وتطويره التي شارك في وضعها لجان وفرق عمل منبثقة عن مجلس الوزراء العرب والمعلومات، بالإضافة إلى الاسكوا ومنظمات إقليمية ودولية:

الدول	إعتماد سنة الاستراتيجية	تسمية الاستراتيجية الأولى	الجهة المسؤولة	الجهة المسؤولة	الجهة المسؤولة	أحداث تسمية إستراتيجية	الجهة المسؤولة
الأردن	2000	R E A ريتشCH	القطاع الخاص لتكنولوجيا المعلومات	الاستراتيجية قطاع الاتصال (2007–2011)	وزارة الاتصالات والتكنولوجية المعلومات	الوطنية الاستراتيجية الاتصالات لقطاع وتكنولوجيا المعلومات (2011–2017)	وزارة الاتصالات وتكنولوجيا المعلومات
الامارات العربية المتحدة	–	كل تعتمد سياسة إمارة خاصة ا	في الحكومة كل إمارة	قطاع سياسة)الاتصال 2006– (2010	تنظيم هيئة الاتصالات	العامة السياسة لقطاع 2011) الاتصالات (2015	تنظيم هيئة الاتصالات
البحرين	2001	الخطة الوطنية للاتصالات	الجهاز المركزي للمعلومات	الخطةالوطنية الثانية للاتصالات	الجهاز المركزي للمعلومات	الثانية الوطنية الخطة للاتصالات	تنظيم هيئة الاتصالات
تونس	–	–	–	–	–	قطاع استراتيجية التكنولوجي الاتصال)تونس الرقمية	اتعليم وزارة العالي والبحث التكنولوجي
الجزائر	–	–	–	–	–	مشروع الجزائر الالكتروني	البريد وزارة والاتصال وتكنولوجيا المعلومات

جدول يوضح الإستراتيجيات الوطنية لتكنولوجيا المعلومات

الفرع الثاني: تقييم حجم الخسائر المعلوماتية بالمقارنة بين الجزائر ونظيراتها فرنسا والولايات المتحدة.

أولا /فرنسا: التقرير الذي نشرته الجمعية الفرنسية لأمن المعلومات عام 1991 تضمن الخسائر وصلت 10,4 مليار فرنك فرنسي % 57 منها يرجع إلى أفعال إجرامية، وفي عام 96 انتهى التقرير الصادر عن الجمعية إلى اجمالي الخسائر الناجمة عن المعلوماتية قدر بحوالي 12,72مليار فرنك فرنسي.

ومن جهة أخرى توصلت الإدارة العامة للشرطة القضائية باعتبارها إحدى الجهات التي يصل إلى علمها الجرائم المختلفة بما فيها الجرائم المعلوماتية إلى أن أكثر من يتعرض لهذا النمط من الاجرام المشروعات التي تتعلق بالمعلومات بنسبة % 25 يليها البنوك بنسبة % 21 ثم المشروعات التجارية المختلفة بنسبة % 18 وأخيرا الجهات الحكومية 17%[1].

ثانيا/ أمريكا: توضح إحصائيات مكتب التحقيقات الفدرالي أن متوسط الخسارة في الجريمة المعلوماتية الواردة حوالي 500 ألف دولار بينما في جريمة سرقة عادية فمتوسط الخسارة 2500 دولار، أي متوسط الخسارة في الجريمة المعلوماتية أعلى ب 150 مرة عنه في الجرائم العادية.

كما بينت دراسة أخرى أجريت من قبل منظمة (institute security the computer) أن خسائر 163 شركة أمريكية من الجرائم المتعلقة بتقنية المعلومات قد بلغت أكثر من 125 مليون دولار سنة2000، كما ورد في التقرير السنوي الثامن لمكتب التحقيقات الفدرالي الأمريكي الصادر عام 2003 بعنوان جرائم الحاسب بأن أكثر خسائر المؤسسات الولايات المتحدة الأمريكية

---

[1] – نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير، جامعة الحاج لخضر، باتنة، كلية الحقوق والعلوم سياسية، تخصص علوم جنائية، 2012–2013، ص 68.

أتى من الاستيلاء على المعلومات والتي كبد ا خسائر تتعدى 70 مليون دولار أمريكي ويأتي في المركز الثاني نشاط تعطيل نظم المعلومات محققا خسائر تتجاوز 65,5 مليون دولار [1].

ثالثا/ الجزائر: أما في الجزائر فإن المحيط الكمي لإجرام المعلوماتي غير واضح لعدم وجود دراسات وبحوث من شأنها كشف اللثام عن أرقام ومؤشرات للخسائر في بلادنا جراء هذا النمط الاجرامي .وإن كانت الجزائر ليست بمنادى عن خطورة الجرائم المعلوماتية طالما أنها تحتل جزءا من الفضاء الالكتروني خاصة فيما يتعلق بالحاسوب المالية وبعض الهيئات الحكومية التي يعتبر اختراق مواقعها ضمن حجم الأضرار الناتجة عن الجريمة المعلوماتية [2].

كشفت دراسة حول" الأمن السيبراني "أجريت سنة 2017 ، عبر 1000 مؤسسة وطنية عمومية وخاصة، بأن نصف عدد المؤسسات الجزائرية غير محمي بنظم معلوماتية واقعية من خطر التهديدات السيبراني، حيث أشار السيد" **مهري زكريا**" ، رئيس القمة الإفريقية للأمن السيبراني المنظمة بوهران، إلى أن تحقيق مستقلا تم إجراءه بالتعاون مع شركة" **ألجيريا ديجيتال تاندرس** الرائد العالمي في قطاع إدارة للتوجيهات الرقمية والمدعم من طرف مؤسسة" **رابيد7** المخاطر، مس مديري وتقنيي المعلومات وكذا مديري أمن المعلومات ومديري الشركات الكبرى والمؤسسات الجزائرية ، حول تطور الهجمات الالكترونية واستخدام التدابير الأمنية، كشف بأن % 50 من المؤسسات التي طالها التحقيق، غير مؤمنة في مجال التهديد المعلوماتي الذي يعرف تطورا كبيرا .

