جامعة باتنة 1

كلية الحقوق والعلوم السياسية

قسم العلوم السياسية

دور الأمن المعلوماتي في الحد من الهجمات السيبرانية (دراسة حالة الجزائر)

مذكرة معدة ضمن متطلبات نيل شهادة الماستر في العلوم السياسية

تخصص: علاقات دولية

إعداد الطالب:

غباش شعلال

إشراف الأستاذ الدكتور:

زياني زيدان

لجنة المناقشة

الاسم واللقب	الرتبة العلمية	المؤسسة الجامعية	الصفة
أ.د. وناسي لزهر	أستاذ التعليم العالي	جامعة باتنة 1	رئيسا
أ.د. زياني زيدان	أستاذ التعليم العالي	جامعة باتنة 1	مشرفا ومقررا
أ.د.لموشي طلال	أستاذ التعليم العالي	جامعة باتنة 1	مناقشا

السنة الجامعية: 2023 / 2024

جامعة باتنة 1

كلية الحقوق والعلوم السياسية

قسم العلوم السياسية

دور الأمن المعلوماتي في الحد من الهجمات السيبرانية (دراسة حالة الجزائر)

مذكرة معدة ضمن متطلبات نيل شهادة الماستر في العلوم السياسية

تخصص: علاقات دولية

إعداد الطالب:

غباش شعلال

إشراف الأستاذ الدكتور:

زياني زيدان

لجنة المناقشة

الاسم واللقب	الرتبة العلمية	المؤسسة الجامعية	الصفة
أ.د. وناسي لزهر	أستاذ التعليم العالي	جامعة باتنة 1	رئيسا
أ.د. زياني زيدان	أستاذ التعليم العالي	جامعة باتنة 1	مشرفا ومقررا
أ.د.لموشي طلال	أستاذ التعليم العالي	جامعة باتنة 1	مناقشا

السنة الجامعية: 2023 / 2024

الإهداء

أهدي ثمرة جهدي المتواضع إلى من جعل الله سبحانه وتعالى الجنة تحت أقدامها.

إلى تلك التي أفنت شبابها لخدمتنا وراحتنا إلى أمي الحبيبة

إلى من جعله الله أوسط أبواب الجنة أبي الغالي

إلى إخوتي وجميع أفراد عائلتي وإلى كل زملائي

إلى كل من ساعدني في كتابة المذكرة

محجوب سلسبيل

سحنوني حسينة

إلى أستاذي المحترم الأستاذ الدكتور زياني زيدان

وأخيرا وليس آخرا أقول العين ترى أشياء كثيرة وفي الذاكرة تبقى أحداث مثيرة

شكر وعرفان

أشكر الله سبحانه وتعالى الذي وفقنا وأعطانا القدرة في إنجاز هذه المذكرة

كما نتقدم بأسمى معاني الشكر والعرفان خاصة إلى أستاذنا الكريم

الأستاذ الدكتور زياني زيدان

الذي أمد لنا يد العون والمساعدة والنصيحة وعلى قبوله الإشراف على المذكرة.

إلى كل من ساهم من قريب أو بعيد في هذا العمل المتواضع

مقدمة

مقدمة:

تشهد العصور الحديثة تطورًا سريعًا في مجال التكنولوجيا الرقمية، ما أدى إلى تعميم استخدام الإنترنت والتفاعل الرقمي في شتى جوانب الحياة. ومع هذا التقدم الهائل، تنشأ تحديات جدية تتعلق بأمان المعلومات والتحديات السيبرانية التي تهدد سلامة الأفراد والمؤسسات. تعتبر الجزائر، كأي دولة أخرى، عرضة لتلك التحديات وتحتل قضايا الأمن المعلوماتي مكانة هامة في جدول اعمالها الوطني.

في هذا السياق، يأتي موضوع "حماية المعلومات وأمنها في الجزائر" كمحور أساسي للبحث، حيث نتعامل مع تحليل التحديات وتطوير رؤية استباقية لتعزيز الأمن المعلوماتي. يعكس هذا البحث التفاعل الحيوي بين التقنية والأمان، ويستند إلى فهم عميق للبيئة الرقمية في الجزائر والتحديات المحتملة التي قد تطرأ عليها.

إن فحص الأمان السيبراني يمتد إلى مجموعة واسعة من القضايا، بدءًا من حماية البيانات الحساسة إلى التصدي للتهديدات السيبرانية الهجمات والاختراقات. وفي هذا السياق، يلعب التحليل الاستباقي دورًا حيويًا في تحديد التهديدات المحتملة ووضع إطار للتصدي لها بشكل فعّال.

يتطلب تعزيز الأمن السيبراني في الجزائر جهودا متكاملة تتضمن التشريعات والسياسات والتقنيات المتقدمة الى جانب مشاريع حيوية تتصل بالنية التحتية الحاضنة لكل متطلبات تفعيل دور المجال السيبراني ومواجهة التهديدات المترتبة على ذلك.

يسعى هذا البحث إلى فهم السياق العام للأمن المعلوماتي في الجزائر، مع التركيز على تطوير استراتيجيات وتقنيات لمواجهة التحديات القائمة والمستقبلية.

أهمية موضوع الدراسة:

يندرج أمن المعلومات ضمن مسعى حماية ما تملكه المؤسسات والهيئات والدول من موارد معلوماتية يتم تخزينها وتداولها من خلال البيئة الحاسوبية، والتي تشكل الأجهزة والشبكات الحاسوبية والبرمجيات والإنترنت أهم عناصرها. وعندما تقوم أي دولة باتخاذ التدابير اللازمة لأمن المعلومات والتي تستهدف تقليل الاحتمالات التي تشكل تهديدا لها، والحد من الأضرار الناجمة عن سوء الأداء، وضمان التعافي في أعقاب وقوع أي حوادث عارضة –سواء كانت مقصودة أو غير مقصودة أثناء فترة زمنية مقبولة وبتكلفة مقبولة، فإنها بذلك تحافظ على مواردها المالية والمادية، وعلى سمعتها ووضعها القانوني ومواطنيها .فالدولة، أي دولة، هي المعنية الأولى بالأمن المعلوماتي، لأنها هي المنتج الأكبر للبيانات والمعلومات العامة والخاصة، كما أنها هي التي تضع النظم والقواعد التي تحدد الممنوع والمسموح.

مقدمة

ولقد شاع استخدام مصطلح الأمن المعلوماتي بعد أن انتشر مفهوم الفضاء المعلوماتي الذي يرتبط ارتباطا وثيقا بالإنترنت وبتكنولوجيا الاتصالات والمعلومات، عبر البنى التحتية المختلفة للاتصالات والأنظمة المعلوماتية، فضلا عن العديد من الخدمات المعلوماتية التي لم نكن لنحصل عليها من دونه. لذا، فسنقوم في هذه الدراسة باستخدام مصطلحي "أمن المعلومات" و "الأمن السيبراني" كمترادفين. في أي منشأة يجب أن يتضمن وسائل وضوابط رقابية على البيانات حتى يتم تقديم تقارير تحتوي على معلومات موثوق بها من قبل مستخدمي نظام المعلومات. وننوه بمدى أهمية هذا الموضوع لتسارع وتيرة التطورات التكنولوجية وظهور فواعل متعددة ساهمت في السيطرة على كل مصادر المعلومات وتنوع أجهزة الإتصال وانتشار مخاطر كثيرة تهدد امن هذه المعلومات بكل مصادرها لذا نؤكد على أهمية موضع أمن المعلومات.

أسباب اختيار الموضوع:

يمكننا تحديد نوعين من أنواع المبررات وهما:

أ- المبررات الموضوعية:

- ✓ هيمنت الدراسات الأمنية على حقل العلاقات الدولية –مجال التخصص – خاصة مع ظهور تهديدات أمنية جديدة من قبيل التهديدات التي يطرحها عبر التعامل عبر العالم الإفتراضي .
- ✓ ضرورة تناول مواضيع ذات صلة بمجال التخصص، وذلك من خلال التركيز على الجوانب النظرية وربطها بالقضايا الواقعية الحالية التي تواكب التطورات التكنولوجية عالميا ومحليا، وماتطرحه من تعقيدات أمنية، وما يتم في المقابل إعداده لفك هذه التعقيدات وتجاوز تهديداتها .
- ✓ مواصلة البناء التراكمي المتنوع للبحث العلمي من خلال فتح مجالات جديدة تصب الاهتمام على مواضيع حديثة كالأمن المعلوماتي ، ومدى مواكتبه في سلم اهتمامات المنظومات الجزائرية المختلفة.

ب-المبررات الذاتية:

- ✓ أما المبررات الذاتية المحفزة لاختيار الموضوع، لا تعدو إلا ان تكون تلبية لرغبة وميل ذاتي للطالب، وهذا لتطرقه وصلته بالدراسات الأمنية وحبه لهذا التخصص، في مستوياتها المختلفة، وذلك لما لها من جاذبية خاصة في أوساط النخب العلمية والإعلامية وحتى الرأي العام البسيط .
- ✓ إضافة إلى ذلك رغبة الطالب في التعرف على أحد المفاهيم الأمنية المستجدة الأمن المعلوماتي ومدى الاهتمام الذي يحظى به تعزيزه بالجزائر كنموذج امبريقي محلي مرتبط ارتباطا مباشرا بالطالب.

أهمية الدراسة:

تكمن أهمية هذه الدراسة المعنونة بـ: دور الأمن المعلوماتي في الحد من الهجمات السيبرانية (دراسة حالة الجزائر) في:

1. **تطوير البيئة الرقمية:** يأتي تعزيز الأمن المعلوماتي في الجزائر بأهمية بالغة في تطوير البيئة الرقمية وتشجيع اعتماد التكنولوجيا الرقمية في مختلف القطاعات. تحسين الأمن المعلوماتي يعزز الثقة في استخدام الإنترنت والتكنولوجيا، مما يسهم في تعزيز التفاعل الرقمي وتقدم البلاد في الاقتصاد الرقمي.
2. **حماية المعلومات والبيانات:** يشكل التحسين في الأمن المعلوماتي وسيلة لحماية المعلومات والبيانات الحساسة للأفراد والمؤسسات. وبذلك يحافظ على خصوصية الأفراد ويمنع الوصول غير المصرح به إلى المعلومات الحساسة، مما يقلل من تهديدات السرقة الإلكترونية والتجسس السيبراني.
3. **مكافحة التهديدات السيبرانية:** تعتبر الجزائر عرضة لمختلف أنواع التهديدات السيبرانية، بدءًا من هجمات القرصنة والبرمجيات الخبيثة إلى الاختراقات الإلكترونية. يساهم تعزيز الأمن السيبراني في تعزيز القدرة على مكافحة هذه التحديات بفعالية وتحديد الثغرات الأمنية والتصدي لها.
4. **تعزيز الاستقرار الوطني:** يلعب الأمن المعلوماتي دورًا حاسمًا في الحفاظ على استقرار الدولة والحفاظ على سلامة الهياكل الحيوية مثل البنية التحتية الحكومية والمؤسسات الحيوية. التأكيد على الأمان السيبراني يقوي المقاومة ضد الهجمات التي قد تستهدف هذه الهياكل.

أهداف الدراسة:

- فحص التحديات السيبرانية التي تواجهها الجزائر حاليا، وفهم طبيعتها وأسبابها.
- تحديد وتحليل الثغرات الأمنية المحتملة في النظام السيبراني الجزائري.
- وضع إطار لسياسات وإجراءات تعزز الأمن المعلوماتي بشكل شامل وفعّال.
- تحديد كيفية تحقيق التوازن ببن استمرارية التطور التكنولوجي وحاجة البلاد للحفاظ على أمان المعلومات.
- تعزيز التوعية بأهمية الأمان المعلوماتي وتشجيع الجمهور والشركات على تبني ممارسات أمن معلوماتي .
- تعزيز التدريب وبناء القدرات للكوادر الفنية والمتخصصة في مجال الأمن المعلوماتي لتحقيق فاعلية أكبر في مكافحة التهديدات الرقمية.

الإشكالية: عطفا على أهمية موضوع الدراسة الدائر حول دور الأمن المعلوماتي في الحد من الهجمات السيبرانية دراسة حالة الجزائر، تتمحور إشكالية البحث أساسا حول ما يلي:

كيف تتم عملية ضمان الأمن المعلوماتي بالقدر الذي يساهم في تجاوز التهديدات السيبرانية الراهنة والمستقبلية بهدف تعزيز الاستقرار الوطني في الجزائر؟

تندرج تحت هذه الإشكالية التساؤلات الفرعية التالية:

الأسئلة الفرعية:

- ما هي المفاهيم المفتاحية المساهمة في فهم الأمن السيبراني؟
- ماهي أهم طرق الإختراق التي يطرحها التعامل عبر الفضاء المعلوماتي الجزائري؟
- فيما تتمثل الاستراتيجيات الأمنية للحد من الهجمات السيبرانية في الجزائر ؟

فرضية الدراسة:

إذا تم تنفيذ استراتيجيات فعّالة لتعزيز الأمن المعلوماتي في الجزائر، بتوجيه الجهود نحو تأهيل البنية التحتية الرقمية إلى جانب تعزيز الوعي السيبراني، فإن ذلك سيساهم بشكل كبير في التصدي للتحديات السيبرانية وتعزيز الثقة في استخدام المنصات والمواقع ، مما يعزز الاستقرار الوطني في الجزائر.

المنهج العلمي المتبع:

تم انتقاء **المنهج الوصفي والمنهج التحليلي** في هذه الدراسة بهدف تحقيق الأهداف البحثية والتحقق من صحة الفرضية المطروحة. يستند هذا المنهج إلى جمع بيانات شاملة ومعلومات مفصلة لتمكين تحليل دقيق لمسألة الدراسة. من خلال هذا التحليل، يمكن فهم مفهوم الحماية المعلوماتية وتعزيز الأمن المعلوماتي في السياق الجزائري بطريقة توقعيه.

بالإضافة إلى ذلك، تم اعتماد **منهج دراسة الحالة** لاستكمال رؤية شاملة حول الحماية المعلوماتية وتعزيز الأمن المعلوماتي في الجزائر بنهج استباقي. من خلال التركيز على دراسة الحالة، يمكن استكشاف التفاصيل الدقيقة حول تعزيز الأمن السيبراني في السياق الجزائري بطريقة شاملة ومعمقة.

بشكل عام، يجمع استخدام هاتين الطريقتين البحثيتين على التفصيل الوصفي من منهج الوصف التحليلي.

حدود موضوع الدراسة:

تتسع حدود هذه الدراسة زمانيا بين أول ظهور لمفهوم الأمن المعلوماتي، إلى أول اهتمام تنظيمي قانوني أمني جزائري بتكريس الأمن السيبراني العام 2006، أي بعد صدور القانون 15/04 الذي تضمن أول مرة عقوبة المساس بأمن أنظمة المعالجة الآلية للمعطيات، إلى غاية بدء اجراء هذه الدراسة مارس 2024 وتعد الجزائر المدى المكاني لإجراء الدراسة، وذلك بغية فهم التعامل المحلي – الوطني مع التهديدات السيبرانية وكيفية تعزيز الأمن المعلوماتي كبعد من أبعاد السياسة الأمنية الجزائرية .

الدراسات السابقة:

تبلور موضوع الدراسة إنطلاقا من مجموعة الأدبيات السابقة التي تعتبر منطلقا مهما في خوض هذه التجربة البحثية، وفي هذا الصدد يمكن الإشارة إلى مجموعة منها:

دراسة شعيب قاسمي، فؤاد بلغيث بعنوان: "**الإستراتيجيات الدولية في مكافحة الجريمة السيبرانية**": **دراسة حالة الجزائر ،2020**. مذكرة لنيل شهادة الماستر تخصص دراسات أمنية واستراتيجة جامعة العربي تبسي تبسة ، تناولت دراستهم طبيعة التهديدات والجرائم السيبرانية ، كما تطرقوا أيضا في مفهوم الأمن السيبراني وعلاقته بالأمن القومي وأيضا الإستراتيجية الروسية في المجال السيبراني . ولكن لم يتطرقا إلى انعكاسات التهديدات السيبرانية على الأمن الوطني الجزائري .

ساسوي خالد ومحمد بن حسين، "**الحروب السيبرانية والأمن العالمي: التحديات والمواجهة**"، مذكرة لنيل شهادة الماستر، دراسات أمنية واستراتيجية، الجلفة، جامعة زيان عاشور، 2020.

تناول الباحثان موضوع الحروب السيبرانية من منظور الأمن العالمي، أين قاما باستكشاف مختلف أبعادها العسكرية، الاقتصادية والسياسية، ثم قاما بإبراز مختلف التحديات التي يواجهها عالم اليوم لتحقيق الأمن على مستوى الفضاء السيبراني: الجريمة السيبرانية، الإرهاب السيبراني ..، لينتهيا بالتطرق للآليات القانونية والسياسية لمواجهة الحروب السيبرانية. ومما يؤخذ على الدراسة عدم اثارتها لأثر الحرب السيبرانية على استقرار وامن الدولة الجزائرية .

دراسة د محمد الجندي، "**الأمن السيبراني من حروب المعلومات إلى الجرائم السيبرانية**"، كتاب جديد في طبعته الأولى صدر عن دار المعارف بالقاهرة في 2024. إذ تناول الباحث في الشؤون الأمنية العديد من الجوانب الخاصة بالفضاء السيبراني وكيفية استغلاله من قبل أجهزة الاستخبارات والمجرمين وخبراء الأمن السيبراني والمحققين في الجرائم السيبرانية، وتناول أيضا علاقة الأنترنيت بتطور النزاعات والحروب والتأثير الجيوسياسي لهذه التقنيات الحديثة، وعلاقتها بالمن القومي للدول ، حيث ساهم الفضاء السيبراني في تطور

وتعزيز الأنشطة الإستخباراتية والأمنية بين الدول، مما فتح بابا جديدا للبحث في هذا المجال من الناحية السيساية والمدنية والإقتصادية والإجتماعية والقانونية .ومما يؤخذ على الدراسة عدم تركيزها على تبيين التحديات التي تعترض تحقيق المن المعلوماتي خصوصا في دول المنطقة العربية .

الدراسة الرابعة: "**الأمن السيبراني: الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبري**"، للأستاذ بوغرارة يوسف، باحث في الدراسات الأمنية والاستراتيجية بجامعة مستغانم ، ينطلق الباحث في دراسته المنشورة بمجلة الدراسات الإفريقية وحوض النيل شهر سبتمبر 2018، من إشكالية أساسها أن التطور التكنولوجي الذي يشهده العالم والذي أفضى على الاعتماد على خصائص العالم الإفتراضي في إنهاء التعاملات العالمية المختلفة، والتي انخرطت فيها الدول بشكل كبير، يستلزم بالمقابل إيجاد آليات حماية دفاعية ضد أي تهديدات سيبرانية محتملة ، مفترضا أن الجزائر قدمت في هذا الصدد مجموعة من الإجراءات من شانها تأمين التعامل عبر الفضاء المعلوماتي داخليا وخارجيا، وقد تطرق الباحث في مقاله إلى البيئة المفاهيمية للأمن المعلوماتي والمفاهيم المشابهة له، إظافة إلى تحديد مجمل التهديدات الأمنية السيبرانية المحتملة، ليتطرق إلى اهم الآليات القانونية والمؤسسية التي تبنتها الجزائر لحماية فضاء تعاملاتها السيبرانية، كما تطرق الباحث إلى اهم الآليات الدفاعية التي ينتهجها الجيش الجزائري في سبيل مكافحة التهديدات الأمنية السيبرانية ، ليخلص في الأخير إلى جملة من النتائج نختصرها في نقطتين :

- ✓ تعقد مفهوم الأمن السيبراني بسبب تعدد الفواعل سواء الرسمية كالدول أو غيرها وتباين الوسائل التكنولوجية والأنظمة المعلوماتية.
- ✓ تمكن الجزائر من وضع آليات قانونية ومؤسسية ورسم سياسات دفاعية من أجل حماية امنها السيبراني لكنها ، تبقى قاصرة امام التطور المستمر للفضاء الإلكتروني.

إن هذه الدراسات تسلط الضوء على أهمية فهم ومواجهة التحديات السيبرانية في العالم الحديث، وتقدم مدخلًا قيمًا للتفكير في كيفية تطوير آليات ووسائل للحد من هذه التهديدات.

صعوبات الدراسة:

صادفت هذه الدراسة في سبيل تحقيقها تحديين موضوعيين اثنين، الأول هو حداثة الموضوع وتسارع تطوراته وظهور تخصصات أخرى اكثر تعقيدا على غرار الذكاء الإصطناعي بالنسبة للمنتوج الأكاديمي المحلي، حيث اقتصرت المراجع على بعض مذكرات التخرج، والأوراق البحثية والمداخلات في المقابل شكلت وفرة المراجع باللغة الإنجليزية مع ضيق الوقت عائقا ثانيا من اجل ترجمة المادة العلمية والإستفادة منها فيما يخدم البحث.

تبرير الخطة:

للإلمام بجميع جوانب الدراسة تم تقسيمها إلى مقدمة عامة توضح أهمية الموضوع ، وأسباب ومبررات اختياره، كما تؤصل له منهجيا بوضعه في إطاره الصحيح بكل مايتبعه من إجراءات منهجية من ضبط للإشكالية التي تدور حولها الدراسة وتساؤلات فرعية، والفرضية الأساسية التي تنطلق منها لإثبات أو نفي العلاقة بين متغيرات الموضوع ، إضافة إلى الأدبيات المشابهة التي شكلت بتقاطعها وموضوع الدراسة قاعدة بيانات أولية مهدت للمضي قدما في تناوله فيما تم تقسيم الدراسة إلى ثلاثة فصول ، تندرج ضمنها مجموعة من المباحث والمطالب، يقدم الفصل الأول اطارا تعريفيا ومفاهيميا ونظريا لموضوع الدراسة ، من جهة الأدوات النظرية والمفاهيمية المستخدمة لنتطرق في الفصل الثاني لأهم طرق الإختراق الرقمي في الفضاء المعلوماتي الجزائري، فيما يهتم الفصل الثالث بوضع الدراسة في حيزها الواقعي من خلال التطرق لطرق الأمن المعلوماتي المتوفرة والمعتمدة في الجزائر وإبراز الجهود الجزائرية في التصدي لمخاطر الهجمات السيبرانية وأهم التحديات التي تواجهها ، لنخاص في الخاتمة إلى الإجابة عن الإشكالية المطروحة واختبار فرضية الدراسة، ملمحين إلى جملة من التوصيات التي من شأنها إعطاء تعزيز أفضل للأمن المعلوماتي الجزائري.

الفصل الأول

الإطار المفاهيمي للأمن المعلوماتي

تمهيد:

حازت مسألة "**الأمن المعلوماتي**" المزيد من الاهتمام على جميع المستويات العالمية والإقليمية والوطنية سواء من جهة ارتفاع عدد الهجمات والتهديدات أو الأضرار الناجمة عنها، حيث شهدت جل دول العالم بما فيهم الجزائر في الآونة الأخيرة اختراقات أمنية مقلقة استهدفت المؤسسات والشركات وحتى الأفراد إلى سرقة البيانات والقرصنة والتجسس والتجنيد والإرهاب الإلكتروني وغيرها. فقد أصبحت هذه التهديدات السيبرانية الجديدة أكثر وسيتم في هذا الفصل التركيز على مفهوم الأمن المعلوماتي والمفاهيم المقاربة له وكذلك نتطرق لمعنى الهجمات السيبرانية وأهم النظريات المفسرة لحقل الأمن المعلوماتي ؟

المبحث الأول: مفهوم الأمن المعلوماتي وعلاقته بالأمن القومي

سنحاول من خلال هذا المبحث الإقتراب من مفهوم الأمن، من خلال التطرق إلى المضامين التي يشتمل عليها ومحاولة التوصل إلى توليفة مفاهيمية بإمكانها التوفيق بين زوايا النظر المتباينة استنادا إلى اختلاف الطروحات الفكرية التي يتم الإنطلاق منها لتحديد هذا المفهوم.

المطلب الأول: تعريف الأمن المعلوماتي:

تعريف أمن المعلومات:Information Security

يقصد بأمن المعلومات حماية وتأمين كافة الموارد المستخدمة في معالجة المعلومات، حيث تؤمن المنشأة نفسها والأفراد العاملين فيها وأجهزة الحاسب المستخدمة فيها ووسائط المعلومات التي تحتوي على بيانات المنشأة وذلك في جميع مراحل تواجد المعلومة(التخزين – النقل – المعالجة). [1]

ويمكن تعريفها من خلال تقسيمها الى ثلاث اقسام عامة:

من الناحية النظرية: هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها.

ومن الناحية التقنية: هي الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية.[2]

[1] مزاش نبيل، أثر الحرب السيبرانية على العلاقات الدولية بين القوى الكبرى في النظام الدولي، مذكرة ماستر (جامعة الحاج لخضر، كلية الحقوق والعلوم السياسية، تخصص: علاقات دولية، 2020–2021). ص12.

