الجمهورية الجزائرية الديمقراطية الشعبية
People's Democratic Republic of Algeria
وزارة التعليم العالي والبحث العلمي
Ministry of High Education and Scientific Research
جامعة محمد البشير الإبراهيمي برج بوعريريج
University of Mohamed el Bachir el Ibrahimi-BBA
كلية الحقوق والعلوم السياسية
Faculty of Law and Political Sciences

مذكرة مقدمة متطلبات لنيل شهادة ماستر أكاديمي في الحقوق
تخصص: اعلام الي وإنترانت
الموسومة بـ:

الأمن السيبراني وتأثيراته على الاقتصاد الوطني

إعداد الطالبتين:
- بسمة مقلاتي
- سمية قصري

تحت إشراف الأستاذ:
- نجار امين

لجنة المناقشة:

الإسم واللقب	الرتبة	الصفة
حاجي عبدالحليم	استاذ محاضر ا	رئيسا
نجار امين	استاذ محاضر	مشرفا ومقررا
عجيري عبدالوهاب	استاذ مساعد ا	مناقش

السنة الجامعية 2025/2024


بسم الله الرحمن الرحيم

الشكر والعرفان

من باب قوله عز وجل " ألن شكرتكم لأزيدنكم "

وقوله صل الله عليه وسلم تسليما◆من لم يشكر الناس لم يشكر الله

تشكر ونحمد الله الذي رزقنا من العلم ما استعلمنا ومنحنا القوة والمقدرة على التعلم حتى وصلنا إلى هذا المستوى كي تتم هذا العمل المتواضع

تتقدم بجزيل الشكر والثناء والتقدير والاحترام، الى الأستاذ المشرف امين نجار" الذي لم يبخل علينا بتوجهاته وارشاداته ونصائحه القيمة ومساعدته وتشجيعاته لنا راجين من المولى أن يجعل مجهوداته المبذولة في ميزان حسناته وجزاه كل خير

نتقدم بالشكر الجزيل الى الجنة أعضاء المناقشة بالخصوص الأستاذ رئيس اللجنة والأستاذ الممتحن على قبولهما دعوة مناقشة ها العمل البسيط.

الشكر موصول إلى جميع أساتذة كلية الحقوق والعلوم السياسية

الشكر الى كل من ساهم من قريب أبو بعيد في انجاز هذا العمل ولو بكلمة أبو بنصيحة أو بابت

مقدمة

يشهد العالم في العقود الأخيرة ثورة رقمية غير مسبوقة غيّرت ملامح الحياة البشرية في جميع مجالاتها، وجعلت من الفضاء السيبراني عنصرًا أساسيًا في إدارة الأنشطة الاقتصادية، التجارية، والإدارية. فقد أصبحت التكنولوجيا الحديثة، وشبكات الاتصال، والأنظمة المعلوماتية الركيزة الأساسية التي تقوم عليها مختلف القطاعات الحيوية في الدول، من بنوك ومؤسسات مالية، إلى قطاعات الطاقة، النقل، والصناعة. غير أن هذا الاعتماد المتزايد على الوسائل الرقمية ترافق مع بروز مخاطر وتهديدات جديدة تُعرف بالهجمات السيبرانية، التي باتت تشكل خطرًا حقيقيًا على الأمن القومي والاقتصاد الوطني على حد سواء.

فالأمن السيبراني لم يعد مجرد مسألة تقنية تهدف إلى حماية البيانات والمعلومات، بل أصبح قضية إستراتيجية تمس استقرار الدول وتنميتها الاقتصادية. إذ إن أي اختراق أو هجوم إلكتروني قد يؤدي إلى تعطيل أنظمة مالية، أو توقف خدمات حيوية، أو خسائر مالية ضخمة قد تزعزع ثقة المستثمرين وتؤثر سلبًا على النمو الاقتصادي. ومع تطور أساليب الجريمة الإلكترونية، وتنوع أهدافها بين سرقة البيانات الحساسة، والتجسس الصناعي، والابتزاز المالي، أصبح لزامًا على الدول أن تتبنى سياسات وطنية فعّالة لتعزيز قدراتها الدفاعية في الفضاء السيبراني.

في هذا السياق، تبرز أهمية دراسة العلاقة بين الأمن السيبراني والاقتصاد الوطني، إذ يشكل الأمن الرقمي أحد الركائز الأساسية لجذب الاستثمارات وضمان بيئة اقتصادية مستقرة وآمنة. فالدول التي تتمتع ببنية تحتية رقمية آمنة تستطيع تحقيق تنمية اقتصادية مستدامة وتنافسية عالية في السوق العالمية، في حين أن ضعف الأمن السيبراني يؤدي إلى خسائر اقتصادية مباشرة وغير مباشرة، سواء من خلال توقف الأنشطة الإنتاجية، أو من خلال تراجع الثقة في المؤسسات الاقتصادية.

ولأن الاقتصاد الحديث يعتمد بشكل متزايد على التحول الرقمي، فقد أصبح من الضروري فهم تأثيرات الأمن السيبراني على الأداء الاقتصادي العام، وتحليل مدى ارتباط أمن المعلومات بالاستقرار المالي والازدهار الاقتصادي. فكلما كانت نظم الحماية أكثر تطورًا وكفاءة، كانت فرص النمو الاقتصادي أكبر، والعكس صحيح.

أ. إشكالية الموضوع:

يشهد العالم المعاصر تزايدًا مستمرًا في الاعتماد على التقنيات الرقمية والأنظمة المعلوماتية في مختلف المجالات، خاصة في القطاع الاقتصادي الذي أصبح مرتبطًا بشكل وثيق بالتكنولوجيا الحديثة. ومع هذا التحول الرقمي، ظهرت تهديدات جديدة تمس أمن المعلومات واستقرار الاقتصاد، تمثلت في الهجمات السيبرانية التي تستهدف المؤسسات الحكومية والمالية والشركات الخاصة على حد سواء، مما يؤدي إلى خسائر مالية كبيرة، وإلى زعزعة الثقة في المعاملات الإلكترونية والأنظمة البنكية.

وانطلاقًا من هذه المعطيات، يبرز التساؤل الجوهري الذي تسعى هذه الدراسة إلى معالجته:

إلى أي مدى يؤثر الأمن السيبراني على الاقتصاد الوطني، وكيف يمكن تعزيز الحماية الرقمية لضمان استقرار التنمية الاقتصادية؟

ب.أهمية الموضوع:

تنبع أهمية هذا الموضوع من كونه يتناول قضية معاصرة تمس جميع جوانب الحياة الاقتصادية في الدولة، حيث:

- يُعتبر الأمن السيبراني شرطًا أساسيًا لجذب الاستثمارات الأجنبية والمحافظة على ثقة المستثمرين.
- يؤثر بشكل مباشر على استقرار الأسواق والمؤسسات البنكية.
- يمثل خط الدفاع الأول لحماية البيانات الوطنية والمصالح الاقتصادية الحيوية.
- يسهم في بناء اقتصاد رقمي آمن ومستدام يعتمد على الابتكار والتكنولوجيا.

ت.الأسباب الموضوعية لاختيار الموضوع:

1. الانتشار الواسع للتكنولوجيا الرقمية في مختلف القطاعات الاقتصادية.
2. تزايد حدة الهجمات الإلكترونية التي تستهدف مؤسسات اقتصادية وحكومية.

3. ارتباط الأمن السيبراني ارتباطًا وثيقًا بالتنمية الاقتصادية والأمن القومي.

4. الأسباب الذاتية لاختيار الموضوع:

1. الرغبة في فهم العلاقة بين التكنولوجيا الحديثة والأمن الاقتصادي.
2. الاهتمام الشخصي بمجال الأمن السيبراني والتحولات الرقمية.
3. السعي للمساهمة في رفع الوعي بأهمية حماية المعلومات في دعم الاقتصاد الوطني.

ث.أهداف الموضوع:

1. التعرف على مفهوم الأمن السيبراني ومجالاته الأساسية.
2. تحليل تأثيراته المباشرة وغير المباشرة على الاقتصاد الوطني.
3. إبراز أهم التحديات التي تواجه الدول في حماية فضائها السيبراني.
4. اقتراح آليات واستراتيجيات لتعزيز الأمن السيبراني ودعم الاقتصاد الرقمي الآمن.

الفصل الأول:

الإطار النظري والمفاهيمي الأمن السيبراني والاقتصاد الرقمي

يشهد العالم في السنوات الأخيرة تحولات جذرية بفعل الثورة الرقمية التي مست مختلف مجالات الحياة الاقتصادية والاجتماعية والإدارية، حيث أصبح الاعتماد على التكنولوجيا الرقمية والاتصال عبر الشبكات الإلكترونية ضرورة حتمية لتحقيق التنمية والتنافسية. ومع هذا التحول، برزت تحديات جديدة تتعلق بأمن المعلومات وحماية الأنظمة الرقمية من التهديدات والهجمات الإلكترونية، ما أفرز مفهوم الأمن السيبراني كأحد الركائز الأساسية لضمان سلامة البنية التحتية الرقمية وحماية المعاملات والبيانات الحساسة.

في المقابل، يمثل الاقتصاد الرقمي الإطار الأوسع الذي يدمج التقنيات الرقمية في العملية الاقتصادية من إنتاج وتوزيع واستهلاك، معتمداً على الإنترنت، الذكاء الاصطناعي، البيانات الضخمة، والخدمات الإلكترونية كعناصر رئيسية في خلق القيمة المضافة. ويعد الأمن السيبراني في هذا السياق شرطاً جوهرياً لنجاح التحول نحو الاقتصاد الرقمي، إذ لا يمكن تحقيق النمو والابتكار دون ضمان بيئة رقمية آمنة ومستقرة.

ومن ثم، فإن دراسة الإطارين النظري والمفاهيمي لكل من الأمن السيبراني والاقتصاد الرقمي تكتسي أهمية علمية وعملية كبيرة، فهي تمكّن من فهم العلاقة التكاملية بين حماية الفضاء الرقمي وتعزيز الأنشطة الاقتصادية المعتمدة على التكنولوجيا، وتساعد صناع القرار على تبني سياسات واستراتيجيات فعالة لمواكبة التطور الرقمي العالمي.

المبحث الاول: الامن السيبيراني

الأمن السيبراني هو مجموعة من الإجراءات والتقنيات الهادفة إلى حماية الأنظمة والشبكات والمعلومات من الهجمات أو الوصول غير المصرح به. يهدف إلى ضمان سرية البيانات وسلامتها وتوافرها، خاصة في ظل الاعتماد المتزايد على التكنولوجيا الرقمية. ويُعدّ ركيزة أساسية للحفاظ على استقرار المجتمعات والاقتصادات الحديثة.

المطلب الأول: تعريف الامن السيبيراني

مع تزايد الاعتماد على الفضاء الرقمي في مختلف مجالات الحياة برز مفهوم الأمن السيبراني كعنصر أساسي في حماية الأفراد والمؤسسات والدول من التهديدات والمخاطر المرتبطة باستخدام تكنولوجيا المعلومات والاتصالات. وقد تعددت المقاربات المفاهيمية لهذا المصطلح نظرا لتداخله مع مجالات تقنية وقانونية وأمنية، مما يجعل من الضروري الوقوف على معانيه اللغوية وأصوله الاصطلاحية، واستعراض أبرز التعريفات التي قدمتها الأدبيات الفقهية والدولية. ومن هذا المنطلق سنخصص هذا الفرع لبيان مفهوم الأمن السيبراني، من خلال تناول تعريفه اللغوي، وأصل مصطلح "السيبرانية"، والتعريفات الاصطلاحية المتداولة له في الأوساط الأكاديمية والرسمية.

الفرع الاول: التعريف اللغوي

يتكون الأمن السيبراني من كلمتين:" الأمن"، و" السيبرانية".

الأمن: هو نقيض الخوف، أي بمعنى السلام، والأمن مصدر الفعل أمن من الشر، أي سلم منه وقد عرفه قاموس بنغوين للعلاقات الدولية بأنه: "مصطلح يشير إلى غياب ما يهدد القيم النادرة".[1]

السيبرانية: مصطلح "السيبراني" من أكثر المفاهيم تداولا في ميدان الأمن الدولي اليوم، وأصل الكلمة "Cyber" يوناني، مأخوذ من "Kybernetes" بمعنى من يدير دفة السفينة، واستخدمت مجازا للدلالة على المتحكم. ويرى بعض المؤرخين أن عالم الرياضيات الأمريكي نوربرت وينر هو من أعاد إحياء المصطلح ليعبر عن التحكم الآلي، ويُعتبر المؤسس للسبرنتيقية من خلال كتابه الشهير:

[1] فارس محمد العمارات الأمن السيبراني مفهوم وتحديات العصر، من الأولى، دار الخليج للنشر والتوزيع الأردن – عمان، 2022، ص 13

"Cybernetics or Control and Communication in The Animal and Machine".[1]

حيث عرف نوربرت وينر Norbert Wieners " السبرنتيقية " Cybernetics" "التحكم والتواصل عند الحيوان والآلة ".[2]

الفرع الثاني: التعريف الاصطلاحي

هناك العديد من التعاريف التي قدمت لمفهوم الأمن السيبراني، حيث يُعرف على بأنه مجموعة من الاجراءات المتخذة في مجال الدفاع ضد الهجمات السيبرانية ونتائجها التي تشمل تنفيذ التدابير المضادة المطلوبة[3]."

وهذا ما ذهب إليه الكاتبان"Neittaanmaki Pekka, Lehto Martti " في كتابهما " Cyber Security: Analytics, Technology and Automation "حيث عرفا الأمن السيبراني بأنه عبارة "عن مجموعة من الإجراءات التي اتخذت في الدفاع ضد هجمات قراصنة الكومبيوتر وعواقبها، ويتضمن تنفيذ التدابير المضادة المطلوبة"[4].

عرف التقرير الصادر عن الاتحاد الدولي للاتصالات حول اتجاهات الإصلاح في عام 2010-2011 الأمن السيبراني بأنه: "مجموعة من المهمات مثل تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية ومقاربات لإدارة المخاطر، وتدريبات وممارسة

[1] فرح يحي زعاترة، التهديدات السيبرانية علي الأمن القومي الأمريكي، العربي للنشر والتوزيع،مصر،2023 ، ص 21

[2] Neittaanmaki Pekka, Lehto Martti, Cyber Security: Analytics, Technology and Automation,

Spnger international Publishing, volume 78, Inteellingent System, control and Automation Science and Enerineering, Switzerland, 2015, p 3.

[3] مني عبد الله السمحان، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية جامعة المنصورة، العدد 111 يوليو 2020، ص 9

[4] Neittaanmaki Pekka, Lehto Martti, Ibid .p 25

فضلى وتقنيات يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين".[1]

وقدمت وزارة الدفاع الأمريكية " البنتاغون " تعريفا دقيقا لمصطلح الأمن السيبراني فاعتبرته "جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية، من مختلف الجرائم الهجمات التخريب التجسس، والحوادث"[2].

نظراً للطابع الشامل لمفهوم الأمن السيبراني، فإن فهمه يستدعي التطرق إلى مجموعة من المفاهيم المتداخلة التي تشكل أبعاده أو أدواته الأساسية، والتي تتكامل فيما بينها لضمان حماية الفضاء الرقمي.

- **القوة السيبرانية:** تعبر عن قدرة الدولة أو الجهات الفاعلة على التحكم في المعلومات والبنى التحتية الرقمية من خلال موارد تقنية وبشرية متخصصة[3].
- **الدفاع السيبراني:** يتمثل في حماية الأنظمة الرقمية من خلال رصد التهديدات وتحليلها والتقليل من آثارها، مع القدرة على الرد في الوقت المناسب[4].
- **الردع السيبراني:** يهدف إلى منع الهجمات الإلكترونية عبر إظهار القدرة على الرد أو المعاقبة مما يشكل وسيلة ردع استراتيجية للخصوم[5].
- **الهجمات السيبرانية:** أفعال ضارة تستغل ثغرات رقمية لتعطيل أو التلاعب بالأنظمة، غالبا لتحقيق أهداف سياسية أو شخصية[1].

---

[1] راشد محمد المري، الأمن السيبراني وحماية الأنظمة الإلكترونية (دراسة تحليلية تأصيلية)، مجلة الدراسات القانونية والاقتصادية، المجلد 09، العدد 01 مارس 2023، ص964

[2] فرح يحي زعاترة، مرجع سبق ذكره، ص 22

[3] تغريد صفاء مهدي لبني خميس مهدي، أثر السيبرانية في تطور القوة، مجلة حمورابي للدراسات، مركز حمورابي للبحوث، والدراسات الاستراتيجية، العددان 33-34 السنة الثامنة (شتاء ربيع)، 2020، ص 152

[4] ة إيهاب خليفة، الحرب السيبرانية الاستعداد لقيادة المعارك العسكرية في الميدان الخامس العربي للنشر والتوزيع، الطبعة الأولى، القاهرة، 2020، ص 188

[5] وفاء مطروح ابتسام أونيس، تداعيات جائحة كوفيد – 19 وتأثيرها على تحقيق الأمن السيبراني في الجزائر، المجلة الدولية للاتصال، الاجتماعي، المجلد 09، العدد 02، ص222

- **الفضاء السيبراني:** عرفته الوكالة الفرنسية لأمن أنظمة الإعلام "ANSSI"، بأنه: فضاء تواصلي ناشئ عن الربط البيئي العالمي لمعدات المعالجة الآلية للمعطيات الرقمية"[2].
- **أمن المعلومات:** يشير إلى الإجراءات والتقنيات المعتمدة لحماية المعلومات من الضياع أو التسريب أو التلاعب، ويعد أحد مكونات الأمن السيبراني[3].

الفرع الثالث: التعريف القانوني

يُعد الأمن السيبراني منظومة شاملة من التدابير والإجراءات ومفاهيم الأمن وطرق إدارة المخاطر والأعمال والتكوينات وأفضل الممارسات والتكنولوجيات، تهدف إلى تمكين نظام المعلومات من مقاومة الأحداث المرتبطة بالفضاء السيبراني التي قد تمس بتوافر وسلامة وسرية المعطيات المخزنة أو المعالجة أو المرسلة، وكذا الخدمات التي يقدمها هذا النظام أو التي تتيح الولوج إليه. وتشمل الجرائم السيبرانية كل الأفعال المخالفة للتشريعات الوطنية أو الاتفاقيات الدولية المصادق عليها، والتي تستهدف شبكات ونظم المعلومات أو تستخدمها كوسيلة لارتكاب جنحة أو جناية. أما التهديد السيبراني فهو كل عمل يهدف إلى الإخلال بأمن نظام معلومات من خلال المساس بتوافره أو سلامته أو سريته. وتُحدد الأخلاقيات السيبرانية مجموعة من القواعد والمعايير التي تضبط السلوك المسؤول داخل الفضاء السيبراني. كما تُعتبر البنيات التحتية ذات الأهمية الحيوية التجهيزات والمنشآت والأنظمة الضرورية لاستمرارية الوظائف الحيوية للمجتمع كالصحة

---

[1] المرجع نفسه، ص 223

[2] Agence nationale de la sécurité des systèmes d'information (ANSSI), CyberDico de P'ANSSI (FR/EN), Gouvernement français, 2020, disponible sur: https://www.info.gouv.fr/upload/media/content/0001/11/a5fcaf7ccf1f6058d70e3a17570037569b979d8

[3] حياة حميدي، نسيمة طايلب مدخل مفاهيمي حول الأمن السيبراني، مجلة مدار للدراسات الاتصالية الرقمية، المجلد 02، العدد 02 نوفمبر 2022، ص 07

والأمن والسلامة والتقدم الاقتصادي والاجتماعي، حيث إن أي ضرر أو تلف يصيبها يؤدي إلى خلل في تلك الوظائف. ويشمل قطاع الأنشطة ذات الأهمية الحيوية مختلف الأنشطة المرتبطة بالبنيات التحتية الحيوية والتي تضمن تلبية الحاجات الأساسية للمواطنين أو تمكّن الدولة من ممارسة صلاحياتها والحفاظ على أمنها واستقرارها الاقتصادي، نظراً لعدم قابليتها للاستبدال أو التعويض. أما نظام المعلومات فهو مجموعة منظمة من الموارد تشمل المستخدمين والمعدات والبرامج والمعطيات والإجراءات، التي تتيح تجميع المعلومات وتصنيفها ومعالجتها ونشرها. ويُعد نظام المعلومات الحساس النظام الذي يعالج بيانات حساسة قد يؤدي المساس بسريتها أو سلامتها أو توافرها إلى ضرر بالهيئات أو بالبنيات التحتية الحيوية[1].