وكشف التحقيق ن بأن 54 من المؤسسات تعتقد أن الهجمات الالكترونية تؤثر على تطورها، فيما لا تملك % 16 من المؤسسات نظم أمن سيبراني، مقابل % 12 من المؤسسات لا تعرف النظم الأمنية للمعلومات و % 17 من المؤسسات لا تفكر في إنشاء النظم الخاصة

---

[1] – نعيم سعيداني، المرجع نفسه، ص 69.

[2] – نفس المرجع، نفس ص.

بالحماية، رغم أهميتها.

كما تبين الدراسة أن 52 % من المؤسسات لا تملك سياسة لحماية المنظومات المعلوماتية، ولا موظفين متخصصين ومؤهلين في مجال تقنيات الاعلام والإتصال، مع تأكيد سهولة ولوج نظم التخزين والتوثيق في هذه المؤسسات، حيث تؤكد الدراسة بأن معظم المؤسسات التي شملتها الدراسة يستطيع أي موظف فيها استخدام بطاقات ذكية وقارئ ذاكرة بسهولة ودون استشارة المصلحة المعينة، ما يجعلها عرضة للهجمات عن طريق الفيروسات أو القرصنة، فضلا عن السهولة في ولوج المواقع الالكترونية عبر أجهزة الاعلام الآلي لهذه المؤسسات [1].

كما أن أماطت نتائج مقاييس الأمن السيبراني لعام 2018 اللثام عن واقع تسيير الشركات الجزائرية، باعتبار أن نسبة 45 % من الشركات المستجوبة لا تملك أي استراتيجية لحماية نظامها المعلوماتي، من بينها نسبة 17 % عبرت عن نيتها في إرساء هذه الاستراتيجية مستقبلا، فضلا عن إحصاء نسبة 42 % من الشركات التي اعترفت بعدم إجراء أي خبرة داخلية دورية لحماية نظامها المعلوماتي، ونسبة 33 % من الشركات التي تقر بعدم تصنيف وتحديد الوثائق والبيانات، من بينها 13 % تجهل هذا الاجرام أصلا.

فأهم العراقيل التي تعترض الأمن السيبراني تكمن في نقص الكفاءات المؤهلة بنسبة 52% ونقص الموارد المالية بنسبة 35% .

الفرع الثالث: نتائج تصدي المن السيبراني للتهديدات السيبرانية.

أفاد بيان لـ"تراند ميكرو" الشركة المتخصصة في الأمن السيبراني العالمي، بأن برمجياته اكتشفت وأحبطت أكثر من 19 مليون تهديد طال عناوين بريد إلكتروني لجزائريين، كما منعت أكثر من 400 ألف هجوم ضار استهدف عناوينURL ، و34 ألف مس مضيفي عناوينURL ، إلى جانب تحديد وإيقاف أكثر من نصف مليون هجوم باستعمال برمجيات خبيثة .

---

[1] – رضوان قادة، 50 % من المؤسسات غير مؤمنة الكترونيا، جريدة المساء، العدد6462 ، 2018، ص6 .

وصرح المدير الإقليمي لمنطقة شمال إفريقيا بـ"تراند ميكرو" أشرف سراج"، بأن التطورات التكنولوجية أتاحت عالما من الفرص للمنظمات في الجزائر، لكنها جاءت أيضا بتحديات مختلفة في مجال الأمن السيبراني، كما أدى تعقيد المشهد الرقمي إلى زيادة كبيرة في التهديدات السيبرانية التي يمكن أن تعرض العمليات والبيانات الساسة للشركات إلى الخطر .

وأضاف أنه من الأهمية أن يكون لدى الشركات فهم شامل لنقاط الضعف لديها، واعتماد نهج أمني متعدد الطبقات لتأمين بنيتها التحتية الرقمية، و"تراند ميكرو" ملتزمة بتزويد الشركات الجزائرية بالأدوات والخبرات اللازمة لتتمكن من الإبحار المشهد السيبراني الذي يتطور ويتحول باستمرار[1].

وعلى الصعيد الدولي، سلط التقرير الذي حمل عنوان "إعادة التفكير في الأساليب الدفاعية"، الضوء على الزيادة كبيرة في عمليات اكتشاف التهديدات العالمية، حيث كشفت عن نموها بنسبة 55 بالمائة، فضلا عن ارتفاع في عدد البرمجيات الخبيثة بواقع 242 بالمائة. والتقرير الذي أعدته مؤسسة "تراند ميكرو" اليابانية، سلط الضوء على الاتجاهات التي لها آثار مهمة على مستقبل الأمن السيبراني، وشدد على أن الجهات الفاعلة في التهديد كانت تستهدف بشكل عشوائي المستهلكين والمؤسسات، مما جعل عام 2022 عاما صعبا لمحترفي الأمن السيبراني[2].