[2] حمدون توريه، "الأمن السيبراني في البلدان النامية"، الاتحاد الدولي للاتصالات،(2006)، ص15.

من الناحية القانونية: هي محل الدراسات والتدابير اللازمة لضمان سرية وسلامة محتوى المعلومات وتوفرها ومكافحة أنشطة الاعتداء عليها أو استغلالها في ارتكاب جرائم معلوماتية. وهناك بعض التعريفات الأخرى منها: [1]

تعريف المنظمة الامريكية للتكنولوجيا والمقاييس(CNCS,1994) أن المصطلح يعني: "حماية المعلومات والعناصر التي تساهم في ذلك كالمكونات المادية المستخدمة, في معالجة وتخزين ونقل المعلومات".

تعريف مجمع اللغة العربية في معجم الحاسبات لأمن المعلومات بانها ": حماية المعلومات من الكشف أو الاستنساخ أو التدمير من قبل اشخاص غير مصرح لهم سواء كان عرض اً أو عمداً (معجم الحاسبات، 1995)

تعريف كل من (Whitman& Mattord, 2011) في كتابهما المعنون" مبادئ أمن المعلومات "بأنه "الحفاظ على سرية وتوفر وسلامة المعلومات كأصل، في م ا رحل المعالجة والحفظ والنقل، ويتحقق ذلك عبر التطبيق الفعلي للسياسات الأمنية ومن خلال تعزيز الوعي والتعلم والتدريب."[2]

من خلال ما سبق، يمكن صياغة التعريف الإجرائي التالي:

يتأكد الأمن المعلوماتي من سلامة المعلومات أثناء تواجدها في الفضاء الرقمي، وخلال عمليات نقلها ومعالجتها وتخزينها، مقاوماً جميع التهديدات التي قد تعرض سلامتها للخطر أو تؤدي إلى استغلالها لإلحاق أي ضرر مادي أو معنوي، سواء كان ذلك بالأفراد، أو المجتمعات، أو الهيئات، أو الدول.[3]

خصائص ومميزات أمن المعلومات: Characteristics of Information Security

- يجب أن تكون مناسبة اقتصاديا (ذات جدوى اقتصادية) ـ يجب أن تكون مفهومة للمستخدمين.
- يجب أن تكون واقعية تتناسب مع واقع المنظمة ـ يجب أن تكون متناغمة مع أهداف المنظمة
- يجب أن تكون مرنة وقابلة للمعالجة ـ يجب أن توفر حماية معقولة لأهداف الإدارة المعلنة.

[1] ليال بيطار، "ماذا يعني الأمن السيبارني"؟ من الموقع :https//www.anbaaoline.com 20 جانفي 2018، التوقيت 58:17

[2] سعد علي الحاج علي بكري، "الأمن السيبارني ومعضلة حمايته، عولمة التعليم العالي الرقمي"، جريدة العرب الإقتصادية الدولية، العدد 25، (24 أوت 2017)، ص24.

[3] بن حرز الله فؤاد، الأمن السيبراني وجودة السياسات الأمنية (دراسة في بعض التجارب العربية)، مذكرة ماستر (جامعة الحاج لخضر كلية الحقوق والعلوم السياسية، تخصص: تنظيم سياسي وإداري، 2022-2023).

- يجب أن تكون مستقلة أي (لا تعتمد على أجهزة Hardware ولا برامج Software محددة).

المطلب الثاني: علاقة الامن المعلوماتي بالمفاهيم المشابهة

يرتبط مفهوم الأمن المعلوماتي بعدة مفاهيم مشابهة، لذلك يجب توضيح علاقتين، الأولى بين الأمن المعلوماتي وأمن المعلومات، والثانية بين الأمن المعلوماتي والأمن الإلكتروني.[1]

أ. **الأمن المعلوماتي وأمن المعلومات:** يتجاوز الكثير من الأشخاص الفرق بين "الأمن المعلوماتي" و"أمن المعلومات". من الناحية اللغوية، يتألف مصطلح "الأمن المعلوماتي" من صفة وموصوف، حيث يشير "الأمن" إلى الموضوع الكلي، و"المعلوماتي" إلى الجزء المحدد. وبالتالي، تكون "المعلوماتي" صفة تخص الموضوع الكلي الذي هو الأمن، مما يشير إلى أن الأمن المعلوماتي هو جزء من مجال الأمن بشكل عام، ويعتبر موضوعًا يستحق الدراسة والبحث ضمن إطار العلوم السياسية والعلاقات الدولية.[2]

أما مصطلح "أمن المعلومات" فيتألف من مضاف ومضاف إليه، حيث يُركز على المعلومات ككيان رئيسي، و"الأمن" يأتي كجزء مُحدد منها. وبذلك، يُعتبر "أمن المعلومات" جزءًا تقنيًا من مجال المعلومات، مركزًا على حماية وتأمين المعلومات. ونحن نتناول "أمن المعلومات" كجانب تقني يشمل الدراسة الأكاديمية في مجال الأمن المعلوماتي.[3]

ب. **الأمن المعلوماتي والأمن الإلكتروني:** يهتم الأمن المعلوماتي(Informatiom-Security) بالأمن المتعلق بالمعلومات بغض النظر عن أشكال وطرق حفظ وتخزين هذه المعلومات، بينما يطلق الأمن الإلكتروني(Cyber-Security) (ويسمى كذلك بالأمن السايبيري) على الأمن المتعلق بالمعلومات الموجودة على الوسائط الإلكترونية من وسائط وشبكات. وبذلك تكون العلاقة بين الأمن المعلوماتي والأمن الإلكتروني هي علاقة الكل بالجزء.[4]

---

[1] *Dan Craiyen and others, "Defining cybrescurity", Technology innovation management review, Montreal, Canada, (october 2014).*

[2] Martin C.libicki , Conquestion Cyberspace :National Security and information warfare (New York) :Combridge University Press, 2007.

[3] صحيفة المرصد، "ما هو الأمن السيبراني"، موقع إلكتروني

تاريخ التصفح 2019/3/11. https://al-marsd.com/168664.html

[4] أحمد مختار ،"Cyber Security، هل يمكن تجنب الدولة مخاطر الهجمات الإلكترونية؟"، مجلة مفاهيم المستقبل، العدد 06، بيوت ،لبنان، يناير 2015، ص5.

القوة المعلوماتية:

منذ القدم، كانت المعلومات تحظى بالاهتمام البالغ من القادة في مختلف الحقول، ولاسيما في فترات الحروب. وقد وصف صن زو (sun tzu) الأهمية الاستراتيجية للمعرفة في الحروب قائلاً: "إن معرفتك لنفسك ولخصومك في المعارك المئات لن تجعلك تخسر. وعندما تتجاهل خصومك وتعرف نفسك، ففرصك في النصر أو الهزيمة متساوية. وإذا تجاهلت كليهما، فستكون الخاسر في كل معركة."[1]

أحد المهتمين المعاصرين بالقوة المعلوماتية هو جوزيف ناي، الذي نظر إليها كوسيلة لتحقيق الأهداف باستخدام مصادر المعلومات المرتبطة بالفضاء الإلكتروني. يصف ناي القوة المعلوماتية بأنها "القدرة على استخدام الفضاء الإلكتروني لتحقيق المزايا الاستراتيجية والتأثير على الأحداث ذات الصلة بالبيئات الإلكترونية المختلفة، وذلك من خلال استخدام الأدوات المتاحة."[2]

تتميز القوة المعلوماتية بالنسبية وتقاس بالقدرة على التأثير، مما يعني أن القدرة على التفوق فيها قابلة للتغيير بسرعة، خاصة مع التطورات التكنولوجية السريعة. وقد أظهرت الهند والصين قدرتهما على تحقيق التقدم في هذا المجال بسرعة، مما يجعل الدول الكبرى مثل الولايات المتحدة مقلقة من تلك القوة على الرغم من تفوقها السابق فيها. ويمكن للأجهزة الرقمية البسيطة أن تتسبب في إلحاق الضرر بالتجهيزات التكنولوجية والمعلوماتية الضخمة، مما يظهر مدى الفعالية الكبيرة للقوة المعلوماتية.[3]

المطلب الثالث: أبعاد الأمن المعلوماتي .

أبعاد الأمن المعلوماتي: باعتبار توسع مفهوم الأمن وشموله لقطاعات جديدة، وباعتبار معلومات تشمل كل النواحي السياسية والعسكرية والاقتصادية والاجتماعية، فإن الأمن المعلوماتي ينسحب على قطاعات مختلفة يمكن إجمالها في الأبعاد التالية:

أ. البعد السياسي:

توسيع نطاق الخدمات الإدارية عبر الإنترنت، ونشر حكومات إلكترونية وربط الدوائر الحكومية

[1] بوزيدي ذكرى، " الحرب السيبرانية واستخداماتها الأمنية والإستراتيجية : دراسة حالة الحرب السيبرانية الروسية تجاه إستونيا، جورجيا، أوكرانيا مذكرة ماستر (جامعة الحاج لخضر كلية الحقوق والعلوم السياسية، تخصص: علاقات دولية، 2022-2023).

[2] Joseph S. Nye, "Cyber security",(Cambridge : Harvard Kennedy School, Belfer center for science and international affairs), May 2010, P4.

[3] أوس مجيد غالب العوادي، "الأمن المعلوماتي السيبارني"، (بيروت، مركز البيان للدراسات والتخطيط، 2016)، ص06.

بشبكات المعلومات، جعل أمن البيانات والشبكات أحد جوانب الأمن القومي، حيث يمثل خطر الاختراق أو الكشف عن هذه البيانات أو تعرضها للتدمير تهديدًا جديًا.[1]

تمكين المواطنين للاستفادة من خدمات الإنترنت يعزز سرعة الخدمة ويوفر الوقت والجهد، مما يجعل حماية هذه الشبكات وأمانها وضمان استمرارية الخدمة ضرورة ملحة.[2]

يزيد من أهمية البعد السياسي للأمن المعلوماتي تسريب المعلومات واستخدامها في الحملات الانتخابية، كما حدث في الانتخابات الرئاسية الأمريكية عام 2016، حيث تبادلت الاتهامات بشأن القرصنة الروسية. كما يؤثر ذلك على الرأي العام وإدارة الاحتجاجات والمظاهرات، كما في حالة "أوراق بنما".[3]

ب. البعد العسكري:

تتعرض الأنظمة العسكرية بشكل متزايد لهجمات في عمليات التجسس، حيث تستهدف العديد من الدول هذه الأنظمة بهدف الحصول على تصاميم الأسلحة، أو الاستيلاء على المعلومات الحساسة، أو فهم طرق التفكير للأعداء المحتملين، أو التحضير لتعطيل الشبكات وحجب الخدمات الأساسية أثناء الحروب. يُعتبر أي نظام مرتبط بالإنترنت عرضة للخطر في هذا السياق.

تأخذ أهمية السيطرة على المجال الإلكتروني زيادة مع استخدام التكنولوجيات المتقدمة والأسلحة الحديثة التي تخلو عن العنصر البشري لتحل محله بالعناصر الآلية والبرمجية. ومن بين هذه التقنيات، طائرات بدون طيار وصواريخ ذكية تستند إلى معلوماتها عن البيئة المحيطة بها لتحديد مساراتها.[4]

كما تعد حروب الفضاء الإلكتروني اليوم أحد المخاطر دائمة التوقع، حيث تنظم العمليات العسكرية في الفضاء الإلكتروني وتستهدف فيها المعلومات فتستولي عليها أو تدمرها، وتستهدف المعدات فتعطلها أو تفجرها، وتستهدف المعنويات فتثبطها أو تشوشها، فضلا عن طرق البرمجة والزرع وإمكانيات الظهور والتنفيذ في أي لحظة. اعتبرت المملكة المتحدة (بريطانيا) أن الهجوم عبر الفضاء الإلكتروني يشمل أحد التهديدات الأمنية اربعة الأكثر خطورة التي تواجهها بريطانيا إلى جانب الإرهاب، والصراعات الإقليمية، والكوارث الطبيعية، حيث عمدت وفي ظل حالة تقشف إلى إضافة نحو 650 مليون جنيه استرليني إلى التمويل المتاح للفترة 2011 إلى 2015 لتعزيز أمن الفضاء الإلكتروني.

---

[1] نوارن شفيق، "أثر التهديدات الالكترونية على العلاقات الدولية، دارسة في أبعاد الأمن الالكتروني"، (القاهرة، المكتب العربي للمعارف، 2014)، ص23.

[2] سوسن زهير المهتدي، تكنولوجيا الحكومة الإلكترونية، عمان: دار أسامة، 2011، ص 24.

[3] سعد علي الحاج بكري، "الأمن السيبراني ومعضلة حمايته"،الرابط: www.alegt.com/article1241506.html، تاريخ التصفح يوم 2019/03/04.

[4] Fred Schreier, On Cyberwarefare, DCAF horzon 2015 Working paper No, 07.

ت. البعد الشخصي:

ما يتركه المستخدمون من معلومات وبيانات على مواقع التواصل الاجتماعي، بمحض إرادتهم وترددهم في استعمالها بشكل يومي، يجعل عملية فحص ومراقبة هذه البيانات واستخراج المعلومات الصحيحة منها عملية سهلة للغاية. هذا يزيد من إمكانيات استغلال وتوظيف المعلومات الشخصية والهويات بواسطة المحترفين في الجريمة، مما قد يؤدي إلى عواقب مدمرة على صعيد الأفراد وخصوصياتهم.[1]

بالإضافة إلى ذلك، جهود الحكومات في اعتماد نظم الحكومات الإلكترونية وجمع وتخزين كافة المعلومات الشخصية والبيولوجية والاجتماعية لكل فرد في ملف خاص به، تجعل اختراق تلك الأنظمة أو تسرب المعلومات منها يحمل عواقب شخصية وأمنية خطيرة قد لا تُضاهى بالخطر الأكبر.[2]

ث. البعد الاقتصادي:

تورد شركة سيمنتاك الأمريكية المتخصصة في أمن المعلومات وصاحبة مضاد الفيروسات الشهير نورتون (Norton Antivirus) في تقريرها لسنة 2011 أن تكلفة جرائم المعلومات سنة 2011 قدرت بنحو 388 مليار دولار أمريكي، وهي أكبر من السوق السوداء لمخدرات الماريخوانا والكوكايين والهيروين مجتمعين التي تقدر ب 288 مليار دولار، وهي اعلى من الإنفاق السنوي لمنظمة الأمم المتحدة للأمومة والطفولة "اليونيسيف" بنحو 100 ضعف، حيث تصل ميزانيتها إلى 3.65 ملايير دولار.[3]

تسود معظم اقتصاديات العالم اليوم بواسطة شبكة اتصالات عالمية مترابطة، وأي انقطاع في أي منطقة من العالم سيؤثر سلبًا على الجميع. ونظرًا لامتداد هذه الشبكة عبر العالم، فإن ذلك يعني أن هناك أجزاءً كبيرة معرضة للهجوم وغير محمية بشكل كافٍ. ومع ذلك، فإن الهجوم لا يتطلب أدوات كبيرة أو تكاليف عالية أو أعدادًا كبيرة من الأفراد، لكن الأضرار التي يمكن أن تلحقها الهجمات تكون كبيرة ومدمرة.[4] لذلك، فإن حماية هذه المصالح الاقتصادية المنتشرة عبر العالم تعد هدفًا حيويًا لجميع الأطراف: الدول، والمنظمات غير الحكومية، والمؤسسات الحكومية، مما يزيد من الحاجة إلى تطبيق استراتيجيات عالمية لتعزيز الأمن.

تتحد الأطراف العظمى وغير العظمى مصالحها في الحفاظ على استمرارية النظام الاقتصادي العالمي، وتحقيق أمنه وسلامته.[5] وتبرز أهمية الأمن المعلوماتي في الجانب الاقتصادي بشكل واضح، حيث

---

[1] عنترة بن مرزوق، "الأمن السيبراني كبعد جديد من السياسة الجزائرية"، محاضرات مقدمة لطلبة جامعة محمد بوضياف – المسيلة، كلية الحقوق والعلوم السياسية، د س، ص65.

[2] سوسن زهير المهتدي، مرجع سابق، ص27-28.

[3] تقرير نورتون لجرائم المعلوماتية 2011.

[4] عامر مصباح، المنظورات الاستراتيجية في بناء الأمن. القاهرة: دار الكتاب الحديث، 2013، ص149.

[5] مصباح، المرجع السابق، الصفحة نفسها.

يشكل التجسس الصناعي خطرًا على السباق التكنولوجي ويهدد استغلال المعلومات والسيطرة على الصفقات والأسواق.

ج. البعد الاجتماعي:

إن ارتباط أكثر من نصف سكان الأرض بالشبكة المعلوماتية العملاقة،[1] والتواصل المتاح بها، يحدث في سياق تنوع الثقافات والإيديولوجيات، وتواجد عمليات الاستقطاب المذهبية والطائفية. يُعتبر توظيف الاختلافات المذهبية والعرقية أحد أسباب الحروب والنزاعات، ويُعتبر من أهم التهديدات التي تُعرض لها استقرار الدول سياسيًا واجتماعيًا.

بفضل تطور قدرة التفاعل اللحظي عبر شبكات التواصل الاجتماعي في الإنترنت، وقدرة هذه الشبكات على التأثير والتوظيف في زرع المذهبية والطائفية، فقد أصبحت عمليات التجنيد لصالح تنظيمات الإرهاب والجريمة المنظمة أسهل وأكثر فعالية. وهذا يجعل من حماية المجتمع ومكوناته الاجتماعية والثقافية أحد أبعاد الأمن المعلوماتي، الذي كانت ثورات الربيع العربي تجسده واحدًا من جوانبه. فعلى الرغم من الفوائد الكبيرة للتكنولوجيا والاتصالات، إلا أنها أيضًا تثير تحديات جديدة تتعلق بالأمن والاستقرار، وتستدعي استراتيجيات شاملة لمواجهتها بشكل فعال ومنع استغلالها في الأنشطة الإرهابية والمتطرفة.

المبحث الثاني: مفهوم الهجمات السيبرانية

يهدف هذا المبحث إلى إبراز معنى الهجمات السيبرانية وانواعها ومن هم المتضررون من هذه الهجمات .

المطلب الأول: تعريف الهجوم السيبراني

إن الهجوم السيبراني أو الهجوم الإلكتروني عبارة عن شن هجمات من قبل بعض المجرمين أو المحتالين أو المخترقين من خلال جهاز كمبيوتر أو مجموعة من الأجهزة أو من خلال شبكات لمداهمة جهاز شخص أو شبكة شخص أخر أو لهدف تعطيل جهاز الكمبيوتر المستهدف أو الغرض منها الوصول إلى بيانات جهاز الكمبيوتر المستهدف أو سرقتها أو استغلالها في أمور احتيالية، فالهجمات السيبرانية في صحيح الأمر عبارة عن القيام باختراق أنظمة خاصة سواء بأفراد أو شركات أو مؤسسات، حيث أنه في أغلب الأوقات يقوم المهاجمون بخرق الأنظمة الإلكترونية الضعيفة، ويقومون بطلب أموال مقابل إعادتها أو عدم تعطيلها، بحيث يسفر هذا الهجوم السيبرانى عن خسارة لأموال الأفراد أو الشركات أو مؤسسات[2].

[1] مجموعة البنك الدولي، تقرير عن التنمية في العالم 2016: العوائد الرقمية، ص6.

[2] منى الأشقر جبور، "الأمن السيبراني: التحديات ومستلزمات المواجهة"، (جامعة الدول العربية: المركز العربي للبحوث القانونية والقضائية، 2012)، ص03.

والجدير بالإشارة أن هؤلاء المجرمين والمخترقين يقومون بهجماتهم السيبرانية باستخدام مجموعة متعددة من الأساليب التي تساعدهم على شنها، كما أنه للأسف قد تكون تلك الهجمات السيبرانية جزء من شن حرب إلكترونية ما على مؤسسات دولة بأكملها[1].

المطلب الثاني: أنواع الهجمات السيبرانية أو الإلكترونية

يوجد العديد من أنواع الهجمات السيبرانية المختلفة، ويعد من أشهر أنواع الهجمات السيبرانية حول العالم :

1-الهجوم السيبرانى من خلال استخدام البرامج الضارة: حيث أنه في حين استخدام الأشخاص لبرامج أو تطبيقات غير موثقة أو غير متعارف على مصدرها، فإنه من المحتمل أن تحمل تلك البرامج برامج ضمنها تتثمل في برامج تجسس، أو تحمل ملفات تتضمن فيروسات مضرة للجهاز المستخدم أو الديدان الإلكترونية التي تعمل على تعطيل أو وقف وظائف الأجهزة المستخدمة[2].

كما أنه أيضاً في حال زيارة بعض المواقع الغير موثوق فيها والنقر على الروابط التي تتضمنها، فإنه من المحتمل حدوث تثبيت تلقائي لبعض البرامج الضارة، والتي تقوم بالحصول على المعلومات والبيانات سراً عن طريق نقلها من القرص الصلب الخاص بالجهاز أو الهاتف المستخدم، أو تقوم بتعطيل بعض مهام النظام المستخدم في العمل، أو تعطيل ومنع الوصول إلى الشبكات الرئيسية مما قد يحمل معه العديد من الخسائر الفادحة[3].

2-الهجوم السيبرانى من خلال استخدام تصعيد المعلومات: يعد الهجوم السيبرانى من خلال استخدام تصعيد المعلومات أحد أخطر التهديدات الإلكترونية الشائعة، وتتم تلك الهجمات بإرسال رسائل إحتيالية لتبدو وكأنها من مصدر موثوق عبر البريد الإلكتروني لخداع المستهدف للقيام بالعديد من الأعمال الضارة كسرقة البيانات التي تكون في غاية السرية، كمعلومات بطاقة الائتمان، ومعلومات تسجيل الدخول، أو حتى لتثبيت برامج ضارة على الجهاز المعنى بالهجمة السيبرانية[4].

3-الهجوم السيبرانى من خلال هجوم الوسيط: حيث تسمى هنا بالهجمات السيبرانية الوسيطة وهي هجمات التنصت، والتي تسفر عن سرقتهم للبيانات بمجرد حصولهم على إمكانية المرور، حيث يتمكن

---

[1] أحمد عبيس نعمة الفتلاوي، "الهجمات السيبارنية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر"، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد الرابع، (السنة الثامنة، 2016)، ص 24.

[2] بن الشريف لامية، خلالفة خديجة، "مكانة الأمن السيبراني في السياسات الدفاعية الجزائرية" مذكرة ماستر (جامعة الحاج لخضر كلية الحقوق والعلوم السياسية ،تخصص: علاقات دولية، 2018-2019).

[3] تولاي آسر، "ما هي السيبارنية؟ وما دورها في صناعة القرار"؟ 20 جانفي 53:17/2018

http//Zeitgeistarrabia.com

[4] أحمد المشد، القرصنة الإلكترونية وأمن المعلومات، ط1، مصر: مؤسسة الأمة العربية للنشر والتوزيع، 2017.

المهاجم من إقحام نفسه بين المستخدم وشبكات الاتصال بالإنترنت والوصول إلى كافة البيانات بمجرد الارتباط بتلك الشبكات غير الموثوقة، أو القيام بتثبيت برامج ضارة للتمكن من اختراق جميع المعلومات بمجرد اختراق الجهاز[1].

4- الهجوم السيبرانى من خلال هجوم الحرمان من الخدمات: تعمل هجمات الحرمان من الخدمات على اقتحام الأنظمة أو الخوادم أو الشبكات بهدف السيطرة على مواردها ومعدل نقل بياناتها، بحيث يصبح النظام غير قادر على تلبية الأوامر اللازمة أو المطلوبة منه.

5- الهجوم السيبرانى من خلال الهجمات دون الانتظار أو هجمات يوم الصفر: فالهجمات دون انتظار عبارة عن ثغرات لم تحل، فهي تحدث دون الانتظار عقب إعلان وجود ثغرة أمنية في الشبكة أو النظام قبل إمكانية تنفيذ معالجة تلك الثغرات أو تصحيحها وتلك التقنيات المستخدمة والتي تسمى بتقنيات استغلال الثغرات تباع معظمها على الدارك ويب، كما أن المهاجمون دائماً ما يستهدفون الثغرة الأمنية التي جرى الكشف عنها خلال فترة إيجاد الحل لها[2].

6- الهجوم السيبرانى من خلال الاتصال النفقي عبر أسماء النطاقات: وتتم تلك الهجمات من خلال التلاعب بطلبات أسماء النطاقات بغرض نقل البيانات من النظام المخترق إلى جعبة المهاجم، ويُمكن استخدامها كذلك في تمرير الأوامر، وإرسالها من جانب المهاجم إلى النظام الذي تم اختراقه[3].