وأخيراً، تُعرف خدمة الأمن السيبراني بأنها كل خدمة أمنية تقدمها الجهات المختصة لتعزيز أمن نظم المعلومات لدى الهيئات أو البنيات التحتية الحيوية، وتشمل رصد وتشخيص الحوادث الأمنية وتقوية قدرات الحماية ضد التهديدات السيبرانية.

المطلب الثاني: أهداف وأهمية الأمن السيبيراني

يهدف الأمن السيبراني إلى حماية الأنظمة والمعلومات من الاختراقات والهجمات الإلكترونية، مما يضمن سرية البيانات واستمرارية الخدمات. وتكمن أهميته في الحفاظ على استقرار الاقتصاد الوطني وتعزيز الثقة في البيئة الرقمية الحديثة.

الفرع الأول: أهداف السيبيراني

تُعدّ حماية أنظمة التقنيات التشغيلية بمختلف مكوناتها من أجهزة وبرمجيات وخدمات وبيانات ضرورة أساسية لضمان أمن واستقرار البنى التحتية الحيوية. ويتطلب ذلك التركيز على مواجهة الهجمات والحوادث السيبرانية التي تستهدف الأجهزة الحكومية

[1] المادة 2 من الجريدة الرسمية، عدد 6904، الصادر في 9ذو الحجة 1441 هـ (30 يوليو 2020)، قسم نصوص عامة، ص4160-4161

ومؤسسات القطاعين العام والخاص، إضافة إلى توفير بيئة رقمية آمنة وموثوقة للتعاملات داخل مجتمع المعلومات. كما يستلزم تحقيق هذه الغاية تبني استراتيجيات دفاعية متطورة، وتطوير بنية تحتية متينة للأمن السيبراني تضمن استمرارية الأعمال وحماية المعلومات الحساسة من التهديدات الإلكترونية المتزايدة.

ومن أجل الحد من المخاطر والجرائم الإلكترونية التي تستهدف المستخدمين، لا بد من معالجة نقاط الضعف في أنظمة الحواسيب والأجهزة المحمولة بمختلف أنواعها، وسد الثغرات الأمنية في نظم المعلومات، إلى جانب مكافحة البرمجيات الخبيثة التي قد تُحدث أضرارًا جسيمة بالمستخدمين. ويتحقق ذلك من خلال اعتماد استراتيجيات شاملة للأمان الرقمي تهدف إلى تعزيز الحماية الإلكترونية ورفع جاهزية المستخدمين في مواجهة الهجمات السيبرانية.

كما أن الحد من أنشطة التجسس والتخريب الإلكتروني على مستوى الأفراد والهيئات الحكومية يتطلب اتخاذ تدابير وقائية فعّالة لحماية المواطنين والمستهلكين من المخاطر المحتملة المرتبطة باستخدام الإنترنت. ويشمل ذلك تدريب الأفراد على آليات واستراتيجيات حديثة لمواجهة محاولات اختراق أجهزتهم وسرقة بياناتهم أو إتلافها. ويتطلب تحقيق هذه الأهداف تنفيذ سياسات وطنية متكاملة، وتوفير برامج تدريب وتوعية مستمرة تعزز ثقافة الأمان الرقمي، وتسهم في حماية البيانات الشخصية من التهديدات السيبرانية المتصاعدة[1].

الفرع الثاني: أهمية الأمن السيبيراني

في عالمنا المترابط عبر الشبكات الرقمية، يستفيد الأفراد والمؤسسات على حد سواء من برامج الدفاع السيبراني. فعلى المستوى الشخصي، قد يؤدي الهجوم السيبراني إلى سرقة الهوية، أو محاولات الابتزاز، أو فقدان البيانات الهامة مثل الصور والملفات

[1] على عبد الله السمحان، مرجع سبق ذكره، ص 12

الشخصية.

كما تعتمد المجتمعات على البنية التحتية الحيوية، بما في ذلك محطات الطاقة، والمستشفيات، والشركات المالية والخدماتية، لذا يصبح تأمين هذه المؤسسات وغيرها أمرًا بالغ الأهمية لضمان استمرارية عمل المجتمع بطريقة آمنة وسلسة[1].

كما تتمثل أهمية الأمن السيبراني فيما يلي:

- **ضمان سلامة المعلومات وتكاملها** :حماية البيانات من أي تدخل أو العبث، وضمان توفرها وجاهزيتها عند الحاجة.
- **حماية الأجهزة والشبكات** :تأمين جميع المكونات الرقمية لتكون بمثابة درع واقٍ يحمي البيانات والمعلومات من الاختراقات والهجمات.
- **كشف ومعالجة الثغرات** :استكشاف نقاط الضعف في الأنظمة والعمل على إصلاحها لتقليل المخاطر الأمنية.
- **استخدام وتطوير أدوات المصادر المفتوحة** :توظيف الأدوات الرقمية المتاحة وتطويرها بما يخدم مبادئ الأمن السيبراني ويعزز القدرة الدفاعية.
- **توفير بيئة عمل آمنة على الشبكة** :ضمان سلامة العمليات الرقمية أثناء العمل عبر الإنترنت، بما يضمن حماية المعلومات والمستخدمين على حد سواء.[2].
- ضمان توافر استمرارية عمل نظم المعلومات.

المطلب الثالث: أبعاد الامن السيبراني

[1] منى عبد الله السمحان، مرجع سبق ذكره، ص 12

[2] المرجع نفسه، ص 12

يُعدّ الأمن السيبراني من أهم مجالات العصر الرقمي، إذ يهدف إلى حماية الأنظمة والمعلومات من التهديدات الإلكترونية المتزايدة. فهو يشكل درعًا واقيًا يضمن استقرار المؤسسات وحماية الاقتصاد الوطني في ظل التطور التكنولوجي السريع.

الفرع الأول: البعد الاقتصادي

لقد أصبح الفضاء الإلكتروني جاذباً لقطاعات المجتمع كافة، وباتت المعرفة محرك الانتاج والنمو الاقتصادي، كما أيقن الجميع أن مبدأ التركيز على المعلومات والتكنولوجيا يعد عاملا من العوامل الأساسية للنهوض بالاقتصاد ، وهو ما دفع بالدول في الآونة الأخيرة تزيد من استثمارها في المعرفة ، وأصبحت عصرنة الاقتصاد مرتبطة بالتحكم في الاقتصاد الرقمي من طرف مختلف الفاعلين الاقتصاديين والاجتماعيين[1] كما أن استخدام الكمبيوتر وشبكة الانترنت في تطوير الصناعات وتحريك الاقتصاد ، ومعالجة كل المعاملات الاقتصادية والمالية، زاد من أهمية ضرورة توفير الأمن السيبراني لضمان حماية هذه المعلومات.

فعلى سبيل المثال ، يشير تقرير صادر عن شركة Emarketer إلى أن حجما لتجارة الإلكترونية بلغ 1.5 تريليون دولار في عام 2014 بزيادة نسبتها 20% مقارنة بعام 2013 الذي بلغت فيه 1.2 تريليون دولار، ونظرا لارتفاع معدل الجرائم السيبرية المنظمة والخطيرة، فإن ذلك يمثل تهديدا صريحا لنمو الاقتصاد الرقمي، ما لم تقم الدول بتعظيم معايير الأمن السيبراني بما يضمن الحد من هذه الجرائم[2].

الفرع الثاني: البعد الاجتماعي

[1] آمال بوجليدة، "للتوسع حول الاقتصاد الرقمي، الاقتصاد الرقمي التحول من الاقتصاد الصناعي إلى اقتصاد المعلومات"، مجلة الجيش العدد: 630 جانفي 2016، ص 45-47

[2] محمد مختار، هل يمكن أن تتجنب الدول مخاطر الهجمات الإلكترونية؟"، مجلة اتجاهات الأحداث. العدد 6، يناير 2015، ص 6

من الضروري تعميم المفهوم الصحيح والسليم للأمن إلى كل المشتركين في الشبكة الدولية للمعلومات، إذ تعتبر من الخطوات الأساسية التي تقوي مستوى الأمن إذا ما صيغت بطريقة واضحة وعُرفت ونفذت بذكاء، ولذلك يعتبر تنظيم الحملات الإعلامية والتثقيف المدني لأجل مجتمع معلومات مسؤول من الضرورة بمكان، بحيث تغطي التحديات والمخاطر، وتدابير الأمن والوقائية والرادعة لأجل تثقيف جميع الأفراد السيبرانيين للتعاطي مع عملية الأمن.

وينبغي التشديد على واجب الأمن والمسؤولية الفردية والتدابير الرادعة ، وكذلك التداعيات المحتملة في إطار القانون الجنائي التي تترتب على عدم احترام الالتزامات التي يوجبها الأمن، وبصورة أكثر عمومية، فإن من الضروري توفير التثقيف والتدريب على تكنولوجيات المعلومات والاتصال، وليس فقط على الأمن والتدابير الرادعة. إذ يجب للثقافة الأمنية أن تغرس داخل ثقافة تكنولوجيا المعلومات.

ينبغي جعل الشبكة الدولية للمعلومات مشاعا مفتوحا للجميع بحيث يمكن لجميع المتعاملين السيبرانيين أن يستفيدوا من البنى التحتية والخدمات المتاحة لهم دون تحمل مخاطر أمنية زائدة ويحتاج الأمر إلى بلورة مدونة أخلاقيات الأمن، تكون مقبولة ومحترمة من جانب جميع العاملين في الفضاء السيبراني[1].

الفرع الثالث: البعد القانوني

يترتب على النشاط الفردي والمؤسساتي والحكومي، في الفضاء السيبراني، نتائج قانونية، وموجبات تستدعي اهتماما خاص، لحل النزاعات التي يمكن أن تنشأ عنها. وهو ما يستدعي مواكبة التحولات التي رافقت ظهور مجتمع المعلومات فظهرت حقوق أخرى، كحق النفاذ إلى الشبكة العالمية للمعلومات، وتوسعت بعض المفاهيم، لتشمل أساليب الممارسة الجديدة باستخدام تقنيات المعلومات والاتصالات، كالحق في إنشاء المدونات

[1] الاتحاد الأوروبي للاتصالات دليل الأمن السيبراني للبلدان النامية جنيف الاتحاد الدولي للاتصالات، 2006، ص، 17-16

الالكترونية، والحق في إنشاء التجمعات على الانترنت، والحق في حماية ملكية البرامج المعلوماتية.

كما ظهرت موجبات جديدة، ذات انعكاسات اقتصادية مثل موجب الاحتفاظ ببيانات الاتصالات، وموجب الإبلاغ عن مخالفات وجرائم خاصة بالمحتوى[1].

كل هذه التغيرات والتحولات تستدعي وجود ترسانة قانونية تنسجم مع التطورات الحاصلة، إن على مستوى الحقوق، أو على مستوى البيئات والعمليات

الفرع الرابع: البعد السياسي

هناك أمثلة كثيرة تدفع نحو الاهتمام بالبعد السياسي للأمن السيبراني، كالتسريبات المختلفة للوثائق الحساسة، التي تؤدي إلى مشكلات عويصة جدا، على المستوى الخارجي والدولي، كما أنه لا ينكر أحد الدور المتعاظم لشبكات التواصل الاجتماعي على المستوى السياسي (حملات انتخابية، تظاهرات افتراضية، حركات احتجاجية إلكترونية، كما يتم استغلال هذه المواقع من طرف العديد من الحكومات لتمرير سياساتها.

وفي سياق آخر يجب ألا نغفل عن استخدام هذه المواقع من طرف الحركات الإرهابية لتجنيد أفرادها وجمع التمويل لعملياتها، وآلية للاتصال بينها كأفراد وكجماعات، وهو ما استوجب على الدول العمل على حماية أمنها من التهديدات والمخاطر التي قد تتعرض لها من خلال شبكة الانترنت.[2]

الفرع الخامس: البعد العسكري

تكمن الميزة النسبية للقوة السيبرانية في قدرتها على ربط الوحدات العسكرية ببعضها البعض عبر الشبكات العسكرية في الفضاء الإلكتروني، بما يسمح بسهولة تبادل

[1] منى الأشقر، الأمن السيبري: التحديات ومستلزمات المواجهة، اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني، بيروت 27-28 أغسطس 2012 القاهرة جامعة الدول العربية المركز العربي للبحوث القانونية والقضائية، ص 17

[2] محمد مختار، نفس المرجع السابق، ص 7

المعلومات وتدفقها ، وكذا السرعة وإعطاء الأوامر العسكرية والقدرة على إيصال الأهداف عن بعد وتدميرها، وقد تتحول هذه الميزة إلى نقطة ضعف لا قوة إن لم تكن شبكة الإلكترونية المستخدمة في ذلك مؤمنة جيدا من أي إختراق خارجي قد يتسبب في شن هجمات إلكترونية مضادة على شبكات القوات المسلحة وأجهزة الإستخبارات والقيام بعمليات التجسس على أمن العسكري للدول، وتعطيل قدرة الدولة على النشر السريع لقدراتها وقواتها، أو قطع أنظمة الإتصال بين الوحدات العسكرية وتعطيل شبكات الكمبيوتر، كما يمكن أن يتم شل وتعطيل عمل أنظمة الدفاع الجوي أو التوجيه الإلكتروني فضلا عن إمكانية فقدان السيطرة على وحدات القيادة.[1]

المطلب الرابع: التدابير الموضوعية والإجرائية المتبعة لتحقيق الأمن السيبراني وفق التشريع الجزائري

تفطن المشرع الجزائري للإجرام الإلكتروني وتدارك الوضع فبادر إلى سن مجموعة من القوانين بدأها بتعديل قانون العقوبات بالقانون 04-15 وسماه بالجرائم الماسة لأنظمة المعالجة الآلية للمعطيات" وبعدها بالقانون 2206 لتعديل قانون الإجراءات الجزائية والقانون 09-04 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال واتخاذ عدة تدابير نوضحها كما يأتي: التدابير القانونية والتقنية (أولا)، التدابير الهيكلية والتعاون الدولي (ثانيا).

الفرع الأول: التدابير الموضوعية والتقنية للأمن السيبراني

سار المشرع الجزائري على نهج الدول المتقدمة خاصة فرنسا في سن قوانين خاصة بتجريم السلوكات الماسة بأنظمة المعالجة الآلية للمعلومات، واستحدات إجراءات مستحدثة في القانون 06-22 وهو ما نراه في التدابير القانونية، ثم التدابير التقنية والإجرائية.

[1] إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مجلة مصداقية، كلية الحقوق والعلوم السياسية جامعة العربي التبسي، تبسة الجزائر، المجلد 01، العدد 01، 2019، ص105

1- التدابير القانونية للأمن السيبراني

تطرق المشرع الجزائري على غرار الدول الأخرى مثل فرنسا لتجريم أفعال المساس بأنظمة الحاسب الآلي وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام التي لم تشهدها البشرية من قبل، مما دفع بالمشرع إلى تعديل قانون العقوبات بموجب القانون رقم 04-15 المتمم للأمر رقم 66- 156 المتضمن قانون العقوبات، والذي أفرد القسم السابع مكرر منه تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات" من المادة 394 مكرر إلى 394 مكرر 7 ونص على عدة جرائم، أما في عام 2006 أدخل المشرع الجزائري تعديلا آخر على قانون العقوبات بموجب القانون رقم 06-23[1] حيث مس ذلك التعديل القسم السابع مكرر الخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وقد تم تشديد العقوبة المقررة لهذه الأفعال فقط دون المساس بالنصوص التجريمية الواردة في هذا القسم من قانون 15-04، وربما يرجع سبب هذا التعديل إلى ازدياد الوعي بخطورة هذا النوع المستحدث من الإجرام باعتباره يؤثر على الاقتصاد الوطني بالدرجة الأولى وشيوع ارتكابه، كما أدخل المشرع الجزائري بالقانون رقم 16-02[2] المعدل والمتمم لقانون العقوبات مادتين وهما 87 مكرر 11 ، و 394 مكرر 8 فاستعمل في الأولى عبارة تكنولوجيات الإعلام والاتصال، وفي الثانية عبارة (مقدم خدمات الانترنت)[3].

---

[1] محمد أحمد سليمان عيسى، التعاون الدولي لمواجهة الجرائم الإلكترونية، المجلة الأكاديمية للبحث القانوني، كلية العلوم والدراسات الانسانية بالغاط، جامعة المجمعة، المملكة العربية السعودية، المجلد / 14 العدد 02، 2016

[2] محمد السعيد زناتي الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية، مجلة إيليزا للبحوث والدراسات، المركز الجامعي إيليزي، الجزائر، المجلد 02، العدد 01، ديسمبر 2017

[3] مراد مشوش الجريمة المعلوماتية في ظل قانون العقوبات وقانون الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، مجلة القانون المجلد 09، العدد 01، 2020.

2- التدابير التقنية والإجرائية للأمن السيبراني

لقد أدرك المشرع الجزائري جيدا بأن المواجهة الفعالة للإجرام الإلكتروني لا تكون فقط بإرساء قواعد قانونية موضوعية ذات طبيعة ردعية، إنما لا بد من مصاحبة هذه القواعد بقواعد أخرى إجرائية وقائية وتحفظية، والتي من شأنها تفادى وقوع الجريمة الإلكترونية أو على الأقل الكشف عنها في وقت مبكر يسمح بتدارك مخاطرها، وهو ما إستدركه المشرع بتضمين القانون رقم 06-22[1] - المعدل لقانون الإجراءات الجزائية تدابير إجرائية مستحدثة تتعلق بالتحقيق في الجرائم الإلكترونية تتمثل في مراقبة الإتصالات الإلكترونية وتسجيلها والتسرب. ويقصد بإعتراض المراسلات إعتراض أو تسجيل أو نسخ المراسلات التي تكون في شكل بيانات قابلة للإنتاج والتوزيع، التخزين الإستقبال والعرض التي تتم عن طريق قنوات أو وسائل الإتصال السلكية واللاسلكية في إطار البحث والتحري عن الجريمة وجمع الأدلة عنها.

ولقد أشار المشرع الجزائري إلى ظروف وكيفية اللجوء هذا الإجراء في المادة 65 مكرر 5 من قانون الإجراءات الجزائية بموجب هذه المادة فان المشرع الجزائري يسمح لسلطات التحقيق والإستدلال إذا إستدعت ضرورة التحري في الجريمة المتلبس بها أو التحقيق في الجريمة الإلكترونية، اللجوء الى إجراء إعتراض المراسلات السلكية واللاسلكية وتسجيل المحادثات و الأصوات و التقاط الصور و الإستعانة بكل الترتيبات التقنية اللازمة لذلك، لأجل الوصول إلى الكشف عن ملابسات الجريمة وإثباتها دون أن يتقيدوا بقواعد التفتيش والضبط المألوفة[2].

[1]- أبو المعالي محمد عيسى الحاجة إلى تحديث آليات التعاون الدولي في مجال مكافحة الجريمة المعلوماتية، ورقة بحثية مقدمة في إطار المؤتمر العلمي المغاربي الأول حول المعلوماتية والقانون. أكاديمية الدراسات العليا، طرابلس، ليبيا، المنعقد في الفترة من 28 إلى 29 أكتوبر 2009

[2]عبد العزيز بن فهد بن محمد بن داود الجرائم السيبرانية: دراسة تأصيلية مقارنة مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 09، العدد 03، 2020، ص14

ومع هذا فان المشرع الجزائري لم يطلق حق اللجوء إلى هذا الإجراء، بل أحاطه بمجموعة من الضمانات القانونية التي تحد من تعسف سلطات الإستدلال والتحري وتصون الحقوق والحريات العامة والحياة الخاصة للأفراد.