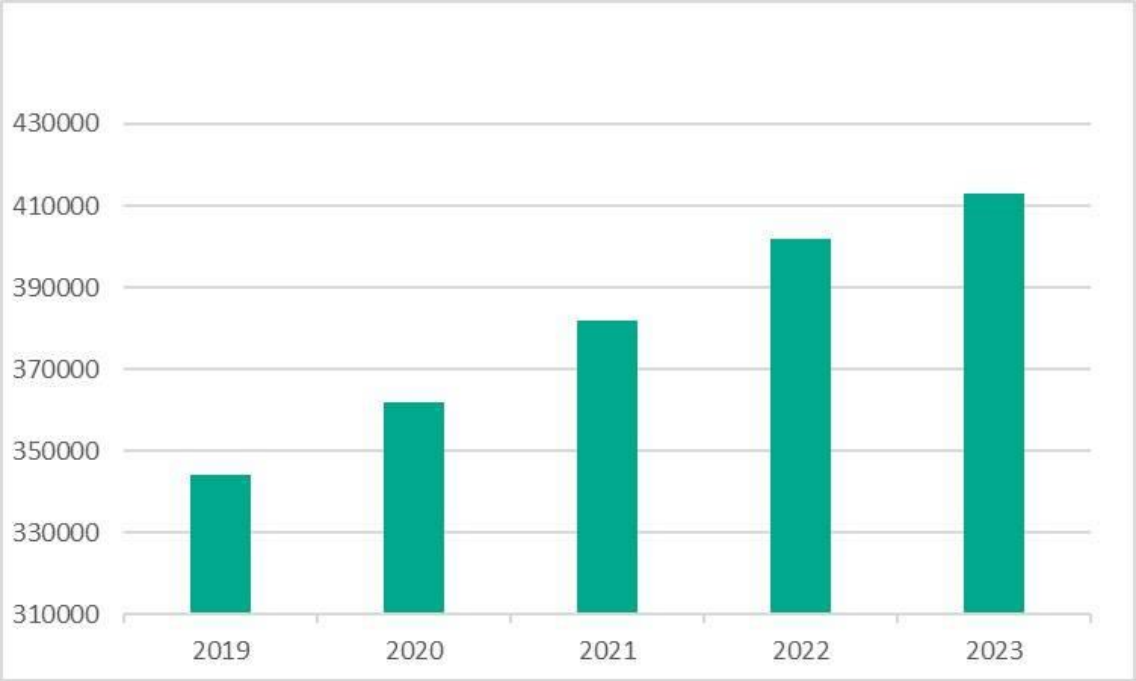
ما عن نوع البرمجيات الخبيثة الأكثر انتشاراً، لا تزال برمجيات «حصان طروادة» تتولى الصدارة. وشهد عام 2023 زيادة في استخدام «الأبواب الخلفية» من 15 ألف ملف مكتشف يومياً في عام 2022 إلى 40 ألف ملف في عام 2023. وتُبرز هذه الأرقام أن الأبواب الخلفية

---

[1] – حسان حويشة، تقرير دولي حول الأمن الرقمي في 2022 ،إحباط قرابة 30 مليون تهديد سيبراني ضد الجزائر، https://www.echoroukonline.com، 27 ماي 2024،15:12.

[2] – نسيم رمضان، كاسبرسكي: 411 ألف ملف خبيث يومياً خلال عام 2023، مقال على الرابط، https://aawsat.com، 27 ماي 2024، 17:05.

هي واحدة من أخطر أنواع برمجيات «حصان طروادة»؛ إذ إنها توفر للمهاجمين إمكانية التحكم عن بُعد في نظام الضحية لتنفيذ مهام، مثل إرسال الملفات، واستلامها، وتشغيلها، وحذفها، بالإضافة إلى جمع البيانات السرية وتسجيل أنشطة حاسوب الضحية [1].



متوسط عدد الملفات الخبيثة التي اكتشفتها حلول «كاسبرسكي» الأمنية يومياً من 2019 إلى 2023

المطلب الثالث: معيقات تحقيق الأمن السيبراني في الجزائر ومستقبله.

سنتطرق في هذا المطلب الى معيقات تحقيق الامن السيبراني في الجزائر كمطلب اول ومستقبل الامن السيبراني في المطلب الثاني

(1) – نسيم رمضان، المرجع السابق.

الفرع الأول: معيقات تحقيق الأمن السيبراني الجزائري في ظل تحديات الراهنة

إن الأطروحات الجديدة للأمن تستوجب علينا التوقف والتمعن في هذا المفهوم بما ينسجم والتغيرات الحاصلة في العالم، لاسيما في ظل التطور الرهيب في مجال الإعلام الآلي وتكنولوجيا الإتصالات والمعلومات، إلى حد التوجه إلى إنشاء ما اصطلح على تسميته بالمدن الذكية، والتي تحولت فيها الخدمات من الشكل التقليدي إلى الإلكتروني، لتخلق بذلك ميداناً جديداً يختلف عن سابقيه، وعلى الرغم من إيجابياته إلا أنه يستلزم توفير الأمن لنجاح هذه الخدمات.

وعلى الرغم من حداثة التوجه الجزائري نحو الحوكمة الإلكترونية، إلا أن عدد الجرائم المرتكبة يوحي بحجم الأخطار التي تتربصها، وهو ما يجعل الجزائر أمام تحديات وعوائق جديدة وهو تحقيق الأمن السيبراني حاليا ومستقبلا.

إذ تواجه مصالح الدرك الوطني ومصالح الأمن الوطني العديد من العوائق والتحديات التي تعيقها في تحقيق الأمن السيبراني في الجزائر، يمكن أن نذكر أهمها فيما يلي:

- التطور التكنولوجي وظهور الأنترنت (Wi-Fi/3G/4G/5G) عبر هذه التقنيات لم يعد المجرم يحتاج للجلوس وراء الحواسيب الموصولة سلكيا بشبكة الأنترنت للقيام بجريمته، مما يستدعي من الجهات الأمنية رفع التحدي والاستعداد بأحدث التقنيات لمواجهة والتصدي لهذه التطورات [1].