7-الهجوم السيبرانى من خلال التعدين الخبيث: ومن خلال هذا الهجوم يتم السيطرة على جهاز الكمبيوتر الخاص بأحد الأشخاص واستغلالها في تعدين العملات الرقمية المشفرة.

8-الهجوم السيبرانى من خلال هجمات طلب الفدية: وتتم تلك الهجمات من خلال بعض البرمجيات الخبيثة والتي تسمى بالرانسوم وير والتي تصمم لتشفير ملفات الضحايا المستهدفين بالهجمات أو التهديد بنشر البيانات الخاصة بهم ما لم يتم دفع المبالغ المطلوبة خلال المدة المحددة[4].

المطلب الثالث: ضحايا الهجمات السيبرانية

[1] منى الأشقر جبور، "السيبارنية هاجس العصر"، (بيروت، المركز العربي للبحوث القانونية والقضائية، 2013)، ص29

[2] فتيحة ليتيم، ونادية ليتيم، "الأمن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة"، (جامعة بسكرة، مجلة المفكر، العدد 12، (د.س.ن) ص239.

[3] منى الأشقر جبور، "الأمن السيبارني: التحديات ومستلزمات المواجهة"، المركز العربي للبحوث القانونية والقضائية، (مايو2012)، ص16.

[4] كلثوم بيبيمون، السياقات "الثقافية الموجهة للهوية الرقمية في ضوء تحديات المجتمع الشبكي من التداول الافتراضي إلى الممارسات الواقعية"، مجلة "إضافات" العدد 23، (ربيع2016)، ص26.

ضحايا الجرائم السيبرانية يمكن أن يكونوا أفرادًا أو منظمات. كما أنهم يتعرضون للهجمات السيبرانية التي تستهدف الأنظمة والشبكات والمواقع الإلكترونية والحسابات الشخصية، وتتركز الجرائم السيبرانية في سرقة البيانات والمعلومات الحساسة والمال والهوية الشخصية والحقوق الفكرية[1]. وتتضمن الضحايا:

1/ الأفراد: قد يكون الأفراد ضحايا للهجمات السيبرانية عبر اختراق حساباتهم الشخصية، سرقة هويتهم الرقمية، انتهاك خصوصيتهم، احتيال إلكتروني، أو انتهاك سرية المعلومات الشخصية.

2/ الشركات والمؤسسات: كما قد تستهدف الشركات والمؤسسات بغرض سرقة المعلومات التجارية، تعطيل العمليات، تشويه السمعة، ابتزاز المال، أو تعريض بيانات العملاء للخطر[2].

3/ الجهات الحكومية: فمن الممكن أن تكون الحكومات ضحية للهجمات السيبرانية التي تستهدف البنية التحتية للدولة أو السرية الوطنية أو البيانات الحكومية الحساسة[3].

4/ المؤسسات العامة والمنظمات غير الربحية: كما قد يتعرض مستشفيات وجامعات ومؤسسات غير ربحية أخرى لهجمات سيبرانية تهدف إلى تعطيل الخدمات أو سرقة المعلومات أو انتهاك خصوصية البيانات.

بشكل عام يمكن أن تتسبب الجرائم السيبرانية في خسائر مادية ومعنوية للضحايا، بما في ذلك فقدان الأموال والبيانات والثقة والسمعة والخصوصية[4].

---

[1] نوارن شفيق، "أثر التهديدات الالكترونية على العلاقات الدولية، دارسة في أبعاد الأمن الالكتروني"، (القاهرة ،المكتب العربي للمعارف، 2014)، ص40.

[2] عادل عبد الصادق، "الحروب السيبرانية: تصاعد القدرات والتحديات للأمن العالمي"، (المركز العربي لأبحاث الفضاء الإلكتروني، د.ش ،2017)، ص02.

[3] سعيدة رشاش، "مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري"، مذكرة ماستر (جامعة العربي التبسي تبسة، تخصص: دراسات استراتيجة، 2017-2018).

[4] مزيود، سليم، الجرائم المعلوماتية واقعها في الجزائر وآليات مكافحتها، جامعة المدية، الجزائر، (2015).

المبحث الثالث: النظريات المفسرة للأمن المعلوماتي

إن صياغة مفهوم دقيق للأمن قد يبدو أمرا صعبا بالنظر لتعدد الأطر النظرية والاتجاهات الفكرية التي تناولته فقد قدمت هذه الأخيرة تصورات مختلفة وعديدة لهذا المفهوم، الذي لا يزال حتى الأن يتبلور وفق ما تقتضيه المتغيرات والتحولات المتسارعة في السياسة الدولية. لقد أتت هذه المقاربات التفسيرية للأمن كتعبير عن شواغل القوى العالمية ورد فعل تجاه المعطيات الجديدة، الأمر الذي أتاح لها إجراء تغيير وتحديث في فكرها الإستراتيجي بفضل أرمادة من الباحثين والمنظرين في حقلي العلاقات الدولية والدراسات الأمنية بالأخص الذين أسهموا بشكل بارز (الحوارات الأمنية) في تجاوز الأطر التقليدية للأمن، حيث – بحسبهم– أنها لم تعد قادرة على التحليل والتفسير في ظل التحديات والرهانات الجديدة في البيئة الدولية الراهنة.

المطلب الأول: الأمن في الاتجاه الواقعي الجديد:

يعد الأمن الهدف الأسمى الذي يصبو إلى تحقيقه الواقعيون الجدد في تنظيرهم للعلاقات الدولية في إطار الواقعية الجديدة وذلك بدلا وذلك بديلا عن الكلاسيكيين الذين يسعون إلى القوة وهو ما أدى ببعض المحللين في العلاقات الدولية إلى تصنيف الواقعية الجديدة.[1]

ورغم إقرار الواقعيين الجدد بالهدف الأمني، إلا أن والتز وغيره من الواقعيين جدد يعترفون بفكرة مفادها أن الدولة العقلانية هي تلك التي تسعى إلى القوة عندما يكون الهدف الأمني قد تحقق، وفي هذا السياق ظهر المفكر مارشهيمر وكأنه يناقض والتز في هذه الفكرة معتبرا أن الدول تهدف بشكل أو بأخر إلى زيادة قوتها وبالتحديد قوتها العسكرية، ثم يعود ليعترف بأهمية الهدف الأمني على أن لا يكون ذلك على حساب هذه القوة، فالدول تسعى إلى تحقيق أقصى قدر ممكن من الأمن تدعيم قوتها العسكرية في نفس الوقت، فرغم تراجع الترتيب الاستراتيجي العسكري العالمي، إلا أن الواقعيين الجدد بزعامة مارشهيمر يصرون على أهمية القوة العسكرية كمحدد أساسي للتأثير على الدول الكبرى والتحكم في علاقاتها.[2]

علما أن مفهوم الأمن لدى الواقعين الجدد أقترن بعنصر الخوف لاعتقادهم أن هذا الأخير ناتج عن حالات الأمن المنبثقة من الفوضى وهو ما يميزهم عن الواقعين الكلاسيكيين الذين يربطون القوة بالغريزة

[1] عبد الناصر جندلي، التنظير في العلاقات الدولية بين الاتجاهات التفسيرية والنظريات التكوينية. ط1، (الجزائر: دار الخلدونية للنشر والتوزيع، 2007)، ص100.

[2] عبد الناصر جندلي، أثر الحرب الباردة على الاتجاهات الكبرى والنظام الدولي، مرجع سابق، ص 201.

العدوانية والشريرة للطبيعة البشرية، أما إذا كان الأمن من حيث نظرته أو توافره مرتبط بعملية إدراكية من طرف صانع القرار، فإن فكرة الأمن في الواقعية الجديدة أدت إلى إنقسام أنصارها إلى فريقين:[1]

الواقعين الهجوميون والواقعيون الدفاعيون، فالواقعيون الهجوميون وعلى رأسهم جون مارشهيمر وروبرت غيبلين يرون بصعوبة توفير الأمن في النظام الدولي، بينما يرى الواقعيون المدافعون وعلى رأسهم كينيث والتز وغريكو بتوافره رغم الفوضى التي يتميز بها النظام الدولي، وينظرون إليه كلعبة غير صفرية مع تفاؤلهم لوضع حد لوقوع الحرب، كما أن القوة حسب الواقعيين الهجوميين هي وسيلة ذات أهمية قصوى لتعظيم المكاسب معتبرين العلاقات الدولية بأنها لعبة صفرية أما القوة حسب الواقعيين الدفاعيين فإنها وسيلة لتحقيق الأهداف الضرورية، وهي أهداف ترتبط بالأمن معتبرين أن العلاقات الدولية هي عبارة عن مأزق السجين أو مأزق أمني معقد وهي إختلافات عميقة ظهرت من خلال المحاورة بين الواقعيين الهجوميين والدفاعيين حسب جاك سنايدر[2].

المطلب الثاني: الأمن من وجهة نظر مدرسة كوبنهاغن

تأسّس الاتجاه النقدي في الدراسات الأمنية مكوّنا من ثلاث مدارس متميّزة، بحيث تطورت مدرستي أبريستويث و**كوبنهاغن** عبر اجتهادات خبراء العلاقات الدولية والأمن الدولي والدراسات الإستراتيجية وبرامج البحث في السلام الدولي، بينما استعانت مدرسة باريس بخبراء علم الإجتماع السياسي والإجرام والقانون والعلاقات الدولية وخبراء في الأمن الداخلي.

وتعتبر مدرسة كوبنهاغن من المدارس الأمنية التي نادت بضرورة توسيع الأجندة الأمنية خاصة بعد الحرب الباردة، وذلك بعد ظهور العديد من التهديدات الجديدة التي تهدد أمن الدول[3]، فإن أهمية موضوع المن يكمن في كونه المحور الأساسي في الأطر والمقتربات النظرية ، فهو إحدى عمليات السياسة العالمية ، وظل يشكل هاجس كبير لرجال الدولة وصناع القرار الذين اعتبروا أن ضمان البقاء والاستمرار هي من أولويات السياسة العليا للدولة.

---

[1] عبد الناصر جندلي، نفس المرجع، ص 203-202.

[2] عادل زقاغ، مترجما (مفهوم الأمن في نظرية العلاقات الدولية)، الموسوعة الجزائرية للدراسات السياسية والإستراتيجية، 16جانفي 2021، على الرابط https://www.polityics-dz.com

[3] أمينة دير، أثر التهديدات البيئية على واقع الأمن الإنساني في إفريقيا: دراسة حالة دول القرن الإفريقي، مذكرة مقدمة لنيل شهادة الماجيستير في العلوم السياسية والعلاقات الدولية، تخصص علاقات دولية واستراتيجية، جامعة محمد خيضر، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية، 2014، ص18.

ومع تزايد اعتماد الدول على الأنترنيت لتسيير المهام والتحول الكامل نحو السيبرانية في كافة جوانب الحياة تزايد نشاط القراصنة مستغلين ضعف الثقافة الأمنية وهذا سبب في تهديد أمن الدول والأفراد ، وفي ضمن مجالات الدراسات الأمنية يمكن فهم دور الأمن السيبراني وهو ما تجلى في أعمال مدرسة كوبنهاغن وروادها أمثال، أولي ويفر وباري بوزان حيث اكتسبت أعمالهم أهمية كبيرة خاصة عند التفكير في الأمن السيبراني، لأن تركيزهم لم يقم على محاولة موضوعية لتصنيف ماهو التهديد أو ماهي الثغرة المنية، بل ماهي الشروط أو الحالة الراهنة التي يجب أن تباشرها جهات فاعلة محددة من أجل إظهار فعل ما بأنه تهديد وهو ما يعرف بـ: عملية الأمننة the process of securisation.[1]

ويتمحور جوهر نظرية الأمننة Securisation theory حول تبيان ان السياسات المؤطرة للأمن ليست مفروضة على الدول وليست أمر مسلم به في حد ذاته ولكنها سياسات مصممة من قبل السياسيين وصناع القرار أو ما يعرف بـ الفاعل المؤمنن a securizing actor حينما يقومون باستغلال ظرفا دوليا بتصويره للمستهدفين بهذه السياسات كما ولو انه أمرا جللا أو تهديدا بالغ الضراوة أو جائحة مهلكة[2]، فالأمننة هي عملية يتم فيها تحويل المشاكل إلى قضايا أمنية من خلال إضفاء الطابع الأمني عليها.

ومن اسهامات مدرسة كوبنهاغن وباري بوزان على وجه التحديد في الدراسات الأمنية هو توسيع مفهوم الأمن وعدم حصره بالجانب التقليدي العسكري ليشمل بعد ذلك أبعاد وقطاعات توسعية جديدة كالقطاع السياسي والإجتماعي والإقتصادي والبيئي، مؤكدا على أنه لا يمكن من هذه القطاعات منفردة التعبير بشكل كافي عن المسألة الأمنية ، فكلها مرتبطة ارتباط وثيق.[3]

ومن الأمور المتعارف عليها في العلاقات الدولية أن مصادر قوة الدول تتغير فإلى جانب القوة الصلبة المتمثلة في القدرات العسكرية ومع ظهور ثورة المعلومات ظهر شكل جديد من القوة وهو القوة السيبرانية cyber power فأدت إلى انتشار القوة بين عدد لأكبر من الفاعلين ما جعل قدرة الدولة على السيطرة موضع شك.[4]

---

[1] صباح بالة، مدرسة كوبنهاغن في تفسير الدراسات الأمنية، الموسوعة السياسية، 9 ديسمبر 2020، متاح على الرابط التالي: https://political-encyclopedia.org/dictionary

[2] عادل زعلوك، نظريات الأمننة في مجال العلاقات الدولية: مدرسة كوبنهاغن نحو نظرية اتصالية مقترحة لدراسة الأمننة، مجلة السياسة والإقتصاد، المجلد 15، العدد 14، أفريل 2022، ص1-37.

[3] سليم قسوم، الاتجاهات الجديدة في الدراسات الأمنية: دراسة في تطور مفهوم الأمن في العلاقات الدولية. الإمارات العربية المتحدة، مركز الامارات العربية للدراسات والبحوث الإستراتيجية.

[4] سيد أحمد قوجيلي، " الدراسات الأمنية النقدية –مقاربة جديدة لإعادة تعريف الأمن، ط1، عمان، المركز العربي للدراسات السياسية،2014، ص45.

المطلب الثالث: نظرية القوة السيبرانية(Cyber Power Theory)

تشير هذه النظرية إلى أن الدول يمكنها استخدام القوة السيبرانية كأداة لتحقيق أهدافها السياسية، سواء من خلال الدفاع عن أنظمتها أو الهجوم على أنظمة الدول الأخرى[1]. ومع تحول الفضاء الإلكتروني إلي ساحة للتفاعلات الدولية، برز العديد من الأنماط التوظيفية له، سواء على صعيد الاستخدامات ذات الطبيعة المدنية أو العسكرية، الأمر الذي جعل هذا الفضاء مجالا للصراعات المختلفة، سواء للفاعلين من الدول أو غير الدول لحيازة أكبر قدر من النفوذ والتأثير السيبراني.

في هذا السياق، تبلورت ظاهرة «الحروب السيبرانية» Cyber Wars، التي اتسمت بخصائص مختلفة عن نظيراتها التقليدية، من حيث طبيعة الأنشطة العدائية، والفواعل، والتأثيرات في بنية الأمن العالمي. وعبرت تلك الحرب عن نمطين من القوة (الناعمة والصلبة) في عملية توظيف التفاعلات في الفضاء الإلكتروني، مما يعكس تنامي القدرات والتهديدات المتصاعدة لأمن البنية التحتية الكونية للمعلومات.

يتعلق مضمون الحرب الإلكترونية بالتطبيقات العسكرية للفضاء السيبراني، حيث تعني –في أحد تعريفاتها– قيام دولة أو فواعل من غير الدول بشن هجوم إلكتروني في إطار متبادل، أو من قبل طرف واحد. وبرغم ذيوع مسمي "الحرب الإلكترونية" إعلاميا، فإنه يعد مصطلحا قديما كان بالأساس مقصورا على رصد حالات التشويش على أنظمة الاتصال، والرادار، وأجهزة الإنذار، بينما يكشف الواقع الراهن في الفضاء الإلكتروني دخول شبكات الاتصال والمعلومات إلى بنية ومجال الاستخدامات الحربية.[2]

وفقا للمفهوم التقليدي للحرب، فإنها تنطوي على استخدام الجيوش النظامية، ويسبقها إعلان واضح لحالة الحرب، وميدان قتال محدد، بينما تبدو هجمات الفضاء الإلكتروني غير محددة المجال، وغامضة الأهداف، لكونها تتحرك عبر شبكات المعلومات والاتصالات المتعدية للحدود الدولية، إضافة إلى اعتمادها على أسلحة إلكترونية جديدة تلائم طبيعة السياق التكنولوجي لعصر المعلومات، إذ يتم توجيهها ضد المنشآت الحيوية، أو دسها عن طريق عملاء لأجهزة الاستخبارات.

4 Nye, J. S. (2010). "Cyber Power." Harvard Kennedy School. Belfer Center for Science and International Affairs.

[2] عبد الله زراب، النظرية السيبرانية، توظيف الفضاء الإلكتروني في تعظيم قوة الدول، تاريخ النشر: 21نوفمبر2017 تم الإطلاع عليه في 2024/05/22 من الموقع :https://aafaq.kku.edu.sa/news /

خلاصة الفصل:

من خلال ماتم التطرق له في الجانب النظري للأمن السيبراني هو مجموعة من الإجراءات والتدابير التي يتم اتخاذها للحد من مخاطر الهجمات السيبرانية التي تستهدف عادة الوصول إلى المعلومات الحساسة أو تغييرها أو إتلافها أو ابتزاز المستخدمين لها، حيث صار الأمن السيبراني وسيلة هامة لتأمين هذه المعلومات البالغة الأهمية والبيانات الشخصية، فالهدف منه إذن هو حماية الفضاء السيبراني من التهديدات والمخاطر الإلكترونية التي تستهدفه.

ونظرا للعلاقة القوية بين الأمن السيبراني والأمن القومي للدول ، نجدها تسعى جاهدة لاستخدام أحدث التقنيات الإلكترونية ورفع كفاءة المتخصصين في مجال الأمن السيبراني مع تظافر الجهود القانونية وتعزيز وعي المجتمع بضرورة وأهمية الأمن السيبراني للوقاية من مخاطر الهجمات السيبرانية.

الفصل الثاني

طرق الإختراق الرقمي في الجزائر

تمهيد

لقد أفرزت التحولات الأمنية خاصة بعد الحرب الباردة إلى يومنا هذا أثرا كبيرا على الأمن الوطني لجميع الدول، وكانت الدولة الجزائرية واحدة من تلك الدول، حيث عرفت الجزائر ومنذ استقلالها مجموعة من التهديدات الأمنية أثرت على أمنها واستقرارها، وبروز العديد من الفواعل الداخلية والخارجية ساهمت في المساس وتخريب بعض المنصات والمواقع لقطاعات مختلفة وهذا راجع لهشاشة نظم الحماية ومن أبرزها الإختراق الذي هو جزء من الهجمات السيبرانية الأقل خطرا .

المبحث الأول: مفهوم الإختراق الرقمي

يهدف هذا المبحث إلى تقديم نظرة عن مشكلة الإختراق التي غزت العالم بكل منظوماته ولم تسلم منه أي جهة لذا كان لزاما علينا التعريج على مصطلح الإختراق وأسبابه واهم فواعله .

المطلب الأول: تعريف الإختراق الرقمي

تتصل أنظمة الحواسيب بالشبكات لتسهيل التواصل مع الأطراف الأخرى وإنجاز الأعمال بطريقة سلسة وسهلة، ولكن يعرض الاتصال بالشبكة الحواسيب للاختراق الإلكتروني، ويُقصد باختراق النظام استخدام أجهزة الكمبيوتر لارتكاب أعمال احتيالية مثل الاحتيال، وانتهاك الخصوصية، وسرقة بيانات الشركة أو البيانات الشخصية، وما إلى ذلك، حيث تكلف الجرائم الإلكترونية العديد من المؤسسات ملايين الدولارات كل عام لحماية نفسها ضد مثل هذه الهجمات.[1]

يشير الاختراق الإلكتروني إلى الأنشطة التي تسعى إلى اختراق الأجهزة الرقمية، مثل أجهزة الكمبيوتر والهواتف الذكية والأجهزة اللوحية وحتى الشبكات بأكملها، وعلى الرغم من أن القرصنة قد لا تكون دائمًا للأغراض الخبيثة، إلّا أنها نشاط غير قانوني من قبل مجرمي الإنترنت – مدفوعًا بالمكاسب المالية والاحتجاج وجمع المعلومات (التجسس)، وحتى لمجرد "المتعة" من التحدي.[2]

يعد الاختراق الإلكتروني نشاط يحدد نقاط الضعف في نظام الكمبيوتر أو الشبكة لاستغلال الأمان، يمكن أن يكون أحد الأمثلة على قرصنة الكمبيوتر: استخدام خوارزمية تكسير كلمة المرور للوصول إلى نظام الكمبيوتر.

[1] Lawrence Williams (11/12/2021), "What is Hacking? Types of Hackers: Introduction to Cybercrime", guru99, Retrieved 20/1/2022.

[2] "Hacking", malwarebytes, Retrieved 20/1/2022.

المطلب الثاني: دوافع وخصائص الإختراق الرقمي

أ- الدوافع:

لم تنتشر هذه الظاهرة لمجرد العبث وإن كان العبث وقضاء وقت الفراغ من أبرز العوامل التي ساهمت في تطورها وبروزها الي عالم الوجود. وقد أجمل المؤلفين الثلاثة للمراجع التي استعنت بها في هذه الدروة الدوافع الرئيسية للاختراق في ثلاث نقاط أوجزها هنا على النحو التالي:

- **الدافع السياسي والعسكري:** مما لاشك فيه أن التطور العلمي والتقني أديا إلى الاعتماد بشكل شبة كامل على أنظمة الكمبيوتر في أغلب الاحتياجات التقنية والمعلوماتية. فمنذ الحرب الباردة والصراع المعلوماتي والتجسسي بين الدولتين العظميين على أشده. ومع بروز مناطق جديده للصراع في العالم وتغير الطبيعة المعلوماتيه للأنظمة والدول، أصبح الإعتماد كليا على الحاسب الألي وعن طريقة أصبح الاختراق من اجل الحصول على معلومات سياسية وعسكرية واقتصادية مسالة أكثر أهمية.
- **الدافع التجاري:** من المعروف أن الشركات التجارية الكبرى تعيش هي ايضا فيما بينها حربا مستعرة (الكوكا كولا والبيبسي كولا على سبيل المثال) وقد بينت الدراسات الحديثة أن عددا من كبريات الشركات التجارية يجرى عليها أكثر من خمسين محاولة إختراق لشبكاتها كل يوم[1].
- **الدافع الفردي:** بدأت أولى محاولات الاختراق الفردية بين طلاب الجامعات بالولايات المتحدة كنوع من التباهي بالنجاح في إختراق اجهزة شخصية لأصدقائهم ومعارفهم وما لبثت أن تحولت تلك الظاهرة الي تحدي فيما بينهم في اختراق الأنظمة بالشركات ثم بمواقع الأنترنت. ولا يقتصر الدافع على الأفراد فقط بل توجد مجموعات ونقابات أشبه ما تكون بالأندية وليست بذات أهداف تجارية. بعض الأفراد بشركات كبرى بالولايات المتحدة ممن كانوا يعملون مبرمجين ومحللي نظم تم تسريحهم من اعمالهم للفائض الزائد بالعمالة فصبوا جم غضبهم على أنظمة شركاتهم السابقة مقتحمينها ومخربين لكل ما تقع ايديهم عليه من معلومات حساسة بقصد الإنتقام.[2]

وفي المقابل هناك هاكرز محترفين تم القبض عليه بالولايات المتحدة وبعد التفاوض معهم تم تعيينهم بوكالة المخابرات الأمريكية الس أي اي وبمكتب التحقيقات الفيدرالي الأف بي أي وتركزت معظم مهماتهم في مطاردة الهاكرز وتحديد مواقعهم لإرشاد الشرطة اليهم.

---

[1] https://www.suezbalady.com/index.php جوان 2013 أحمد السيد

[2] Matheus M. Hoscheidt, Elisa Felber Eichner, LEGAL AND POLITICAL MEASURES TO ADDRESS CYBERCRIME, United Nations: UFRGSMUN UFRGS Model, v.2, 2014, p 446.

ب –الخصائص: من خصائص الإختراق الرقمي ما يلي

الطبيعة الرقمية: استخدام التقنيات الرقمية. **إخفاء الهوية والتخفي:** استخدام وسائل متطورة لإخفاء هوية المجرم.

البعد الدولي: الجريمة السيبرانية لا تعرف حدوداً جغرافية. **السرعة والكفاءة:** يمكن تنفيذ الهجمات الإلكترونية بسرعة وفعالية.

الدافع المالي: العديد من الجرائم الإلكترونية لها دوافع مالية.