الفرع الثاني: التعاون الدولي والتدابير الهيكلية والفعالية الأمن السيبراني

إن المواجهة القانونية لا تكفي لوحدها لمكافحة الجريمة الإلكترونية لأنها جريمة عابرة للحدود ولا تعترف بالحدود الوطنية أيضا يصعب إكتشافها، فبادر المشرع الجزائري إنشاء هياكل مؤسساتية المجابهتها وشجع على التعاون الدولي في مجال جمع المعلومات والأدلة وتبادل المجرمين بين الدول والمساعدة القضائية بصفة عامة ونوضح ذلك في التعاون الدولي ثم التدابير الهيكلية.

أولا- التعاون الدولي لمكافحة الاجرام السيبراني:

أصبحت الدولة لوحدها غير قادرة على مواجهة المخاطر السيبرانية، مما أوجب على الدول التعاون فيما بينها لحصر هذا الإجرام المستحدث والقضاء عليه نهائيا وعليه سنتطرق إلى التعاون الأمني الدولي ثم المساعدة القضائية فيما يلي.

أ- التعاون الأمني الدولي:

ضرورة التعاون الأمني الدولي لقد أثبت الواقع العملي أن الدولة أي دولة لا تستطيع بجهودها المنفردة القضاء على الجريمة مع هذا التطور الملموس والمذهل فى كافة ميادين الحياة. لذلك أصبحت الحاجة ماسة إلى وجود كيان دولي يأخذ على عاتقه القيام بهذه المهمة وتتعاون من خلاله أجهزة الشرطة في الدول المختلفة. خاصة فيما يتعلق بتبادل المعلومات المتعلقة بالجريمة والمجرمين بأقصى سرعة ممكنة بالإضافة إلى تعقب المجرمين الفارين من وجه العدالة[1].

[1] إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري مجلة مصداقية، كلية الحقوق والعلوم السياسية جامعة العربي التبسي، تبسة الجزائر المجلد 01، العدد 01، 2019، ص103

ب- المساعدة القضائية الدولية:

فتحديث آليات التعاون القضائي دوليا في المادة الجنائية يبدأ بخطوة أولى غايتها ضرورة تطوير القوانين الوطنية على نحو أكثر شمولية ومرونة حتى تواكب القوانين الوطنية حركة التشريع الدولية بشأن مكافحة الجريمة، وأن توثق التعاون بين أجهزة التنفيذية للدول وتنشئ أجهزة متخصصة لمواجهة الإجرام المنظم، و أن تصوغ نظرية متكاملة تستفيد من التطور التكنولوجي في إجراءات جمع الأدلة وتبادل المعلومات، للتصدي للمنظمات الإجرامية التي تعمل بأسلوب علمي مدروس على تشتيت الأدلة والتخلص منها مما يستدعي تطوير التعاون القضائي في مختلف مراحله ، بما فيها مرحلة تنفيذ الأحكام[1].

ج - تكريس المشرع الجزائري لمبدأ التعاون الدولي والمساعدة القضائية للأمن السيبراني:

بالنسبة للمشرع الجزائري تؤكد المادة (16) من القانون 09-04 سالف الذكر في هذا الجاني على أنه وفي إطار التحقيقات والتحريات التي تمت مباشرتها بخصوص الجرائم الإلكترونية، فيمكن للسلطات القضائية المختصة تبادل المساعدة القضائية على المستوى الدولي قصد جمع الأدلة الخاصة بالجريمة الإلكترونية على أساس ما تشكله هذه الجرائم المستحدثة من صعوبات تقنية بالغة على مستوى كشفها واثابتها وملاحقة مرتكبيها، إذ لا يمكن لدولة بمفردها القيام بذلك. ونظرا لحالة الاستعجال التي تتطلبها إجراءات التحقيق الجمع الأدلة الخاصة لهذا النوع من الجرائم المستحدثة وما يتطلبه من سرعة لاتخاذ هذه الاجراءات، أقر المشرع قبول طلبات المساعدة القضائية حتى وإن جاءت عن طريق وسائل الاتصال السريعة كالبريد الإلكتروني أو الفاكس بشرط التأكد من

[1] المرجع نفسه، ص 104

صحتها فقط[1]، وتخضع لمبدا المعاملة بالمثل، احتراما لمبدأ سيادة الدولة حسب المادة 17 من القانون 09-04 السالف الذكر[2].

وكما هو معروف لا تستطيع الدولة لوحدها مواجهة الاجرام السيبراني مهما بلغت من تطور في مجال الأمن السيبراني، ولا سبيل للمكافحة هذا النوع من الاجرام المستحدث إلا نهج التعاون الدولي خاصة التعاون القضائي الدولي والمساعدة القضائية، وقد نصت على ذلك إتفاقية بودابست لمكافحة الإجرام السيبراني لسنة 2001، وأيضا الاتفاقية العربية لمكافحة تقنية المعلومات 2010 ، اللتان حرصنا على التعاون الدولي وكيفية التصدي للإجرام السيبراني وخاصة إتفاقية بودابست 2001 التي تعتبر إقليميا، لكن هي ذات طابع دولي وهي مصدر ومرجع الدول في رسم سياسة التصدي لهذه المخاطر التي باتت تهديد حقيقي للدول والافراد.

ثانيا- التدابير الهيكلية لفعالية الأمن السيبراني:

عكف المشرع الجزائري في محاربته للجريمة الإلكترونية بإنشائه لعدة هياكل وظيفتها مكافحة الجريمة السيبرانية نذكر منها:

أ- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال:

نصت على إنشاء هذه الهيئة المادة 13 من القانون 09/04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها «تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام

[1] جمال بوازدية الإستراتيجية الجزائرية في مواجهة السيبرانية التحديات والأفاق المستقبلية"، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 01 أفريل 2019، ص 1267

[2] أنظر المادة 10/3 من القانون رقم 18-04 المؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018، الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الصادر في الجريج العدد 27، بتاريخ 13 مايو 2018، ص 03

والإتصال ومكافحته. تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم »، أما مهامها فقد أوردتها المادة 14 من نفس القانون[1].

ومن مهامها حسب المادة 04 من المرسوم الرئاسي رقم: (21-439)، المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والذي بعدها حول الإشراف على الهيئة إلى أمانة رئاسة الجمهورية، ومن أهم إختصاصاتها مبينة كالتالي[2]:

1- الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال؛

2- مكافحة كافة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال؛

3- تبادل المعلومات مع الدول لأجل تعزيز التعاون الدولي والمساعدة القضائية.

ب- الهيئات القضائية الجزائية المتخصصة:

يقصد بها الأقطاب الجزائية المتخصصة المنشاة بموجب القانون 14-04 المؤرخ في 10 نوفمبر 2014، وتختص هذه الجهات القضائية بموجب المواد 37-329.40 من قانون الإجراءات الجزائية بالنظر في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، بالإضافة إلى الصلاحيات الأخرى الممنوحة للجهات القضائية او للضبطية القضائية في إطار معالجة مثل هذه الجرائم.

ج- جهازي الأمن الوطني والدرك الوطني:

حيث سعت المديرية العامة للأمن الوطني وكذا جهاز الدرك الوطني التي إنشاء فرق خاصة لمكافحة الجرائم المعلوماتية، وكذا تكوين عناصر متخصصة في هذا المجال سواء على المستوى الداخلي أو المستوى الخارجي، بالإضافة إلى توفر على هاذين

[1] الأمر رقم 15666 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 المتضمن قانون العقوبات المعدل والمتم. المنشور بالج ر ج عدد 49 مؤرخة في 11 يونيو 1966، ص 702

[2] انظر المواد من 394 مكرر إلى 394 مكرر 7 من القانون 04-15 المؤرخ في 10 نوفمبر 2004، الصادر في الج ر ج رقم: 71 المتضمن تعديل قانون العقوبات لسنة 2004، ص 11 و 12.

الجهازين من مخبرين علميين للشرطة العلمية والتقنية يتوفران على أحدث الأجهزة ذات تكنولوجيا متطورة لكشف هذا النوع من الإجرام[1].

د- المعهد الوطني للأدلة الجنائية على الإجرام:

يتكون من إحدى عشرة دائرة متخصصة في مجالات مختلفة، جميعها تضمن إنجاز الخبرة، التكوين والتعليم وتقديم المساعدات التقنية ودائرة الإعلام الآلي والإلكتروني مكلفة بمعالجة وتحليل وتقديم كل دليل رقمي يساعد العدالة، كما تقدم مساعدة تقنية للمحققين في المعاينات[2].

يبدو أن الجزائر وتشريعاتها الموضوعية والإجرائية تسعى جاهدة للقضاء على أثار هذا النوع من الإجرام بشتى الطرق والأساليب دون الإصطدام بجدار حقوق الإنسان التي صانها دستور 2020 في مواده والحرص على تطبيقها واحترام الحياة الخاصة للفرد من أجل التكفل بحياة كريمة مصونة.

المبحث الثاني: الاقتصاد الرقمي

يُعدّ الاقتصاد الرقمي من أبرز ملامح العصر الحديث، إذ يعتمد على التكنولوجيا والمعلوماتية في تسيير الأنشطة الاقتصادية والإنتاجية. فهو يقوم على استخدام الإنترنت والابتكار الرقمي لتحسين الخدمات، وتعزيز النمو الاقتصادي، وتحقيق التنمية المستدامة.

المطلب الأول: مفهوم الاقتصاد الرقمي

يقصد بالاقتصاد الرقمي ذلك النمط الاقتصادي الذي يعتمد على التكنولوجيا الرقمية

[1] بدري فيصل مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة لنيل شهادة دكتوراه علوم تخصص قانون عام. كلية الحقوق، جامعة الجزائر 1 بن يوسف بن خدة 2018، ص 154

[2] أنظر المادة 102 من القانون رقم 09 - 04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المنشور بالج ر ج العدد 47 بتاريخ 16 غشت سنة 2009.

في إنتاج السلع والخدمات وتبادلها، مستفيدًا من الإنترنت والاتصال الذكي في تسيير المعاملات التجارية. ويُعدّ هذا الاقتصاد من الركائز الأساسية للتحول الرقمي والتنمية المستدامة في العصر الحديث.

الفرع الأول: تعريف الاقتصاد الرقمي

يُعرف الاقتصاد الرقمي بأنه: "التفاعل والتكامل والتنسيق المستمر بين تكنولوجيا المعلومات وتكنولوجيا الاتصالات من جهة، وبين الاقتصاد القومي والقطاعي والدولي من جهة أخرى بما يحقق الشفافية الفورية والإتاحة الجميع المؤشرات الاقتصادية المساندة الجميع القرارات الاقتصادية والتجارية والمالية في الدولة خلال فترة ما."[1]

كما يشير الاقتصاد الرقمي إلى الاقتصاد القائم على الانترنت أو الويب، وهو الاقتصاد الذي يتعامل مع الرقميات أو المعلومات الرقمية الزبائن الرقميين الشركات والتكنولوجيا الرقميتين مثل : تكنولوجيا الاتصالات عن بعد الوسائط المتعددة التكنولوجيا الخلوية, بالإضافة إلى المنتجات الرقمية مثل قواعد ومستودعات البيانات المعلومات البرمجيات كتب ودوريات الويب الألعاب الالكترونية الموسيقى وكذلك المنتجات المادية المزودة بالمعالجات المصغرة.[2]

ويمكن تعريف الاقتصاد الرقمي كذلك على انه لممارسة الأنشطة الاقتصادية في المجال الإلكتروني باستخدام تقنية ووسائط الإتصالات وتكنولوجيا المعلومات من خلال إيجاد روابط فعالة ما بين أطراف النشاط الاقتصادي بهدف تحسين نوعية الحياة بكافة مجالاتها وأنشطتها."[3]

كما عرف بأنه: " ذلك الاقتصاد الذي يدور حول الحصول على المعرفة وتوظيفها وابتكارها بهدف تحسين نوعية الحياة بمجالاتها كافة من خلال الإفادة من خدمة معلوماتية ثرية، وتطبيقات تكنولوجية متطورة واستخدام العقل البشري كرأس للمال، وتوظيف البحث

[1] فريد راغب النجار، الاستثمار بالنظم الالكترونية والاقتصاد الرقمي، مؤسسة الشباب الجامعية، الإسكندرية، مصر،2004، ص 11.

[2] نجم عبود نجم، الإدارة الالكترونية الإستراتيجية، الوظائف والمشكلات دار المريخ، السعودية ،2004،ص 88.

[3] خالد محمد البراهمه (2017)، التجارة الالكترونية كمدخل لهيكلة الاقتصاد الرقمي، مقالة منشورة عبر الموقع: http://www.academy-news.com/articles.php?action=show&id=597

العلمي لأحداث مجموعة من التغييرات الإستراتيجية في طبيعة المحيط الاقتصادي وتنظيمه ليصبح أكثر استجابة وانسجاماً مع تحديات العولمة وتكنولوجيا المعلومات والاتصالات وعالمية المعرفة والتنمية المستدامة."[1]

ومن خلال التعاريف السابقة يمكن القول بأن الاقتصاد الرقمي هو ذلك الاقتصاد الذي يقوم اساسا على استخدام تكنولوجيا المعلومات والاتصال واستخدام العقل البشري، وتوظيف البحث العلمي لتطوير المنتجات والخدمات وبالتالي تحسين نوعية الحياة بمختلف مجالاتها.

الفرع الثاني: خصائص الاقتصاد الرقمي

يعمل الاقتصاد الرقمي على نشر مجتمع المعلومات والمعرفة، أو ما يطلق عليه اقتصاد المعرفة، أو المجتمع الشبكي.

أولا: سهولة الوصول إلى مصادر المعلومات

يعتمد نجاح ونمو الاقتصاد الرقمي على قدرة الأفراد والمؤسسات على المشاركة في شبكات المعلومات ومواقع الإنترنت المختلفة، ويتطلب الاشتراك الفعال في تلك الشبكات وفي الاقتصاد الرقمي ضرورة توفر البنية التحتية، مثل شبكات الكهرباء، وشبكات الهواتف، وانخفاض تكلفة ورسوم تلك الخدمات، وتوفر الآلات والأجهزة والمعدات والمهارات والتعليم والتدريب وتوفر الموارد المالية واستخدام الأموال الإلكترونية والبلاستكية مثل: بطاقات الائتمان الدائنة والمدينة [2].

ثانيا: يلغي أهمية الموقع

يسمح استخدام التقنية الملائمة خلق أسواق ومنشآت افتراضية تلغى فيها حدود المكان والزمان، ومثال ذلك التجارة الالكترونية التي توفر الكثير من المزايا منها تخفيض التكلفة، رفع الكفاءة والسرعة في انجاز المعاملات على مدار الساعة وعلى نطاق العالم. ونتيجة لذلك ينصب التركيز أولا على تطوير الأسواق والشراكة والتحالف الاستراتيجي مع

[1] محمد جبار طاهر الشمري (2008)، دور اقتصاد المعرفة في تحقيق النمو الاقتصادي – مصر أنموذجا مجلة الغري للعلوم الاقتصادية المجلد 02، العدد 10، كلية الإدارة والاقتصاد جامعة الكوفة العراق، متاح على الرابط: http://www.uokufa.edu.iq/journals/index.php/ghjec/article/view/1727

[2] فريد النجار، الاقتصاد الرقمي، الدار الجامعية لنشر والتوزيع، الاسكندرية، مصر، الطبعة الأولى، 2007، ص 25.

أطراف خارجية قبل التركيز على تطوير المنتجات[1].

ثالثا: الاقتصاد الرقمي يوفر المعلومات لاتخاذ القرارات

يمكن التحكم في المعلومات بالاستخدام الفعال للمعلومات وتوظيفها لخدمة القرارات والسياسات الاقتصادية وتساعد مهارات إدارة المعلومات في نجاح اتخاذ القرارات الاستثمارية بعيدة المدى بدقة، ويوفر الاقتصاد الرقمي المعلومات عن طريق تعلم كيفية تحديد الاحتياجات المعلوماتية ثم اختيار المصادر المناسبة للمعلومات الأساسية والهامة أي إدارة الصادر والوارد من المعلومات بطريقة أكثر كفاءة وتكون هذه المعلومات إما[2]:

1- معلومات إلكترونية وتشمل البريد الإلكتروني والإنترنت والمواد المسجلة على أشرطة الفيديو والمعلومات الموجودة على الأقراص الصلبة أو المرنة.

2- معلومات منطوقة تتمثل في المكالمات الهاتفية والحوارات.

3- معلومات مطبوعة مثل التقارير والفاكسات.

يوفر الاقتصاد الرقمي المعلومات المثالية من الحداثة والكفاءة والأهمية والدقة وإمكانية التحقق من صحتها.

بالإضافة إلى الخصائص السابقة يمكن إضافة الخصائص التالية[3]:

- **الاقتصاد الرقمي يسمى كذلك الاقتصاد الجديد:** ليس له علاقة التي نعرفها، وإنما هو جديد لأن الأفكار والمناهج والوسائل والزبائن جدد، فالاقتصاد الجديد يبنى على تخصيص المستهلكين الجانب الاجتماعي التطوير والمعرفة بالنسبة للمؤسسات القطب الاقتصادي، والقطب التكنولوجي المرتكز على تطوير الوسائل التكنولوجية الاتصالات وسائل الإنتاج، البيع ... الخ.
- **اقتصاد مرتبط باليقظة:** من اقتصاديات الحجم في سنوات الستينات إلى أول حاسوب

[1] بطاهر بختة، توجهات الاقتصاد الرقمي في البلدان العربية في ظل رغبتها في تطبيقه، مجلة منتدى للدراسات والأبحاث العلمية، جامعة زيان عاشور الجلفة الجزائر، العدد 02، 2020، ص 147

[2] سعيد بن دنيدة، عامر بوعا كاز، سبل ووسائل حماية المستهلك الالكتروني من مخاطر الاقتصاد الرقمي، مجلة البناء الاقتصادي، جامعة الجلفة الجزائر، العدد 01 2018، ص 69.

[3] متناوي محمد، الاقتصاد الرقمي واشكالية التجارة الالكترونية في الدول العربية، الملتقى الدولي الثاني حول المعرفة في ضل الاقتصاد الرقمي ومساهمتها في تكوين المزايا التنافسية للبلدان العربية، جامعة حسيبة بن بو علي بالشلف، يومي 4-5 ديسمبر 2007، ص 4.

في الثمانينات والآن الاقتصاد الجديد الذي أصبح ينظم التجارة بين منشأة أعمال ز منشأة أعمال أخرى وأيضا ساعد في تسهيل التجارة ما بين منشأة الأعمال والمستهلك. فأصبح اليوم قانون العرض والطلب هو السائد مما خلق اهتمام بسلوك الزبون حتى يضمن ولاءه كما يجب الاستجابة السريعة والفورية لأي تغيير في هذا السلوك.

- **اقتصاد مضاعف بالأنترنت:** إذ أنه اقتصاد لا يعترف بحدود الدول، يعرض منتجاته وخدماته في كل مكان في العالم.
- **اقتصاد الأسواق الإقليمية:** اقتصاد يتجسد حيث يقطن الزبون إذ يعتبر الاقتصاد الرقمي محصلة التفاعل بين اتجاهات تقدم تكنولوجيا المعلومات والاتصال وبين المنظومة الاقتصادية الاقتصاد الكلي الاقتصاد الجزئي واقتصاد القطاعات النوعية في الصناعة والزراعة والتجارة والبنوك والمال والصحة والتعليم والعلاقات الاقتصادية الدولية والسياسات النقدية والسياسات المالية وغيرها ويساعد الاقتصاد الرقمي في معرفة أثر الاقتصاد على المجتمع وتشخيص المشكلات.

يؤثر الاقتصاد الرقمي في فروع الاقتصاد المختلفة بالربط بين النماذج الاقتصادية والبرمجيات والإنترنت وذلك لتحقيق المثلية[1].

المطلب الثاني: مكونات وملامح الاقتصاد الرقمي

يتكون الاقتصاد الرقمي من عدة عناصر أساسية تشمل البنية التحتية الرقمية مثل الإنترنت وشبكات الاتصالات، والمنصات الإلكترونية التي تتيح التبادل التجاري والخدمات المالية، إضافة إلى البيانات الرقمية التي تُعدّ موردًا اقتصاديًا مهمًا، والتقنيات الحديثة كالذكاء الاصطناعي والحوسبة السحابية التي تدعم الابتكار وتحسين الإنتاجية.