- الإستعمال الواسع لشبكات التواصل الإجتماعي، إذ وصل عدد مستعملي هذه المواقع في الجزائر الإلكترونية لأكثر من 13 مليون مستعمل ما ساهم بشكل كبير في ارتفاع أنواع متعددة من الجرائم الإلكترونية مثل القذف، التحرش الجنسي، إستغلال القصر، وغيرها وهذا ما يستوجب وضع إستراتيجيات جد مكملة لضمان الأمن السيبراني عند إستخدام مواقع

---

[1]– سهام بوعموشة، الفضاء السيبراني يتميز بانفتاح شبكة المعلوماتية وانعدام الحواجز الجغرافية ، جريدة الشعب، العدد 17345، 24ماي 2017، ص06 .

التواصل الإجتماعي .[1]

- عمليات التخفي أثناء إستعمال خدمات شبكة الأنترنت(Proxy) ، يعد من أكبر الإشكاليات التي تواجهها الجهات المتخصصة بالتحقيق، ويتطلب تعاون جهات متعددة والتسلح.

الفرع الثاني: مستقبل الامن السيبراني في الجزائر.

لا يمكن مناقشة مستقبل **الأمن السيبراني** دون النظر في الإتجاهات الناشئة في مجال التكنولوجيا والتهديدات المرتبطة بإستخدامها، إذ تقوم المنظمات المختصة بتطوير وإعتماد التكنولوجيات المتصلة بالبيانات الكبيرة والحوسبة الإدراكية، مما يجعل الأبعاد السيبرانية تنمو في الحجم والتعقيد بصورة مطردة، ولقد طور المختصون نماذج وطرق حديثة ومناسبة للإستفادة من هذه المعلومات في حملات الدعاية والتسويق الذكي ، لكن نظرة المختصين في أمن المعلومات كانت حتى فترة قريبة تركز على تكنولوجيا الأجهزة والابتكارات التي تشكل ترابط عالمنا، حيث تصدر كميات هائلة من البيانات بسرعة مع تزايد عدد الأجهزة المرتبطة بالقضاء السيبراني [2].

بينما تمثل البيانات الكبيرة وإستخداماتها أهدافاً محتملةً للمحتالين ، فإن هذه البيانات يمكن أن تساعد المختصين في أمن المعلومات على كشف النشاط الإجرامي الذي يترك دائما وراءه أدلة رقمية، إذ يقوم المحللون المعنيون بإستخدام هذه البيانات للتنبؤ بالهجمات وتحديد الهجمات الفاعلة الخبيثة قبل وقوع الضرر بيد أن عملية تحليل الملايين من السجلاّت قد تستغرق أياما من العمل الحاسوبي، وهنا تأتي الإستفادة من منهجية الأمن المعرفي التي ترتكز على مبدأ آلة التعلم، إذ يقوم محترفو تكنولوجيا المعلومات بصياغة نماذج ذكية يمكنها معالجة بيانات التهديد بصورة أكثر كفاءة وفاعلية ودقة للتنبؤ بالنشاط الإجرامي [3].

---

[1] – نسيمة سحواذ، الطموح لتوسيع دائرة الاعتماد المتبادل بإدراج طرق تحليلية لفائدة مخابر أخرى، http//Dikanews1322-pdf04L36/44.com، 20 ماي 2024، 11:33.

[2] – إدريس عطية، تطبيقات الهندسة الأمنية في سياسة الجزائر الإفريقية، دار الامة، الجزائر،2019 ، ص 34.

[3] – إسماعيل جنة، حماية منظومتنا الوطنية للمعلومات من خلال تطبيق القانون، مجلة الجيش، العدد599 ، جوان2013 ، ص14.

وثمة ضرورة للتصدي بشكل إستباقي للتهديدات الجيوسياسية التي أدت إلى ظهور هجمات أمنية معلوماتية من نوع جديد ومُعقّد توجهه بعض الدول أو الأفراد، إذ تتصدى العديد من المؤسسات لذلك من خلال نشر أدوات متخصصة، مثل رصد المعلومات وتحليلها وتبادلها بشكل مباشر، إضافةً إلى بناء ثقافة أمنية مقبولة، وكل ذلك بهدف الإسهام في خلق بيئة آمنة في المجتمع والأعمال المختلفة [1].

كما أن التوجهات العالمية الجديدة تفرض تحقيق خطة التنمية لعام**2030** ، وذلك من خلال إبداء الإلتزام السياسي اللازم وتحديث الإستراتيجيات، لاسيما تكنولوجيا المعلومات والإتصالات، بما يتلاءم مع الأهداف التنموية الجديدة ووفقا لأولويات الدول العربية بما فيهم الجزائر [2].

بالإضافة إلى الجريمة السيبرانية، يجب أن تهتم الجزائر ودول الجوار بالإرهاب السيبراني والحرب السيبرانية، ويجب أن تضمن إستراتيجية حقيقية شاملة للأبعاد الثلاثة في إستراتيجية الدفاع السيبراني، كما أنه من التحديات المستقبلية ستشمل على نحو متزايد صراعات في الفضاء السيبراني في جميع الأبعاد، وبما أن الفضاء الإلكتروني هو مسرح جديد للعمليات فإن القوات المسلحة الحديثة لا يمكنها ببساطة أن تعمل بفعالية دون وجود شبكة اتصالات ومعلومات مؤثرة بها ومرنة، لذلك من المهم أن تتمتع الدولة الجزائرية بقدرة على التحكم في الفضاء السيبراني ويعد إطلاق الجزائر أول قمر صناعي للاتصالات بالتعاون مع الصين خطوة مهمة نحو تأمين مؤسساتها وتحقيق الأمن السيبراني [3].

---

[1] – مصطفى عباني، التدابير الأخرى في مجال نزع السلاح والأمن الدولي، اللجنة الأولى للدورة ال 71 الجمعية العامة للأمم المتحدة، بعثة الجزائر الدائمة لدى الأمم المتحدة، نيويورك، 24 أكتوبر 2016 ، ص02 .