التعقيد التقني: غالبًا ما تتضمن الجرائم الإلكترونية مهارات تقنية متقدمة، مثل التشفير والبرامج الضارة **التطور السريع:** تتطور الجرائم السيبرانية باستمرار مع تطور التقنيات الجديدة[1].

المطلب الثالث: فواعل الإختراق الرقمي

المبرمجين الأذكياء: هؤلاء كانوا يتحدوا الأنظمة المختلفة ويحاولوا اقتحامها وليس بالضرورة أن تكون في نيتهم ارتكاب جريمة ولكن نجاحهم في الاختراق يعتبر نجاحا لقد ارتهم ومهارتهم إلا أن القانون اعتبرهم دخلاء تمكنوا من دخول مكان افت ارضي لا يجب أن يكونوا فيه وقيامهم بهذا يعتبر عملية اختيارية يمتحن فيها المبرمج قد ارته بصورة إجرامية تخريبية لمسح المعلومات والبعض الآخر لأغراض تجارية وآخر لأغراض التجسس والبعض لسرقة الأموال دون أن يعرف باسمه الحقيقي. [2]

رغم ذلك ما ازل الخلاف بين الخبراء حول تحديد ما إذا كان الهاكر الفضوليون أو من لهم هواية

التعمق المعلوماتي: شخص مطور ومبدع لان شبكة الإنترنت في الأصل تزخر بمشاريع طورت من نشاط جماعي للهاكرز لأنهم ينظرون فيه الوجه السلبي المدمر على شاكلة قرصان الحاسوب وذلك بتأثير من بعض ما ورد في الإعلام، حيث يرجع السبب لجهلهم حقيقة الهاكر واقترانه بكلمة القرصنة (Piracy) لأن هذا التعبير الذي يصف عمليات البيع غير المشروع لنسخ من الأعمال الإبداعية وهي مستخدمة في انتهاك حقوق الملكية الفكرية وبرامج الحاسوب والتي أصبحت الشبكة العنكبوتية إحدى وسائل تسويقها. [3]

الكراكر: المحترفون الأكثر خطورة في إرتكاب الجريمة الالكترونية: فهو مصطلح أطلق فيما بعد للتفريق بين الهاكر الصالح والهاكر المفسد، وبالرغم من تميز الإثنين بالذكاء وروح التحدي وعدم خوفهم من مواجهة

---

[1] https://fs.mpt.gov.dz/cybercriminalite

[2] Home ofice, Cyber Crime Strategy, March 2010, p9, .pdf Available at :http:// www.knox.edu/offices-andservices/information-technologyservices/computer-usepolicies/online-speech.html.

[3] شفيق نوارن، "أثر التهديدات الإلكترونية على العلاقات الدولية، دارسة في أبعاد الأمن الإلكتروني"، (القاهرة، المكتب العربي للمعارف، 2014)، ص 40.

المجهول إلا أن الكراكر يقوم دائما بأعمال التخريب والاقتحام لأسباب غير ايجابية وهذا الشخص هو الذي يستحق تسميته قرصان الحاسوب بينما الهاكر يبتكر الحلول للمشاكل ويحاول أن يبدع في عمله. [1]

القبعات: أصل المصطلح مرتبط بتاريخ السينما وخصوصا أفلام رعاة البقر حيث كان الرجل الطيب يرتدي دائما قبعة بيضاء بينما يرتدي الرجل الشرير قبعة سوداء والرمادية لمن يقع دوره بين هاتين الحالتين.

الطائفة الناقمة: التي تستهدف المنشآت للإنتقام أو المنفعة: في كلتا الحالتين تتميز هذه الفصيلة من المجرمين عن غيرهم بما يكتسبونه من مهارات عالية في إستخدام التكنولوجيا ومستويات علمية مذهلة مما يسمح لهم التعامل بكل سهولة مع كل شبكات التواصل الالكترونية وصولا إلى المعلومات السرية لتحقيق الأهداف المسطرة، [2]

المبحث الثاني: أنماط التهديدات السيبرانية في الجزائر

نتطرق في هذا المبحث إلى إبراز اهم طرق الإختراق التي تهدد المساس بمحتوى المعلومات بكل أنواعها وأخطرها.

المطلب الأول: خطر الهجوم بطريقة DDOS

تعتبر هجمات ديدوس DDoS أحد أخطر التهديدات التي يمكن التصادم بها في العالم الرقمي في الفترة الراهنة، ولاسيما أنها تستهدف إغلاق خدمات وتعطيل شبكات الإنترنت بصورة دائمة أو مؤقتة.

وتتخذ أشكالًا تخريبية عديدة جميعها تستهدف تصويب مجموعة ضخمة من البيانات الزائفة والغير مرغوب فيها لتشتيت الخادم المستهدف. والتسبب في اخفاقه في السداد فيما يتعلق بمعالجة الطلبات الحقيقية للمستخدمين والزوار الشرعيين مما يتسبب في تعطيل الخدمة أو تراجع مستواها إلى حد كبير[3].

وتعد هجمات ديدوس DDoS من الهجمات متعددة الأنواع التي سوف نتعرف عليها من خلال السطور التالية. علاوة على أننا سنحاول إلقاء الضوء على إجراءات الحماية من الوقوع في هجمات ديدوس في

[1] عادل عبد الصادق، "خطر الحروب "السيبارنية" عبر الفضاء الإلكتروني"، مجلة الأهرام لكمبيوتر الانترنت والاتصالات، (مارس2017)، ص27.

[2] عبد النور بن عنتر، "عقيدة الجزائر الأمنية: ضغوطات البيئة الإقليمية ومقتضيات المصالح الأمنية"، من الرابط:

تاريخ التصفح: 24-05-2019.http://studies.aljazeera.net/ar/reports/2018/05/180502110656159.html

[3] Zhang ,Yuan , et al. (2017). Solution of Media Risk and Social Responsibility Governance of Social Media. ITM Web of Conferences,1 November, available at: https//:www.researchgate.net/.

محاولة لتقليل فرص التعرض للهجمات والمحافظة على استقرار الخدمات الرقمية واستمرار نجاحها في مواجهة هجمات.DDoS .[1]

ما هي هجمات ddos أو الحرمان من الخدمة الموزعة؟

يعرف هجوم ديدوس (DDOS) أو الهجوم الموزع لحجب الخدمة بوصفه هجوم موجه للخوادم ومواقع الويب للمساهمة في تعطيل الخدمات. حيث تقوم جهة الهجوم بخلق وتوجيه حركات مرورية زائفة للموقع بهدف عرقلة الوظائف التي يؤديها أو شل حركتها تمامًا[2].

ويمكن القول أن هجوم ديدوس (DDOS) من أنواع الهجمات الأكثر انتشارًا بشكل موسع بالنسبة للمجالات المختلفة وفي شتى أرجاء العالم. إلا أن هناك عدة مجالات تعد هي المستهدفة من هجوم ديدوس بشكل أكبر من غيرها ومن بينها مجال التجارة والتسويق الإلكتروني والألعاب الإلكترونية. ويتمتع هجوم ديدوس بالقدرة البالغة على إحداث أضرار جسيمة من شأنها تعريض الأمن العام والسمعة والمبيعات للمخاطر.

هل هجوم ديدوس هو أحد الهجمات السيبرانية؟

نعم، يعتبر هجوم ديدوس (DDOS) أحد أنواع الهجمات السيبرانية التي تهدف إلى زيادة أعباء تشغيل موقع إلكتروني ما أو سيرفر بما يتجاوز طاقة تحمله القصوى. مما يتسبب في حرمان المستخدمين والزوار الشرعيين من امكانية الوصول إلى الموقع المقصود أو بطء أداء هذا الموقع بصورة كبيرة[3].

أنواع هجماتDDOS: هجوم ديدوس (DDOS) أو الهجوم الموزع لحجب الخدمة هو أحد أنواع الهجمات الإلكترونية التي تستهدف العمل على تعطيل خدمة رقمية أو موقع إلكتروني عبر تكديس حركات المرور واستغلال قصور وضعف النظم. وهناك مجموعة من أنماط هجمات DDOS الأكثر شيوعًا وانتشارًا لعلنا نذكر منها:

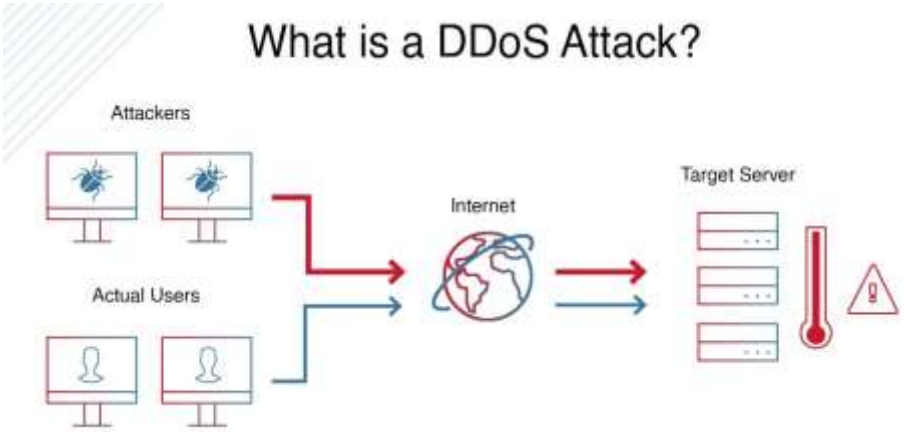
هجمات User Datagram Protocol UDP Flood هجمات حجب الخدمةSYN Flood

هجماتICMP Flood هجماتDNS Amplification هجماتHTTP Flood

[1] https://academy.binance.com/ar/articles/what-is-a-dos-attack تاريخ النشر Jan 7, 2019 تاريخ التحديث Oct 25, 2023.

[2] عادل عبد الصادق ،مرجع سابق ص27.

[3] Dan Craiyen and others, "Defining cybrescurity", Technology innovation management review, Montreal, Canada, (october 2014).



هذه أمثلة شائعة لأبرز أنواع هجماتDDOS، ومن الجدير بالذكر أنه يمكن اختلاف آليات وطرق الهجمات استنادًا على الأدوات التي يستخدمها المهاجمين ضمن المخطط الهجومي.

طريقة الوقاية من هجمات ديدوس2024 ddos

يمكنك العمل على فرض الحماية اللازمة على الشبكة الخاصة بك في مواجهة الهجمات المستقبلية، وذلك للمساهمة في تأمين الأعمال الخاصة بك من خلال اتباع وتطبيق الإجراءات التالية:

- العمل على بلورة خطط دفاعية للوقاية من هجمات الحرمان من الخدمات والتصدي لها بالمنع أو على أقل تقدير المساهمة في تقليل أعدادها لحماية اعمالك وتأمينها من المخاطر.
- تقدير وتوقع الهجمات المحتمل مواجهتها جراء ثغرات أمنية ودعم الأماكن التي تحتاج إلى توقيتها لإبقائها خارج دائرة التهديد.
- تحديث برامج الحماية والتحقق من عملها على نحو أمثل[1].
- عين فريق متخصص في مواجهة هجمات ديدوس، والتزم بتوزيع الأدوار على فريق المكافحة استعدادًا للسداد عن مواجهة أي هجوم حقيقي والعمل على تقليل حدته ومن ثم تداعياته.
- أبحث في ما هي أدوات هجمات DDOS المستخدمة في الكشف عن الهجمات الحادثة أو الوقاية من التعرض الهجمات لاستخدام الأدوات الأمثل.
- احرص على تقييم الاستراتيجية التي تتبعها للوقاية من هجمات ديدوس بصفة مستمرة للتأكد من فعاليتها والعمل على تطويرها.
- تعلم بالخطوات طريقة إفشال أي هجمة ضارة بمساعدة من الخبراء والمتخصصين الرواد.

ويمكن القول أن هجمات ديدوس تتضمن أنواع عديدة مما يجعل من أمر اتباع إجراءات الوقاية والحماية منها ضرورة واجبة تتطلب اتباع مجموعة من الإجراءات في سبيل الكشف عن الهجمات أولًا بأول لتتمكن من التصدي لها ومواجهتها بنجاح.

[1] Cameron S. D. Brown, "Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice", International Journal of Cyber Criminology. Vol 9, Issue 1, January – June 2015, p 57.

أي أنه باختصار شديد يجب على الجميع تعزيز الوعي العميق بالهجمات الإلكترونية ومختلف أنواعها وآليات حدوثها والإجراءات الواجب اتباعها من أجل الكشف المبكر عنها ومنع حدوثها وكيفية الوقاية منها لضمان تقديم خدمات إلكترونية مثالية وامتلاك شبكات محمية تمامًا[1].

المطلب الثاني: الإختراق بطريقة البوتنات

مزيج من الكلمتين robot و network، والبوتنت هو عبارة عن مجموعة من أجهزة الكمبيوتر ("الروبوتات") التي تتواصل مع بعضها ومع خوادم الأوامر والتحكم (C&C) الخاصة بها.

في مجال أمن المعلومات، تُعرف الروبوتات بأنها أجهزة كمبيوتر تم اختراق دفاعاتها الأمنية. إنها تشغل برامج ضارة تمكن طرفاً ثالثاً من التحكم فيها دون موافقة مالك الكمبيوتر أو المشغل الشرعي. غالباً ما يتم اختراق أجهزة الكمبيوتر المنزلية بهذه الطريقة، ولكن تم العثور على الروبوتات في أجهزة الكمبيوتر المدرسية والشركات والحكومة. ومع ذلك، في بعض الحالات، تكون الروبوتات عبارة عن خوادم مخترقة. على سبيل المثال، اكتشف باحثو شركة ESET عملية كبيرة ومعقدة تسمى"Windigo"، إذ اخترقت مجموعة منظمة من المجرمين أكثر من 25000 خادم Linux و UNIX فريد2.

تُستخدم البوتنت عادةً لإنشاء البريد العشوائي أو نشر برمجيات خبيثة أخرى (بما في ذلك نسخ من هذا البريد العشوائي) أو ملء الشبكة أو خادم الويب بطلبات زائدة تؤدي إلى فشلها (هجوم الحرمان من الخدمة، DDoS) كما تم استخدام البوتنت أيضاً في التصيد الاحتيالي ونقل البيانات المسروقة والجرائم المالية الأخرى[3].

تستخدم ESET تقنية الحماية ضد البوتنت التي تبحث في اتصالات الشبكة الصادرة عن الأنماط الضارة المعروفة وتطابق الموقع البعيد مع قائمة سوداء من الأنماط الضارة. يتم حظر أي اتصال ضار مُكتشف والإبلاغ عنه للمستخدم واختيارياً إلى.ESET

[1] Asenio .T.Gumahad , Cyber troopes and Netuvar :the profession of Arms in the information Age.(Alabama Air University ,Air war college, 1996) :57-156.

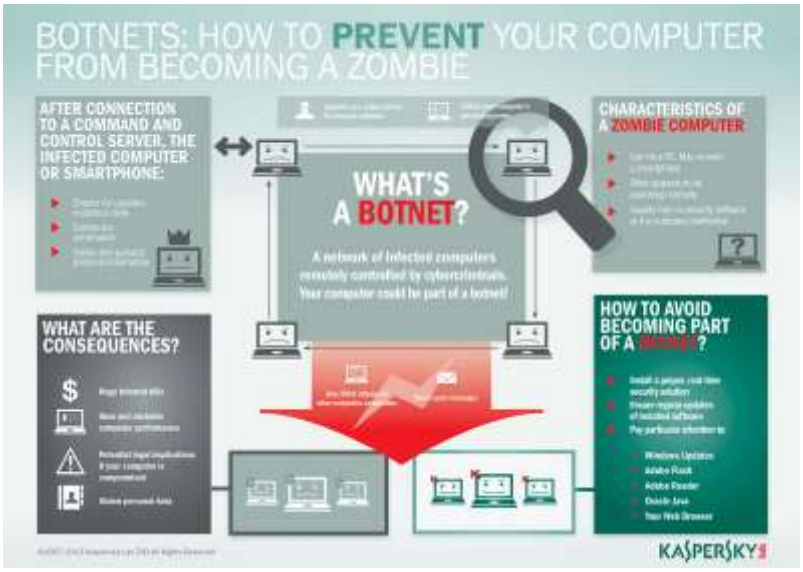
[2] https://help.eset.com/glossary/ar-EG/botnet.html8

[3] إسماعيل كاخيل، "الحرب الإلكترونية"، موقع مجلة الدفاع العربي، من الرابط:

www.arahdefancejournal.com/article560.htm 2019/03/1

كيف تكتشف البوت نت Botnet وتحمي نفسك منه ؟؟

اكتشاف البوت نت من الممكن ان يكون صعباً، حيث تم تصمم هذه البرمجيات لتعمل بدون علم مالك الجهاز المصاب، ولكن توجد بعض الاشارات والعلامات التي يمكنك استخدامها لتكتشف اذا كان حاسوبك مصابا أم لا، اعرض لك بعضها[1]



-اتصالات آي آر سي IRC Traffic يستخدمه اسياد البوت للتواصل مع البوت نت

-استخدام مرتفع، والكثير من اتصالات بروتوكول ارسال البريد STMP،

-نوافذ منبثقة غير متوقعة.

-حاسوبك بطيء على غير المعتاد، واستخدام مرتفع للمعالج.

-ارتفاع مفاجئ و كبير في استخدام الانترنت ثم انخفاضه، خصوصا عن طريق بورت 6667 (الذي يستخدم لاتصالات (آي آر سي)، وبورت 25 الذي يستخدم لـ Spam ، وبورت 1080 (الذي يستخدم لخوادم البروكسي.[2]

-رسائل لم تقم بإرسالها. -مشاكل في الاتصال بالأنترنت

المطلب الثالث: التجسس

التجسس الإلكتروني أو ما يعرف بحرب التجسس المعلوماتي هي عبارة عن عدة طرق لاختراق المواقع الالكترونية ومن ثم سرقة بعض المعلومات والتي قد تكون في قائمة الاهمية والخطورة للطرف المتلقي والمسروق منه وقد انتشرت في الالفية الجيدة بانتشار طرق الاختراق واحيانا قد تكون الاختراق من اشخاص عابثين ليس الا وأحيانا بغرض سرقة معلومات مهمه مثل ما حدث لوزارة الدفاع الأمريكية البنتاغون في العامين الماضيين من قبل اشخاص لا يتبعون للقاعدة بل اشخاص عابثين وكما تم اختراق موقع وزارة الدفاع الفرنسية قبل عامين بغرض سرقة معلومات عن الاستطلاعات والمناورات والنظام الصاروخي الفرنسي وليس

[1] Dan Craigen, Nadia Diakun-Thibault, and Randy Purse, Defining Cybersecurity. Technology Innovation Management Review, October 2014,pp 14-.51

[2] Dan Craigen, Nadia Diakun-Thibault, and Randy Purse ,id ,pp 14-.51 .

الاختراق محصور على المؤسسات العسكرية فكذلك قد تتعرض له المؤسسات النقدية وخصوصا البنوك المركزية والمؤسسات العملاقة.[1]

يُطوّر قطاع المراقبة برمجيات التجسس لتجاوز الدفاعات الأمنية التي تزداد قوة في أجهزة الحاسوب، وأجهزة الهاتف الخليوي، ومنصات الاتصالات. ويسعى فنيّو المراقبة إلى اختراق الأجهزة حتى يتسنى لهم الدخول إلى كافة البيانات المخزنة فيها.وفي حين أن أدوات برمجيات التجسس تُستخدم منذ زمن طويل، فإزدياد التشفير عقب المعلومات التي أفشاها إدوارد سنودن عام 2013 صعّب جمع البيانات الخاصة عبر طرق المراقبة الأخرى، مما وَلَّد طلبًا أكبر على برمجيات التجسس[2].

تقول الحكومات والشركات إن أدوات المراقبة هذه لا تُستخدم إلا لاستهداف 'المجرمين والإرهابيين .لكن في الواقع، جرى استهداف نشطاء حقوق الإنسان، والصحفيين، وكثيرين غيرهم في شتى أنحاء العالم على نحو غير قانوني بواسطة برمجيات التجسس[3].

ولكي يستطيع الناس حماية أنفسهم من برمجيات التجسس يجب أن يتبعون بعض النصائح أبرزها:

- واظبوا على تحديث برامج متصفحكم على الشبكة العنكبوتية وأنظمة تشغيل هواتفكم الخليوية.
- فعّلوا "حالة الإغلاق (Lockdown Mode) "الأمني المشدد على أجهزة أبل.
- احرصوا على عدم النقر على الروابط المرسلة من غرباء.
- تنبهوا للتغييرات في عمل الأجهزة[4].
- يمكن لاستخدام شبكة خاصة افتراضية (VPN) معروفة وآمنة أن يساعد على منع بعض أشكال المراقبة والرقابة.
- غيّروا إعدادات الخصوصية في حسابكم على فيسبوك مع الأصدقاء الحاليين، وأجروا تقييمًا لطلبات الإضافة الجديدة قبل قبولها[5].

[1] ضرغام جابر عطوش آل مواش، "جريمة التجسس المعلوماتي" المركز العربي للدراسات والبحوث العلمية للنشر، ط1، الإمارات العربية المتحدة ،2017، ص 25.

[2] عادل عبد الصادق، "الفضاء الالكتروني وتهديدات جديدة للأمن القومي"، المركز العربي للأبحاث الإلكترونية.

[3] سليمة مق ارني، "الجيش الوطني الشعبي: ملتقى حول الدفاع السيبارني، مكون أساسي للأمن والدفاع الوطني" hltps :www.eljoumhouria.dg، من الموقع:17:51/2018مارس 07 نشر في

[4] مادلين آر كريدين،"الفضاء والفضاء الالكتروني: التحديات المشتركة، مجلة الفضاء والفضاء الالكتروني التابعة للقيادة الإستراتيجية الأمريكية"، (يناير 2012)، ص 35.

5

المبحث الثالث: التهديدات السيبرانية التي تواجهها الجزائر

سنتطرق في هذا المبحث إلى إعطاء نماذج لحالات إختراق حقيقة مست العديد من الجهات الحساسة في قطاعات مختلفة على سبيل الحصر فقط .

المطلب الأول: وكالة الأنباء الجزائرية

تعرض موقع وكالة الأنباء الجزائرية (APS) مؤخرًا لسلسلة من الهجمات السيبرانية التي تسببت في حجبه مؤقتًا. وقد أُعلنت وكالة الأنباء الجزائرية في بيان لها أن هذه الهجمات تأتي من مصادر جغرافية متعددة تشمل الكيان الصهيوني المحتل والمغرب وبعض المناطق من أوروبا.[1] أكدت الوكالة أنها تمكنت من صد هذه الهجمات بفضل التدابير والأنظمة التقنية المتبعة، مما حال دون تمكن محاولات الاختراق من الوصول إلى قاعدة البيانات جريدة الناس، الهجمات السيبرانية المستمرة ضد مواقع رسمية في الجزائر، بما في ذلك [2]وكالة الأنباء الجزائرية، تأتي في إطار ما وصفته الوكالة بالحرب الإعلامية والإلكترونية التي تستهدف الجزائر. ورغم هذه الهجمات، لم تتأثر خدمات الوكالة الأخرى الموجهة لمشتركيها، حيث استمرت في بث الأخبار والصور الفوتوغرافية عبر القنوات المعتادة مثل الإنترنت والأقمار الصناعية هذا الوضع يثير القلق حول تأمين المواقع الإلكترونية الرسمية[3] الجزائرية وحمايتها من الاختراقات المتكررة، خاصة وأنها ليست المرة الأولى التي تتعرض فيها المواقع الرسمية الجزائرية لمثل هذه الهجمات[4]

المطلب الثاني: الهجمات السيبرانية ضد الجزائر

أظهر تقرير حديث لرائد عالمي في الأمن السيبراني أن برمجياته الدفاعية أحبطت ما لا يقل عن 29.7 مليون هجمة ضد الجزائر في عام 2022، منها أكثر من 19 مليون تهديد طال عناوين بريد إلكتروني جزائرية.

وأفاد بيان لـ"تراند ميكرو" الشركة المتخصصة في الأمن السيبراني العالمي، تلقت "الشروق" نسخة منه، بأن برمجياته اكتشفت وأحبطت أكثر من 19 مليون تهديد طال عناوين بريد إلكتروني لجزائريين، كما

[1] محمد درقي،" النظام المعلوماتي للشركات الجزائرية غير مؤمن"، جريدة الخبر، العدد 7638، (04 أفريل2018)، ص 08

[2] حمد الأمين بن عائشة، "مفهوم الأمن الوطني الجزائري"، في: 03 فيفري 2018 33:21/ www.maqualaty.com

[3] جريدة الشروق الجزائرية، عدد 1253 الصادرة بتاريخ:2023/09/20.

[4] وكالة الأنباء الجزائرية، الإرهاب الإلكتروني: " الجزائر حريصة على حماية أمنها ". من موقع:
https://algpress.com/article-50021.htm

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.

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[1]."

وأضاف أنه "من الأهمية بمكان 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."