الفرع الأول: مكونات الاقتصاد الرقمي

يتكون الاقتصاد الرقمي من عدة عناصر ترتبط من خلال شبكة الاتصالات التكنولوجية الرقمية عن طريق البريد الالكتروني ومواقع التواصل الالكترونية التي تعد القاعدة الأساسية لتحقيق الفاعلية الاقتصادية بين القطاعات والمؤسسات والحكومات في

[1] صالح عبد الحميد، العملات الرقمية، طيبة لنشر والتوزيع مصر القاهرة، الطبعة الأولى 2018 ، ص 13

بلدان العالم المختلفة مع الأخذ بنظر الاعتبار مبدأ تقليل التكاليف من خلال استخدام التكنولوجيا الرقمية حيث إن التكلفة الحدية في هذا الاقتصاد تقترب من الصفر عن طريق استعمال الحواسيب والهواتف الرقمية التي أصبحت ملازمة لحياة الإنسان وساهمت في سرعة النمو والنضوج الاقتصادي الذي ظهر نتيجة للابتكار والتجديد حيث تفاعل الاقتصاد المحلي والدولي[1].

وهناك أربعة أجزاء رئيسية للاقتصاد الرقمي[2]:

1 – السلع والخدمات الرقمية غير الملموسة، حيث يتم تداولها رقمياً عبر أجهزة الاتصالات والحاسوب مثل خدمات المعلومات عبر الانترنت، ومبيعات البرامج، والتعليم الالكتروني.

2 – السلع والخدمات الملموسة وعمليات الإنتاج التداول التسويق المرتبطة بها عبر أجهزة الاتصالات وتقنيات الانترنت.

3– خدمات الإنتاج المعتمدة على تكنولوجيا المعلومات في تصنيع السلع الملموسة مثل التصاميم الهندسية المعقدة، والآلات الدقيقة التي تستخدم التحكم الرقمي المحوسب والعمليات الكيميائية التي تسيطر الحاسبات الالكترونية على تصنيعها.

4 – قطاعات صناعة تكنولوجيا المعلومات الداعمة لمكونات الاقتصاد الرقمي، وتشمل صناعة أجهزة الكمبيوتر والهواتف والأجهزة الرقمية الذكية، فضلاً عن خدمات البث والاتصالات.

ومن مكونات الاقتصاد الرقمي أيضا المستهلكون الرقميون فكل مستهلك يدخل على شبكة الانترنت يمتلك حساب أو منصة إلكترونية يقوم بالبحث عن السلعة أو الخدمة التي يطلبها ويختارها ويشتريها إلكترونيا ومن العناصر المكونة للاقتصاد الرقمي (البائعون الرقميون الذين يمثلون الشركات والمؤسسات التسويقية التي تروج لسلعها أو خدماتها من خلال الدعاية والإعلان الكترونياً عن طريق الانترنت وتعد الأنظمة المسئولة عن الرقمنة

[1] عليان ربحي مصطفى، اقتصاد المعرفة دار الصفاء النشر والتوزيع، عمان الأردن 2012، ص 109

[2] Bukht, Rumana&Heeks, Richard, Defining, Conceptualising and Measuring the Digital Economy, University of Manchester, Arthur Lewis Building. Manchester M13 9PL, UK, 2017, P5

من مكونات الاقتصاد الرقمي وتشمل الجهات التي توفر الأجهزة الالكترونية الذكية والحاسبات وتقوم بإدارة شبكات الاتصالات والمعلومات مثل شركة مايكروسوفت وأمازون وغيرها وهناك أيضاً مكون القوانين والأنظمة التي تضبط التعاملات والتفاعلات الاقتصادية الرقمية[1].

ويمكن القول أيضاً أن عناصر الاقتصاد الرقمي تتكون من[2]:

اولا. الأجهزة الذكية والبرمجيات

تعد الأجهزة التقنية قاعدة البنية الهيكلية التي تعالج المعاملات والتفاعلات للاقتصاد الرقمي، وتوجد أنواع كثيرة من الأجهزة ذات التكنولوجيا الرقمية الذكية تتفاعل مكونات الاقتصاد الرقمي وتستخدم فيها المعالجات التقنية الدقيقة المتوازنة وتكنولوجيا الاستخدام الأخرى من خلال البرمجيات التي يكون على عاتقها تطوير السلع والخدمات المنتجة من قبل الشركات المساهمة في الاقتصاد الرقمي عن طريق أنظمة تخطيط الموارد وإعداد لبيانات وخدمات إدارة المعلومات.

ثانيا. تقنيات الاتصالات

ويساهم هذا المكون في خلق منتجات الاتصالات والخدمات اللازمة للأعمال التجارية الكترونياً وتمثل منتجات وخدمات الاتصالات الهاتفية والبث الإذاعي والتلفزيوني الخ، كما تعد هذه الاتصالات أكبر من كونها شبكة الكترونية، حيث أنها تشمل أنظمة الاتصال وتبادل المعلومات مثل الهاتف النقال وشبكة الأقمار الصناعية والكاميرات الرقمية وجميع الخدمات التي تدفع بعجلة النمو الاقتصادي مثل خدمات الحكومة الالكترونية ومظاهر التجارة الالكترونية.

ثالثا. آليات التجارة الالكترونية

يعد هذا عنصراً آخر من مكونات الاقتصاد الرقمي من خلال استخدام المنصات الالكترونية في المعاملات التجارية وتلعب الشركات دورا هاما في هذا المجال، فالشركات

[1] الموسوي صفاء عبد الجبار، كاظم سعد الأعرجي، زينب هادي نعمة الاقتصاد الرقمي الأيام المنشر والتوزيع، عمان الأردن 2016، ص 22-23

[2] علي محمد مدلول الاقتصاد الرقمي رؤى وآفاق دراسة حالة البلدان العربية مجلة جامعة بابل العدد (2) لسنة 2020، ص 234-235

تكون قادرة على تبادل الاتصال من خلال تدفق المعلومات مع الزبائن والوكلاء حيث تكون أكثر فعالية وأقل تكلفة، لذا فان الأعمال التجارية الالكترونية تعمل على تحسين وقت الاستجابة لتجهيز العملاء من خلال البريد الالكتروني والتبادل الالكتروني.

رابعا. منظمو العمليات الرقمية

ويمكن وصفهم برأس المال البشري والمعرفة الجماعية ومهارات القوة العاملة ويعتبرون عنصراً مهماً من مكونات الاقتصاد الرقمي، يتم من خلالهم تحديد فشلا ونجاح الشركات، وسط بيئة تنافسية، فرأس المال البشري يشمل المتخصصين في مجال تكنولوجيا المعلومات لاسيما الخبرة المستندة إلى نظام من مستندات النص الفائق المرتبطة ببعضها وتعمل خلال الإنترنت، ويستطيع المستخدم تصفح هذه المستندات باستخدام متصفح ويب، وكذلك التنقل بين هذه الصفحات عبر وصلات النص الفائق، وتحتوي هذه المستندات على نص صرف وصور ووسائط متعددة، عن طريق الوصول لي خدمات المعلومات وتطبيقات اقتصاد المعلومات.

خامسا. التكنولوجيا الناشئة

وهو دور التكنولوجيا الناشئة في تطوير الاقتصاد الرقمي وذلك من خلال تحديث وتطوير تطبيقات ومواقع الانترنت، والهدف من ذلك تخفيض التكاليف وتوفير البرامج بأسعار معقولة للأفراد والمؤسسات والشركات محلياً ودوليا.

سادسا. شبكة الاتصالات والمعلومات التكنولوجية العالمية (الانترنت)

أدى تطور تقنيات المعلومات والاتصالات إلى تداخل الأنشطة الاقتصادية في الشبكة العالمية للاتصالات والمعلومات (الانترنت) حيث اضمحلت الحدود المادية والجغرافية الأمر الذي سهل عمل القطاعات الاقتصادية ضمن أنشطة الأفراد والشركات والمؤسسات في البلدان العالم المختلفة. وتعد الانترنت الشبكة العالمية الكبرى التي تستخدم من قبل ملايين الإفراد لغرض تبادل المعلومات وعقد الصفقات وتكون خدماتها متوفرة وفق مرونة في الاشتراك والتوزيع بكلفة منخفضة أو معدومة، وهي شبكة الاتصالات التي يستخدمها الأفراد للدخول إلى مواقع الشركات من أجل شراء السلع

والخدمات ومعرفة المعلومات المتعلقة بتسويق السلع والخدمات[1].

الفرع الثاني: ملامح الاقتصاد الرقمي

إن لشبكة الانترنت القدرة على جعل الاقتصاد يبدو شفافا من ناحية وضوح مدخلات ومخرجات الأسواق العالمية لتوفر كافة المعلومات عن الأسعار والمنتجات بدون أي وسطاء في عمليات التبادل حيث يستطيع البائعون والمشترون المقارنة بين أسعار البيع والشراء بكل وسهولة وتكون الوفرة هي الصفة البارزة وليس مفيدا بالندرة كما في الاقتصاد التقليدي حيث كلما زاد عدد المستهلكين أصبح للسلعة قيمة ومنفعة أكبر، لذلك نرى أكثر الشركات تخفض الأسعار وخاصة السلع الجديدة أو المطورة وتستخدم أساليب الدعاية والإعلان الالكتروني للترويج لها، وبعد الإقبال الواسع إلى شرائها ترتفع الإيرادات كما نلاحظ في سياسات شركات الاتصالات الهاتفية ذات الدفع المسبق حيث ان أنجح نموذج للعمل في الاقتصاد الرقمي هو الفاعلية التي ترفع من كفاءة المنتجات، ومع زيادة المنافسة فإن المردود يرتكز على الاستفادة من اقتصاديات الحجم، أما فيما يخص كلفة العمل في الاقتصاد الرقمي فإن علاقات العمل في السوق الرقمية، تقوم على أساس الضمان والمشاركة والمهارة التي تتطلب كفاءة في التعليم وتدريب مستمر.

وإن الهدف الأساسي من التحول نحو الاقتصاد الرقمي هو تدنية التكاليف سيما تكلفة عنصر العمل وزيادة المنفعة والأرباح للمنتجين، وبالتالي زيادة الناتج المحلي الإجمالي ودفع أجهزة النمو وزيادة الثروة وهو الهدف الأسمى في علم الاقتصاد[2].

بلغت مساهمة الاقتصاد الرقمي 11.5 تريليون دولار ، أي ما يعادل 15.5% من الناتج المحلي الإجمالي العالمي، منها 18.4% في الاقتصادات المتقدمة و 10% في الاقتصاديات النامية وبلغ معدل سرعة نمو الاقتصاد الرقمي (2.5) مرة في الناتج المحلي الإجمالي العالمي منذ بداية عام 2000 حيث كانت الدول المتقدمة صاحبة المساهمة الأكبر في خلق القيمة المضافة من خلال الاقتصاد الرقمي وأبرز هذه الدول الولايات

[1] النعيمي يوسف خليل إبراهيم على انعكاس تكنولوجيا المعلومات والاتصالات في الاقتصاد المعرفي دراسة استطلاعية لشركتي آسيا سيل وزين العراق بمحافظة أربيل، رسالة ماجستير، جامعة تكريت 2015، ص 46

[2] التجار اخلاص باقر هاشم، الاقتصاد الرقمي والفجوة الرقمية في الوطن العربي، أطروحة دكتوراه جامعة البصرة 2007، ص 27-29

المتحدة حيث بلغت حصتها 35% ، والصين 13%، واليابان 8%، وساهم الاتحاد الأوروبي بـ 25%، وباقي دول العالم 19% كما ورد خلال مؤتمر الأمم المتحدة للتجارة والتنمية المنعقد في نيويورك عام 2019.[1]

حيث أثر الاقتصاد الرقمي بشكل كبير في مبيعات سلع المنتجات الاستهلاكية ولاسيما مبيعات التجزئة بسبب انتشار تجار التجزئة الرقميون مثل (أمازون) وقد تمت إعادة هيكلة نشاطات تجار التجزئة التقليديين لمواكبة الاقتصاد الرقمي، وأفلس بعض التجار لإخفاقهم في التكيف مع الاقتصاد الرقمي وعمل بعض تجار التجزئة مع وسطاء خارجيين من أجل تطوير أعمالهم التجارية وتحويلها إلى تجارة رقمية بالكامل، واستطاع صغار تجار التجزئة أن يتنافسوا مع الشركات التجارية الكبيرة متعددة الجنسية[2].

ولغرض رفع مستوى خدمة الانترنت في العالم عقد في مدينة ووتشن الصينية (المؤتمر العالمي للإنترنت – منتدى تطوير الإنترنت في شهر تشرين الأول 2020، وقد صدر عنه تقرير أكد فيه على أهمية الانترنت والاقتصاد الرقمي كقوة هامة للتخفيف من أثر وباء كوفيد – 19– المتفشي وإعادة تنظيم الاقتصاد وتعزيز السيطرة الرقمية للحكومات، حيث إن تفشي وباء كورونا أثر على النمو الاقتصادي والتطور الاجتماعي العالمي، فظهر الاقتصاد الرقمي كمنقذ أنعش الاقتصاد العالمي، وبناء على ما جاء في التقرير، فإن وباء كورونا قد نشط الطلب على التكنولوجيا لوجود المحطات السحابية، وقد لاقت الصناعات المرتبطة بالإنترنت رواجاً حيث بلغت نسبة الاقتصاد الرقمي ما بين 4.5% و 15.5% من الناتج المحلي الإجمالي العالمي في عام 2019، وفقا لتقرير الاقتصاد الرقمي عن مؤتمر الأمم المتحدة للتجارة والتنمية الصادر في بداية عام 2020، وبلغ عدد مستخدمي الانترنت أكثر من 4.5 مليار شخص أي 60% من عدد سكان

[1] United Nation Conference On Trade And Development(UNCTAD), Digital Economy Report 2019 P69

[2] يوسف نورة عبد الرحمن ، الاقتصاد الرقمي مقالة في جريدة العرب الاقتصادية الدولية الالكترونية ، متاحة على الموقع
www.aleqat.com

العالم، منهم 3.8 مليار شخص يستخدم وسائل التواصل الاجتماعي[1].

وقد عقد الاتحاد الدولي للاتصالات ندوة بعنوان (التوصيلية الشاملة ، مستقبل التنظيم) حيث أشار منظمو تقنيات الاتصالات إلى ضرورة توصيل خدمات الاتصالات إلى البلدان النامية لكي تواكب التطورات الاقتصادية والثقافية والتكنولوجية، ولتحقيق ذلك لابد من توفر البنية الارتكازية القادرة على تنظيم بيانات المواطن التي تحتاجها الدول النامية لتفعيل الاقتصاد الرقمي وازدهاره ومن ثم الانتقال الى الجيل الرقمي السادس (IPv6)، حيث أن الكثير من دول العالم الثالث تكافح بسبب افتقارها إلى المعرفة البشرية وانخفاض الفكر العلمي حيث شهدت بعض الدول النامية تطوراً كبيراً في مجال تقنية الاتصالات وتكنولوجيا المعلومات ، وارتفع فيها معدل الأعمال الرقمية وفق المنهج التنظيمي المبني على الابتكار، والاعتماد على الخدمات المالية الرقمية وتهيئة الظروف لتزيد من مهارة المشغلين لخدمات الاقتصاد الرقمي وزيادة نسبة المستخدمين من السكان ورفع مستوى الاستثمار في هذا المجال وبالتالي زياد حصيلة الضريبة على أجهزة الاتصال والخدمات فتكون بذلك فرصة لتحقيق الإيراد وزيادة النمو[2].

المطلب الثالث: متطلبات الاقتصاد الرقمي ومؤشراته

يتطلب الاقتصاد الرقمي توفر بنية تحتية تقنية متطورة وكفاءات بشرية قادرة على التعامل مع التكنولوجيا الحديثة، إضافة إلى تشريعات داعمة وأمن سيبراني قوي. وتعكس مؤشرات مثل انتشار الإنترنت وحجم التجارة الإلكترونية ومستوى الابتكار الرقمي مدى تقدم الدولة في هذا المجال وقدرتها على المنافسة عالميًا.

الفرع الأول: متطلبات الاقتصاد الرقمي

- يحتاج الاقتصاد الرقمي إلى مجموعة متكاملة من المتطلبات من أهمها ما يلي[3]:

---

[1] صحيفة الشعب اليومية الصينية الاقتصاد الرقمي يدفع الانتعاش الاقتصادي العالمي 25/11/2020 متاحة على الموقع الالكتروني
http://arabic.people.com.cn

[2] الندوة العالمية لمنظمي الاتصالات التوصيلية الشاملة، مستقبل التنظيم، بورت فيلا فانواتو، من 9 إلى 12 تموز 2019، ص 7.

[3] ايمان صالح عبد الفاتح التخطيط الاستراتيجي في المنظمات الرقمية، إيبيس كوم للنشر والتوزيع القاهرة، مصر، طبعة الأولى، 2007، ص22-23

- ✧ وعي وثقافة جماهيرية بحيث يمكن من الوصول إلى المواقع الاقتصادية المختلفة.
- ✧ توفير البنية التحتية اللازمة من تقنية وشبكات اتصال، ونقل معلومات تساعد على اتخاذ القرارات الاقتصادية.
- ✧ بنية معلوماتية تساعد على تدفق المعلومات بسرعة ودقة بين فروع الاقتصاد، وسلسلة من النظم مترابطة تساعد صانع القرار على اتخاذ القرار الاقتصادي السليم.
- ✧ القوانين والتشريعات التي تلائم مع الاقتصاد الرقمي، بالإضافة الى مناخ عام يضمن حرية وشفافية كاملة في تداول وتدوير المعلومات بلا عوائق.
- ✧ تحديث معلومات المواقع أنيا وتقديم الدعم المستمر المستخدمي الاقتصاد الرقمي.
- ✧ المحافظة على الخصوصية في المعاملات، وذلك لضمان ثقة الاقتصاديين والجمهور والإقبال على الاقتصاد الرقمي.
- ✧ ضمان الحماية ضد غسيل الأموال وتوفير القوانين المالية التي تحقق الأمان في المعاملات.
- ✧ توفير متطلبات الاستثمار الإلكتروني من إعداد البرامج الخاصة بالاستثمار الإلكتروني.
- ✧ تطبيق آليات الحكومة الإلكترونية، وهي قدرة الحكومة على التبادل المعلومات وتقديم الخدمات فيما بينها وبين المواطن وبين قطاع الأعمال بسرعة ودقة عالية وبأقل تكلفة عبر شبكة الإنترنت.
- ✧ تطبيق آليات التجارة الإلكترونية، وهي تشمل على أنشطة إنتاج السلع والخدمات وتوزيعها وتسويقها وبيعها من خلال الوسائط الإلكترونية.

الفرع الثاني: مؤشرات الاقتصاد الرقمي

توجد العديد من مؤشرات الخاصة بالاقتصاد الرقمي، حيث توجد 4 عناصر تحتوي على مجموعة من المؤشرات المطلوبة وهي كما يلي:

أولا: البحث والتطوير وهو يقيس مستوى البحث والتطوير التقني الذي يعكس القدرة

على الابتكار وتطبيق التقنيات الجديدة، ويشمل المؤشرات التالية[1]:

- تصدير التقنية العالية كنسبة من التصدير الصناعي
- عدد العلماء والمهندسين العاملين في مجال البحث والتطوير.
- إجمالي العاملين في البحث والتطوير على المستوى الوطني كنسبة للسكان.
- إجمالي الإنفاق على البحث والتطوير كنسبة من الناتج الوطني الإجمالي
- المتوسط السنوي الأعداد براءات الاختراعات الممنوحة.
- ما يتم إنفاقه على البحث والتطوير من رجال الأعمال للفرد

ثانيا: التعليم والتدريب وبعد المدخل الأساسي للاقتصاد المبني على المعرفة، وهو يركز على الموارد البشرية، ويشمل المؤشرات التالية:

- إجمالي الإنفاق على التعليم لكل فرد
- معدل معرفة القراءة والكتابة.
- نسبة الطالب / المدرس في المرحلة الابتدائية.
- نسبة الطالب / المدرس في المرحلة الثانوية.
- التسجيل في المرحلة الثانوية.
- التسجيل في المرحلة الجامعية.