[2] – فواز العنزي، أمن المعلومات والقرصنة الإلكترونية، مجلة التقدم العلمي، العدد99 ،2017 ، ص96 .

[3] – صالح ميهوبي، جرائم الانترنت تنخر المجتمع الجزائري، جريدة البلاد، العدد5369 ،2017، ص 07.

خلاصة الفصل الثالث:

خاضت الجزائر تجربة فريدة من نوعها في ظل التطور التكنولوجي والمعلوماتي، يتمثل في إنشاء مؤسسات أمنية مختصة في مكافحة التهديدات السيبرانية المحدقة بها، كالمعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني المختص في الجرائم الالكترونية، بالإضافة إلى المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني وهي مختصة في اعتقال ومتابعة الجرائم الالكترونية.

حيث تعمل على تطوير تلك المؤسسات لإستكمال إقامة منظومة إتصال آلية، على شكل شبكة تربط مختلف وحداتها وهياكلها للاتصال الآلي للمعلومات، مما يسهل عليها التحقق والتحري عن التهديدات والمخاطر السيبرانية التي تواجه أمن الدولة وممتلكاتها وأفراده، فالأمن السيبراني يحتل مكانة عظيمة في منظومة الأمن الوطني الجزائري، ولقد سايرت الجزائر مختلف الجهود الدولية والإقليمية والمبادرات ذات الطابع الدولي والاقليمي لمواجهة التحديات السيبرانية سواء من حيث التصدي لها قبل وقوعها أو التنسيق الدولي مع الأخذ بعين الاعتبار الإمكانيات والأطر التشريعية المحلية.

الخـاتمـــة

الخاتمة:

من خلال ما تطرقنا إليه تبين انه بات لزاما على دول العالم مواكبة التطور التكنولوجي الحاصل في العالم الافتراضي الجديد، والتهديدات السيبرانية هي خطر الحاضر والمستقبل، والأخطبوط الذي أنتجته الحضارة التقنية والثورة المعلوماتية التكنولوجية، الذي إمتدت أذرعه في جميع أنحاء العالم، ولم تفلت من قبضته الدول الضعيفة والمتطورة على حد سواء، وبات خطراً مدمراً لمختلف القطاعات الحياتية، الإقتصادية منها والإجتماعية والسياسية، وحتى الشخصية.

تعد مسألة تحقيق الأمن السيبراني في الجزائر، أحد أهم التحديات الجديدة للسياسة الأمنية الجزائرية التي فرضتها التطورات التكنولوجية المتسارعة، ورغم الجهود المبذولة في سبيل تحقيق ذلك إلا أن المراتب التي تحتلها الجزائر عربيا ودوليا تشير إلى أنها بحاجة إلى المزيد من الجهود، وهذا حتى يمكن لها أن تنجح في مجال مكافحة مختلف المخاطر والتهديدات التي يفرزها الفضاء الالكتروني، والتي يأتي على أ رسها الإرهاب الالكتروني وغيره من التهديدات التي يمثل الانتصار عليها انتصارا جديدا للسياسة الأمنية الجزائرية التي أثبتت نجاعتها في المكافحة خارج الفضاء الالكتروني، ولن تدخر أي جهد في إثبات مكانتها في هذا الفضاء الذي لا يعترف لا بالحدود ولا بالقيود.

ويمكن حصر أهم النتائج والتوصيات المتوصل إليها في النقاط التالية:

النتائج

أولا: إن دراسة الأمن السيبراني التي تم الوصول لها بعد التطرق الى توسيع قطاعات الأمن، من أهم المجالات التي تواجه الدول، حيث إن تحقيق الأمن السيبراني للدولة يؤدي بالدولة إلى الاستقرار في المجال التكنولوجي وتحقيق امنها ومنعه من التعرض للاختراق.

ثانيا: القصور في البنية التشريعية والتنظيمية وعدم إلمام قوانينها بمختلف الاجزاء المكونة للثورة

المعلوماتية (التعاملات البنكية، الشبكة العنكبوتية) والتوجه نحو الاجراءات الردعية والتدابير الوقائية للحد من القرصنة، أثبت عدم التحكم في تكنولوجيات الاعلام والاتصال.

ثانيا: أصبحت العلاقة بين الأمن والتكنولوجيا علاقة متزايدة مع إمكانات تعرض المصالح الإستراتيجية ذات الطبيعة الإلكترونية إلى أخطار وتهديدات سيبرانية، تؤدي إلى تحول الفضاء السيبراني لوسيط ومصدر لأدوات للصراع المتعدد الأطراف.

رابعا: من بين العوامل التي تسهم في تطور المقاربة الأمنية الجزائرية، الدور البارز للعولمة والثورات التكنولوجية في مجالات الإتصالات، السايبر والفضاء الخارجي، وما لا يُلاحظ أن العقيدة الأمنية الجزائرية تحاول التكيّف مع ما هو مستجد من تهديدات أمنية خاصةً تلك التي تتعلق بالتهديدات السيبرانية والتكنولوجية التي أصبحت هاجسا يُهدد أمن كل الدول.

خامسا: تطابق موازين القوى الدولية على واقع الحروب السيبرانية فغالبية الدول العظمى أصبحت هي المسيطرة في مجال الأمن السيبراني العالمي، عكس الدول النامية والضعيفة التي لا نجد لها أثرا في هذا المجال.

سادسا: الصراعات الدولية أصبحت حافز رئيسي لطغيان الجريمة السيبرانية على جميع مجالات الحياة، لدرجة أن المخاطر الأنية والمستقبلية قد بلغت مستويات من شأنها المساس بالأمن الوطني، القومي والعالمي، مما يستدعي إطلاق صفرات الإنذار لإعادة النظر في المنظومة الأمنية.