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[2].

والتقرير الذي أعدته مؤسسة "تراند ميكرو" اليابانية، سلط الضوء على الاتجاهات التي لها آثار مهمة على مستقبل الأمن الرقمي والسيبراني، وشدد على أن الجهات الفاعلة في التهديد كانت تستهدف بشكل عشوائي المستهلكين والمؤسسات، مما جعل عام 2022 عاما صعبا لمحترفي الأمن السيبراني. وقبل أشهر، أكد رئيس الجمهورية عبد المجيد تبون، أن الجزائر تواجه حربا سيبرانية مسعورة للتشويش على البناء الوطني، منوها بجهود منتسبي الصحافة الوطنية في التصدي لها[3].

المطلب الثالث: إمكانية اختراق منصات التعليم عن بعد

اضطرت العديد من المدارس والمؤسسات التعليمية في الجزائر مع بداية العام الدراسي 2020-2021 لاعتماد التعليم عن بعد في عملياتها التعليمية، بشكل كليّ أو من خلال التعليم المدمج والذي يجمع بين الحضور إلى الصفوف أو الدراسة من خلال الوسائل التقنية. تتنوع الوسائل التقنية المستخدمة لتحقيق التعليم عن بعد بين منصات خاصة لكل مدرسة، أو استخدام الخدمات التي تقدمها شركات كبرى مثل Google و Microsft، بالإضافة إلى استخدام تطبيقات المحادثة والاجتماع المتنوعة مثل Whatsapp و Zoom

[1] سليم مزيود، "الجرائم المعلوماتية واقعها في الجزائر وآليات مكافحتها"، جامعة المدية، الجزائر، (2015)، ص96.

[2] عادل عبد الصادق، "أنماط "الحرب السيبارنية" وتداعياتها على الأمن العالمي"، مجلة الاتجاهات النظرية، البنك العربي الافريقي، (14 ماي 2017)، ص32.

[3] إيهاب خليفة،" نمط جديد لممارسة التأثيارت غير التقليدية في العلاقات الدولية"، اتجاهات الأحداث، العدد 06،

مستمر. هذا الانتقال السريع كان مترافقاً مع غياب التدريب المتخصص للطلاب والأطقم التعليمية على مواجهة المخاطر السيبرانية التي قد يتعرضون لها، خاصة مع ضعف المنصات، أو غياب التدريب على استخدام التقنيات الرقمية. حيث تسجل في هذا الإطار مجموعة من المخاطر التي قد تعترض العملية التعليمية على أكثر من صعيد وتشمل:[1]

أولاً. تعطيل الخدمات التعليمية:

تعطيل الخدمات التعليمية يحول دون امكانية إتصال العديد من الطلاب بفصولهم الدراسية عبر الإنترنت. يعود هذا التعطيل لمجموعة من الأسباب أبرزها:

- الحجم الكبير لحركة المرور التي تحاول الوصول إلى المنصات في وقت واحد.
- ضعف في المنصة ووجود أخطاء برمجية، أو في البنية التحتية للخوادم ومصادر الاتصال بالإنترنت.
- ضعف شبكة الاتصالات في لبنان، ما يقطع الاتصال مع الشبكة المنصات لدى العديد من الطلاب أو المدارس.
- الهجمات السيبرانية على المنصات الخاصة وبالأخص هجمات حجب الخدمة (DDoS Attack)، بهدف تجاوز قدرة المنصة على معالجة الطلبات المتعددة وبالتالي منعها من العمل بشكل صحيح.

ثانياً. التصيُّد الاحتيالي (Phishing):

سبق أن تعرضت مؤسسات تربوية في العالم لعمليات تصيّد احتيالي تهدف إلى سرقة بيانات عن الموظفين والطلاب. يعمد المتصيد إلى استخدام رسائل بريد الكتروني تظهر كأنها صادرة عن جهات ذات صلة او حتى رسائل على تطبيقات الدردشة تحتوي على عروض مغرية تطلب بيانات أو كلمات مرور أو حتى تسجيل حسابات التواصل الاجتماعي ما يتيح للمتصيد سرقة البيانات أو الحسابات الشخصية للشخص المستهدف أو آخرين. ويستغل المتصيد في تنفيذ عمليات التصيد التراسل بين المدرسة أو المعلمين والطلاب، وهي عملية لم تستخدم الوسائط الرقمية سابقاً.

[1] العريشي، جبريل بن حسن.، الدوسري، سلمى عبد الرحمن." **دور مؤسسات التعليم العالي في تعزيز ثقافة أمن المعلومات في المجتمع**"، كلية العلوم الاجتماعية، جامعة الأميرة نورة بنت عبد الرحمن، السعودية ، مجلة مكتبة الملك فهد الوطنية. مج. 24، ع. 2، أبريل – سبتمبر 2018، ص 302.

ثالثاً. البرمجيات الخبيثة (Malware):

تتعرض أنظمة المدارس وأجهزة الطلاب للعديد من البرمجيات الخبيث، والتي تتنوع أهدافها لتشمل:

- **برامج الفدية (Ransomware):** يبدأ هذا الهجوم الإلكتروني المتمثل ببرامج الفدية مع وصول رسالة أو رابط من شخص مجهول يطلب تحميل الملف على أنه ملف مهم أو شخصي، وفور تحميل الملف في الكمبيوتر أو الهاتف الذكي تبدأ عملية تشفير البيانات ويصبح بعدها صاحب الجهاز غير قادر على الوصول إليها. ويقوم برنامج "الفدية" بإقفال ملفات المستخدمين المستهدفين ويرغمهم على دفع مبلغ من المال على هيئة العملة الإلكترونية "بيتكوينز" مقابل إعادة فتحها. التعاطي المحلي في لبنان مع برامج الفدية هو حذف الملفات مع غياب ثقافة الدفع لاستعادتها، ما يعرض المستهدف لخسائر خطيرة مع غياب النسخ الاحتياطية في العملية التربوية، يمكن أن تؤدي برامج الفدية إلى الإضرار بملفات الوظائف المدرسية والدروس والاختبارات، كما تتضرر الملفات الإدارية المستخدمة من قبل المدرسين والإدارة.
- **سرقة البيانات:** تُعرض مجموعة من البرمجيات الخبيثة ملفات المستخدم للسرقة، بهدف إساءة استخدامها بما يسيء ويضر بالشخص المستهدف. وهو ما يعرض الطلاب لسرقة صورهم ورسائلهم الخاصة، واستغلالها من قبل القراصنة لأهدافهم السيئة.
- **برمجيات تجسسية (Spyware):** يستخدم الطالب خلال التعليم عن بعد الكاميرا والمايكيروفون، وهي إضافات يمكن التحكم بها عند إصابة الجهاز ببرمجيات تجسسية من قبل القراصنة، فيتم تفعيلها بما يضرّ به. كما تسهم هذه البرمجيات في تتبع النشاط على الجهاز والشبكة وتستغلها بطرق مختلفة.[1]

رابعاً. إساءة الاستخدام:

انتشر على مواقع التواصل الاجتماعي فيديو لأحد الطلاب يستحم خلال الفصل الدراسي عبر تطبيق Zoom، هذا الحدث قد يتكرر بصيغ مختلفة في الفصول الدراسية مع إمكانية تعرض الطلاب لمواقف أكثر إساءة خاصة الاطفال منهم لأسباب مختلفة تربوية او ثقافية او حتى نفسية.

[1] سارة تيتيلة، تصميم أساليب تقويم التعليم الإلكتروني بالجامعة الجزائرية: واقع التطبيق ومميزات الإستخدام، جامعة سطيف02، مجلة العلوم الاجتماعية، جامعة الأغواط، مجلد 07، العدد 28 جانفي 2018.

نعم، هناك إمكانية لاختراق منصات التعليم عن بعد في الجزائر، كما هو الحال في أي بلد آخر. يعتمد ذلك على عدة عوامل منها الإجراءات الأمنية المتبعة من قبل المنصة التعليمية، مهارات المخترقين، والتكنولوجيا المستخدمة في الحماية.

لتقليل مخاطر الاختراق، يجب على منصات التعليم عن بعد في الجزائر اتباع أفضل الممارسات الأمنية مثل:

- ✓ استخدام تقنيات التشفير القوية لحماية البيانات.
- ✓ تنفيذ جدران الحماية وأنظمة كشف التسلل.
- ✓ تطبيق سياسات قوية لكلمات المرور وتوفير المصادقة الثنائية(Two-Factor Authentication)
- ✓ تدريب الموظفين والمستخدمين على الوعي الأمني وتجنب الهجمات الهندسة الاجتماعية.
- ✓ إجراء تحديثات وصيانة منتظمة للبرمجيات والأنظمة المستخدمة[1].

لا توجد تقارير واضحة أو موثوقة تشير إلى اختراق منصة "بروقرس" التعليمية في الجزائر. ومع ذلك، يمكن القول بأن منصة "بروقرس"، التي تديرها وزارة التعليم العالي والبحث العلمي، هي جزء من مجموعة منصات تقدم خدمات متعددة للطلاب والأساتذة مثل إدارة الطلبات الأكاديمية، التوجيه، وشهادات الدبلومات وغيرها. وهل هناك ثغرات في منصة بروغرس ؟

لا توجد معلومات مؤكدة أو منشورة حول وجود ثغرات أمنية محددة في منصة "بروقرس" التعليمية في الجزائر. هذه المنصة تُستخدم لإدارة العمليات الأكاديمية المختلفة وتشمل خدمات مثل تسجيل الطلبة، إدارة الشهادات، والتوجيه الأكاديمي.

بشكل عام، يمكن القول بأن أي نظام إلكتروني قد يكون عرضة للثغرات الأمنية إذا لم يتم اتخاذ التدابير الأمنية المناسبة. هذه التدابير تشمل استخدام التشفير القوي، تحديثات البرمجيات المنتظمة، وتدقيقات الأمان الدورية. لضمان الأمان، يجب على المؤسسات التي تدير هذه المنصات اعتماد أفضل الممارسات الأمنية وحماية البيانات الحساسة من الوصول غير المصرح به.

[1] خديم رابح، واقع أرضيات التعليم الإلكتروني عن بعد في الجامعة الجزائرية، جامعة عمار ثليجي الأغواط، مجلة الإبتكار والتنمية الصناعية، المجلد 03، العدد 03.

خلاصة الفصل:

خلص هذا الفصل إلى أن الجزائر كغيرها من الدول الأخرى وفي ظل حتمية الإنخراط في المجال السيبراني واجهت العديد من التهديدات السيبرانية خاصة فيمايتعلق بأشهر طرق الإختراق ومختلف طرق الهجمات السيبرانية كما وضحنا في بداية الفصل والتطور السريع في مجال تكنولوجيات الإعلام والإتصال وفي المقابل تشهد المنظومة المعلوماتية العيديد من الثغرات الأمنية التي شكلت تهديدا مباشرا وسهولة للإختراق كما وضحنا ببعض النماذج التي تم اختراقها في الجزائر.

الفصل الثالث

التوجه الاستراتيجي لإرساء الأمن المعلوماتي في الجزائر

تمهيد:

يعتبر العصر الحالي "عصر سيبراني" بامتياز، فقد أصبح العمود الفقري لمعظم التفاعلات اليومية ،وأصبحت الانترنت سلاحا ذا حدين، فكما هي وسيلة لتحقيق التقدم البشري، هناك جانب آخر يتمثل في تزايد التهديدات والمخاطر السيبرانية الناجمة على الاعتماد المتزايد عليه، في ظل عالم مفتوح تحكمه تفاعلات غير مرئية وغياب سلطة قانونية عليا تسيطر عليه، حيث اتجهت معظم الد ول والحكومات لتبني استراتيجيات وسياسات لتعظيم أمنها من التهديدات والتحديات دف تحقيق الأمن السيبراني، والجزائر وكغيرها من الدول اهتمت هذه الأخيرة وتحاول أن تتبنى نموذج حكومة ذكية في ظل مجتمع جزائري معلوماتي، كما أنها تعمل على إنشاء هيئات أمنية مختصة لمكافحة تلك المخاطر السيبرانية.

المبحث الأول: إخفاء الهوية في الفضاء الإلكتروني

يُعَدُّ مفهوم عدم الكشف عن الهوية جانبًا أساسيًا للإنترنت، وقد كان في قلب العديد من الأنشطة عبر الويب. غالبًا ما يستخدم الأفراد الإنترنت للتعبير عن أنفسهم دون الكشف عن هوياتهم، وقد كان هذا عاملاً حاسمًا في تعزيز حرية التعبير والخصوصية. ومع ذلك، كما أن عدم الكشف عن الهوية يُعَدُّ سلاحًا ذا حدين، حيث يُمكن لمجرمي الإنترنت استغلاله لتنفيذ أنشطتهم الشائنة. في السنوات الأخيرة، أصبحت مسألة إلغاء الهوية تشكل تحديًا كبيرًا للأمن السيبراني وأثارت مخاوف بين مستخدمي الإنترنت. في هذا القسم، سوف نبحث في طبيعة إلغاء الهوية، وتأثيرها على الأمن السيبراني، وبعض السبل التي يُمكن اتباعها لمواجهتها.[1]

المطلب الأول: مفهوم إخفاء الهوية وحدودها

إخفاء الهوية هو مفهوم أصبح ذا أهمية متزايدة في عالمنا المعاصر. مع انتشار وسائل التواصل الاجتماعي وتزايد النشاط عبر الإنترنت بشكل عام، أصبح الأفراد أكثر قلقًا بشأن خصوصيتهم والمعلومات التي يتبادلونها عبر الشبكة العنكبوتية. ومع ذلك، ينبغي أن ندرك أن عدم الكشف عن الهوية ليس دائمًا الحل الأمثل. هناك حدود لمدى يمكن أن يكون فيه خفاء الهوية فعَّالًا، ومن المهم فهم هذه القيود لاتخاذ قرارات مناسبة حول كيفية حماية الخصوصية.

إن القيود المفروضة على عدم كشف الهوية تشير إلى استخدام الأدوات أو التكنولوجيا لإخفاءها عبر الإنترنت. يمكن أن تشمل هذه الأدوات استخدام شبكة افتراضية خاصة (VPN)، أو متصفح Tor، أو التشفير. وعلى الرغم من أن هذه الأدوات يمكن أن توفر مستوى من الحماية لخصوصية الفرد، إلا أنها

[1] إخفاء الهوية: كشف النقاب عن كابوس الأمن السيبراني. تم الاطلاع بتاريخ: 20 ماي 2024
https://fastercapital.com/arabpreneur

ليست خالية تمامًا من المخاطر. على سبيل المثال، قد يتمكن مزود خدمة VPN من الوصول إلى البيانات وقد يشاركها مع أطراف ثالثة، ومن ناحية أخرى، على الرغم من أن متصفح Tor مصمم لتوفير تصفح مجهول، إلا أنه ليس محصنًا تمامًا ضد الهجمات والنقاط الضعيفة. يجب على المستخدمين فهم هذه الاحتمالات والمخاطر المرتبطة بكل أداة واتخاذ الاحتياطات المناسبة لحماية خصوصيتهم.

لماذا يعد إلغاء الهوية كابوس للأمن السيبراني؟

إلغاء الهوية يُعَد كابوساً حقيقياً في سياق الأمن السيبراني، وتواجه المجتمعات والأفراد تحديات متزايدة في التعامل معه. إليك بعض الأسباب التي تجعل إخفاء الهوية مصدر قلق مستمر في هذا السياق:

- **فقدان الخصوصية:** تُعَدُّ الخصوصية حقاً أساسياً للأفراد على الإنترنت. عندما يتم الكشف عن هوية الشخص، يمكن أن يتعرض لانتهاكات خطيرة للخصوصية، مما يؤثر على حياته الشخصية والمهنية.
- **الخسارة المالية:** يُعَدُّ إلغاء الهوية بوابة للعديد من الجرائم المالية، بما في ذلك سرقة الهوية، واختراق الحسابات المصرفية، واستنزاف الأموال، مما يؤدي إلى خسائر مالية جسيمة للأفراد والمؤسسات.
- **سرقة الهوية:** يمكن للمجرمين السيبرانيين استخدام المعلومات الشخصية المسروقة لارتكاب جرائم سرقة الهوية، مثل فتح حسابات جديدة أو التقدم بطلبات قروض بالشخصية المسروقة، مما يترتب عنه آثار ضارة وطويلة الأمد على الضحايا.
- **التسلط والتنمر عبر الإنترنت:** يمكن استخدام الهوية المجهولة لمهاجمة الأفراد بشكل متكرر، سواء عبر التنمر عبر الإنترنت أو الابتزاز أو الاحتيال، مما يسبب آثار نفسية واجتماعية خطيرة.
- **الأذى الجسدي:** في حالات الإلغاء الهوية المتطرفة، يمكن أن تؤدي الإفشاء الجسدي للهوية إلى أذى جسدي خطير، مثل الاعتداءات الجسدية أو التهديدات بالعنف.

بالنظر إلى هذه الأسباب، فإن إخفاء الهوية يُعَدُّ تحدياً جسيماً للأمن السيبراني ويستدعي استراتيجيات شاملة للحماية والتوعية. تشمل هذه الاستراتيجيات التوعية بأمان الإنترنت وتعزيز الحماية الشخصية والمؤسساتية وتطوير السياسات والتشريعات المناسبة لمكافحة جرائم الإنترنت وحماية الخصوصية.[1]

المطلب الثاني: تطوير أدوات تقنية لأمان المشروع الرقمي في 2024

تعتمد المؤسسات في كل قطاع – بما في ذلك قطاع الأعمال والحكومة والطب والمنظمات غير الربحية – على تخزين البيانات التي غالبًا ما تكون حساسة في الوصول إليها. وهذا يحفز المتسللين على سرقة البيانات أو تعطيل الوصول إليها، لذلك من الضروري استخدام أدوات الأمن السيبراني بصورة مستمرة.

[1] إخفاء الهوية: كشف النقاب عن كابوس الأمن السيبراني. تم الاطلاع بتاريخ: 20 ماي 2024 .
https://fastercapital.com/arabpreneur

تأخذ استراتيجية الأمن السيبراني الجيدة نهجا شاملا لأمن البيانات. فهو يحد من الوصول الفعلي إلى الخوادم والمجالات الرئيسية الأخرى، ويقوم بتدريب الموظفين بشكل كامل على أمن البيانات، ولديه نظام لضمان تشفير البيانات وتحديث البرامج.

1. Intruder

أداة Intruder هي ماسح ضوئي للثغرات الأمنية قائم على السحابة. يستخدم البرنامج نفس مستوى الأمان الذي تستخدمه البنوك والحكومات لحمايتك من الهجمات الإلكترونية بتنسيق بسيط وسهل الفهم. لذلك تعد أحد أفضل أدوات الأمن السيبراني.[1]

2. Nikto

أداة Nikto هي ماسح ضوئي لتقييم نقاط الضعف يقوم باختبار التهديدات ضد خوادم الويب. كما أنه يبحث أيضًا عن مشكلات التكوينات التي يمكن أن تجعل المؤسسات معرضة للخطر. لذلك تعد أحد أفضل أدوات الأمن السيبراني.

3. Wireshark:

أداة Wireshark هي محلل لبروتوكولات الشبكة، يُشار إليه أحيانًا باسم مكتشف الحزم. يقوم مكتشف الحزم بمراقبة البيانات التي تتحرك عبر طبقة بروتوكول التحكم في الإرسال/بروتوكول الإنترنت (TCP/IP) الخاصة بالشركة. تمكن المراقبة الشركة من تحليل حركة المرور الخاصة بها بحثًا عن التهديدات. لذلك تعد أحد أفضل أدوات الأمن السيبراني.[2]

4. Metasploit:

أداة Metasploit هي أداة لاختبار الاختراق تبحث عن نقاط الضعف في الشبكات والخوادم. يتم استخدامه من قبل مجموعة متنوعة من المتخصصين في مجال الأمن السيبراني للعثور على نقاط الضعف

[1] Douwe Korff, CYBER SECURITY DEFINITIONS – a selection. P1, in: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CPDP%202015%20-%20KORFF%20Handout.pdf

[2] Cameron S. D. Brown, "Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice", International Journal of Cyber Criminology. Vol 9, Issue 1, January – June 2015, p120.

داخل أنظمتهم، وهذا بدوره يسمح لهم بتعزيز تلك المناطق قبل أن تستغلها الهجمات السيبرانية. لذلك تعد أحد أفضل أدوات الأمن السيبراني.[1]

المطلب الثالث: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال

في القرن العشرين، شهد العالم ثورةً من نوعٍ جديدٍ في مجال المعلومات والاتصالات، نتيجةً للتقدم الذي أحدثه العلماء والمكتشفون في مجالات عدة، بما في ذلك علوم الحاسوب وتكنولوجيا الإنترنت.

وبناءً على هذا التقدم الهائل، أصبح من الممكن التعبير عن هذه الفترة الزمنية باسم "قرن المعلوماتية". حيث تتدفق المعلومات بشكل لم يسبق له مثيل، وتصبح متاحة بشكل وافر وسلس.[2]

لذلك، حرصت الدولة الجزائرية على إنشاء هيئة متخصصة وتوفير الموارد البشرية المناسبة لمواجهة الجرائم المعلوماتية والإلكترونية، والعمل على الوقاية منها. وتأتي هذه الجهود في إطار تنفيذ الخطة الجزائرية للتعامل مع الجرائم المتصلة بتكنولوجيا المعلومات والاتصالات. وفي هذا السياق، قام المشرع بإصدار قانون رقم 04-09 الذي يحتوي على القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا المعلومات والاتصالات، وكذلك مكافحتها.[3]

تبنت الدولة الجزائرية سلسلة من المراسيم الرئاسية لمكافحة هذه الظاهرة الإجرامية والحد من انتشارها، وذلك من خلال إبرام اتفاقيات دولية وسن نصوص تشريعية وتنظيمية جديدة تهدف إلى الوقاية والمكافحة والحد من انتشار هذه الجرائم المتصلة بتكنولوجيا المعلومات والاتصالات.

من بين هذه المراسيم الرئاسية، المرسوم الرئاسي رقم 15-261[4]، والمرسوم الرئاسي رقم 19-172[5] ، وأخيرًا المرسوم الرئاسي رقم 20-183[6] الساري المفعول. تهدف هذه المراسيم إلى استئصال الجرائم

---

[1] Home ofice, Cyber Crime Strategy, March 2010, p9, in https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf

[2] غنية باطلي، الجريمة الإلكترونية (دراسة مقارنة)، أطروحة مقدمة لنيل شهادة دكتوراه، شعبة القانون الخاص، كلية الحقوق قسم القانون الخاص، جامعة باجي مختار، عنابة، د. س . م.

[3] القانون رقم 04-09 مؤرخ في 5 أوت2009 يتضمن القواعد الخاصة لوقاية من الجرائم المتصلة بتكنولوجيات العالم والاتصال ومكافحتها، ج ر، عدد ،47 صادر في 16 أوت 2009.

[4] المرسوم الرئاسي رقم 15-261 مؤرخ في 8 أكتوبر2015 يحدد تشكيلة وتنظيم وكيفيات سير البيئة الوطنية لوقاية من الجرائم المتصلة بتكنولوجيات العالم والاتصال ومكافحتها، ج ر، عدد 53 ، صادر في 8 أكتوبر 2015 .

[5] المرسوم الرئاسي رقم 19-172 مؤرخ في 6 يونيو ،2019 يحدد تشكيلة البيئة الوطنية لوقاية من الجرائم المتصلة بتكنولوجيات العالم والاتصال ومكافحتها وتنظيميا وكيفيات سيرها، ج ر، عدد 37 ، صادر في 9 يونيو 2019.

[6] المرسوم الرئاسي رقم 20-183 مؤرخ في 13 يوليو 2020، يتضمن إعادة تنظيم البيئة الوطنية لوقاية من الجرائم المتصلة بتكنولوجيات العالم والاتصال ومكافحتها، ج ر ، عدد ،40 صادر في 18 يوليو .2020

المعلوماتية والحد من انتشارها، سواء من خلال إبرام اتفاقيات دولية[1] أو بواسطة سن نصوص تشريعية وتنظيمية جديدة.