ثالثا: البنية المعلوماتية وهو عنصر يشمل كل ما يتعلق بالجوانب المتعلقة بنشر المعلومات عبر وسائل الاتصالات والإعلام، ويشمل المؤشرات التالية:

- مقدار الاستثمار في وسائل الاتصالات
- الهواتف العاملة المستخدمة لكل ألف من السكان.
- اشتراكات الهاتف المحمول لكل ألف من السكان.
- التلفونات العاملة لكل ألف من السكان.
- التلفزيون والراديو لكل ألف من السكان
- أجهزة الفاكس لكل ألف من السكان.

[1] مراد علة جاهزية الدول العربية للاندماج في اقتصاد المعرفة دراسة نظرية تحليلية المؤتمر العالمي الثامن للاقتصاد والتمويل الإسلامي النمو المستدام والتنمية الاقتصادية الشاملة من المنظور الإسلامي، كلية الدراسات الإسلامية، الدوحة، قطر 2018 ديسمبر 2011، ص 19.

- تكلفة المكالمة الدولية.

رابعا: البنية الأساسية للحاسوب ويعكس هذا العنصر مدى توافر الحاسوب بوصفه أداة لتقويم القاعدة المعلوماتية، ويشمل المؤشرات التالية:

- نسبة المشاركة الدولية في الحاسوب
- أعداد أجهزة الحاسوب لكل ألف من السكان.
- نسبة المشاركة الدولية في البنية الأساسية للحاسوب بالثانية.
- طاقة الحاسوب لكل فرد.
- أعداد مستخدمي الإنترنت لكل ألف نسمة من السكان.
- مواقع الإنترنت لكل عشرة آلاف نسمة من السكان.

المطلب الرابع: تطبيقات الاقتصاد الرقمي

يشمل الاقتصاد الرقمي مجموعة واسعة من التطبيقات التي تؤثر في مختلف جوانب الحياة الاقتصادية والاجتماعية، أبرزها:

الفرع الأول: التجارة الالكترونية: Electronic Commerce

وهي عبارة عن استخدام الوسائل التكنولوجية وشبكات المعلومات والاتصالات الممارسة أي نشاط تجاري وتشمل وسائل الاتصال التي تعمل كوسيط في عمليات تصميم وإنتاج وإعلان وعرض وتوزيع وبيع السلع والخدمات، وكذلك عمليات الدفع والسداد[1].

وبعد عن التجارة الالكترونية كنشاط اقتصادي رقمي يتم فيه تداول السلع والخدمات على وفق ما متفق عليه من قواعد وأنظمة باستخدام تقنية الانترنت وتكنولوجيا الاتصالات الالكترونية، وتتضمن أعمال تصريف السلع والخدمات وتسديد المدفوعات عن طريق الانترنت[2].

كما يعبر عنها بكل نشاط تجاري يعتمد على تكنولوجيا الأنترنت ويتم من خلاله بيع وشراء السلع والمنتجات الملموسة وغير الملموسة، وتعرف أيضاً بعملية عرض منتج أو

[1] عبد الخالق السيد أحمد، التجارة الالكترونية والعولمة المنظمة العربية للتنمية والإدارة، الطبعة الثانية، القاهرة مصر 2008، ص 32

[2] الموسوي، المرجع السابق، 2017، ص49-50

خدمة وبيعها وتسليمها للمشتري واستلام ثمنها، ومن أمثلتها المتاجر الالكترونية الكبيرة مثل أمازون وإيباي (ebay) ، ويوبير (Uber) وغيرها ، وهي عبارة عن مواقع الكترونية تعرض مجموعة من السلع والخدمات يمكن للمشتري إن يطلب ما يرغب منها باستخدام وسيلة دفع الكترونية ، حيث تتم عملية الشراء ثم يقوم المتجر الالكتروني بتوصيل المنتج إلى عنوان الزيون بالوقت المحدد، وهي عبارة عن تزاوج بين التجارة التقليدية والانترنت، ومن خلال هذه الآلية يمكن لأي شخص لديه حساب رقمي على الفيسبوك ضمن مجموعة أن يبيع سلعة معينة إلى أصدقائه الافتراضيين، ويمكن اعتباره من ضمن العاملين في قطاع التجارة الرقمية[1].

اولا. أهمية التجارة الالكترونية

إن للتجارة الرقمية أهمية بالغة في الاقتصاد العالمي حيث حققت نسبة (80%) من مجموع التبادل التجاري الدولي، وتستطيع التجارة الالكترونية التحكم بمخزون السلع التجارية وتقليل خطورة الخزن واختصار الوقت اللازم لتجهيز الطلابيات، وتسهل وتسرع عمليات تسوية المدفوعات الدولية والمحلية الناجمة عن الصفقات التجارية باستخدام وسائل الدفع الالكترونية، وتوضح التجارة الالكترونية أنواع المنتجات وأسعارها وكمياتها ومنشئها، وكل المعلومات التي يحتاجها البائع والمشتري بأسلوب مباشر وضمن شفافية وكفاءة توفرها تقنية الانترنت بأقل التكاليف في الأسواق المحلية والعالمية، فأصبحت الأسواق مفتوحة ومشتركة غير محددة بزمان ومكان، كما في الأسواق التقليدية[2].

ثانيا. أنواع التجارة الالكترونية

إن أبرز أنواع التجارة الالكترونية تشمل[3]:

- التجارة من المنتج إلى المستهلك (B)to (C) وهي عملية بيع السلعة أو الخدمة من المنتج إلى المستهلك مباشرة عن طريق دخول المستهلك إلى الموقع (المتجر) الالكتروني للشركة أو الجهة البائعة.

[1] Khazragui, h (2011). Export Promotion Of Small And Medium Sized Enterprises In Developing Countries: The Perceived Usefulness Of International Trade Points By Smes In Egypt, Thesis, Manchester: University Of Manchester. P100

[2] الموسوي، المرجع السابق، 2017، ص 51-52

[3] Djan-Ohene,J. (2008). Electronic commerce. London: University of London, P8-9

- التجارة من منتج إلى منتج (B)to(B)) وهي عمليات البيع والشراء التي تحدث ما بين المنتجين كأن تكون بين المصنعين وتجار التجزئة.
- التجارة من مستهلك إلى مستهلك (C)to (C) وهي عملية بيع سلعة يقوم بها مستهلك اشتراها سابقاً وقد انتفت حاجته منها إلى مستهلك آخر يرغب في شرائها، ويحدث ذلك كثيراً في مواقع التواصل بين المستهلكين وخاصة على موقع (فيسبوك).
- التجارة من مستهلك إلى منتج (C)to(B) وهي عملية بيع خدمة أو سلعة رقمية يقوم بها مستهلك إلى شركة أو مشروع، مثل البرمجيات والتصاميم الرقمية.
- . إضافة إلى التجارة بين الشركات والحكومة (B)to (G) وهو حصول الحكومة على السلع والخدمات التي توفرها الشركات الخاصة وبالعكس، والتجارة بين المستهلكين والحكومة (G)to (C) بتوفير الخدمات والسلع من قبل الحكومة للأفراد إلكترونيا بتكاليف قليلة والحصول على بيانات الأفراد وخدماتهم[1].
- . فضلا عن التجارة بين الحكومة وحكومات الدول الأخرى (G)to(G) ، والتجارة من الحكومة إلى الأعمال (G) to (B) وذلك باستخدام الوسائل التكنولوجية انجاز المعاملات وعرض القوانين وإدارة وجمع الضرائب، ومن الحكومة إلى الموظفين (G) to (E).[2]

ثالثا. التسويق الالكتروني

وهو جزء من التجارة الالكترونية يتم من خلاله تحديد احتياجات المستهلكين والترويج للسلع والخدمات في الأسواق الافتراضية عن طريق تكنولوجيا الاتصالات المتطورة وتقنية الانترنت ومحركات البحث الالكترونية فأصبح من خلال التسويق الالكتروني بالإمكان نشر المعلومات عن أي سلعة أو خدمة وبيعها للمستهلكين بغض النظر عن الحدود المكانية والزمانية وبذلك تكون السلع والخدمات معروفة ومتاحة عالميا وبآليات ترويجية قليلة التكلفة وبدون تمييز بين الشركات الكبيرة والشركات الصغيرة التي تتكون في بعض الأحيان من فرد واحد ويمكن أيضاً قياس مدى نجاح الحملات الإعلانية

[1] عبد الخالق السيد احمد التجارة الالكترونية والعولمة المنظمة العربية للتنمية والإدارة، الطبعة الثانية، القاهرة مصر 2008، ص 44.

[2] عليان ريحي مصطفى، اقتصاد المعرفة، دار صفاء للنشر والتوزيع، عمان الأردن 2012، ص 286-288

وتحديد الفئة التي يستهدفها التسويق، كل ذلك بفضل التسويق الرقمي (الالكتروني).[1]

الفرع الثاني: الحوكمة الالكترونية: Electronic Governance

وهي استخدام الوسائل التكنولوجية للاتصالات والمعلومات وتطبيقها على الوظائف العامة المقدمة من قبل المؤسسات الحكومية للأفراد بكفاءة وشفافية وتكون على أكبر قدر من المشاركة للمواطنين وعلى أعلى مستوى من الفعالية، والكفاءة لإنجاز الوظائف الحكومية وتسهيل المعاملات وتقديم الخدمة العامة وفق معايير الجودة ودعم التواصل السريع المتقن بين المكاتب والمؤسسات الحكومية، وتهدف الحوكمة إلى خلق أفضل بيئة لقيام واستمرار المشاريع الربحية وغير الربحية ، وتعزيز الشفافية بين الحكومة والمواطنين وتوسيع المشاركة، وتقليل التكاليف الناجمة عن الإجراءات الورقية وتخفيض النفقات العامة، وزيادة المنافع المتأتية من جمع البيانات وتبويبها وتدقيقها مما يساعد على ضبط التحصيل الضريبي وواردات الحكومة من جهة، والسعي من اجل رفاه المواطنين وجذب الفئات المهمشة من الشعب وإشراكهم في وسائل الحياة المتطورة من جهة أخرى[2].

وهناك فرق بين مصطلح الحوكمة الالكترونية ومصطلح الحكومة الالكترونية

فالحوكمة الالكترونية: هي سلسلة العمليات والإجراءات المحاطة بإطار قانوني والتي تهدف إلى تنظيم المعاملات والمعلومات والمخاطبات والمستندات الرسمية وغير الرسمية بين الحكومة والمواطن وتامين سبل حفظها وأرشفتها ورقمتنها وتوفير آلية لاسترجاعها بالاعتماد على تطبيقات تكنولوجيا المعلومات ووسائل الاتصالات المتطورة ويكون هدفها الأبرز تنظيم الأمور الإدارية، أما الحكومة الالكترونية فهي الخدمات الالكترونية المقدمة من الحكومات لمواطنيها وللأعمال الاقتصادية بالاعتماد على الشبكة العالمية للاتصالات والمعلومات (الانترنت وتهدف إلى تبسيط إجراءات انجاز التعاملات الرسمية بين الحكومة ورعاياها على مستوى الأفراد والمنظمات والمشاريع الاقتصادية بشفافية عالية، بالاعتماد على البوابات الالكترونية التفاعلية وتكون مؤمنه بشكل كامل

[1] الحداد وسيم محمد وآخرون الخدمات المصرفية الالكترونية، الطبعة الأولى، دار المسيرة للنشر والتوزيع، عمان 2012، ص 212-213

[2] الجبوري عدنان جاسم عبد الآثار الاقتصادية لتطبيق الحوكمة في العراق دراسة تحليلية، رسالة الماجستير ، جامعة تكريت 2014، ص 60-61

وتغذى بشكل مستمر بالمعلومات المحدثة ويكون تنظيم الأنشطة الاقتصادية الهدف الأبرز لها.[1]

الفرع الثالث: السياحة الالكترونية : Electronic Tourism

وهي استخدام الوسائل الالكترونية والانترنت في مجالات السفر والسياحة ومساعدة العاملين في قطاع السياحة في التعاملات مع الزبائن، من أجل حصول السائحين على أفضل الخدمات السياحية من خلال عرض الخدمة السياحية التي تشمل البرامج السياحية وحجز الرحلات السياحية وتنظيمها عبر شبكة المعلومات الدولية (الانترنت) بحيث تلتقي هذه العروض السياحية مع رغبات المستهلكين (السائحين) وبالتالي حصول مقدمي الخدمة السياحية على منافع كبيرة من جانب، وإشباع رغبات السائحين من جانب آخر، من خلال توفير المعلومات عن مدى جودة الخدمات السياحية التي توفرها المؤسسات والشركات السياحية عن طريق تقنية الانترنت، مثل مواعيد وحجوزات الطيران ومعلومات الفنادق ومدن الألعاب ومراكز الترفيه ، وأماكن تأجير السيارات ، وغيرها ويتم ذلك من خلال تصفح مواقع شركات السياحة الالكتروني قبل الانطلاق في الرحلة السياحية حيث تختصر الوقت والجهد على السائح، وتكون الخدمة السياحية في ظل السياحة الرقمية، منخفضة التكاليف، ويمكن تطويرها بما يلبي أذواق المستهلكين، ضمن مجال تنافسي في ما بين شركات السياحة الالكترونية، ويكون للسياحة ضمن البيئة الالكترونية تأثير قوي على جذب الاستثمارات الأجنبية.[2]

الفرع الرابع: الصيرفة الالكترونية: Electronic Banking

وهي إجراء العمليات المصرفية وتقديم الخدمات المصرفية باستخدام تكنولوجيا الاتصال وشبكة الاتصالات والمعلومات (الانترنت) وإنجازها للعملاء في أي وقت ومكان بدون المجيء إلى البن، من خلال منافذ ومواقع البنوك الافتراضية (الرقمية) التي يمنح العملاء صلاحية دخولها ضمن إجراءات وشروط محددة وقد أدت ثورة الاتصالات

[1] الزهيري طلال ناظم تكنولوجيا المعلومات، مقالة عن الحكومة الالكترونية والحوكمة الالكترونية العدد 3 لسنة 2016، متاحة على الموقع: drtazzuhairi.blogspot.com

[2] ورداني يوسف محمد، كيفية تنظيم السياحة الالكترونية ومردودها على صناعة السياحة مجلة التراث الثقافي 2008، ص 2-4.

والمعلومات والتجارة الالكترونية، والمنافسة الشديدة بين البنوك من جانب وظهور المؤسسات المالية ومنافستها للبنوك من جانب آخر، ومواكبة البنوك للتطور المستمر لتقديم أفضل الخدمات للعملاء وقيام بعض المؤسسات التجارية بأعمال مصرفية كل هذه العناصر أدت إلى ظهور الصيرفة الالكترونية التي أضحت وسيلة لتدنية تكاليف الخدمات المصرفية ، ولضمان الحصول على الحصة الأكبر في أسواق المال، وتوسيع النشاط ليصبح عابراً للحدود الدولية، وتوفير المعلومات عن الخدمات البنكية، وتسهيل حصول العملاء على الخدمات المصرفية في أي زمان ومكان[1].

الفرع الخامس: الاستثمار الرقمي: Digital Investment

لقد تبنت معظم دول العالم في الآونة الأخيرة تحولات اقتصادية مبنية على استخدام الوسائل العلمية والتكنولوجية في كل القطاعات والأنشطة الاقتصادية، حيث أضحى الاستثمار الرقمي مطبقا في الكثير من النشاطات الاقتصادية عن طريق الاستثمارات المالية عبر شبكة المعلومات والاتصالات العالمية الانترنت) ، حيث رصدت مبالغ ضخمة ليتم استثمارها في أسواق التداول الرقمي عن طريق منصات التبادل في السلع الأولية مثل النفط، وأيضا المعادن مثل الذهب والفضة والألماس وتداول العملات الدولية الكترونيا وتحقيق أرباح مالية طائلة من ذلك، وهذا يعكس فاعلية الاستثمار الرقمي وقوته، وسهولة وصول الناس إليه من خلال تطبيقات بسيطة وفتح حسابات تجريبية وتحويل الأموال الكترونيا عن طريق البنوك الالكترونية في وقت قصير[2].

وتكمن أهمية الاستثمار الرقمي في تفاعل وتواصل شركاء التنمية في المجتمع القطاع العام، مؤسسات المجتمع المدني، القطاع الخاص مما ينعكس إيجاباً على تطوير رأس المال البشري، وتعزيز التنافسية، والتحسين المستمر لمخرجات الاستثمار في مجال الاقتصاد القائم على المعرفة[3].

---

[1] الحداد وسيم محمد وآخرون الخدمات المصرفية الالكترونية، الطبعة الأولى دار المسيرة للنشر والتوزيع عمان 2012، ص 55-57

[2] صلاح محمود أحمد عباد، سلسلة الاقتصاد الاقتصاد الرقمي، دار العلم والإيمان للنشر والتوزيع، تسوق عصر 2020، ص 20

[3] با طويح محمد بابق اعلم الدين، معهد التخطيط العربي، استراتيجيات وسياسات الاستثمار في اقتصاد المعرفة في الدول العربية 2019، ص 8.

ملخص الفصل

يتناول هذا الفصل الإطارين النظري والمفاهيمي لموضوعي الأمن السيبراني والاقتصاد الرقمي، من خلال توضيح المفاهيم الأساسية والعلاقة التكاملية بينهما. فالأمن السيبراني يُعدّ حجر الأساس لحماية الأنظمة والمعلومات الرقمية من المخاطر والتهديدات الإلكترونية، مما يضمن استقرار البيئة الرقمية وثقة المستخدمين. أما الاقتصاد الرقمي فيمثل توجهاً حديثاً يرتكز على استخدام التقنيات الرقمية والذكاء الاصطناعي في مختلف الأنشطة الاقتصادية لتحقيق النمو والابتكار. ويبرز من خلال هذا الفصل أنّ نجاح التحول نحو الاقتصاد الرقمي يعتمد بدرجة كبيرة على فعالية منظومة الأمن السيبراني، لما توفره من حماية للبنية التحتية الرقمية ودعم للاستثمار والحوكمة الإلكترونية.

الفصل الثاني:

آليات تفعيل الأمن السيبراني من أجل حماية الاقتصاد الرقمي في الجزائر

يشهد العالم اليوم ثورة رقمية متسارعة أفرزت تحولات عميقة في بنية الاقتصاد العالمي، حيث أصبح الاقتصاد الرقمي أحد أهم محركات النمو والتنمية. وفي ظل هذا التحول، تبرز الحاجة الملحة إلى تفعيل آليات فعّالة للأمن السيبراني لحماية البنى التحتية الرقمية وضمان استمرارية الأنشطة الاقتصادية في بيئة آمنة ومستقرة. فالاعتماد المتزايد على التقنيات الرقمية في المؤسسات الجزائرية، سواء في مجالات التمويل، التجارة الإلكترونية، أو الخدمات العمومية، يجعلها عرضة لمخاطر الهجمات الإلكترونية وتسريب البيانات. ومن هنا تبرز أهمية وضع استراتيجية وطنية متكاملة للأمن السيبراني تعتمد على التشريعات، القدرات التقنية، التكوين البشري، والتعاون المؤسساتي، بهدف تعزيز الثقة الرقمية وحماية الاقتصاد الوطني من التهديدات السيبرانية المتزايدة.

المبحث الأول: الهيئة الوطنية لتفعيل الامن السيبراني

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

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

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

المطلب الأول: من الناحية القانونية والعملية

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

الفرع الأول: من الناحية القانونية

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

أولا/ الدستور الجزائري: كفل دستور 1996 وكذا التعديل الطارئ عليه 2016 حماية الحقوق الأساسية والحريات الفردية وذلك عن طريق أهم المبادئ الدستورية في مواده المادة 38 الحريات الأساسية وحقوق الإنسان والمواطن مضمونة.

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

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

ثالثا / قانون الإجراءات الجزائية: تتابع الجريمة الإلكترونية بنفس إجراءات تتبع الجريمة التقليدية التفتيش المعاينة، الإستجواب الضبط التسرب الشهادة الخبرة ...)، مع زيادة

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

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

تمديد الإختصاص المحلي لوكيل الجمهورية في الجرائم الإلكترونية في المادة 37 من قانون الإجراءات الجزائية.