التوصيات

أولا: يجب تعميم إنشاء مدارس في جميع الاطوار، بغية تعليم الأطفال مبادي الاعلام الآلي والأمن السيبراني، ولا تقتصر فقط على الجامعات كما جاء في المرسوم الرئاسي رقم 24-181، الذي يتضمن إنشاء مدرسة وطنية عليا في الأمن السيبراني.

ثانيا: تدريب وتأهيل وحدات عسكرية وأمنية خاصة، يمكنها مراقبة البنى التحتية للاتصالات، بحيث تقوم بتحديد المخاطر المحتملة وإزالتها.

ثالثا: تأهيل وحدات أمنية وعسكرية خاصة، تتولى التعاون على المستوى الخارجي، مع الهيئات العاملة على مكافحة المخاطر والحد منها ومن آثارها.

رابعا: الاسراع في رسم استراتيجية شاملة، تعمم فيها ثقافة مواجهة ا لخطار في أوساط مستخدمي تكنولوجيا الاعلام سواء في القطا ع العام أو الخاص للتفاعل مع الاجراءات العملية والمنية لمكافحة القرصنة، مع تنظيم دورات تكوينية في التطبيقات الصحيحة لاستغلال ثورة المعلومات وفق المواصفات الدولية التي أوصت بها علامة أيزو والاتحاد الدولي للاتصالات، مع إشراك كل الفاعلين في المجال المني والمعلوماتي.

خامسا: تطوير التشريعات السيبرانية تماشيا مع التطورات الحاصلة في عالم التكنولوجيا، من أجل بناء مجتمع معرفي، مع غلق كل منافذ الخطر والتهديد، تسهيل التعاملات في جميع المجالات، تحفيز التكامل داخليا وخارجيا، تدعيم التعاون الفعلي لمواجهة المخاطر وبالتالي تأهيل المناخ لحد من الجريمة وحماية الأنظمة المعلوماتية.

سادسا: الانضمام الى الاتفاقيات الدولية في مجال حماية الأنظمة المعلوماتية على غرار اتفاقية بودابست، مما يحفز على التنسيق والتعاون مع الناشطين من خبراء ومؤسسات في ميدان المن السيبراني إقليميا ودوليا، المواظبة على المشاركة في اللقاءات العلمية والدورات التكوينية للاستفادة من الخبرات في مجال التوظيف والاستغلال العقلاني لعالم التكنولوجيا.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

أولا/ المؤلفات

بالعربية

1- إدريس عطية، تطبيقات الهندسة الأمنية في سياسة الجزائر الإفريقية، دار الامة، الجزائر، 2019.

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

3- بيتر بي سيل، الكون الرقمي الثورة العالمية في الاتصالات، ترجمة ضياء وارد، مؤسسة هنداويCIC، إنجلترا،2017 .

4- جمال محمد غيطاس، الأمن المعلوماتي والجرائم الالكترونية، أدوات جديدة للصراع، مركز الجزيرة للدراسات، القاهرة،2012 ،

5- حسن بن أحمد الشهري، الأنظمة الالكترونية الرقمية المطورة لحفظ وحماية سرية المعلومات من التجسس، مركز النور للأبحاث الإلكترونية، 2010.

6- حمدون تورية، الأمن السيبراني في لبلدان النامية، الاتحاد الدولي للاتصالات، 2006

7- ذيب بن عايض القحطاني، أمن المعلومات، مدينة الملك عبد العزيز للتعليم والتقنية، الرياض، المملكة العربية السعودية،2015

8- ذياب موسى البداينة،"الأمن الوطني في عصر العولمة"، الرياض، جامعة نايف العربية للعلوم الأمنية، 2011.

9- سالم المعوش،"مجتمع المعرفة وتعزيز الأمن القومي، المشهد العالمي الجديد"، لبنان، مركز الأبحاث العلمية، 2011،

10- عبد النور بن عنتر،" البعد المتوسطي للأمن الجزائري :الجزائر، أوربا، الحلف الأطلسي"، الجزائر :مكتبة العصر للطبع والنشر والتوزيع، 2005.

11- كمال المنوفي، السياسة العامة وأداء النظام السياسي، القاهرة، مكتبة النهضة المصرية، 1988.

12- منير البعلبكي، قاموس المورد دار العلم للملايين، بيروت، 2004.

13- منى الشقر جبور، الأمن السيبراني، التحديات ومستلزمات المواجهة"، اللقاء السنوي الاول للمختصين في امن وسلامة الفضاء السيبراني، بيروت ، لبنان، 2012.08.28 .

14- نوران شفيق، أثر التهديدات الإلكترونية على العلاقات الدولية، دراسة في أبعاد الأمن الالكتروني، المكتب العربي للمعارف، القاهرة، 2014.

15- وصال نجيب العزاوي، مبادئ السياسة العامة، الأردن، دار أسامة للنشر والتوزيع، 2003.

بالأجنبية

1- Dictionnaire français Le petit Larousse, (France, Edition, 2001), p104

2 - English dictionary Oxford dictionaries language, P299

ثانيا/ الاطروحات والمذكرات

1- باديس لونيس، جمهور الطلبة الجزائريين والأنترنت، دراسة في استخدامات إشباعات طلبة جامعة منتوري قسنطينة، رسالة ماجستير، جامعة منتوري –قسنطينة، كلية العلوم الإنسانية والعلوم الإجتماعية، قسم علوم الإعلام والاتصال2008، 2007 .

2- حنان بن عبد الرزاق،"تأثير المأزق الأمني الاثني على الاستقرار الداخلي لدولة، د راسة للنموذج الاسباني" أطروحة دكتورا، جامعة محمد خيضر، بسكرة، كلية العلوم السياسية، تخصص :

علاقات دولية ود راسات استراتيجية،2017.