أولا: اختصاصات الهيئة بشكل عام

يقوم المرسوم الرئاسي رقم 21-439 بتحديد الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا المعلومات والاتصال، وتطبيقها على أرض الواقع. ومن بين مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا المعلومات والاتصال:

- تنشيط وتنسيق الجهود للوقاية من الجرائم المتصلة بتكنولوجيا المعلومات والاتصال ومكافحتها.
- ضمان المراقبة الوقائية والاتصالات الإلكترونية بإشراف السلطة القضائية المختصة، بهدف كشف الجرائم ذات الطابع الإرهابي أو التخريبي أو التي تشكل تهديداً لأمن الدولة.
- التنسيق مع الجهات المختصة في وزارة الدفاع الوطني للقيام بمراقبة إلكترونية تتعلق بأمن الجيش.
- جمع وتسجيل وحفظ البيانات الرقمية للأنظمة المعلوماتية وتحديد مصادرها ومصاريفها للاستفادة منها في الإجراءات القضائية.
- مساعدة السلطات القضائية ومصالح الشرطة القضائية في مكافحة الجرائم المرتبطة بتكنولوجيا المعلومات والاتصال، وذلك من خلال جمع المعلومات وتوفيرها لهم، بالإضافة إلى إنجاز الخبرات القضائية.
- تطوير التعاون مع المؤسسات والهيئات الوطنية في مجال الوقاية من الجرائم المتصلة بتكنولوجيا المعلومات والاتصال.
- العمل على تنفيذ الطلبات المساعدة الصادرة من البلدان الأجنبية، وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها، بهدف مكافحة الجرائم التقنية عبر الحدود الوطنية.

ثانيا: دور الهيئة في حماية من الجرائم الإلكترونية

توجد العديد من الجرائم الإلكترونية التي تؤثر على الأفراد بغض النظر عن جنسهم، عمرهم، مستواهم الثقافي أو التعليمي. في الجزائر، على سبيل المثال، تم تسجيل 1023 ضحية في قضايا متعلقة بالجرائم الإلكترونية في عام 2016، بينهم 138 قاصرًا و76 ضحية معنوية. وفي الوقت نفسه، ارتكب 104 قاصرين جرائم إلكترونية، بالإضافة إلى 946 متهمًا في قضايا أخرى.

[1] مثال عن هذه الاتفاقيات الدولية: اتفاقية بودابست مؤرخة في،23/11/2001المتعمقة بالإجرام المعلوماتي) cybercriminalité la sur convention) المتضمنة توصيات حول تفعيل دور القانون لمواجهة الأفعال غير المشروعة عبر الحاسوب.

تشمل هذه الجرائم الاعتداء الإلكتروني، والاستغلال، والتجارة غير المشروعة، وجرائم الاعتداء على الأموال، واختراق الأنظمة المعلوماتية والقرصنة. وبموجب القانون رقم 09-04، تلعب الهيئة دورًا هامًا في الحماية من هذه الجرائم الإلكترونية، سواء من خلال تدخلها الوقائي أو في مراحل متأخرة بعد ارتكاب الجرائم.

على المستوى الداخلي، تقوم الهيئة بتنفيذ إجراءات التفتيش على أنظمة المعلومات ومراقبة الاتصالات الإلكترونية، بناءً على إذن من السلطة القضائية، خاصة في الحالات التي يكون من الصعب فيها الوصول إلى نتائج من دون هذه الإجراءات.[1]

وعلى الصعيد الدولي، تقوم الهيئة بتبادل المعلومات وتنفيذ طلبات المساعدة القضائية، وتتخذ إجراءات تحفظية[2] فيما يتعلق بالجرائم الإلكترونية. في الجملة، تظهر الأرقام والإحصائيات السابقة أهمية دور الهيئة في مجال اختصاصها والمساهمة في تحقيق الحماية المناسبة في هذا المجال.

المبحث الثاني: الجزائر في مواجهة الحروب السيبرانية

يهدف هذا المبحث إلى تقديم نظرة حول الجهود الجزائرية التي تبذلها في مختلف قطاعاتها الحساسة ودورها الفعال في حماية بيانات مؤسساتها وأشخاصها المتعاملين لمواكبة التكنولوجيات المتقدمة .

المطلب الأول: الاستراتيجية الوطنية لتحقيق الأمن السيبراني

في إطار التوجه الدولي نحو الحكومة الإلكترونية، تعتبر قضية الأمن المعلوماتي السيبراني واحدة من التحديات الرئيسية على الصعيدين الإقليمي والعالمي، وذلك بسبب زيادة التهديدات الأمنية الإلكترونية. تسعى الجزائر، كغيرها من الدول، إلى حماية منظومتها المعلوماتية بشكل أكبر بعد انتقالها للإدارة الإلكترونية، من خلال تفعيل العديد من الأجهزة والخلايا الأمنية. لقد أصبح الأمن المعلوماتي السيبراني عنصرًا أساسيًا ضمن المنظومة الأمنية الحديثة، ويتطلب الدفاع الوطني، وخاصةً من خلال جهاز الدرك الوطني الجزائري، اهتمامًا متزايدًا في مواجهة الجريمة الرقمية المتنامية.[3] وبالإضافة إلى ذلك، يتوجب التصدي للاستغلال المتنامي للشبكات الإلكترونية لأغراض إجرامية، والتي تؤثر سلبًا على سلامة البنية التحتية للمعلومات الوطنية الحساسة، خاصةً عندما يتعلق الأمر بالمعلومات الشخصية. في هذا السياق، يتعين على الجزائر، وغيرها من الدول، تعزيز التعاون الدولي وتبادل الخبرات في مجال الأمن السيبراني لمواجهة هذه التحديات.

---

[1] امال حابت، دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال في مواجهة دور الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، المجلة الدولية للبحوث القانونية والسياسية، المجلد 05، العدد 03 ،2021، ص474.

[2] نفس المرجع، ص476-477.

[3] سمير بارة، "الدفاع الوطني والسياسات الوطنية للأمن السيبارني (Cyber Security) في الجزائر: الدور والتحديات"، جامعة قاصدي مرباح، ورقلة، ص445.

علاوة على ذلك، ينبغي تطوير استراتيجيات دفاعية فعّالة لحماية البنية التحتية الرقمية الوطنية ومواجهة التهديدات السيبرانية بشكل شامل. ومن الضروري أيضًا دعم البحث والتطوير في مجال الأمن المعلوماتي، وتعزيز التدريب والتوعية لدى المؤسسات والمواطنين حول مخاطر الأمن السيبراني. يتعين على القطاع العام والخاص الالتزام بتطبيق أفضل الممارسات والمعايير الدولية في مجال الأمن المعلوماتي، مما يشمل إجراءات الحماية الوقائية والاستجابة للحوادث وإدارة المخاطر. إن تحقيق الأمن السيبراني يشكل تحديًا متناميًا في ظل تطور التكنولوجيا، ولكن التعاون والتنسيق الدوليين يمكن أن يسهما بشكل كبير في تعزيز الحماية وتعزيز الاستقرار السيبراني للدولة.[1]

المطلب الثاني: الدور الحكومي في حماية البيانات الشخصية للأفراد

أدى إنتشار وتطور التقنيات التكنولوجية الحديثة إلى رقمنة حياة الأفراد، وتم التحول من المعالجة الورقية للبيانات إلى المعالجة الإلكترونية، فلم تعد البيانات الشخصية للأفراد حبيسة الأوراق والدفاتر، بل غدت موضوعة فى بيئة رقمية متاحة للجميع يسهل الوصول إليها، مما يعرض تلك البيانات للعديد من الإنتهاكات.[2]

أولا: المخاطر التي تهدد خصوصية البيانات الشخصية للأفراد

تتفاوت تلك المخاطر بحسب المراحل التي تمر بها البيانات الشخصية من تجميع ومعالجة وإتاحة عبر الإنترنت، وأي إجراء ينطوي على أي مساس بخصوصية البيانات الشخصية ويهدد حقوق وحريات الأفراد.

ثانيا: المخاطر المتعلقة بتجميع البيانات الشخصية

عملية التجميع تُعرف عادةً بأنها أي عملية تتضمن جمع وتنظيم عناصر البيانات لشخص ما، ثم إدراجها في بطاقة معلومات، سواء كانت ورقية أو إلكترونية. تعتبر عملية جمع البيانات أمرًا حتميًا لإجراء عمليات المعالجة التي لا تخلو من مخاطر الاعتداء على خصوصية تلك البيانات المجمعة.

---

[1] بن الشريف لامية، خلالفة خديجة ، "مكتبة المن السيبراني في السياسات الدفاعية الجزائرية، مذكرة تخرج مكملة لنيل شهادة الماستر في العلوم السياسية، تخصص علاقات دولية، جامعة الحاج لخضر باتنة، 2019/2018، ص 57.

[2] عبد القادر سعيدي،" المصلحة المركزية الإلكترونية في مواجهة مجرمي العالم الافتارضي"، في:

www.essalamonline.com 2018/17:42 مارس03

في كثير من الأحيان، تقوم الجهات الحكومية أو الهيئات الخاصة بتجميع البيانات المفصلة خاصة بالمتعاملين معها، وهذا قد يؤدي لسوء استخدام تلك البيانات المحفوظة، خصوصًا إذا تم ربط الأجهزة المشتركة عبر شبكات العمل، مما يسهل عملية تبادل المعلومات الشخصية بينها.[1]

ويمكن أيضًا تجميع البيانات الشخصية للأفراد دون علمهم باستخدام تقنيات التكنولوجيا الحديثة عبر شبكة الإنترنت، مثل ملفات الكوكيز التي تستخدمها الشركات التجارية في أغراض الدعاية لخدماتها ومنتجاتها. وعلى الرغم من فوائدها العديدة، فإن ملفات الكوكيز تعد من أنجح الوسائل المستخدمة لملاحقة خصوصية الأفراد وكشف بياناتهم الشخصية، مما قد يؤدي إلى سوء استخدامها في أغراض غير مشروعة.

وتعتبر الوسيلة الأكثر خطورة من ذلك هي أنظمة جمع البيانات، أو ما يُعرف بالبرمجيات التتبع والالتقاط، حيث تُمكِّن هذه الوسيلة مستخدميها من جمع أكبر قدر ممكن من المعلومات السرية ومعالجتها بسرعة فائقة، مما يزيد من خطورة انتهاك الخصوصية والتعرض للاختراق.[2]

ثالثا: المخاطر الناجمة عن حوسبة البيانات الشخصية

تقنية حوسبة البيانات الشخصية، المعروفة أيضًا بتقنية تعلم الآلة، تتميز عادة بتطبيقاتها التي تتكيف مع البيانات التي تم الحصول عليها. فمثلاً، في حالة المتاجر المتعددة الأقسام، سيأخذ النظام في الاعتبار المشتريات السابقة للعملاء لغرض الدعاية للمنتجات، وتوجيههم إلى المنتجات الأخرى التي قد تكون ملائمة لهم.[3]

دور الحكومة في حماية البيانات الشخصية

قام المشرع الجزائري بتجسيد مجموعة من التدابير الوقائية لحماية البيانات الشخصية، وقد تضمنتها عدة نصوص قانونية، مثل الأمر رقم 05-03 الذي يتعلق بحقوق المؤلف والحقوق المجاورة، بالإضافة إلى بعض أحكام القانون رقم 09-04الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. كما تضمنت بعض مواد القانون رقم 15-04 التي تحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكتروني. تعتبر حماية البيانات الشخصية في هذا السياق من أهم العوامل التي تسهم في تعزيز الثقة وتشجيع التجارة وتقديم مختلف الخدمات الإلكترونية. وبفضل هذه التدابير الوقائية، يتم

[1] Myriam Dunn Cavelty, Information Age Conflicts : A Study of the Informatiun Revolution and Changing International Operating Environment.

[2] حنان بن عاتق، توفيق حجماوي، "واقع التطور التكنولوجي وتأثيره على آداء المنظمة في الجزائر"، ملتقى دولي حول: الإبداع والتغيير التنظيمي في المنظمات الحديثة، جامعة سعد دحلب، البليدة، كلية العلوم الاقتصادية، وعلوم التسيير، 2013، ص17.

[3] نبيل مزاش، أثر الحرب السيبرانية على العلاقات الدولية بين القوى الكبرى في النظام الدولي، مذكرة ماستر (جامعة الحاج لخضر كلية الحقوق والعلوم السياسية، تخصص: علاقات دولية، 2020-2021).

توفير بيئة قانونية ملائمة تعزز الحماية للبيانات الشخصية وتضمن سلامتها من الاستخدام غير القانوني أو الإساءة إليها.[1]

كما أضاف القانون 18-04 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، إجراءات تساهم في حماية المعطيات الشخصية. ليتم بعده إصدار نص قانوني يخص مباشرة الأشخاص الطبيعيين في مجال معالجة معطياتهم ذات الطابع الشخصي بموجب أحكام القانون 18-07، والذي كرس آليات تخص مختلف تفاصيل معالجة المعطيات ذات الطابع الشخصي.

لقد كرس المشرع الجزائري على غرار مختلف التشريعات الدولية الأخرى سلطات إدارية مستقلة تتكفل بحماية البيانات الشخصية بصورة مباشرة أو غير مباشرة، حيث نميز السلطة الأساس المكرسة في إطار حماية الأشخاص الطبيعيين في مجال معالجة معطياتهم ذات الطابع الشخصي، والتي تسمى بموجب أحكام القانون 18-07 بـ "السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي"، هذا بالإضافة إلى السلطات المخولة بصفة غير مباشرة للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، لاسيما عندما يتعلق الأمر بجرائم تخص البيانات الشخصية وتتطلب في متابعتها الحصول على معلومات من خارج التراب الوطني، مما يتيح المجال لطلب المساعدة وتبادل المعلومات قصد جمع الأدلة للتعرف على مرتكبي الجرائم المتصلة بتقنية المعلومات.

جاء إقرار إنشاء السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، تجسيدا لأحكام الدستور الجزائري المعدل سنة ،2016 لاسيما أحكام المادة 46 منه، وما تم إقراره بموجب أحكام القانون ،07-18 وكذا تأكيد التعديل الدستوري الأخير لسنة 2020 مبدأ تكريس حماية المعطيات الشخصية بموجب أحكام الفقرتين الرابعة والخامسة من المادة 47 منه.[2]

المطلب الرابع: دور الذكاء الإصطناعي في الحد من الهجمات السيبرانية

يمكن للذكاء الاصطناعي أن يلعب دوراً هاماً في مكافحة الجرائم السيبرانية. كما أنه يمكن استخدامه لتحليل البيانات والكشف عن التهديدات السيبرانية وتحديد الممارسات الغير عادية والأنماط السلوكية التي

[1] تومي يحي، الحماية القانونية للمعطيات ذات الطابع الشخصي على ضوء القانون 18- 07 دراسة تحليلية، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد04، العدد02، سنة2019، ص1524.

[2] نصت المادة 47 من الدستور الجزائري المصادق عليه بموجب استفتاء أول نوفمبر2020 على ما يلي:

" لكل شخص الحق في حماية حياته الخاصة وشرفه".

" لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت. لا مساس بالحقوق المذكورة في الفقرتين الأولى والثانية إلا بأمر معلل من السلطة القضائية.

"حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي. يعاقب القانون على كل انتهاك لهذه الحقوق" .

تشير إلى وجود هجمات سيبرانية.

ومن بين الأدوار التي يمكن للذكاء الاصطناعي القيام بها في مكافحة الجرائم السيبرانية:

1/الكشف عن التهديدات السيبرانية: حيث يمكن استخدام تقنيات الذكاء الاصطناعي لتحليل البيانات والأنماط السلوكية للأنظمة والشبكات.

كما يمكن الكشف عن التهديدات السيبرانية وتحديد درجة الخطورة الخاصة بها.

ويمكن أن يتم ذلك باستخدام تقنيات التعلم الآلي والتحليل الضخم للبيانات.

2/ التحليل السلوكي: يمكن استخدام الذكاء الاصطناعي لتحليل السلوك والأنماط الغير عادية للمستخدمين والأنظمة والتطبيقات، والتعرف على الأنشطة الغير مشروعة والتهديدات السيبرانية المحتملة.

3/ الوقاية والاستجابة الفورية: كما يمكن استخدام الذكاء الاصطناعي لتحليل البيانات والأنماط السلوكية في الوقت الفعلي، وتنبيه المختصين في الأمن السيبراني عندما يتم اكتشاف أنشطة غير عادية أو تهديد سيبراني محتمل. ويمكن أيضاً الاستفادة من هذه المعلومات لاتخاذ إجراءات وقائية فورية للحد من التأثير السلبي للهجمات السيبرانية[1].

4/ تحسين الأمن السيبراني: حيث يمكن استخدام الذكاء الاصطناعي لتحسين الأمن السيبراني عن طريق تحليل البيانات والأنماط السلوكية للأنظمة والشبكات والتطبيقات.

كما يمكن تحديد الثغرات الأمنية وتوفير الحماية اللازمة للحد من التهديدات السيبرانية.

5/**التعرف على الجرائم السيبرانية:** حيث يمكن استخدام الذكاء الاصطناعي لتحليل البيانات والأنماط السلوكية والتعرف على أنماط الجرائم السيبرانية، وذلك يمكن أن يساعد في تحديد المجرمين وتوفير الأدلة الرقمية اللازمة لمقاضاتهم.

6/ **تطوير حلول الأمن السيبراني:** كما يمكن استخدام الذكاء الاصطناعي لتطوير حلول الأمن السيبراني المتقدمة، وذلك من خلال تحليل البيانات والأنماط السلوكية وتطوير تقنيات جديدة ومتطورة للحماية من الهجمات السيبرانية.

بشكل عام، يمكن للذكاء الاصطناعي أن يلعب دوراً هاماً في مكافحة الجرائم السيبرانية. وذلك من خلال تحليل البيانات والأنماط السلوكية والتعرف على التهديدات السيبرانية المحتملة وتحديد الثغرات الأمنية وتطوير

[1] عائشة عبد الحميد، الإطار القانوني والتشريعي للرقمنة والذكاء الإصطناعي،دراسة منشورة، المجلة الدولية للتعليم بالإنترنت، المجلد 19، العدد 01، يوليو 2020، ص103.

حلول الأمن السيبراني المتقدمة[1]. ومع تطور تقنيات الذكاء الاصطناعي، يمكن أن يتحسن الأمن السيبراني ويتم مكافحة الجرائم السيبرانية بشكل أكثر فعالية وتحديد المجرمين ومقاضاتهم بشكل أسرع.

مفهوم الجرائم السيبرانية وأنواعها وأساليب ارتكابها وطرق مكافحتها.

المبحث الثالث: التحديات التي تعترض تحقيق الأمن المعلوماتي في الجزائر

يهدف هذا المبحث إلى تقديم جملة من التحديات التي تعيق عملية تحقيق الأمن المعلوماتي وهذا راجع لجملة من الأسباب تحاول الدولة الجزائرية تخطيها بتوفير كل التقنيات اللازمة.

المطلب الأول: ضعف خدمة الإنترنت

إن التوجه العالمي نحو الاقتصاد الرقمي، يحتم على كل الدول منها الجزائر انتهاج هذا النمط، الذي كان وليدا لمختلف التطورات التكنولوجية الضخمة، كما يحتم عليها إرساءا فعالا لمختلف البنى التحتية التي من شأنها تسهيل تبنيه؛ وتعد تكنولوجيا المعلومات والاتصالات أهم قاعدة لتطبيق الاقتصاد الرقمي، لذا فالجزائر اليوم أمام تحديات كبرى للوصول إلى استثمار فعال قادر على تحديث الاقتصاد، وإرساء قاعدة تمكن من مواكبة العصر.

تكنولوجيا المعلومات والاتصالات تُعَدُّ أحد الأسس الأساسية لبناء الاقتصاد والمجتمع، وقد قامت منظمات دولية بتقديم مجموعة من المؤشرات لقياس مستوى تطور تلك التكنولوجيا وحجم الفجوة الرقمية بين الدول المتقدمة والمتخلفة. تتنوع هذه المؤشرات وتشمل عدة جوانب مختلفة تؤثر في نمو وتطور هذا القطاع. يُعدُّ من بين أهم تلك المؤشرات:[2]

- ✓ مؤشرات الكثافة الاتصالية: تُقاس بواسطة عدد الهواتف النقالة والثابتة لكل 100 فرد، وسعة الشبكات الاتصالية، بما في ذلك معدل تدفق البيانات وغيرها.
- ✓ مؤشرات التقدم التكنولوجي: تُقاس بواسطة عدد الحواسيب وعدد مستخدمي الإنترنت، وحجم امتلاك الأجهزة الإلكترونية مثل الفاكس والهواتف من قِبل الأفراد والمؤسسات.
- ✓ مؤشرات الإنجاز التكنولوجي، سواء كانت مستوردة أو مصدرة.

هذه المؤشرات أدت إلى تقسيم العالم وظهور ما يُعرف بفجوة الرقمية، والتي تشير إلى التفاوت الكبير الناتج عن ثورة التكنولوجيا في ميدان الاتصالات والمعلومات، بين الدول المتقدمة والنامية. على الرغم من

[1] شركة تقنين للمحاماة والإستشارات القانونية.TAQNEEN LAW FIRM تاريخ النشر 4 أبريل 2023

[2] تقرير الإتحاد الدولي للإحصاءات تكنولوجيا المعلومات والاتصالات للمجلس الاقتصادي والاجتماعي.

الاستثمارات الكبيرة التي تُخصص للتطوير في الدول النامية، إلا أنها لا تزال تعاني من تأخر ملحوظ في هذا المجال مقارنةً بالدول المتقدمة.[1]

تقع الجزائر بالاستناد إلى التقرير العالمي لتكنولوجيا الإعلام والاتصال ضمن مرحلة الدول المجبرة على الانتقال للاقتصاد الرقمي، والتي تقع فيها مجموعة من الدول مثل تونس، اليمن، مالي، العراق، سوريا، المغرب، جنوب إفريقيا، مصر وغيرها، كما يؤكد التقرير على أن الجزائر من الدول التي تحتل المراتب الأخيرة عالميا وعربيا كذلك، ويمكن رصد تطور مراتب الجزائر عالميا بالاستعانة بالجدول التالي:

السنة	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
الترتيب/ العدد الاجمالي	/87 102	/80 104	/87 115	/80 122	/88 127	/108 134	/113 133	/117 138	/118 142	/114 166	/114 166	/113 167	/112 175	/104 174

جدول: تطور ترتيب الجزائر حسب مؤشرات تنمية تكنولوجيا المعلومات والاتصالات

يتضح من الجدول السابق كيف أن الجزائر تحتل المراتب الأخيرة عالميًا، على الرغم من التحسنات الملحوظة والتي يمكن اعتبارها طفيفة إذا ما تم مقارنتها بتداعيات تبني الاقتصاد الرقمي. هذا يعكس وضعية تطبيق التكنولوجيا ومستوى الأنشطة المختلفة في هذا القطاع. بالرغم من الاستثمارات والتجهيزات التي توفرها الجزائر، إلا أنها تظل في المراتب الأخيرة عالميًا. هذا يجعلها ملزمةً بمراجعة مختلف الخطط والإستراتيجيات للقطاع والسعي وراء التحديث، وتوفير كل المستلزمات اللازمة. فهي مجبرة على توفير البنية التحتية الأساسية وغيرها من الإجراءات التي من شأنها دفع عجلة النمو لتحسين وضعية الجزائر ومرتبتها على المستوى العالمي.

تأثرت الجزائر بثورة المعلومات وتكنولوجيا الاتصالات، حيث وجدت نفسها مرغمة على مواكبة العصر وفتح باب المنافسة، وإرساء دعائم قادرة على بناء الاقتصاد ومواكبة العصر، وقامت بتوفير أغلفة مالية ضخمة خلال مختلف برامج الإنعاش التي انتهجتها لتأهيل مستوى الشبكة الاتصالية، وقد قامت الجزائر بما يلي:[2]

- ✓ تحديث الشبكة الوطنية للاتصالات وذلك بإدخال مكثف للتكنولوجيا المتجددة، وكالرقمنة الكاملة للشبكات وتشغيل خدمات جديدة.
- ✓ رفع طاقة الشبكة الوطنية والخطوط الدولية كذلك.

[1] محمد شايب هدار لحسن، تقييم قطاع الاتصال وتكنولوجيا الاعلام في الجزائر، أبحاث المؤتمر الدولي: تقييم أثار برامج الاستثمارات والنمو الاقتصادي خلال الفترة 2001-2014، ص11.

[2] www.andi.dz

- ✓ توسيع الشبكة للتكفل بحاجيات كل الهيئات الاقتصادية والمالية مثل شبكات البنوك وغيرها.
- ✓ إدخال خدمات الهاتف النقال عبر الساتل.
- ✓ تشغيل أرضية انترنت ذات نطاق واسع وتوفير كل الخدمات العادية منها والمميزة.

بالرغم من كل هذا سجلت الجزائر رداءة في مستوى خدماتها، خاصة فيما يتعلق بمختلف خدمات سوق الانترنت لأسباب متنوعة، منها العجز التكنولوجي كما ونوعا، والمسجل على مستوى البنى التحتية للقطاع، لعدم قدرتها الفعلية على إرساء دعائم قادرة على سد الفجوة الرقمية رغم ضخامة حجم الغلاف المالي الذي خصص في هذا الجانب، فمثلا طول الشبكة الأرضية 6للألياف البصرية على 47000 كلم في منتصف 2013،[1] وهي تمثل حوالي 44 % فقط من مد الألياف البصرية على مستوى التراب الوطني، وهي نسبة ضئيلة مقارنة بالميزانيات المالية المخصصة لهذا؛ وهذا يرجع لعدة أسباب على رأسها تفرد اتصالات الجزائر بتوفير خدمات الانترنت، وفي كل المراحل المعتمدة لتقديم الخدمة، وهذا يعد جد صعب نظرا لكبر مساحة الجزائر من جهة، وضعف إمكانيات المؤسسة سواء البشرية أو التقنية مقارنة مع الطلب المتزايد من جهة أخرى.