وتكمن القوانين التي أقرها المشرع الجزائري للجريمة الإلكترونية:

1-قانون البريد والإتصالات السلكية واللاسلكية: حيث نصت عدة مواد منه فيما يخص المجال السيبراني، المادة 87، والتي نصت على سهولة إجراء التحويلات المالية إلكترونيا، والمادة 84/2 على استعمال حوالات الدفع العادية والإلكترونية أما المادة 127 بخصوص جزاء كل من يفتح أو يخرب بريد

2-قانون التأمينات وقد نص هذا القانون على تنظيم الجريمة الإلكترونية من خلال مؤسسات

3-وهيئات الضمان الإجتماعي، وذلك من عدة نصوص تخص البطاقة الذهبية.

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

الفرع الثاني: من الناحية العملية

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

أولا/ مركز الوقاية من جرائم الإعلام الآلي وجرائم المعلوماتية للدرك الوطني: يعتبر هذا المركز الذي أنشئ سنة 2008 ببئر مراد رايس جهازا يهدف إلى تأثير تأمين منظومة المعلومات الخدمة الأمن العمومي، ويعكف على تحليل معطيات وبيانات الجرائم

[1] يوسف بوغرارة، مرجع سابق، ص 109

المعلوماتية، المرتكبة وكذا تحديد هويه أصحابها سواء كانو أشخاص فرادى أو عصابات أو غيرها[1].

ثانيا / المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني: يعتبر المعهد أحد المشاريع المنجزة في إطار تطوير سلك الدرك الوطني" ببوشاوي"، حيث تم إنشاءه بموجب مرسوم رئاسي 04-133 المؤرخ في 26 جوان 2004، ودخل حيز الخدمة إبتداءا من الفاتح جانفي 2009، أما الفترة الممتدة بين 2004 و 2009 كرست لتكوين المورد البشري واقتناء المعدات العلمية والتقنية الضرورية، ويقوم المعهد بالعديد من المهام التي من شأنها تلبية الطلبات الواردة من السلطة القضائية ضباط الشرطة القضائية والسلطات المؤهلة ، قانونيا خاصة أثناء معالجة القضايا المعقدة[2].

ثالثا/ المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني: إستجابة لمطلب الأمن المعلوماتي ومحاربة التهديدات الأمنية الناجمة عن الجرائم الإلكترونية قامت مصالح الأمن بإنشاء المصلحة المركزية للجريمة الإلكترونية التي عملت على تكييف التشكيل الأمني لمديرية الشرطة القضائية، والتي كانت عبارة عن فصيلة شكلت النواة الأولى لتشكيل أمني خاص لمحاربة الجريمة الإلكترونية وعلى مستوى المديرية العامة للأمن الوطني والتي أنشئت سنة 2011 ليتم بعدها إنشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال بقرار من المدير العام للأمن الوطني وأضيف للهيكل التنظيمي المديرية الشرطة القضائية في جانفي 2015[3].

المطلب الثاني: من الناحية الإدارية والتقنية

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

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

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

لتفادي الوقوع في تداخل الصلاحيات بين مختلف الاجهزة الفاعلة في مسائل الأمن والدفاع الوطني، حرص المشرع الجزائري على وضع ضوابط لاحترام الإطار الإداري المنظم لصلاحيات الهيئات المدنية والعسكرية والتقنية في إدارة الاستراتيجية الجزائرية للأمن السيبراني، ويمكن تقسيم المطلب إلى فرعين أساسيين هما: الفرع الأول: من الناحية الإدارية والفرع الثاني: من الناحية التقنية

الفرع الأول: من الناحية الإدارية

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

- ✧ استغلال المعطيات المتوفرة بطريقة تسمح بمتابعة كل ما يجري في الفضاء السيبراني من نشاطات غير شرعية وبالتالي توجيه القدرات البشرية والمالية للحد من الثغرات.
- ✧ تعزيز التنسيق بين مختلف الفاعلين في الميدان والتشديد على ضرورة التعاون بين القطاعين العام والخاص والمجتمع المدني، من أجل نشر ثقافة المواجهة لكل الممارسات التي تخالف القانون في الفضاء السيبراني وحماية الحقوق والحريات السياسية[1].
- ✧ العمل من أجل خلق إطار مركزي للمعلوماتية على شاكلة وحدة بحث، يتم من خلالها جمع المعطيات والاحصائيات في هذا المجال من أجل التحليل المستمر للتهديدات واقتراح الحلول المناسبة.
- ✧ التنسيق والتعاون بين مختلف الأجهزة الأمنية والمالية والإدارية التي لها علاقة مباشرة بأنشطة تكنولوجيا الاعلام، من اجل تحديد المسؤوليات لفرض مراقبة صارمة بعد حصر المجالات المستهدفة من طرف محترفي الجريمة الالكترونية[1].

[1]– الندوة الافريقية، حوكمة النترنت www.lemaghrebdz.com. CAG، 11 أفريل 2025، 12:07

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

ثانيا / قطاع الدفاع الوطني: أستحدث بتاريخ 2015.06.11، على مستوى دائرة الاستعمال والتحضير لركان الجيش الوطني الشعبي " مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة"، وأوكلت لها مهمة، حماية المنظومات والمنشآت الحيوية للبلاد ضد كل أنواع الجريمة السيبرانية، ومن بين المحاور التي تناولتها الأرضية العملياتية لهذه المصلحة، نذكر ما يلي[2]:

- ✧ – توجيه وتنفيذ وتأطير الأعمال في هذا المجال لا يجب أن يتعدى الإطار الوظيفي أو التنظيمي.
- ✧ تطوير وتعزيز المنظومة القانونية لتفادي التجاوزات أثناء استخدام التكنولوجيا وضمان حماية منظومات الإعلام.
- ✧ إعتماد التكوين التقني والعلمي لنتاج الكفاءات والمهارات القادرة على خلق نظام الدفاع السيبراني في كافة أنشطة المؤسسة العسكرية وبالتالي تفادي الأخطار الإجرامية.
- ✧ غرس ثقافة الإستعمال الكيفي لهذا العنصر الحيوي " تكنولوجيات الإعلام والإتصال من خلال حملات تحسيسية لكافة مستخدمي المؤسسة، بغض النظر عن الرتبة أو الوظيفة.
- ✧ الإعتماد وبطريقة مستمرة على البحث العلمي لتطوير وسائل الدفاع إستجابة للتطورات الحاصلة في مجال التكنولوجيا.
- ✧ فتح مجال التعاون الدولي مع المؤسسات العسكرية الأجنبية، خاصة تلك التي لها رصيد في المجال، لتبادل الخبرات والإستفادة من تجاربهم في هذا المجال.

---

[1]أستاذ شريف بسام واقع الحوكمة الالكترونية في الدول العربية مجلة العلوم الاجتماعية والإنسانية، جامعة الجزائر 3، العدد 06 2016، ص157

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

الفرع الثاني: من الناحية التقنية

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

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

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

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

---

[1] بوكيشة محمد الأمن والدفاع السيبراني أولوية قصوى، مجلة الجيش، وزارة الدفاع الوطني الجزائر، العدد 651، 2017، ص32-37

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

المطلب الثالث: من الناحية العلمية

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

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

المبحث الثاني: الهجمات السيبرانية

تشكل الهجمات السيبرانية تهديدًا متزايدًا في العصر الرقمي، حيث تستهدف الأنظمة والشبكات والمعلومات بهدف السرقة أو التخريب أو الابتزاز. وتؤثر هذه الهجمات بشكل مباشر على الأفراد والمؤسسات والاقتصادات الوطنية، مما يبرز الحاجة الملحة لتعزيز الأمن السيبراني والحماية الرقمية.

[1] الملتقى الدولي، الدفاع السيبراني مكون أساسي للأمن والدفاع الوطني، المنظم من طرف قيادة الاركان للجيش الوطني الشعبي بتاريخ 15-16/ 05/ 2017، وكذلك الندوة الدولية الخدمات الالكترونية والأمن العمومي، المنظمة من طرف قيادة الدرك الوطني، 2017/03/28، في طبعتها الثانية.

المطلب الأول: مفهوم الهجمات السيبرانية

يعتمد مفهوم الهجمات السيبرانية أساسا على اختراق مواقع الدول في العالم أو أنظمتها المعلوماتية المتعلقة بالقطاعات الاستراتيجية كالدفاع والطاقة والاتصالات، وذلك إما عن طريق التجسس عليها أو تعطيل خدمتها أو سرقة معلوماتها .

الفرع الأول: تعريف الهجمات السيبرانية وتمييزها عن المفاهيم المختلفة

من المعلوم أن الاعتماد على التقنيات الذكية والحديثة وتبني نماذج الحكومات والمدن المتطورة، فإنه يصبح أكثر انكشافا وعرضة للهجمات السيبرانية.

أولا: تعريف الهجمات السيبرانية من خلال الأمن القومي

تظهر المستجدات العديدة في مجال التكنولوجيا، بأن الحرب السيبرانية تعد تحديا للمفاهيم السائدة حول الأمن القومي أو برتب إيلاء قضية الدفاع عن البنى التحتية الحيوية للدولة أهمية قصوى، لاسيما في مجالات الطاقة والمياه والحوسبة، والاتصالات والمواصلات والاقتصاد في القطاعيين المدني والأمني، لذلك تجد أن الركائز الثلاث لمفهوم الأمن القومي، تتمثل فيمايلي:

أ – الردع: إن القدرات السيبرانية المتطورة يمكن أي دولة من ردع أعدائها، فقديما كان من السهل تقييم قدرات الدول و إمكاناتها، وقياس قوتها لكن عبر مضي القرون و ازدهار التكنولوجيا و تطورها، تغيرت مصادر القوة، و أشكال الردع، وأصبحت القوة الالكترونية من أهم أدوات الردع التي تستهدفها الدول في التنافس والتصارع مع بعضها بعضا، ومثال ذلك التغطية الإعلامية الواسعة التي حظي بها فيروس ساكنت" الذي استخدم لتخريب أنظمة الكومبيوتر التي تتحكم بمرافق تخصيب اليورانيوم في إيران المنسوب إلى الولايات المتحدة وإسرائيل، والذي شكل قفزة نوعية في كل ما يتعلق بالقدرة الهجومية السيبرانية للدول، و قوتها و نفوذها

ب – الإنذار المبكر: إن القدرات السيبرانية الهائلة للدولة ستمكنها من جمع معلومات كثيرة عن أعدائها، وفي الوقت ذاته ستمنع هؤلاء من الوصول إلى قاعدة بياناتها، وهذا يشكل بالنسبة للدولة إنذارا فعالا بشأن نية أعدائها؛

ج – الحسم: فالدول الرائدة في العالم من حيث قدراتها السيبرانية، تكون متفوقة في المعركة من خلال استخدام أدوات سيبرانية متقدمة بهدف حسم المعركة، فالواضح اليوم أن التفوق السيبراني المتكامل مع قدرات حركية متقدمة، أصبح من شأنه أن يحسم المعارك[1].

ومن هذا المنطلق فإن الهجمات السيبرانية ميدانها الفضاء السيبراني وهي غير محدودة المجال وتكون غامضة الاهداف لأنها تتحرك عبر شبكات المعلومات والاتصالات المتعدية للحدود الدولية فضلا عن اعتمادها على أسلحة الكترونية ذكية ومتطورة تلائم مع عصر المعلومات، أو يتم توجيهها ضد المنشآت الحيوية أو دسها عن طريق عملاء الأجهزة الاستخبارات.

ثانيا: تمييز الهجمات السيبرانية عن المفاهيم المختلفة

تختلف الهجمات السيبرانية عن العديد من المفاهيم الأخرى القريبة منها، سنحاول من خلال هذا العنصر إبداء أوجه التمييز بين المصطلحات المختلفة كالاتي:

1- **التمييز بين الهجمات السيبرانية والجريمة السيبرانية:** بعد الهجوم السيبراني كما ذكرنا سابقا عبارة عن تصرفات إلكترونية تتسبب في قتل أو دمار أو أضرار مادية تقوم بها دولة أو مجموعة مسلحة ضد دولة أخرى، بينما الجريمة السيبرانية تشمل مجالا أوسع بكثير من ذلك أي تتضمن كل النشاطات الالكترونية غير القانونية بما في ذلك استخدام الوسائل المعتمدة على الكومبيوتر[2].

[1] طلال ياسين العيسى و عدي محمد عناب المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر"، مجلة الزرقاء للبحوث والدراسات الإنسانية، كلية الحقوق، جامعة عجلون الوطنية، الأردن، المجلد 19، العدد 01 2019 ، ص 84.

[2] زهراء عماد محمد كلنتر، المسؤولية الدولية الناشئة عن الهجمات السيبرانية مكتبة القانون المقارن 2019 بغداد ، ص 30

إن الحداثة التي تتميز بها الجريمة السيبرانية و اختلاف النظم القانونية و الثقافية بين الدول أدت الى صعوبة وضع نظام لتضييق الجرائم السيبرانية وكذا عدم الاتفاق على تعريف موحد لهذا النمط من الجرائم، وذلك تخوف من حصرها في المجال ضيق[1] .

وقد عرفت بأنها " كل فعل صار بالآخرين عبر استعمال الوسائط الإلكترونية مثل الحواسيب أجهزة الموبايل شبكات الاتصالات الهاتفية شبكات نقل المعلومات شبكة الانترنت أو الاستخدامات غير القانونية للبيانات الحاسوبية أو الالكترونية عموما، ويعرفها آخرون بأنها نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود[2]. إن الجرائم السيبرانية والهجمات السيبرانية يشتركان في البنية التي يحدثان فيها، أي الفضاء السيبراني، إلا أنهما يختلفان من ناحية القانونية، حيث لا يمكن وصف أي اعتداء جريمة سيبرانية في غياب نص قانوني يصفها و يحدد عناصرها، بينما يمكن وصف أي اعتداء أنه هجوم سيبراني و ذلك بمجرد وقوعه خارج الوصف القانوني[3].

ويكمن التباين أيضا من حيث الأشخاص والأهداف، فالجريمة السيبرانية غالبا ما ترتكب من قبل أفراد و توجه ضد مؤسسات مالية أو شركات و حتي أفراد داخل أو خارج إقليم الدولة أما الهجمات السيبرانية فعادة ما ترتكب من قبل دولة أو منظمات حكومية أو غير حكومية ضد دولة أخرى[4].

أما من ناحية الهدف فالجرائم السيبرانية غايتها التعلم والتي يتم استخدام الكمبيوتر والامكانيات المستحدثة لنظم المعلومات على أمل الربح وروح الكسب التي تدفع إلى التعدي على نظم المعلومات بالإضافة إلى الدوافع الشخصية والمؤثرات الخارجية التي قد تكون سببا

---

[1]– اسمهان بعيري، الهجمات السيبرانية وأثرها على تهديد الأمن والسلم الدوليين، مذكرة ماستر، قانون عام معمق، قسم الحقوق كلية الحقوق والعلوم السياسية، جامعة الشاذلي بن جديد، الطارف، 2022 ، ص 20.

[2]وفاء لطفي، الجهود الدولية في مجال مكافحة جرائم الإرهاب السيبراني التجربة الماليزية نموذجا، تاريخ الاطلاع متوفر على الرابط: http://jpsa.journals.ekb.eg/article ، تم الاطلاع بتاريخ 11/أفريل/2025، على 15:55

[3]بلقاسم بن صابر و محمد حيدرة الهجمات السيبرانية ومواجهتها في ضوء القانون الدولي المعاصر"، مجلة حقوق الإنسان والحريات العامة، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس مستغانم العدد 4 جوان 2017، ص90

[4]اسمهان بعيري، المرجع السابق، ص 20

في ارتكاب الجريمة المعلوماتية[1]، خلاف للهجمات السيبرانية التي تهدف إلى المساس بسيادة الدولة وتهديد استقرارها وذلك بزعزعت الأمن القومي والسياسي للدولة، وكذا تحطيم البنى التحتية الكونية للدولة، وتعريض مصالحها للخطر في شتى المجالات[2].

2- التميز بين الهجمات السيبرانية والحرب السيبرانية

يقصد بالحرب السيبرانية أساليب الحرب ووسائلها التي تعتمد على تكنولوجيا المعلومات وتستخدم في سياق نزاع مسلح، أي هي الهجمات والعمليات التي ترتكب ضد أو بواسطة شبكات الحواسيب و أنظمة البيانات بين الدول أو الجماعات المسلحة المنظمة في سياق نزاع مسلح، أو سياسات الردع المتبادل، وتعد الحروب السيبرانية ميدان رابع من ميادين الحروب فهي حروب خفية تقتحم الأنظمة الإلكترونية وتسبق العمل العسكري، وتستهدف الأنظمة العسكرية والبنية التحتية الحيوية للدولة فضلا عن الشبكات الذكية وشبكات المراقبة الإشرافية وحيازة البيانات(SCADA) التي تسمح لها بالعمل والدفاع عن نفسها[3]، إن الحرب السيبرانية و إن كانت تتفق كثيرا مع الهجمات السيبرانية إلا أن ذلك لا يعني عدم وجود ما يميزها عن بعض، فالحرب السيبرانية هي نوع أو جزء من الهجمات السيبرانية التي تحدث أثناء النزاع المسلح، خلافا للهجمات السيبرانية التي تعتبر في النشاط إلكتروني ضار بالدول الأخرى سواء كان وقت السلم أو أثناء النزاع المسلح، كذلك بالنسبة للآثار التي ترتبها الحروب السيبرانية هي عبارة عن آثار مادية " آثار حركية، بينما الهجمات السيبرانية قد ينتج عنها المساس بالأنظمة الرقمية، وذلك لأغراض أمنية وعسكرية أو زعزعت نظام وعمل حكومة دولة ما[4].

3- التمييز بين الهجمات السيبرانية و الإرهاب السيبراني

في ثمانينات القرن العشرين كان أول ظهور لمفهوم الإرهاب السيبراني (cyber Terrorism)، فقد عرفه باري كولين (Barry Collin) بأنه هجمة الكترونية غرضها تهديد

[1]عبد العال الديربي ومحمد صادق إسماعيل الجرائم الالكترونية دراسة قانونية قضائية مقارنة، المركز القومي للإصدارات القانونية القاهرة، 2012، ص 47-48.

[2]سامية صديقي المسؤولية الدولية المترتبة عن الهجوم السيبراني في منظور القانون الدولي، مجلة البحوث القانونية والاقتصادية، جامعة محمد البشير الابراهيمي برج بوعريريج، الجزائر، المجلد 06 ، العدد 01، 2023، ص 822

[3]وفاء لطفي، المرجع السابق، ص 8.

[4]سالم محمد عبود أساسيات الأمن السيبراني، دار الدكتور للعلوم الإدارية و الاقتصادية، بغداد، 2022، ص 64.

الحكومات أو العدوان عليها، سعيا لتحقيق أهداف سياسية أو دينية أو إيديولوجية، وأن الهجمة يجب أن تكون ذات أثر مدمر و تخريب مكافئ للأفعال المادية للإرهاب"، ويعتبر الإرهاب السيبراني حسب الموسوعة السياسية أنه: "استخدام العنف غير القانوني أو التهديد به بأشكاله المختلفة كالاغتيال والتشويه والتعذيب والتخريب بغية تحقيق هدف سياسي معين مثل كسر روح المقاومة والتقيد عند الأفراد،

ونقض المعنويات عند الهيئات والمؤسسات، أو كسبيل للحصول على المعلومات أو مال، وبشكل عام هو استخدام الإكراه الإخضاع طرف مضاد لمشيئة الجهة الإرهابية، والإرهاب السيبراني كما عرفه دروثي دينينغ (Dorothy Denningg على أنه: " الهجوم القائم على مهاجمة الحاسوب، وأن التهديد به يهدف إلى الترويج أو إجبار الحكومات أو المجتمعات لتحقيق أهداف سياسية أو دينية أو عقائدية وينبغي أن يكون الهجوم مدمرا و مخربا لتوليد الخوف شبيها للأفعال المادية للإرهاب"، ويعرف أيضا على أنه: نقطة التقاء الفضاء الالكتروني والإرهاب وهو يشير إلى الهجمات والتهديدات غير القانونية بالهجوم على أجهزة الكومبيوتر و الشبكات والمعلومات المخزنة فيها عندما يتم ذلك لتخويف أو إكراه حكومة أو شعبها لتحقيق أهداف سياسية أو اجتماعية؛ وهو التهديد أو الهجوم غير القانوني بشن هجمات على أجهزة الكومبيوتر و أنظمة المعلومات والبرامج والبيانات، بهدف ترهيب و إكراه الحكومات تحقيقا لمختلف الأهداف[1].