3- زهوة خلوط، التسويق الابتكاري وأثره على بناء ولاء الزبائن، دراسة حالة :مؤسسة اتصالات الجزائر، رسالة ماجيستير، جامعة امحمد بوقرة، بومرداس، كلية العلوم الاقتصادية تجارة وعلوم التسيير،2014 - 2013.

4- نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير، جامعة الحاج لخضر، باتنة، كلية الحقوق والعلوم سياسية، تخصص علوم جنائية، 2012-2013.

5- نعيمة برنيس، الوظيفة الإعلامية لشبكة الأنترنت في عصر ثورة المعلومات، رسالة ماجستير، جامعة منثوري قسنطينة، كلية العلوم الإنسانية والإجتماعية، فرع :صحافة مكتوبة وسمعية بصري، 2009-2010.

ثالثا/ المجلات والمقالات العلمية

1- أحمد عيسى، نعمة الفتلاوي،" الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم المعاصر"، مجلة المحقق الحليلي، العراق :جامعة الكوفة، كلية القانون،2016.

2- إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائر، مجلة المصداقية، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي، الجزائر، د ن، ص 106.

3- إسماعيل جنة، حماية منظومتنا الوطنية للمعلومات من خلال تطبيق القانون، مجلة الجيش، العدد599 ، جوان2013

4- العبودي، علي عبد الرحيم، هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين، المجلة العلمية الأكاديمية العراقية، العدد57 ، جامعة برداد، كلية العلوم السياسية،2019

5- إيمان بن سالم، جريمة التجنيد الالكتروني للإرهاب وفقا لقانون العقوبات الجزائري، برلين، المركز الديمقراطي العربي لدراسات الاستراتيجية والسياسية والإقتصادية،2008

6- بوبرطخ نسيم، الفضاء السيبراني مسرح الصراعات الجيوسياسية المعاصرة، مجلة الجيش،

العدد 685، 2020.

7- الزهراني، شيخة حسين، التعاون الدولي في مواجهة الهجوم السيبراني"، مجلة جامعة الشارقة للعلوم القانونية، المجلد 17، العدد 1 ، كلية القانون، الامرات العربية المتحدة،2020

8- إلياس شاهد، الحاج عرابة، عبد النعيم دفرو، تقييم تجربة تطبيق الحكومة الإلكترونية في الجزائر، المجلة الجزائرية للدراسات المحاسبية والمالية، العدد الثالث،2016

9- أمحمدي بوزينة آمنة، وسائل وأساليب التحري في مجال مكافحة الجرائم الإلكترونية، دراسة تحليلية لأحكام قانون العقوبات، كلية الحقوق والعلوم السياسية، جامعة حسيبة بن بوعلي، الشلف

10- بورابحة سليمة، السياسات العامة الجزائرية في مجال السيبرانية: الواقع والتحديات، مجلة دفاتر السياسة والقانون، المجلد 15، العدد 01، 2023

11- ب . بوعلام، الجيش الوطني الشعبي ورهانات تداول المعلومة عبر شبكات التواصل الاجتماعي، مجلة الجيش، العدد 603 ، جانفي2016.

12- بوكبشة محمد، الأمن والدفاع السيبراني أولوية قصوى، مجلة الجيش، وزارة الدفاع الوطني، الجزائر، العدد 651، 2017

13- جارش عادل،" مقاربة معرفية حول الإرهاب السيبراني"، مجلة المستقبل العربي، العدد 20 ، بيروت، لبنان،2000

14- جمال بوازدية، الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية، التحديات والافاق المستقبلية، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 01،

15- خالد وليد محمود، الهجمات عبر الإنترنت، ساحة الصراع الإلكتروني الجديدة، سلسلة دراسات ودراسة السياسات، المركز العربي للأبحاث، قطر، 2013 .

16- ربيعي حسين وسمر محمود، الحروب السيبرانية :المخاطر واستراتيجيات تحقيق الأمن السيبراني الدولي والداخلي، المجلة الجزائرية للأمن الإنساني، جامعة الأخوة منتوري قسنطينة1 ، المجلد 07، العدد 2، جويلية 2022

17- قصعة سعاد، تحديات الأمن المعلوماتي في مواجهة الجرائم الإلكترونية في ظل الإعلام الجديد، مجلة المعيار، المجلد 24، العدد 50، 2020

18- سمير بارة، لدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائر، الدور والتحديات، جامعة قاصدي مرباح، ورقلة

19- سهام بوعموشة، الفضاء السيبراني يتميز بانفتاح شبكة المعلوماتية وانعدام الحواجز الجغرافية ، جريدة الشعب، العدد 17345، 24ماي 2017

20- شريف بسام، واقع الحوكمة الالكترونية في الدول العربية، مجلة العلوم الاجتماعية والإنسانية، جامعة الجزائر3، العدد 06، 2016

21- شلوش نورة، القرصنة الإلكترونية في الفضاء السيبراني التهديد المتصاعد لأمن الدول، مجلة مركز بابل للدراسات الأساسية، المجلد08 ، العدد02 ،2015

22- عادل عبد الصاد، " الفضاء الإلكتروني والرأي العام :تغير المجتمع والأدوات والتأثير، المركز العربي لبحاث الفضاء الإلكتروني، قضايا استراتيجية، 2013 ، العدد2459

23- صالح زياني،" مرتكزات عقيدة الأمن القومي الجزائري بين الثبات والتحول"،) محاضرة مقدمة لطلبة جامعة باتنة، كلية الحقوق والعلوم السياسية، د.س

24- صالح ميهوبي، جرائم الانترنت تنخر المجتمع الجزائري، جريدة البلاد، العدد5369 ،

25- عبد الحليم بوقرين، حتمية إنشاء ضبطية خاصة بالجرائم الإلكترونية، مجلة العلوم القانونية والسياسية، المجلد 05 ، العدد 02،2016