تسعى الجزائر للدخول إلى الاقتصاد الرقمي، ويتضح هذا من خلال التجديد والتطوير لتأهيل الشبكات واستيعاب أكثر للطلب، وكذا الزيادة من نوعية وجودة الخدمة، كما تقوم الدولة بإنجاز مجموعة من المشاريع لتحسين بنيتها، ويمكن ذكر البعض منها على سبيل المثال:

- ✓ الانطلاق في أشغال إنجاز كابل بحري جديد يربط وهران بمدينة فلانسيا الإسبانية ويمتد إلى الجزائر العاصمة يبلغ طوله حوالي 550كم وبقدرة استيعاب 100 جيقا وقدرت تكاليف المشروع بحوالي 26 مليون أورو بالنسبة لخط وهران فلانسيا و10 مليون أورو إضافية لفرع اتصالات الجزائر.[2]
- ✓ توسيع شبكة الألياف البصرية (27 مليار دج للتحديث) كبديل للكوابل النحاسية التي أصبحت متقادمة وتكلف المؤسسة المسوقة الكثير من أجل التصليح).
- ✓ توسيع الحظائر التكنولوجية وبناء مراكز لتطوير الأقمار الصناعية
- ✓ بالإضافة إلى أنه يتحتم عليها الإدراج السريع للأنترنت الفائق السرعة وتعميمه، وكذا إدراج التكنولوجيات الحديثة التي من شأنها فعلا تطوير مكانة الجزائر داخليا وخارجيا.

إن مجموع الخطط المستقبلية لعصرنة البنى التحتية للقطاع، السابقة الذكر وغيرها يجب أن تكون قادرة على مواكبة التسارع التكنولوجي، الذي يؤثر بشكل كبير على تقادم مختلف الخطط والقوانين[3].

---

[1] Https://www.algerietelecom.dz.

[2] موقع وزارة البريد وتكنولوجيا الإعلام والإتصال: www.mptic.dz

[3] Lu, Marcus, "Economy Visualized: Where 5G Will Change the World،" Visual Capitalist, (22/03/2021), see the link: https://bit.ly/3C8U9jl ،2020/03/09

المطلب الثاني: تكثيف مراكز الحماية من الهجمات السيبرانية

في إطار السياسات التي ينبغي على الجزائر اعتمادها، خاصة في السنوات الأخيرة مع تزايد الحروب الإلكترونية، يجب على الجزائر ومنظومة الأمن الوطني الجزائرية التركيز بشكل كبير على إنشاء مراكز وإطارات عالية المستوى في مجال السيبرانية، وتعزيز استراتيجياتها في مجال التدريب على الهجمات السيبرانية والردع السيبراني كآلية استباقية ووقائية أمنية جزائرية.

يمثل نظام المعلومات الذي يتيح إتاحة المعلومات وضمان سلامة الدولة ومعرفة أسرار الدول الأخرى نقطة أساسية في هذه الجهود. ومن ثم، تتضمن أبرز أنواع الهجمات والدفاع المدرجة في استراتيجية الحماية والرد الإلكتروني ما يلي:[1]

- ✓ الهجمات السرية: وتعد أحد أنواع التجسس باستخدام وسائل التكنولوجيا الفائقة؛ كالهجمات السيبرانية المتطورة التي تطلق من قبل الدول أو الجماعات الإجرامية التي تقع ضمن هذه الفئة
- ✓ الهجمات المتكاملة: تتمثل في تخريب نظم معلومات الخرم المدنية أو العسكرية الهامة. فيمكن أن ينطوي التخريب على التلاعب بالبيانات داخل نظم المعلومات التي يمكن أن تشوه وعي العدو عن طريق نشر معلومات خاطئة داخل أنظمة ذكائه، أو إخفاء أنشطة محددة قد تكون تحت المراقبة.

وعلى ضوء ما سبق، يمكن تحديد أهم الاستراتيجيات والإجراءات الأمنية مواجهة الجريمة الالكترونية وتأمين الأمن السيبيراني من خلال تقوية وتكثيف الأجهزة الخاصة بالأمن الالكتروني علما أن الجزائر حاليا تحوز على:

1. مركز الوقاية من جرائم الإعلام الآلي للدرك الوطني:

تأسس المركز في عام 2008 ويُعتبر الجهاز الوحيد المختص في هذا المجال في الجزائر. يهدف المركز إلى تأمين منظومة المعلومات لخدمة الأمن العام، ويُنظر إليه كمركز توثيق مقره يقع في بئر مراد رايس. يُكرس المركز جهوده لتحليل بيانات ومعطيات الجرائم المعلوماتية وتحديد هوية مرتكبيها، سواء كانوا أفرادًا فرديين أو عصابات. يهدف ذلك إلى تأمين الأنظمة المعلوماتية والحفاظ عليها، خاصة تلك المستخدمة في المؤسسات الرسمية والمصارف.[2]

---

[1] رغدة البهي، الردع السيبراني: المفهوم والإشكاليات والمتطلبات، Deterrence Cyber Requirements and: Concept The, Dilemmas، برلين: المركز الديمقراطي العربي، مقال منشور يوم 04 فيفري2019، مجلة العلوم السياسية والقانون.

[2] خيرة روابحي، ثقافة الأنترنت: دراسة ميدانية الاستعلامات الشبكة بمدينة تيهرت، رسالة ماجستير، جامعة وهران، كلية العلوم الإنسانية والحضارة الإسلامية، قسم علم المكتبات والعلوم الوثائقية، 2009-2010، ص78.

ويهدف هذ المركز إلى مساعدة الأجهزة الأمنية الأخرى بالتعاون من أجل مكافحة الجرائم المعلوماتية، حيث يعنى المركز بتطوير أساليب التعامل مع هذه الجرائم ووضع قوانين لتنظيم مجال استغلال المعلومة من خلال تنسيق مع وزارة العدل وكذا من خلال معهد خاص بعلم الإجرام لتطوير مستوى التعامل مع الجريمة بصفة عامة والجريمة المعلوماتية بصفة خاصة، فالجزائر تعمل جاهدا على الاستفادة من خبرات البلدان الأخرى في تأمين المنظومة المعلوماتية وحمايتها من الجرائم ضمن مجموعة من العناصر أهمها:[1]

- ✓ **الوقاية:** وتشمل حملة تحسيسية وتوعية بالتنسيق مع وزارة التضامن الوطني والأسرة، والعمل على ملتقيات ومحاضرات وأياما دراسية ومنتديات دولية، ومشاركة في منتديات صحفية وحصص تلفزيونية وإذاعية وغيرها من وسائل النشر والإشهار .
- ✓ **المكافحة:** توعية الجزائريين من خلال استعمالهم لشبكات التواصل واستخدام الأنترنت وذلك من خلال تعليقاتهم المدافعة عن الجزائر ومعرفة الأخطار بسلوكيات مشبوهة أو اعتداءات عبر نشر فيديوهات توصل إلى الجناة، مما يسهل التحقيق لدى مصالح الدرك وإلقاء القبض على المشبوهين ومرتكبي الجرائم في الوقت المناسب.

2. المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني:

تعتبر هذه المؤسسة مؤسسة عمومية ذات طابع إداري تحت الوصاية المباشرة لوزير الدفاع الوطني. وتتولى مهامًا متعددة تشمل إجراء الخبرات والفحوص في إطار التحريات الأولية والتحقيقات القضائية، فضلاً عن ضمان المساعدة العلمية أثناء القيام بالتحريات المعقدة.[2]

يُعَدُّ المعهد أحد المشاريع المنجزة في إطار تطوير سلك الدرك الوطني "ببوشاوي". تم إنشاؤه بموجب مرسوم رئاسي رقم 04/133 المؤرخ في 26 جوان 2004، وقد شملت عملية الإنشاء تجهيز المورد البشري واقتناء المعدات العلمية والتقنية اللازمة. يقوم المعهد بتنفيذ العديد من المهام الخدمية اعتباراً من الفاتح جانفي 2009. وقد تم تخصيص الفترة الممتدة بين عامي 2004 و2009 لتأهيل الكوادر، وتوفير التدريبات

[1] هند علوي، المرصد الوطني لمجتمع المعلومات بالجزائري، قياس النفاذ إلى تكنولوجيا المعلومات والاتصالات بقطاع التعليم بالشرق الجزائري، أطروحة دكتوراه، جامعة منتوري– قسنطينة، كلية العلوم الإنسانية، تخصص: علم المكتبات 2007–2008، ص41.

[2] مراد كريم، مجتمع المعلومات أثره في المكتبات الجامعية، مدينة قسنطينة، أطروحة ذكتوراه، جامعة منتوري، كلية العلوم الإنسانية والاجتماعية، قسم علم المكتبات، 2008–2007، ص 36.

اللازمة التي تسهم في تلبية الطلبات الواردة من السلطة القضائية وضباط الشرطة القضائية والجهات المؤهلة، وذلك خاصةً أثناء معالجة القضايا ذات الطبيعة المعقدة.[1]

كما في تنظيم دورات الإتقان والتكوين لخريجي التخصص في العلوم الجنائية، وذلك لتأهيلهم وتحسين مهاراتهم بعد الانتهاء من التدريب الأكاديمي. ويحتوي المعهد على عدة أقسام ومصالح متخصصة من بينها:

- ✓ مصلحة البصمات: تعنى بتحليل ودراسة البصمات الجنائية للمساهمة في التحقيقات الجنائية وتحديد هويات المتورطين في الجرائم.
- ✓ مصلحة البيئة: تتعامل مع القضايا ذات الصلة بالجرائم البيئية وتقديم الدعم العلمي في هذا المجال.
- ✓ مصلحة الأمن السيبراني: تعمل على رصد ومراقبة وتتبع الاختراقات والقرصنة المعلوماتية، واكتشاف المعلومات المسروقة، وتفكيك البرمجيات الخبيثة.

تتبع هذه المصالح الإجراءات المتقدمة في مجالاتها المختصة لتحسين الأمن الجنائي والتحقيق في الجرائم المعقدة، وتسهم في تطوير القدرات والمهارات الفنية للكوادر العاملة في هذه المجالات.[2]

3. المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني:

لتلبية مطلب الأمن المعلوماتي ومحاربة التهديدات الأمنية الناجمة عن الجرائم الإلكترونية، قامت مصالح الأمن بإنشاء المصلحة المركزية للجريمة الإلكترونية. بدأت هذه المبادرة بتكييف التشكيل الأمني لمديرية الشرطة القضائية، حيث شكلت فصيلة النواة الأولى لتشكيل أمني خاص لمحاربة الجريمة الإلكترونية. وفي مرحلة لاحقة، تم إنشاء المصلحة المركزية لمحاربة الجرائم الإلكترونية التابعة للأمن الوطني، والتي ترتبط بتكنولوجيا الاتصالات والمعلومات، وذلك بقرار من المدير العام للأمن الوطني. تم إضافتها للهيكل التنظيمي لمديرية الشرطة القضائية في يناير 2015.[3]

4. الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها:

تم تشكيل هذه الهيئة بموجب المرسوم الرئاسي رقم 261-15، وهي سلطة إدارية مستقلة تعمل تحت إشراف وزير العدل. تعمل هذه الهيئة تحت إشراف ومراقبة لجنة مديرية يترأسها وزير العدل، وتضم أساسًا

---

[1] آمنة بن عبد ربه، النظام الاقتصادي الجديد المبني على المعرفة وتطور مجتمع المعلومات والتكنولوجيا الحديثة للاتصال، الحلول المقترحة لإرساء مجتمع معلومات ناجح ومتكامل في الجزائر، رسالة ماجستير، جامعة الجزائر كلية العلوم السياسية والاعلام، قسم علوم الاعلام والاتصال،2006-2005، ص35-33.

[2] عادل غزال، مشاريع الحكومة الإلكترونية من الاستراتيجية إلى التطليق، مشروع الجزائر: الحكومة الالكترونية2013، مجلة المكتبات والمعلومات، العدد 34، مارس 2014، ص64.

[3] إلياس شاهد، الحاج عرابة، عبد النعيم دفرو، تقييم تجربة تطبيق الحكومة الالكترونية الجزائرية، المجلة الجزائرية للدراسات المحاسبية والمالية، العدد الثالث، 2016، ص130.

أعضاءً من الحكومة المعنيين بالموضوع، ومسؤولي مصالح الأمن، وقضاة من المحكمة العليا، حيث يُعيّن هؤلاء القضاة من قبل المجلس الأعلى للقضاء.[1]

تم تكليف الهيئة باقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاتصال والمكافحة منها، وتنشيط وتنسيق عمليات الوقاية منها. كما تقوم الهيئة بمساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة هذه الجرائم عبر جمع المعلومات وتوفيرها، بالإضافة إلى تقديم الخبرات القضائية اللازمة. وتضمنت مهام الهيئة أيضًا ضمان المراقبة الوقائية للاتصالات الإلكترونية، بهدف الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والتي تمس بأمن الدولة، وقد نص سابقا على إنشاء هذه الهيئة المادة 13 من القانون 09/04المؤرخ في أوت المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها من خلال "تنشأ هيئة وطنية وتنظيمها وكيفيات سيرها عن طريق التنظيم" أما مهامها فقد أوردت المادة 14 من نفس القانون وتتمثل في:[2]

- ✓ الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: إن إجراءات الوقاية تكون بتوعية مستعملي تكنولوجيات الإعلام والاتصال بخطورة الجرائم التي يمكن أن يكونوا ضحاياها وهم يتصفحون أو يستعملون هذه التكنولوجيات، ومن أهم هذه الجرائم: التجسس على الاتصالات والرسائل الإلكترونية، التلاعب بحسابات العمال، اختراق أجهزة الشركات والمؤسسات الرئيسية أو الجهات الحكومية...الخ
- ✓ مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: بحسب نص المادة 14 من القانون 09/04 هناك نوعان من المكافحة تقوم بهما هذه الهيئة.

- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم المتصلة بتكنولوجيا الاعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية المادة 14 (فقرتب)من القانون 09/04 .
- تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها يقترح المشروع في هذا الفصل إنشاء هيئة وطنية مختصة تتولى مهام أهمها: تنشيط وتنسيق عملية الوقاية من الجرائم المعلوماتية ومساعدة السلطات القضائية ومصالح الشرطة القضائية من التحريات

[1] عبد القادر عبان، تحديات الإدارة الالكترونية في الجزائر،دراسة سوسيولوجية ببلدية الكاليتوس العاصمة، أطروحة الدكتوراه، جامعة محمد خيضر، بسكرة، كلية العلوم الانسانسة والاجتماعية، 2015، تخصص: إدارة وعمل 2016، ص91.

[2] أسامة بن صادق طيب، محمد نور بن ياسين فطاني، عصام بن يحيى الفيلالي، الحكومة الالكترونية، نحو مجتمع المعرفة، معهد البحوث و الاستشارات، العدد التاسع، جامعة الملك عبد العزيز، جدة السعودية، 2013، ص 04.

التي تجريها بشأن هذه الجرائم، وما تقوم به أيضا من تجميع المعلومات من نظيرتها في الخارج قصد محاربة هذا النوع الخطير من الإجرام.[1]

المطلب الثالث: تأطير وتكوين كل الجهات المعنية بالاختراق

كيف نحمي أجهزتنا و بياناتنا من الإختراق أو المراقبة بسبب التهديدات والمخاطر الأمنية والتقنية، التي تواجه العاملات والعاملين في مختلف المجالات لابد من التحصينات لهاجس الهجمات السيبرانية

إن حماية الخصوصية الرقمية والأجهزة يكون: بالدرجة الأولى والأساسية من خلال "**رفع الوعي التقني***" تجاه المخاطر التي تهددنا. لاحقاً تأتي برامج وتطبيقات الأمن التي تساعد في حماية أجهزتنا و بياناتنا وخصوصيتنا الرقمية.[2]

يأتي رفع الوعي التقني من خلال معرفة التهديدات والمخاطر التي نتعرض أو ربما نتعرض لها، وآليات الإستهداف التي يمكن أن نتعرض لها والتي سنذكرها عبر مجموعة من النقاط:

- بسبب التهديدات والتحديات التقنية المستمرة، يقوم الأشخاص بسؤال صديقاتهم وأصدقائهم عن برامج أو تطبيقات تساعدهم في حماية أجهزتهم.
- ثقتنا الشخصية بالأشخاص يجب ألا تجعلنا نثق بـ خياراتهم التقنية. إلا في حال كانوا خبيرات أو خبراء تقنيين.
- بعض الصديقات والأصدقاء يقترحون علينا عن حسن نية برامج وتطبيقات استخدموها، لكن هذه البرامج ليست بالضرورة أن تكون آمنة. لهذا السبب، في حال الحاجة لسؤال أو طلب تقني يجب أن يتم توجيه السؤال للأشخاص أو الجهات التي لديها خبرة تقنية والتي هي موضع ثقة لديكم.
- لا يخفى على أحد أن شبكة الإنترنت تحتوي عدد كبير جداً من المواقع والمنتديات التي تتحدث عن الأمور التقنية وأمن المعلومات، خاصة المجموعات على "فيسبوك".
- عدد من هذه المواقع والمنتديات والمجموعات هي مواقع جيدة وتحتوي نصائح تقنية مفيدة وموثوقة، لكن العدد الأكبر منها يحتوي معلومات مغلوطة خاصة المواقع التي يكون فيها المدونة أو المدون أو الأشخاص اللواتي والذين يقومون بكتابة المواد ليس لديهم خلفية أو معلومات تقنية جيدة.

[1] سمير بارة، الدفاع الوطني و السياسات الوطنية للأمن السيبراني في الجزائر: الدور والتحديات، جامعة قاصدي مرباح، ورقلة، ص 445.

[2] باطلي غنية، الجريمة الإلكترونية (دراسة مقارنة)، أطروحة مقدمة لنيل شهادة دكتوراه، شعبة القانون الخاص، كلية الحقوق قسم القانون الخاص، جامعة باجي مختار، عنابة، د. س . م .2012 .2013.

- وقد تم ملاحظة أن عدد كبير من المواقع والمنتديات والمجموعات والأشخاص، يقومون بالترويج لبعض البرامج والتطبيقات على أنها آمنة أو تقوم بحماية الأجهزة، بينما في الحقيقة عدد من هذه البرامج والتطبيقات هي برامج غير ذي فائدة أو أنها برامج تحتوي برمجيات خبيثة.[1]
- من جهة ثانية، تقوم بعض الجهات باستغلال حاجة الأشخاص لحماية خصوصيتهم وأمنهم الرقمي، فتقوم بالترويج لبعض التطبيقات والبرامج على أنها برامج حماية أو برامج آمنة، بينما في الحقيقة هي برامج تنتهك الخصوصية وتقوم بالتنصت على الأجهزة وسرقة البيانات والمعلومات. مثال، تطبيق "Secure Mail" الذي يقوم بتسريب بيانات دخول حساب "جيميل | Gmail" وإرسالها إلى خادم يستخدمه المهاجمون. تطبيق "iLoud200%" الذي يتم الترويج له على أنه يقوم بمضاعفة صوت جهاز الهاتف لكنه يقوم بتحديد موقع الهاتف حتى لو تم تعطيل ميزة تحديد المواقع GPS.[2]
- تطبيق "IndexY" الذي يتم الترويج له على أنه يُظهر اسم الجهة المتصلة (شبيه بتطبيق "تروكولر Truecaller") لكنه في الحقيقة يقوم بنسخ تفاصيل المكالمات التي أجريت على الهاتف وإرسالها إلى خادم يستخدمه المهاجمون. وغيرها الكثير من التطبيقات التي يتم الترويج لها أو تظهر عند حدث ما، كما يحصل في سوريا منذ فترة عندما بدأت تتوقف وتنقطع الإتصالات عبر تطبيق "واتس اب"، قامت عدد من الجهات والأفراد بالترويج لتطبيقات تواصل بديلة، لكنها غير آمنة والترويج لتطبيقات تخطي الحجب (VPN) غير آمنة.[3]
- كذلك يجب القيام بدورات تكوينية لتوعية مستعملي الأجهزة عبر الشبكات دون الغفلة .

[1] Dan Craigen, Nadia Diakun-Thibault, and Randy Purse, Defining Cybersecurity.

[2] سمير بارة، "الدفاع الوطني والسياسات الوطنية للأمن السيبراني (Cyber Security) في الجزائر: الدور والتحديات"، جامعة قاصدي مرباح، ورقلة.

[3] عبد القادر سعيدي،" المصلحة المركزية الإلكترونية في مواجهة مجرمي العالم الافتراضي"، في: 03 مارس2018 من الموقع www.essalamonline.com

خلاصة الفصل

خلص الفصل الثالث والمعنون بالتوجه الاستراتيجي لإرساء الأمن المعلوماتي في الجزائر إلى جملة من الآليات المتبعة للحد من انتشار الهجمات السيبرانية وتعزيز الحماية الفعالة بتطوير العديد من الأدوات والتقنيات المستحدثة، ولكن لا تخلو المنظومة المعلوماتية لمختلف منصات التعليم أو المواقع الإلكترونية من عيوب وثغرات سهلت للمخترقين والعابثين بالأنظمة إلى إبراز العديد من التحديات التي يجب التطرق لها، وتوفير كل المعدات المادية والبرمجية للحد من هجس الهجمات السيبرانية خصوصا من أطراف معادية للجزائر.

الخاتمة

الخاتمة.

تندرج التهديدات السيبرانية ضمن التهديدات الأمنية الجدية للأمن القومي، والأخطبوط الذي أنتجته الثورة المعلوماتية التكنولوجية، الذي امتدت أذرعه في جميع أنحاء العالم، ولم تفلت من قبضته الدول الضعيفة والمتطورة على حد سواء، واستشرى خطره المدمر على مختلف القطاعات الحياتية الاقتصادية منها والاجتماعية والسياسية، وحتى الشخصية، وأن جميع الأفراد في العالم مستهدفون بجميع فئاتهم وأعمارهم، ومرجعياتهم الفكرية والدينية والثقافية.

ومع تصاعد التحول الجزائري نحو بناء مجتمع معلوماتي، وتكثيف الاعتماد على أدوات تكنولوجيا المعلومات والاتصالات، أدركت الأجهزة الأمينة الجزائرية المختصة في مكافحة المخاطر السيبرانية، أنه يتوجب عليها تأمين هذه المعلومات بشدة، لأن تداولها وإدارتها إلكترونيا عبر شبكات المعلومات والاتصالات، التي ترابطت محليا وإقليميا وعلميا، جعلها معرضة لخطر الاختراقات المعلوماتية، الأمر الذي يخلف الكثير من الآثار على الأمن الوطني الجزائري المعتمد على شبكات المعلومات وأدوات الاتصال لقد كان الهدف من الدراسة معرفة دور الأمن المعلوماتي من الحد من أهم التهديدات السيبرانية في بلادنا .

وعليه نخلص الى التوصيات والمقترحات التالية:

1. **تعزيز التعاون الدولي:** يهدف تعزيز التعاون الدولي في ميدان الأمن السيبراني إلى تيسير تبادل الخبرات وتقديم الدعم المتبادل لمواجهة التحديات السيبرانية المشتركة. يتعين تعزيز هذا التعاون الدولي على مستوى السياسات والتقنيات، مما يساهم في تعزيز قدرة الدول على التصدي للتهديدات السيبرانية بفعالية وفي تعزيز المرونة والأمان الرقمي على الصعيدين الوطني والدولي
2. **تطوير برامج تدريب متقدمة:** ينبغي تطوير وتنفيذ برامج تدريب متقدمة بشكل دوري، تستهدف تعزيز وتطوير مهارات وقدرات الكوادر الفنية المختصة في مجال الأمن السيبراني. يهدف هذا التدريب إلى تزويد الفرق الفنية بالمعرفة والمهارات اللازمة لمواكبة التطورات السريعة في مجال الأمن السيبراني والتصدي للتحديات المتزايدة بفعالية. يسهم هذا النهج في تحسين قدرة الكوادر على تنفيذ استراتيجيات أمان متقدمة وتطبيق أفضل الممارسات في مجال الحماية الرقمية.
3. **الاستثمار في البنية التحتية:** يجب التعزيز في استثمارات تحديث وتعزيز البنية التحتية السيبرانية كجزء أساسي من الاستراتيجية الوطنية في الجزائر. يتعين زيادة حجم الاستثمار لضمان تحديث الأنظمة وتطويرها، مما يعزز فعالية الاستجابة للتحديات الرقمية المتزايدة.
4. **في تفعيل رؤيتنا المستقبلية لمجال الأمن المعلوماتي في الجزائر**، يبرز توجه إيجابي يفيد بالتحول البارز نحو مستقبل يحمل في طياته تقدمًا هامًا في هذا القطاع الحيوي. من خلال تنسيق فعّال للجهود الحكومية وتعاون مستدام مع الشركاء الدوليين، يمكن تحقيق تحسين ملحوظ في جهود تعزيز الأمن السيبراني. يعزز هذا التحول استقرار البلاد ويشكل ركيزة أساسية هامة في هذا العصر الرقمي الذي يتسارع بوتيرة سريعة.