إن الإرهاب الإلكتروني يشير إلى عنصرين أساسين هما: الفضاء الافتراضي (cyber space) والإرهاب (Terrorism)، إضافة إلى ذلك هناك كلمة أخرى تشير إلى الفضاء الإلكتروني وهي العالم الافتراضي (Virtualworld)، والذي يشير إلى التمثيل الرمزي والزائف للمعلومات، إن خطورة الإرهاب الالكتروني تزداد في الدول المتقدمة والتي تؤدي إلى تدمير البنية التحتية بالحاسوب الآلية والشبكات المعلوماتية، وذلك بشن هجوم إرهاب مدمر لإغلاق المواقع الحيوية والحاق الشلل بأنظمة القيادة والسيطرة والاتصالات[2].

4- التمييز بين الجريمة المعلوماتية والجريمة الالكترونية

[1] وفاء لطفي، المرجع السابق، ص 6-7

[2] رقد عيادة الهاشمي، الإرهاب الالكتروني، دار أمجد للنشر والتوزيع، 2019، ص 18

نتيجة ازدياد استخدام شبكة الأنترنيت في كثير من المعاملات الإلكترونية أصبحت مجالا خصبا لكثير من الأفعال الإجرامية والتي أطلق عليها الجريمة الالكترونية (cyber crime) تتميز لها عن الجريمة المعلوماتية، بحيث باشرت الجريمة الإلكترونية في الانتشار مع ظهور مناهج قياس درجات الأمان في أنظمة الكومبيوتر، حيث تم استخدام هذه البرامج لاستقبال المعلومات والتلاعب بأنظمة الكومبيوتر التي تحتوي عليها و ذلك لأغراض غير مشروعة، ولا تتباين الجريمة الالكترونية عن الجريمة المعلوماتية في كثير من الأحوال، باستثناء أنها تتم عن طريق جهازين كومبيوتر أو أكثر متصلين فيما بينهم عبر شبكة الانترنت وإن كانت الثانية تجد مكانها في الفضاء الافتراضي (cyber sace) عبر شبكة الانترنيت[1] والفضاء الافتراضي هو الفضاء السيبراني cyber space الذي يسعى إلى ضم العالم بأسره، ويختلف عن الفضاء الحقيقي وتوجد فيه العديد من المجتمعات الموزعة على نحو غير متساو باستخدام بيئة تقنية الأنترنت في المقام الأول – حيث يستفيد المواطنون و المؤسسات من تكنولوجيا المعلومات والاتصالات في تفاعلاتهم[2].

الفرع الثاني: خصائص الهجمات السيبرانية و أنواعها

تعتبر الهجمات الإلكترونية من الجرائم المستحدثة والسريعة في التغيير والتطور ووليدة ثورة المعلومات الهائلة فهي تتميز بجملة من الخصائص تميزها عن الجرائم العادية التقليدية.

أولا: خصائص الهجمات السيبرانية

تتسم الهجمات السيبرانية بجملة من الخصائص من أهمها:

الهجمات السيبرانية ذات طبيعة تقنية، ومتطورة تعكس التطور الحاصل في مجال البرمجيات والحواسيب والاتصالات التكلفة المتدنية نسبيا، مقارنة مع الميزانيات الضخمة التي تخصص لإنتاج أسلحة تقليدية كالغواصات والمقاتلات المتطورة[3].

---

[1] خالد ممدوح إبراهيم، أمن الجريمة الالكترونية، الدار الجامعية، الإسكندرية، 2008، ص 56

[2] الهجمات السيبرانية الالكترونية والتأمين) تاريخ الاطلاع (2025/05/16) على الساعة: 13:05، متوفر على الموقع https://www.infegypLorg/NewsDetails.aspx ، ص13

[3] بوطلاعة وداد و بوكورو منال المرجع السابق، ص 237

– سرعة التنفيذ هذه الجريمة لا تتطلب الإعداد قبل التنفيذ أو استخدام معدات وبرامج معينة، فيكفي فقط ضغطة واحدة على لوحة المفاتيح، أو أن يتم التنفيذ عبر الهاتف[1].

جريمة مستمرة في معظم أحوالها، كما في حالة التطرف الديني و تغذية المواقع ببعض العقائد الفيديوهات المتطرفة، ما لم يتم ضبط الفاعل والتدخل الفني لإنهاء الجريمة[2].

تتسم بسمات مخصوصة تستهدف معنويات وليست ماديات محسوسة، وتثير في هذا النطاق مشكلات الاعتراف بحماية المال المعلوماتي إن جاز التعبير[3].

الجريمة المعلوماتية جريمة عابرة للحدود، وتتسم غالبا بالطابع الدولي ذلك لأن الطابع العالمي لشبكة الانترنت وما يرتبه من جعل معظم دول العالم في حالة اتصال دائم على الخط (on line)، يسهل ارتكاب الجريمة من دولة إلى دولة أخرى، فهي جريمة عابرة للقارات، وهي من نوع الجرائم التي يتم ارتكابها عبر المسافات حيث لا يتواجد الفاعل على مسرح الجريمة بل يرتكب جريمته عن بعد[4]، وعلاوة على ذلك فهي غير محدودة الأهداف والنتائج، إذ قد تتعدى مخاطرها ميادين القتال التقليدية لتصل بدمارها إلى أكثر المواقع السيادية والحساسة تحصينا وبعدا عن دائرة القتال[5].

- ✧ **صعوبة الإثبات والاكتشاف،** حيث تعتبر جريمة صعبة الإثبات، وأنها لا تترك في الغالب أثرا ماديا ظاهرا يمكن ضبطه، وسهولة محو الدليل أو تدميره في زمن قصير، يضاف إلى ذلك نقص خبرة الشرطة، والنظام العدلي، وعدم كفاية القوانين القائمة، كما أنها جرائم مخفية، لا يمكن أن تلاحظ آثارها، والتخمين بوقوعها؛
- ✧ **جرائم ذات جاذبية،** نظرا لما تمثله سوق الكومبيوتر والانترنت من ثروة كبيرة للمجرمين أو الإجرام المنظم، فقد غدت أكثر جذبا لاستثمار الأموال وغسلها وتوظيف الكثير منها

[1] خالد حسن أحمد لطفي، الإرهاب الالكتروني آفة العصر الحديث والآليات القانونية للمواجهة)، دار الفكر الجامعي، كلية الحقوق الإسكندرية 2019 ، ص 95

[2] منال محمد عباس، الإرهاب الالكتروني والأمن الاجتماعي، دار المعرفة الجامعية، كلية الآداب، جامعة الإسكندرية 2019، ص120

[3] نسرين عبد الحميد نبيه الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف جلال حزي و شركاه 2008، ص132

[4] خالد ممدوح إبراهيم، المرجع السابق، ص 44

[5] – نور أمير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الإنسان، مذكرة ماجستير، الجامعة الافتراضية السورية 2021 ، ص 11.

في تطوير تقنيات وأساليب تمكن من الدخول إلى الشبكات وسرقة المعلومات وبيعها أو سرقة البنوك أو اعتراض العمليات المالية وتحويل مسارها أو استخدام أرقام البطاقات وغيرها[1].

- ✧ **عالمية الجريمة،** نظر الارتباط المجتمع الدولي الكترونيا، فقد أصبح مجتمعنا تخيليا مما أدى إلى إن تكون ساحة المجتمع الدولي بكافة دوله ومجتمعاته مكانا لارتكاب الجريمة من كل مكان، والأمر الذي استدعى أن تكون القوانين ذات صبغة عالمية،
- ✧ **جرائم ناعمة،** بمعنى لا تتطلب عنفا، فنقل بيانات من كمبيوتر إلى آخر أو السطو الالكتروني على أرصدة بنك ما لا يتطلب أي عنف أو تبادل إطلاق نار مع رجال الأمن؛
- ✧ **الفساد الثقافي،** لا يتوقف تأثير الجرائم المتصلة بالكمبيوتر عند الأثر المادي الناجم عنها، وإنما يتعدى ذلك ليهدد نظام القيم والنظام الأخلاقي خاصة في المجتمعات المحافظة والمغلقة[2].
- ✧ **مرتكب الجريمة الالكترونية يكون عادة مخترق ومدرب على كيفية التعامل مع البيانات،** والإنترنت وإرسالها بشكل لا يثير الشبهات في بعض الحالات[3]، إن المجرم المعلوماتي ذو مهارات تقنية عالية والمام بتكنولوجيا النظم المعلوماتية[4].
- ✧ **وقوع الجريمة المعلوماتية أثناء المعالجة الآلية للبيانات،** في أي مرحلة من المراحل الأساسية لتشغيل ضام المعالجة الآلية للبيانات سواء عند مرحلة إدخال البيانات أو أثناء مرحلة إخراج المعلومات[5].
- ✧ **جريمة مستحدثة،** تعد الجريمة الالكترونية من الجرائم المستحدثة، حيث أن التقدم التكنولوجي الذي تحقق خلال السنوات القليلة جعل العالم بمثابة قرية صغيرة، بحيث

[1] خالد حسن أحمد لطفي، المرجع السابق، ص 95.

[2] المرجع نفسه، ص 96-97

[3] منال محمد عباس، المرجع السابق، ص 119

[4] خالد ممدوح إبراهيم، المرجع السابق، ص 47.

[5] خالد ممدوح إبراهيم، المرجع السابق، ص 49-50

يتجاوز هذا التقدم بقدراته وإمكاناته أجهزة الدولة الرقابية، بل أنه أضعف من قدراتها في تطبيق قوانينها بالشكل الذي أصبح يهدد أمنها و أمن مواطنيها[1].

- ✧ **عدم الإبلاغ عن جرائم الانترنت،** وذلك بسبب عدم اكتشاف الفاعل أو الخوف من التشهير، وعليه نجد أن معظم جرائم الانترنت ثم اكتشافها بالمصادفة، وبعد وقت طويل من ارتكابها، والجرائم التي لم تكشف هي أكثر بكثير من تلك التي كشف عنها الستار[2].
- ✧ **تعدد الأوصاف القانونية لمحل الجريمة الالكتروني،** إذ قد يكون محل الجريمة مادي أو معنوي، كما هو الحال بالنسبة للمعلومات، فقد تكون في حالة انتقال أو موجودة في ذاكرة النظام الالكتروني أي أنها في حالة غير مادية، والشكل الآخر أن تكون المعلومات متجسدة في صورة مادية بتخزينها على دعامة الالكترونية، حتى أن المعلومات غير المادية بطبيعتها يمكن أن تخضع لأكثر من نص قانوني[3].

وعليه فالهجوم السيبراني من الافعال الاجرامية خاصة مع التطور التكنولوجي المتسارع، والتي تسمح للمخترقين من الاختراق بسهولة وذلك بإخفاء ومحو الدليل او تدميره في وقت وجيز بمجرد كبسة زر بحيث لا تتمكن سلطات البحث والتحقيق من كشف جرمه واقامة الدليل ضده فهو لا يحتاج الى جهد عضلي بل يعتمد على الذكاء الذهني المحكم والتفكير العلمي المدروس القائم على معرفة تقنية ممتازة للحاسب الآلي والتعامل السليم للشبكة.

ثانيا: أنواع الهجمات السيبرانية

تعددت الهجمات السيبرانية من خلال الغاية منها، إذ تختلف من الغابة في كل هجوم وتختلف باختلاف التي وجدت من أجلها، ولكن عموما يمكن تقسيمها إلى هجمات فعالة وأخرى غير فعالة، وسنتعرض لبعض النماذج منها:

أولا. الهجمات الفعالة

يركز المهاجمون على إيجاد الثغرات الأمنية والأبواب الخلفية لهذه البرامج والنظم ومن بين هذه الهجمات ما يلي:

---

[1] المرجع نفسه، ص 51

[2] خالد حسن أحمد لطفي، المرجع السابق، ص 97

[3] المرجع نفسه، ص 100

1- هجمات الحرمان من الخدمة (DOS)

وتعتبر من أخطر الهجمات، حيث يقوم المهاجم بإطلاق برنامج خبيث يؤدي إلى زيادة قبول البرنامج، وبالتالي يمنع الاستخدام الحقيقي من الوصول إلى الخدمات التي تتوفر عليها البرامج[1] وبمعنى آخر هو إيقاف قدرة الهدف على تقديم الخدمات المعتادة أو المفترض تقديمها، إذا فالهدف الرئيسي من هجمات الحرمان من الخدمة هو إجبار النظام الإلكتروني المستهدف على الاستجابة لعدد معتبر من الطلبات والأوامر الخدماتية بشكل يفوق قدرته، مما يمنعه عن تقديم الخدمات المطلوب منه تقديمها[2].

2- فيروسات الحاسوب

وهي برنامج مثل أي برنامج تطبيق آخر، لكنه مصمم من قبل أحد المخربين لإحداث أكبر قدر ممكن من الضرر للنظام بعد ربطه بالبرامج الأخرى، ولديه القدرة على تكرار نفسه حتى يبدو وكأنه يتوالد ذاتيا، والفيروسات كما حددها التقرير الصادر عن المركز القومي للحاسبات في الولايات المتحدة الأمريكية هي برامج مهاجمة تصيب أنظمة الحاسب بأسلوب يماثل إلى حد كبير الفيروسات الحيوية التي تصيب الإنسان[3]، ويسبب وجود عدد كبير من البرامج التي تقوم بكشف الفيروسات والقضاء عليها، تم تطوير نوع آخر من الفيروسات يسمى بالفيروس متعدد الأشكال (polymophic virus) هذا النوع من الفيروسات يقوم بتغيير نفسه في كل مرة يتم تكراره فيها أو تفعيله ومن يصعب اكتشافه او القضاء عليه[4].

3-أحصنة طروادة

وهو شفرة أو برنامج تغيير مختبئ في برنامج كبير من البرامج ذات الشعبية المالية، وهو مبرمج بمهارة عالية، حيث يقوم بالمهام الخفية مثل: نشر دودة أو فيروس، ومن الصعوبة اكتشافه إذ يعمل دائما على مسح آثاره التي تحمل صنعة تخريبية، ويقوم بإضعاف

[1] سالم محمد عبود، المرجع السابق، ص 91.

[2] نوران شفيق، أثر التهديدات الالكترونية على العلاقات الدولية دراسة في أبعاد الأمن الإلكتروني، المركز العربي للمعارف، القاهرة 2016، ص 21

[3] نور أمير الموصلي، المرجع السابق، ص 17

[4] نوران شفيق، المرجع السابق، ص.26

قوة الدفاع للمستهدف وسهولة اختراق وسرقة بياناته[1]، فضلا عن وجود هذه البرامج الخبيثة القنابل" في عدد من مواقع الأنترنت التي تتضمن مثل هذه البرامج[2].

4-برامج الدودة

تعرف برامج الدودة بالبرامج التي تستفيد من الثغرات الموجودة في نظام تشغيل الكومبيوتر للانتقال من كومبيوتر إلى آخر، مما يؤدي إلى احتلال الشبكة بالكامل والتسبب في نهاية بآثار مدمرة، وبفضل الوصلات التي تربط الشبكات بعضها ببعض، يمكنهم الانتقال من شبكة لأخرى و التكاثر مثل البكتيريا في عملية النقل، ومن أهداف تلك البرامج شغل أكبر قدر ممكن من سعة الشبكة ومن ثم تقليل أو خفض كفاءتها[3]، وهي أيضا برامج قادرة على إعادة إنتاج نفسها، ولكن بعكس الفيروسات فهي برامج قائمة بذاتها بمعنى لا تحتاج إلى مضيف (host) ولا إلى فعل البشر بل تقوم بتفعيل نفسها تلقائيا، ويمكن تكرار نفسها والانتشار إلى جهة أخرى[4].

5-الأبواب الخلفية

وهي ثغرة تترك عن عمد من مصمم النظام للتسلل إليه عند الحاجة، والجدير بالذكر أن الكثير من البرامج والنظم التي تطورها الولايات المتحدة الأمريكية تحتوي على أبواب خلفية تستخدمها عند الحاجة مما يسمح لها بالتجول الحر داخل نظام أي دولة أجنبية[5].

6-الاختناق المروري الالكتروني

ويعني هذا سد وخنق قنوات الاتصال لدى المستهدف بحيث لا يمكنه تبادل المعلومات، أو استبدالها وهي في الطريق بين المرسل والمستقبل بمعلومات مضللة؛

7-القصف الالكتروني

[1]أقوى هجمات سيبرانية استهدفت روسيا، تاريخ الاطلاع (2025/02/24 على الساعة 15:00)، العربية، متوفر على الموقع : http://www.arabic.com

[2]نور أمير الموصلي، المرجع السابق، ص 17

[3]المرجع نفسه، ص 18

[4]نوران شفيق، المرجع السابق، ص 26.

[5]خالد حسن أحمد لطفي، المرجع السابق، ص 65

وهذا يعني الهجوم على شبكة المعلومات عن طريق توجيه مئات الآلاف من الرسائل الالكترونية إلى مواقع هذه الشبكات وبالتالي تسبب ضغط كبير على هذه المواقع، وتفقدها قدرتها على استقبال الرسائل من العملاء، ويؤدي ذلك إلى التوقف عن العمل تماما

8-الهاكرز

وهم أفراد عاديين لديهم قدرات ومهارات عالية في استخدام الكومبيوتر لتحقيق أهدافهم أيا كانت سياسية أو غيره و يرغبوا في اثبات قدرتهم وبالتالي يتم ذلك بطرق غير شرعية، وتتم فيه عملية الاختراق و التدمير[1].

ثانيا: الهجمات الغير فعالة:

وتتمثل فيما يلي:

1-**برامج التجسس:** وهي عبارة عن برامج تثبت خلسة على أجهزة الحاسوب بالتجسس و السيطرة عليها من دون علم المستخدم، وبإمكان هذه البرامج السيطرة على الحاسوب، وتركيب برامج إضافية وإعادة توجيه المواقع الكترونية ضارة والتسبب بمزيد من الفيروسات وتغيير إعدادات الحاسبات وإلحاق الضرر، كما حصل مع الكثير من الشركات العالمية الكبرى، مثل شركة أمازون الأمريكية[2]، وبالتالي هو القيام باختراق شبكة أو جهاز الكتروني، بهدف سرقة المعلومات المخزنة فيه، والتي عادة ما تكون على درجة كبيرة من الأهمية، سواء كانت معلومات عسكرية، أم اقتصادية، أم صناعية، أم تجارية، أم غيرها، و يوصف هذا المستوى بأنه تجاوز الحدود الخصوصية الالكترونية الفردية[3].

[1] المرجع نفسه، ص 66

[2] عبد الحميد بن بادة جريمة التجسس الالكتروني نمط جديد من التهديدات السيبرانية الماسة بأمن دول المنطقة، ورقة بحث قدمت ضمن فعليات الملتقى الدولي الأول الموسم بأمن المعلومات في القضاء السيبراني، المنظم من قبل كلية الحقوق و العلوم السياسية، جامعة غرداية، يومي 17 و 18 فيفري (2020)، ص 9-10

[3] حياة حسين الفضاء الالكتروني وتحديات الأمن العالمي، مجلة العلوم القانونية والسياسية، مخبر الرقمنة والقانون في الجزائر، جامعة البليدة 02 المجلد 12 العدد 01 أفريل 2021، ص 1069

2-التصيد: ويعرف أيضا بالخداع الالكتروني، إذ يخدع المستخدمون ليشاركوا بياناته الشخصية مثل: تفاصيل بطاقات الائتمان وكلمات المرور، مما يسهل وصول المحترفين إلى أجهزتهم، وهي أكثر جرائم الاختراق شيوعا، وتتم عن طريق تقنيات التواصل الاجتماعي مثل رسائل البريد الالكتروني، والرسائل النصية SMS[1].