26- فواز العنزي، أمن المعلومات والقرصنة الإلكترونية، مجلة التقدم العلمي، العدد99 ،2017

لبكي، جورج، المعاهدات الدولية للأنترنت، حقائق وتحديات، مجلة الدفاع الوطني، بيروت، العدد 83

27- كلثوم بيبيمون، السياقات الثقافية الموجهة للهوية الرقمية في ضوء تحديات المجتمع الشبكي من التداول الافتراضي إلى الممارسات الواقعية، مجلة" إضافات"، مركز دراسات الوحدة العربية،

العدد23 ، بيروت، 2016

28- محمد علي قطب، الجرائم المعلومات وطرق مواجهتها، مركز الاعلام الأمني، الأكاديمية الملكية للشرطة، 2009

29 محمد مختار، هل يمكن تجنب الدولة مخاطر الهجمات الإلكترونية؟، مجلة مفاهيم المستقبل، العدد06 ، بيوت، لبنان،2015

30- يوسف بوغرارة ، الأمن السيبراني، الإستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبيري، دراسة منشورة مجلة الدراساتالأفريقية وحوض النيل، المركز الديموقراطي العربي، العدد الثالث، 2018.

31- Léoutre pierre marie, l'appropriation du cyberespace pour la politique, Revue de la sécurité globale, numero25, 2021

رابعا/ المداخلات والمواقع الالكترونية

1- أبو المعالي محمد عيسى، الحاجة إلى تحديث أليات التعاون الدولي في مجال مكافحة الجريمة المعلوماتية"، مداخلة في المؤتمر المغاربي الاول حول (المعلوماتية والقانون) ، طرابلس، ليبيا،2009/10/28

2- أحمد عنتر، تقنيات الأمن السيبراني والتحديات المستقبلية مقال منشور على الانترنت بتاريخ 2023/12/04، https://www.aljazeera.net/tech/2023/12/4/،

3- الندوة الافريقية، حوكمة النترنت CAGI، www.lemaghrebdz.com

4- أماني جهاد، تصنيف الدول الغربية والعربية في مجال الأمن السيبراني، WWW.3ARABINSIDEE.COM

5- الاسكوا، تقرير الملامح الإقليمية لمجتمع المعلومات في المنطقة العربية، اللجنة الإقتصادية والإجتماعية لغربي آسيا، بيروت، لبنان،(2016) ،

6- الملتقى الدولي، الدفاع السيبراني مكون اساسي للأمن والدفاع الوطني، المنظم من طرف قيادة الاركان للجيش الوطني الشعبي.

7- حسان حويشة، تقرير دولي حول الأمن الرقمي في 2022 ،إحباط قرابة 30 مليون تهديد سيبراني ضد الجزائر، https://www.echoroukonline.com

8- سعد علي الحاج بكري،" الأمن السيبراني ومعضلة حمايته"، الرابط www.alegt.com/article1241506.html

9-عبد النور بن عنتر،" عقيدة الجزائر الأمنية :ضغوطات البيئة الإقليمية ومقتضيات المصالح الأمنيةhttp://studies.aljazeera.net/ar/reports/2018/05/180502110656159

10- كريم حميد،"القرصنة الإلكترونية 52639 https://www.alakah.net/culturel/0

11- موقع الموسوعة الجزائرية للدراسات السياسية والاستراتيجية، الحرب السيبرانية وتداعياتها على الأم ماهي" السيبرانية؟ وما دورها في صناعة القرار؟،.

https://ar-ar.facebook.com/zeitgeist.arabic/posts/cybern/

12- نسيمة سحواذ، الطموح لتوسيع دائرة الاعتماد المتبادل بإدراج طرق تحليلية لفائدة مخابر أخرى،www.Dikanews.com ، تاريخ التصفح، 18 ماي 2024، 15:06.

13- نسيم رمضان، كاسبرسكي: 411 ألف ملف خبيث يومياً خلال عام 2023، مقال على الرابط، https://aawsat.com، 27 ماي 2024، 17:05.

فهرس الموضوعات

فهرس الموضوعات

الفصل الثاني: السياسة الأمنية الجزائرية في ظل التطور التكنولوجي

فهرس الموضوعات

فهرس الموضوعات

فهرس الموضوعات

الملخص

في ظل التطورات الحاصلة في مجال التكنولوجيا، أصبحت قضية الأمن المعلوماتي السيبراني من التحديات الكبرى على الصعيدين الإقليمي والعالمي، لا سيما مع تزايد التهديدات السيبرانية التي تعتبر من التهديدات الجديدة التي تصيب أمن معلومات الدول، ما يؤدي إلى انهيار أمنها الوطني واختراقه وبالتالي تنهار الدولة تماما.

إن الجزائر من بين الدول التي تتعرض إلى التهديدات السيبرانية، لذلك أصبحت الجزائر تهتم بالأمن السيبراني بشكل كبير بوضع مجموعة من الآليات المحلية وكذا التنسيق الدولي للحد من إنتشار هذه الظاهرة، كما تحاول وضع استراتيجيات مبنية على التعاون مع العديد من الدول الإقليمية والعالمية للتصدي لهذه التهديدات، وذلك عن طريق إنشاء مراكز تعنى بمكافحة التجسس وحماية أمن المعلومات.

Summary

In light of developments in technology, the issue of cybersecurity has become a major challenge at the regional and global levels, especially with the increasing cyber threats, which are considered new threats to the security of state information, leading to the collapse of national security and penetration and thus the collapse of the state completely.

Algeria is one of the countries that may be exposed to cyber threats. Therefore, Algeria is interested in cybersecurity by developing a set of local mechanisms as well as international coordination to reduce the spread of this phenomenon. It is also trying to develop strategies based on cooperation with many regional and global countries to address these threats, Through the establishment of anti-espionage and information security centers.