قائمة المراجع

قائمة المراجع

أولا: المصادر

القانون رقم 04-09 مؤرخ في 5 أوت2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات العالم والاتصال ومكافحتها، ج ر، عدد ،47 صادر في 16 أوت 2009.

المرسوم الرئاسي رقم 261-15 مؤرخ في 8 أكتوبر2015 يحدد تشكيلة وتنظيم وكيفيات سير البيئة الوطنية لوقاية من الجرائم المتصلة بتكنولوجيات العالم والاتصال ومكافحتها، ج ر، عدد 53 ، صادر في 8 أكتوبر 2015 .

المرسوم الرئاسي رقم 172-19 مؤرخ في 6 يونيو ،2019 يحدد تشكيلة البيئة الوطنية لوقاية من الجرائم المتصلة بتكنولوجيات العالم والاتصال ومكافحتها وتنظيميا وكيفيات سيرها، ج ر، عدد 37 ، صادر في 9 يونيو 2019.

المرسوم الرئاسي رقم 183-20 مؤرخ في 13 يوليو 2020، يتضمن إعادة تنظيم البيئة الوطنية لوقاية من الجرائم المتصلة بتكنولوجيات العالم والاتصال ومكافحتها، ج ر ، عدد ،40 صادر في 18 يوليو 2020.

سعد علي الحاج علي بكري، "الأمن السيبارني ومعضلة حمايته، عولمة التعليم العالي الرقمي"، جريدة العرب الإقتصادية الدولية، العدد 25، (24 أوت 2017)، ص24.

ثانيا: المراجع

أ/ الكتب:

1- أحمد المشد، القرصنة الإلكترونية وأمن المعلومات، ط1، مصر: مؤسسة الأمة العربية للنشر والتوزيع، 2017.

2- أوس مجيد غالب العوادي، "الأمن المعلوماتي السيبارني"، (بيروت، مركز البيان للدراسات والتخطيط، 2016).

3- حمدون توريه، "الأمن السيبراني في البلدان النامية"، الاتحاد الدولي للاتصالات،(2006).

4- سليم قسوم، الاتجاهات الجديدة في الدراسات الأمنية: دراسة في تطور مفهوم الأمن في العلاقات الدولية. الإمارات العربية المتحدة، مركز الامارات العربية للدراسات والبحوث الإستراتيجية.

5- سليم مزيود، "الجرائم المعلوماتية واقعها في الجزائر وآليات مكافحتها"، جامعة المدية، الجزائر، (2015).

6- سوسن زهير المهتدي، تكنولوجيا الحكومة الإلكترونية، عمان: دار أسامة، 2011.

7- سيد أحمد قوجيلي، " الدراسات الأمنية النقدية –مقاربة جديدة لإعادة تعريف الأمن، ط1، عمان، المركز العربي للدراسات السياسية،2014.

8- شفيق نوارن، "أثر التهديدات الإلكترونية على العلاقات الدولية، دارسة في أبعاد الأمن الإلكتروني"، (القاهرة، المكتب العربي للمعارف، 2014).

9- ضرغام جابر عطوش آل مواش، "جريمة التجسس المعلوماتي" المركز العربي للدراسات والبحوث العلمية للنشر، ط1، الإمارات العربية المتحدة ،2017.
10- عادل عبد الصادق، "الحروب السيبرانية: تصاعد القدرات والتحديات للأمن العالمي"، (المركز العربي لأبحاث الفضاء الإلكتروني، د.ش ،2017).
11- عادل عبد الصادق، "الفضاء الالكتروني وتهديدات جديدة للأمن القومي"، المركز العربي للأبحاث الإلكترونية.
12- عامر مصباح، المنظورات الاستراتيجية في بناء الأمن. القاهرة: دار الكتاب الحديث، 2013.
13- منى الأشقر جبور، "الأمن السيبارني: التحديات ومستلزمات المواجهة"، المركز العربي للبحوث القانونية والقضائية، (مايو2012).
14- منى الأشقر جبور، "الأمن السيبراني: التحديات ومستلزمات المواجهة"، (جامعة الدول العربية: المركز العربي للبحوث القانونية والقضائية، 2012).
15- منى الأشقر جبور، "السيبارنية هاجس العصر"، (بيروت، المركز العربي للبحوث القانونية والقضائية، 2013).
16- نوارن شفيق، "أثر التهديدات الإلكترونية على العلاقات الدولية، دارسة في أبعاد الأمن الالكتروني"، (القاهرة، المكتب العربي للمعارف، 2014).

المجلات:

1- أحمد عبيس نعمة الفتلاوي، "الهجمات السيبارنية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر"، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد الرابع، (السنة الثامنة، 2016).
2- أحمد مختار،"Cyber Security، هل يمكن تجنب الدولة مخاطر الهجمات الإلكترونية؟"، مجلة مفاهيم المستقبل، العدد 06، بيوت، لبنان، يناير2015.
3- أسامة بن صادق طيب، محمد نور بن ياسين فطاني، عصام بن يحيى الفيلالي، الحكومة الالكترونية، نحو مجتمع المعرفة، معهد البحوث و الاستشارات، العدد التاسع، جامعة الملك عبد العزيز، جدة السعودية، 2013.
4- إلياس شاهد، الحاج عرابة، عبد النعيم دفرو، تقييم تجربة تطبيق الحكومة الالكترونية الجزائرية، المجلة الجزائرية للدراسات المحاسبية والمالية، العدد الثالث، 2016.
5- امال حابت، دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال في مواجهة دور الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، المجلة الدولية للبحوث القانونية والسياسية، المجلد 05، العدد 03 ،2021.

6- إيهاب خليفة،" نمط جديد لممارسة التأثيارت غير التقليدية في العلاقات الدولية"، اتجاهات الأحداث، العدد 06،

7- تومي يحي، الحماية القانونية للمعطيات ذات الطابع الشخصي على ضوء القانون 18- 07 دراسة تحليلية، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد04، العدد02، سنة2019.

8- حنان بن عاتق، توفيق حجماوي، "واقع التطور التكنولوجي وتأثيره على آداء المنظمة في الجزائر"، ملتقى دولي حول: الإبداع والتغيير التنظيمي في المنظمات الحديثة، جامعة سعد دحلب، البليدة، كلية العلوم الاقتصادية، وعلوم التسيير، 2013.

9- خديم رابح، واقع أرضيات التعليم الإلكتروني عن بعد في الجامعة الجزائرية، جامعة عمار ثليجي الأغواط، مجلة الإبتكار والتنمية الصناعية، المجلد 03، العدد 03.

10- رغدة البهي، الردع السيبراني: المفهوم والإشكاليات والمتطلبات، Deterrence Cyber: Concept The ,Requirements and Dilemmas، برلين: المركز الديمقراطي العربي، مقال منشور يوم 04 فيفري2019، مجلة العلوم السياسية والقانون.

11- سارة تيتيلة، تصميم أساليب تقويم التعليم الإلكتروني بالجامعة الجزائرية: واقع التطبيق ومميزات الإستخدام، جامعة سطيف02، مجلة العلوم الاجتماعية، جامعة الأغواط، مجلد 07، العدد 28 جانفي 2018.

12- عادل زعلوك، نظريات الأمننة في مجال العلاقات الدولية: مدرسة كوبنهاغن نحو نظرية اتصالية مقترحة لدراسة الأمننة، مجلة السياسة والإقتصاد، المجلد 15، العدد 14، أفريل 2022.

13- عادل عبد الصادق، "أنماط "الحرب السيبارنية" وتداعياتها على الأمن العالمي"، مجلة الاتجاهات النظرية، البنك العربي الافريقي، (14 ماي 2017).

14- عادل عبد الصادق، "خطر الحروب "السيبارنية" عبر الفضاء الإلكتروني"، مجلة الأهرام لكمبيوتر الانترنت والاتصالات، (مارس2017).

15- عادل غزال، مشاريع الحكومة الإلكترونية من الاستراتيجية إلى التطليق، مشروع الجزائر: الحكومة الالكترونية2013، مجلة المكتبات والمعلومات، العدد 34، مارس 2014.

16- عائشة عبد الحميد، الإطار القانوني والتشريعي للرقمنة والذكاء الإصطناعي، دراسة منشورة، المجلة الدولية للتعليم بالإنترنت، المجلد 19، العدد 01، يوليو 2020.

17- العريشي، جبريل بن حسن.، الدوسري، سلمى عبد الرحمن." **دور مؤسسات التعليم العالي في تعزيز ثقافة أمن المعلومات في المجتمع**"، كلية العلوم الاجتماعية، جامعة الأميرة نورة بنت عبد الرحمن، السعودية ، مجلة مكتبة الملك فهد الوطنية. مج. 24، ع. 2، أبريل – سبتمبر 2018.

18- فتيحة ليتيم، ونادية ليتيم، "الأمن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة"، (جامعة بسكرة، مجلة المفكر، العدد 12، (د.س.ن).

19- كلثوم بيبيمون، السياقات "الثقافية الموجهة للهوية الرقمية في ضوء تحديات المجتمع الشبكي من التداول الافتراضي إلى الممارسات الواقعية"، مجلة "إضافات" العدد 23، (ربيع2016).

20- مادلين آر كريدين،"الفضاء والفضاء الالكتروني: التحديات المشتركة، مجلة الفضاء والفضاء الالكتروني التابعة للقيادة الإستراتيجية الأمريكية"، (يناير 2012).

21- محمد درقي،" النظام المعلوماتي للشركات الجزائرية غير مؤمن"، جريدة الخبر، العدد 7638، (04 أفريل2018).

الرسائل والأطروحات:

1- آمنة بن عبد ربه، النظام الاقتصادي الجديد المبني على المعرفة وتطور مجتمع المعلومات والتكنولوجيا الحديثة للاتصال، الحلول المقترحة لإرساء مجتمع معلومات ناجح ومتكامل في الجزائر، رسالة ماجستير، جامعة الجزائر كلية العلوم السياسية والاعلام، قسم علوم الاعلام والاتصال،2006-2005.

2- أمينة دير، أثر التهديدات البيئية على واقع الأمن الإنساني في إفريقيا: دراسة حالة دول القرن الإفريقي، مذكرة مقدمة لنيل شهادة الماجيستير في العلوم السياسية والعلاقات الدولية، تخصص علاقات دولية واستراتيجية، جامعة محمد خيضر، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية، 2014.

3- باطلي غنية، الجريمة الإلكترونية (دراسة مقارنة)، أطروحة مقدمة لنيل شهادة دكتوراه، شعبة القانون الخاص، كلية الحقوق قسم القانون الخاص، جامعة باجي مختار، عنابة، د. س . م .2012 .2013.

4- بن الشريف لامية، خلالفة خديجة ، "مكتبة المن السيبراني في السياسات الدفاعية الجزائرية، مذكرة تخرج مكملة لنيل شهادة الماستر في العلوم السياسية، تخصص علاقات دولية، جامعة الحاج لخضر باتنة، 2019/2018.

5- بن الشريف لامية، خلالفة خديجة، "مكانة الأمن السيبراني في السياسات الدفاعية الجزائرية" مذكرة ماستر (جامعة الحاج لخضر كلية الحقوق والعلوم السياسية ،تخصص: علاقات دولية، 2018-2019).

6- بن حرز الله فؤاد، الأمن السيبراني وجودة السياسات الأمنية (دراسة في بعض التجارب العربية)، مذكرة ماستر (جامعة الحاج لخضر كلية الحقوق والعلوم السياسية، تخصص: تنظيم سياسي وإداري، 2022-2023).

7- بوزيدي ذكرى، " الحرب السيبرانية واستخداماتها الأمنية والإستراتيجية : دراسة حالة الحرب السيبرانية الروسية تجاه إستونيا، جورجيا، أوكرانيا مذكرة ماستر (جامعة الحاج لخضر كلية الحقوق والعلوم السياسية، تخصص: علاقات دولية، 2022-2023).

8- خيرة روابحي، ثقافة الأنترنت: دراسة ميدانية الاستعلامات الشبكة بمدينة تيهرت، رسالة ماجستير، جامعة وهران، كلية العلوم الإنسانية والحضارة الإسلامية، قسم علم المكتبات والعلوم الوثائقية، 2009-2010.

9- سعيدة رشاش، "مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري"، مذكرة ماستر (جامعة العربي التبسي تبسة، تخصص: دراسات استراتيجة، 2017-2018).

10- سمير بارة، "الدفاع الوطني والسياسات الوطنية للأمن السيبراني (Cyber Security) في الجزائر: الدور والتحديات"، جامعة قاصدي مرباح، ورقلة.

11- عبد القادر عبان، تحديات الإدارة الالكترونية في الجزائر،دراسة سوسيولوجية ببلدية الكاليتوس العاصمة، أطروحة الدكتوراه، جامعة محمد خيضر، بسكرة، كلية العلوم الانسانسة والاجتماعية، 2015، تخصص: إدارة وعمل 2016، ص91.

12- غنية باطلي، الجريمة الإلكترونية (دراسة مقارنة)، أطروحة مقدمة لنيل شهادة دكتوراه، شعبة القانون الخاص، كلية الحقوق قسم القانون الخاص، جامعة باجي مختار، عنابة، د. س . م.

13- مراد كريم، مجتمع المعلومات أثره في المكتبات الجامعية، مدينة قسنطينة، أطروحة ذكتوراه، جامعة منتوري، كلية العلوم الإنسانية والاجتماعية، قسم علم المكتبات، 2008-2007.

14- مزاش نبيل، أثر الحرب السيبرانية على العلاقات الدولية بين القوى الكبرى في النظام الدولي، مذكرة ماستر (جامعة الحاج لخضر، كلية الحقوق والعلوم السياسية، تخصص: علاقات دولية، 2020-2021).

15- نبيل مزاش، أثر الحرب السيبرانية على العلاقات الدولية بين القوى الكبرى في النظام الدولي، مذكرة ماستر (جامعة الحاج لخضر كلية الحقوق والعلوم السياسية، تخصص: علاقات دولية، 2020-2021).

16- هند علوي، المرصد الوطني لمجتمع المعلومات بالجزائري، قياس النفاذ إلى تكنولوجيا المعلومات والاتصالات بقطاع التعليم بالشرق الجزائري، أطروحة دكتوراه، جامعة منتوري- قسنطينة، كلية العلوم الإنسانية، تخصص: علم المكتبات 2007-2008.

التقارير:

1- تقرير الإتحاد الدولي للإحصاءات تكنولوجيا المعلومات والاتصالات للمجلس الاقتصادي والاجتماعي.

2- تقرير نورتون لجرائم المعلوماتية 2011.

3- مجموعة البنك الدولي، تقرير عن التنمية في العالم 2016: العوائد الرقمية.

4- محمد شايب هدار لحسن، تقييم قطاع الاتصال وتكنولوجيا الاعلام في الجزائر، أبحاث المؤتمر الدولي: تقييم أثار برامج الاستثمارات والنمو الاقتصادي خلال الفترة 2001-2014.

5- تاريخ النشر 4 أبريل 2023 TAQNEEN LAW FIRM شركة تقنين للمحاماة والإستشارات القانونية.

مراجع مختلفة:

6- عنترة بن مرزوق، "الأمن السيبراني كبعد جديد من السياسة الجزائرية"، محاضرات مقدمة لطلبة جامعة محمد بوضياف – المسيلة، كلية الحقوق والعلوم السياسية، د س.

المواقع الإلكترونية:

إخفاء الهوية: كشف النقاب عن كابوس الأمن السيبراني. تم الاطلاع بتاريخ: 20 ماي 2024 . https://fastercapital.com/arabpreneur

عبد القادر سعيدي،" المصلحة المركزية الإلكترونية في مواجهة مجرمي العالم الافتارضي"، في: www.essalamonline.com2018/17:42 مارس03

ليال بيطار، "ماذا يعني الأمن السيبارني"؟ من الموقع :https//www.anbaaoline.com 20 جانفي 2018، التوقيت 58:17

صحيفة المرصد، "ما هو الأمن السيبراني"، موقع إلكتروني

تاريخ التصفح 2019/3/11. https://al-marsd.com/168664.html

سعد علي الحاج بكري، "الأمن السيبراني ومعضلة حمايته"، الرابط: www.alegt.com/article1241506.html، تاريخ التصفح يوم 2019/03/04.

تولاي آسر، "ما هي السيبارنية ؟ وما دورها في صناعة القرار"؟ 20 جانفي 53:17/2018 http//Zeitgeistarrabia.com

عادل زقاغ، مترجما (مفهوم الأمن في نظرية العلاقات الدولية)، الموسوعة الجزائرية للدراسات السياسية والإستراتيجية، 16جانفي 2021، على الرابط https://www.polityics-dz.com

صباح بالة، مدرسة كوبنهاغن في تفسير الدراسات الأمنية، الموسوعة السياسية، 9 ديسمبر 2020، متاح على الرابط التالي: https://political-encyclopedia.org/dictionary

عبد الله زراب، النظرية السيبرانية، توظيف الفضاء الإلكتروني في تعظيم قوة الدول، تاريخ النشر: 21نوفمبر2017 تم الإطلاع عليه في 2024/05/22 من الموقع : https://aafaq.kku.edu.sa/news/

"Hacking", malwarebytes, Retrieved 20/1/2022.

جوان 2013 أحمد السيد https://www.suezbalady.com/index.php

https://fs.mpt.gov.dz/cybercriminalite

Home ofice, Cyber Crime Strategy, March 2010, p9, .pdf Available at :http:// www.knox.edu/offices-andservices/information-technologyservices/computer-usepolicies/online-speech.html.

http://studies.aljazeera.net/ar/reports/2018/05/180502110656159.html.2019-05-24 تاريخ التصفح:

Zhang ,Yuan , et al. (2017). Solution of Media Risk and Social Responsibility Governance of Social Media. ITM Web of Conferences,1 November, available at: https//:www.researchgate.net/.

https://academy.binance.com/ar/articles/what-is-a-dos-attack تاريخ النشر Jan 7, 2019 تاريخ التحديث Oct 25, 2023.

[1] https://help.eset.com/glossary/ar-EG/botnet.html8

إسماعيل كاخيل، "الحرب الإلكترونية"، موقع مجلة الدفاع العربي، من الرابط:

www.arahdefancejournal.com/article560.htm 2019/03/1

سليمة مق ارني، "الجيش الوطني الشعبي: ملتقى حول الدفاع السيبارني، مكون أساسي للأمن والدفاع الوطني" hltps :www.eljoumhouria.dg، من الموقع:17:51/2018مارس 07 نشر في

حمد الأمين بن عائشة، "مفهوم الأمن الوطني الجزائري"، في: 03 فيفري 33:21/2018 www.maqualaty.com

جريدة الشروق الجزائرية، عدد 1253 الصادرة بتاريخ:2023/09/20

وكالة الأنباء الجزائرية، الإرهاب الإلكتروني: " الجزائر حريصة على حماية أمنها ". من موقع:

https://algpress.com/article-50021.htm

عبد القادر سعيدي،" المصلحة المركزية الإلكترونية في مواجهة مجرمي العالم الافتراضي"، في: 03 مارس2018 من الموقع www.essalamonline.com

www.andi.dz

Https://www.algerietelecom.dz.

موقع وزارة البريد وتكنولوجيا الإعلام والإتصال: www.mptic.dz

Lu, Marcus, "Economy Visualized: Where 5G Will Change the World،" Visual Capitalist, (22/03/2021), see the link: https://bit.ly/3C8U9jl، 2020/03/09

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.2019-05-24 تاريخ التصفح:

Douwe Korff, CYBER SECURITY DEFINITIONS – a selection. P1, in: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CPDP%202015%20-%20KORFF%20Handout.pdf

Home ofice, Cyber Crime Strategy, March 2010, p9, in https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf

المراجع باللغة الأجنبية:

1/ Livre:

1- Myriam Dunn Cavelty, Information Age Conflicts : A Study of the Informatiun Revolution and Changing International Operating Environment.
2- Dan Craigen, Nadia Diakun-Thibault, and Randy Purse, Defining Cybersecurity.
3- Nye, J. S. (2010). "Cyber Power." Harvard Kennedy School. Belfer Center for Science and International Affairs.

2/ Revue :

1- Cameron S. D. Brown, "Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice", International Journal of Cyber Criminology. Vol 9, Issue 1, January June 2015, p120.
2- *Dan Craiyen and others, "Defining cybrescurity", Technology innovation management review, Montreal, Canada, (october 2014).*
3- Martin C.libicki , Conquestion Cyberspace :National Security and information warfare (New York) :Combridge University Press, 2007.
4- Joseph S. Nye, "Cyber security",(Cambridge : Harvard Kennedy School, Belfer center for science and international affairs), May 2010.
5- Fred Schreier, On Cyberwarefare, DCAF horzon 2015 Working paper No, 07.

6- Matheus M. Hoscheidt, Elisa Felber Eichner, LEGAL AND POLITICAL MEASURES TO ADDRESS CYBERCRIME, United Nations: UFRGSMUN UFRGS Model, v.2, 2014.

7- Lawrence Williams (11/12/2021), "What is Hacking? Types of Hackers :Introduction to Cybercrime", guru99, Retrieved 20/1/2022.

8- Dan Craiyen and others, "Defining cybrescurity", Technology innovation management review, Montreal, Canada, (October 2014).

9- Cameron S. D. Brown, "Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice", International Journal of Cyber Criminology. Vol 9, Issue 1, January – June 2015.

10- Asenio .T.Gumahad , Cyber troopes and Netuvar :the profession of Arms in the information Age.(Alabama Air University ,Air war college, 1996).

11- Dan Craigen, Nadia Diakun-Thibault, and Randy Purse, Defining Cybersecurity. Technology Innovation Management Review, October 2014.

فهرس المحتويات

الفصل الثالث

التوجه الاستراتيجي لإرساء الأمن المعلوماتي

ملخص الدراسة:

تهدف هذه الدراسة إلى إلقاء الضوء على مفهوم الأمن المعلوماتي ودوره في الحد من الهجمات السيبرانية في الجزائر، حيث يتم التركيز على رؤية استباقية نحو تعزيز الأمن المعلوماتي في هذا السياق. يشهد العصر الحديث تزايدًا مستمرًا في التكنولوجيا واعتماد الشبكات الرقمية، مما يعزز أهمية حماية الأنظمة الإلكترونية والمعلومات. تأخذ الجزائر مكانة بارزة كواحدة من الدول النامية، وتواجهها تحديات خاصة في مجال الأمن المعلوماتي .

يتعامل البحث مع استراتيجيات التحسين والتعزيز للأمن المعلوماتي في الجزائر بشكل استباقي، مع التركيز على الجوانب التنظيمية والتقنية والتدريبية. يتعامل الباحثون مع تحليل التهديدات السيبرانية المحتملة ويقدمون استراتيجيات فعّالة للتصدي لها. كما يتم التطرق إلى ضرورة تعزيز التعاون الدولي والإقليمي لمواجهة التحديات السيبرانية المشتركة.

وفي هذا السياق، يُركز البحث على تحقيق التوازن بين تعزيز الأمن السيبراني وتشجيع التطور التكنولوجي والابتكار. يُشدد على أهمية إشراك كل القطاعات والجهات الحكومية في هذا الجهد المشترك، بما يضمن تحقيق أقصى قدر من الفعالية في مجال الحماية المعلوماتية خصوصا من المخاطر الخارجية في الجزائر.

الكلمات المفتاحية: الأمن المعلوماتي، الهجوم السيبراني، الجزائر، الاختراق الرقمي.

Abstract :

This study aims to shed light on the concept of information security and its role in reducing cyber attacks in Algeria, as the focus is on a proactive vision towards enhancing information security in this context. The modern era is witnessing a continuous increase in technology and the adoption of digital networks, which reinforces the importance of protecting systems Electronic and information. Algeria occupies a prominent position as one of the developing countries, and faces special challenges in research dealing with strategies for improving and enhancing information security in Algeria proactively, with The field of information security.

Focus on organisational, technical and training aspects. Researchers deal with the analysis of potential cyber threats and provide effective strategies to counter them. The need to strengthen international and regional cooperation is also addressed Confronting common cyber challenges.

In this context, the research focuses on achieving a balance between enhancing cybersecurity and encouraging technological development and innovation. Emphasizes the importance of involving all sectors and government agencies in this joint effort to ensure achieving maximum effectiveness in the field of information protection, especially from external risks. in Algeria.

Keywords: information security, cyber attack, Algeria, digital hacking