3-راصد لوحة المفاتيح: وهو أحد أشهر برامج التجسس، ومن أقدم أشكال التهديد السيبراني، يسرق المعلومات الشخصية أو المالية مثل التفاصيل المصرفية إذ يجمع المعلومات ويرسلها إلى طرف ثالث عن طريق برنامج مخفي يرسل عبر الايمايل، حيث سجل هذا البرنامج ضغطات المفاتيح التي يقوم بها المستخدم مثل سرقة كلمات السر، والمعلومات الأخرى المهمة التي تخص الأفراد أو المنظمات أو أرقام بطاقات الائتمان[2].

المطلب الثاني: مخاطر وأبعاد الهجمات السيبرانية

يمثل استخدام شبكة الأنترنت إحدى سمات عصر الفضاء الإلكتروني في العصر الحالي نظرا للمميزات العديدة التي وفرتها تلك التقنية والثورة التكنولوجية على العالم أجمع، ولكن مع هذه المميزات لم يخلو المجتمع من المخاطر الجمة التي ترتبط بكيفية استخدام الأنترنت.

الفرع الأول: مخاطر الهجمات السيبرانية

أولا: المخاطر السياسية والأمنية

1- المخاطر السياسية

من أهم المخاطر السياسية التي تسعى التنظيمات الارهابية إلى تحقيقها من خلال منظومة الإرهاب الالكتروني:

- ✧ تهدد شخصيات سياسية بارزة في المجتمع بالقتل.
- ✧ القيام بتفجير منشآت وطنية، أو بنشر فيروسات من أجل إلحاق الضرر والدمار بالشبكات المعلوماتية والأنظمة الالكترونية.

[1] حياة حسين، المرجع السابق، ص 1069

[2] هاجر ختال الوضع القانوني للحرب السيبرانية على ضوء القانون الدولي، مجلة التواصل في الاقتصاد و الإدارة و القانون، كلية الحقوق و العلوم السياسية، جامعة باجي مختار، عناية المجلد 25 العدد 03 سبتمبر 2019، ص 161

- ✧ اختراق البريد الالكتروني لرؤساء الدول وكبار الشخصيات السياسية وهتك أسرارهم والاطلاع على معلوماتهم وبياناتهم والتجسس عليها لمعرفة مراسلاتهم ومخاطباتهم والاستفادة منها في عملياتهم الإرهابية أو تهديدهم لحملهم على إثبات أفعال معينة يخططون لاقترافها؛

2-المخاطر الأمنية:

من أهم المخاطر الأمنية التي تسعى التنظيمات الإرهابية إلى تحقيقها من خلال منظومة الإرهاب الالكتروني ما يلي:

- ✧ إلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات، أو قطع شبكات الاتصال بين الوحدات والقيادات المركزية، أو تعطيل أنظمة الدفاع الجوي، أو اخراج الصواريخ عن مسارها، مما يهدد أمن الدول.
- ✧ الاختراق الالكتروني إلى الأنظمة الأمنية في دولة ما، وفك الشفرات السرية للتحكم بتشغيل منصات إطلاق الصواريخ الاستراتيجية، والأسلحة الفتاكة، وتعطيل مراكز القيادة والسيطرة العسكرية ووسائل الاتصال للجيوش بهدف عزلها عن قواتها، والنفاذ إلى النظم العسكرية واستخدامها لتوجيه الجنود إلى نقطة غير آمنة قبل قصفها أو تفجيرها[1].

ثانيا: المخاطر الاقتصادية والاجتماعية والثقافية

1- المخاطر الاقتصادية

بظهور العولمة والثورة التكنولوجية أصبح المجتمع يعاني من الكثير من المشكلات الاقتصادية الكبيرة، التي ارتبطت بالتنمية الاقتصادية والتي لها آثار إيجابية وأخرى سلبية، ومن هذه السلبية وجود جيوش جرارة من المتعطلين عن العمل والراغبين فيه من الشباب والمراهقين يسلكون مسلكا غير شرعي مناقض للقانون والعرف السائد في المجتمع، ومن نتائج اللجوء إلى الانترنت الانغماس في عالم الفضاء الالكتروني والحصول على المال بعدة طرق مختلفة كالنصب والاحتيال والسرقات والتلاعب في البورصة، واللجوء بجمع التبرعات الوهمية بقصد القيام بأعمال خيرية وكلها تمثل جرائم اقتصادية قد يقوم بها فرد أو جماعة

[1] خالد حسن أحمد لطفي، المرجع السابق، ص 75

(عصابة)، وكذلك الشراء عبر الانترنت بالبطاقة الائتمانية، ما حول المجتمع إلى استهلاكي لا إنتاجي، وأصبحت القدرة الشرائية تسترق الأموال وتبددها بسلع قد لا يستفاد منها بالطريقة المثلى[1].

ولعل من أهم المخاطر الاقتصادية التي تتحقق من خلال التنظيمات الإرهابية:

- ✧ اختراق النظام المصرفي والحاق الضرر بأعمال البنوك وأسواق المال العالمية .
- ✧ تعطيل عمليات التحويل المالي، مما يلحق الأذى بالاستثمار الأجنبي وبالثقة بالاستثمار عامة، والحاق الأذى بالاقتصادي الوطني[2].

2- المخاطر الاجتماعية والثقافية

رغم التقدم الكبير الذي أحرزته الثورة التكنولوجية و الفضاء الإلكتروني حول العالم في التقارب الزماني و المكاني، وجعلت العالم قرية صغيرة ترتبط بعضها البعض من خلال هذه التكنولوجيا الجديدة إلا أن هناك العديد من المخاطر التي أثرت على العديد من النواحي سواء كانت الاجتماعية أو الثقافية أو الاقتصادية أو البيئية ... الخ، وأصبحت تتجلى بصورة مجسدة تتناول حياة الأفراد وتمس أسلوب معيشتهم مباشرة، فالمخاطر المرتبطة بالمنظومة الثقافية تتضح بوضوح من خلال ما سعت إليه الدول الكبرى من غرس و تحريك الولاء والانتماء لما يسمى بالمجتمع الكوني الجديد، الذي تترابط أطرافه بفضل تكنولوجيا الاتصالات الحديثة، وإلى طمس الهوية الوطنية وسحق الثقافة و الحضارة المحلية وإيجاد حالة من الاغتراب ما بين الانسان وتاريخه الوطني وموروثاته الثقافية والحضارية، والتي تسيطر عليه الثقافة الأمريكية والتي تتباين مع ثقافات كثيرة لاسيما ثقافات الدول النامية، فالعولمة وما جاءت به من ثورة تكنولوجية و معلوماتية بمعناها الثقافي تعني فرض ثقافة الكسي السريع و السهل وتمكين الروح الاستهلاكية لدى الدول الفقيرة، ومن ثم طمس ثقافتها التقليدية و أعرافها و موروثاتها[3].

وعليه تظهر صعوبة في تقييم المخاطر بشكل عام، يرجع ذلك إلى طبيعة الفضاء الالكتروني تضفي عليها صعوبة إضافية لان نقاط الضعف التي يهاجمها الخصم لا يعلمها

[1] منال محمد عباس، المرجع السابق، ص 61-62

[2] خالد حسن أحمد لطفي، المرجع السابق، ص 76

[3] مثال محمد عباس المرجع السابق، ص 58-59.

إلا هو ولا تكون الدولة على علم مسبق بها إلا بعد وقوع الجريمة، وهذا ما يبرر وجوب التدخل التشريعي بسن قانون خاص بالجريمة المعلوماتية.

الفرع الثاني: القانون الواجب التطبيق علي الهجمات السيبرانية

تعد مسألة تحديد القانون الواجب التطبيق على الهجمات السيبرانية من المسائل المهمة، لذا سنحاول تحديد القواعد التي تخضع لها هذه الهجمات.

أولا: خضوع الهجمات السيبرانية لقواعد القانون الدولي التي تحكم العلاقات بين الدول

تأتي في مقدمة هذه القواعد نصوص ميثاق الأمم المتحدة، لاسيما الأحكام المتعلقة بخطر استخدام القوة في العلاقات الدولية، وخطر اللجوء إلى العدوان، وكذا مبدأ احترام سيادة الدولة، واستقلالها السياسي بالإضافة إلى أحكام اتفاقية فينا لقانون المعاهدات لعام 1969، كما تجدر الإشارة إلى أن قواعد دليل تالين الخاصة بالحروب السيبرانية جاءت موافقة لما نص عليه ميثاق الأمم المتحدة فلقد تضمنت المادة الأولى منه مسألة سيادة الدولة بالإضافة إلى أحكام ميثاق الأمم المتحدة فلقد أكدت الجمعية العامة للأمم المتحدة أن حقوق الأشخاص خارج الفضاء السيبراني وداخله يجب أن يحظى بالحماية الكاملة، حيث طلبت الجمعية العامة من المفوضية السامية لحقوق الإنسان إعداد تقرير عن الخصوصية في الحق الرقمي، إذ تناول التقرير حماية الحق في الخصوصية وتعزيز في سياق المراقبة الداخلية والخارجية للاتصالات الرقمية أو اعتراضها وجمع البيانات الشخصية[1].

ثانيا: خضوع الهجمات السيبرانية لمبادئ القانون الدولي الإنساني

تخضع الهجمات السيبرانية التي تنفذ في إطار النزاع المسلح لقواعد القانون الدولي الإنساني، لاسيما القواعد التي تحكم سير العمليات العدائية، وكما جاء في تقرير اللجنة الدولة للصليب الأحمر عام 2011، يجب أن يتوافق توظيف الهجمات السيبرانية في إطار النزاع المسلح مع جميع مبادئ القانون الدولي الإنساني وقواعده، كما هو الحال مع أي سلاح أو وسيلة أو أسلوب حرب آخر جديد أو قديم، وما يؤيد ذلك أنه أشارت إليه محكمة العدل الدولية أن "مبادئ وقواعد القانون الدولي الإنساني المنطبق في النزاع المسلح، تنطبق

[1] اسمهان بعيري، المرجع نفسه، ص 41

على جميع أشكال الحروب وعلى جميع أنواع الأسلحة بما في ذلك تلك المستقبلية"[1]، ولقد استثنت اللجنة الدولية للصليب الأحمر في تقريرها عام 2015 عمليات التجسس من انطباق القانون الدولي الإنساني عليها، ولكنها استدركت على هامش التحرير أنه من الممكن أن يشملها القانون الدولي الإنساني، وذلك للاختراقات التي تنتج عنها الأضرار، حيث أن أغلب العمليات السيبرانية تتم في بدايتها عن طريق التجسس والحصول على البيانات عن طريق اختراقها للأجهزة والحواسيب، أما الاستثناء الثاني فيتعلق بتشويش الاتصالات اللاسلكية والبث التليفزيوني فلم يتم اعتباره من قبل الهجوم الوارد في القانون الدولي الإنساني[2].

ويواجه انطباق القانون الدولي الإنساني على الهجمات السيبرانية تحديات عدة فلا يتضمن القانون الدولي الإنساني على أي قواعد صريحة بشأن الهجمات السيبرانية في السيبراني، والسبب في هذا أنها تكون خطة للهجمات الحركية، أي ليست هجمات مسلحة بالمعنى التقليدي، إلا أنه وبالنظر إلى الهدف الأساسي للقانون الدولي الإنساني المتمثل في حماية المدنيين من ويلات الحرب، يصبح القانون الدولي الإنساني منطبقا وتندرج الهجمات ضمن قواعده إذا كان هدفها تعويض الأشخاص المحميين للخطر[3].

ملخص الفصل

تناول هذا الفصل مختلف الآليات التي تعتمدها الجزائر لتفعيل الأمن السيبراني بهدف حماية الاقتصاد الرقمي وضمان استدامة التحول الرقمي الوطني. حيث تم التركيز على الأطر القانونية والتنظيمية التي أرستها الدولة لمكافحة الجرائم الإلكترونية وتأمين البنى التحتية المعلوماتية، إلى جانب الجهود التقنية المتمثلة في إنشاء مراكز مراقبة وأنظمة إنذار مبكر. كما تمت الإشارة إلى أهمية تطوير الكفاءات البشرية وتعزيز الوعي الأمني الرقمي لدى المستخدمين والمؤسسات، وكذا دعم التعاون بين القطاعات الحكومية والخاصة لتحقيق أمن رقمي شامل. ويخلص الفصل إلى أن تحقيق اقتصاد رقمي قوي وآمن في الجزائر

[1] نور أمير الموصلي، المرجع السابق، ص 44

[2] اسمهان بعيري، المرجع نفسه، ص 40.

[3] نور أمير الموصلي، المرجع السابق، ص 54

يستوجب تكاملاً بين الجوانب التقنية، التشريعية، والمؤسساتية ضمن رؤية استراتيجية وطنية متواصلة.

الخـــاتمة

الخاتمة

يُعدّ الأمن السيبراني اليوم من الركائز الأساسية التي تقوم عليها الدولة الحديثة، إذ يمتد تأثيره ليشمل جميع جوانب الحياة الاقتصادية والاجتماعية والسياسية. فقد أصبح الفضاء الرقمي جزءًا لا يتجزأ من النشاط الاقتصادي، حيث تعتمد المؤسسات المالية، والشركات، والقطاع العام على الأنظمة المعلوماتية لإدارة العمليات وتقديم الخدمات، وهو ما يجعلها عرضة لمجموعة واسعة من الهجمات السيبرانية التي يمكن أن تتسبب بخسائر مالية كبيرة، وتعطيل الخدمات الحيوية، وتقويض الثقة في الاقتصاد الوطني. ومن هذا المنطلق، فإن تعزيز الأمن السيبراني لا يعدّ مسألة تقنية فقط، بل استراتيجية وطنية أساسية لضمان استقرار التنمية الاقتصادية وتحقيق تنافسية مستدامة في السوق العالمية.

النتائج:

1. هناك ارتباط وثيق بين مستوى الأمن السيبراني واستقرار الاقتصاد الوطني، حيث أن ضعف الحماية الرقمية يؤدي إلى تعطيل العمليات الاقتصادية وزيادة المخاطر المالية.
2. الهجمات الإلكترونية أصبحت أكثر تطورًا وتعقيدًا، وتشمل سرقة البيانات، الابتزاز الرقمي، والتجسس الصناعي، مما يستدعي سياسات صارمة ومستمرة للحماية.
3. الاستثمار في البنية التحتية الرقمية وتطوير قدرات المؤسسات والأفراد في مجال الأمن السيبراني يعدّ عاملاً حاسمًا لتحقيق التنمية الاقتصادية المستدامة.
4. الاعتماد على التكنولوجيا الرقمية يضاعف فرص الابتكار والنمو الاقتصادي، شريطة أن يكون مصحوبًا بتدابير فعّالة للحماية الرقمية.

التوصيات:

1. وضع استراتيجية وطنية شاملة للأمن السيبراني تشمل جميع القطاعات الحيوية وتحدد الإجراءات الوقائية والاستجابة للهجمات.

2. تعزيز برامج التوعية والتدريب المستمر للكفاءات الوطنية في مجال الأمن الرقمي، لضمان القدرة على مواجهة التهديدات الحديثة بفعالية.
3. تطوير البنية التحتية الرقمية وتطبيق أحدث التقنيات، مثل الذكاء الاصطناعي والتحليلات المتقدمة، لتعزيز أنظمة الحماية.
4. سن التشريعات والقوانين الرقمية التي تحمي البيانات والمعلومات، وتفرض معايير صارمة على المؤسسات لضمان الالتزام بالأمن السيبراني.
5. تشجيع البحث العلمي والابتكار التكنولوجي في مجال الأمن الرقمي لدعم اقتصاد رقمي آمن ومستدام، قادر على المنافسة عالميًا.

بهذه الخاتمة، يتضح أن الأمن السيبراني ليس مجرد أداة حماية تقنية، بل عنصر أساسي في بناء اقتصاد مستقر وآمن، ودعم التنمية المستدامة، وضمان استمرارية المؤسسات الوطنية في مواجهة التحديات الرقمية المتزايدة.

قائمة المصادر والمراجع

المصادر والمراجع

- **اولا: المصادر**

1. جرائد الرسمية للجمهورية الجزائرية الديمقراطية:

1/ القانون رقم 09 – 04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المنشور بالج ر ج العدد 47 بتاريخ 16 غشت سنة 2009.

2/ القانون رقم 18-04 المؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018، الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الصادر في الج ر ج العدد 27، بتاريخ 13 مايو 2018،

3/ الأمر رقم 15666 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 المتضمن قانون العقوبات المعدل والمتم.

4/ مكرر 7 من القانون 04-15 المؤرخ في 10 نوفمبر 2004، الصادر في الج ر ج رقم: 71 المتضمن تعديل قانون العقوبات لسنة 2004.

5/ المادة 2 من الجريدة الرسمية، عدد 6904، الصادر في 9ذو الحجة 1441 هـ (30 يوليو 2020)، قسم نصوص عامة

- **ثانيا: المراجع**

1. الكتب

1/ نوران شفيق، أثر التهديدات الالكترونية على العلاقات الدولية دراسة في أبعاد الأمن الإلكتروني، المركز العربي للمعارف، القاهرة 2016

2/ الاتحاد الأوروبي للاتصالات دليل الأمن السيبراني للبلدان النامية جنيف الاتحاد الدولي للاتصالات، 2006

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

4/ ايمان صالح عبد الفاتح، التخطيط الاستراتيجي في المنظمات الرقمية، إيبيس كوم للنشر والتوزيع القاهرة، مصر، طبعة الأولى، 2007،
5/ إيهاب خليفة، الحرب السيبرانية الاستعداد لقيادة المعارك العسكرية في الميدان الخامس العربي للنشر والتوزيع، الطبعة الأولى، القاهرة، 2020،
6/ با طويح محمد بابق اعلم الدين، معهد التخطيط العربي، استراتيجيات وسياسات الاستثمار في اقتصاد المعرفة في الدول العربية 2019.
7/ الحداد وسيم محمد وآخرون الخدمات المصرفية الالكترونية، الطبعة الأولى دار المسيرة للنشر والتوزيع عمان 2012،
8/ الحداد وسيم محمد وآخرون، الخدمات المصرفية الالكترونية، الطبعة الأولى، دار المسيرة للنشر والتوزيع، عمان 2012،
9/ خالد حسن أحمد لطفي، الإرهاب الالكتروني آفة العصر الحديث والآليات القانونية للمواجهة)، دار الفكر الجامعي، كلية الحقوق الإسكندرية 2019
10/خالد ممدوح إبراهيم، أمن الجريمة الالكترونية، الدار الجامعية، الإسكندرية، 2008،
11/زهراء عماد محمد كلنتر، المسؤولية الدولية الناشئة عن الهجمات السيبرانية مكتبة القانون المقارن 2019 بغداد
12/سالم محمد عبود أساسيات الأمن السيبراني، دار الدكتور للعلوم الإدارية والاقتصادية، بغداد، 2022.
13/سمير بارة، الدفاع الوطني والسياسات الوطنية للأمن السيبراني في الجزائر الدور والتحديات، جامعة قاصدي مرباح ورقلة،
14/صالح عبد الحميد، العملات الرقمية، طيبة لنشر والتوزيع مصر القاهرة، الطبعة الأولى 2018
15/صحيفة الشعب اليومية الصينية الاقتصاد الرقمي يدفع الانتعاش الاقتصادي العالمي 25/11/2020 متاحة على الموقع الالكتروني
16/صلاح محمود أحمد عباد، سلسلة الاقتصاد الاقتصاد الرقمي، دار العلم والإيمان للنشر والتوزيع، تسوق عصر 2020،

17/ عبد الخالق السيد احمد، التجارة الالكترونية والعولمة المنظمة العربية للتنمية والإدارة، الطبعة الثانية، القاهرة مصر 2008.
18/ عبد الخالق السيد أحمد، التجارة الالكترونية والعولمة المنظمة العربية للتنمية والإدارة، الطبعة الثانية، القاهرة مصر 2008،
19/ عبد العال الديربي ومحمد صادق إسماعيل، الجرائم الالكترونية دراسة قانونية قضائية مقارنة، المركز القومي للإصدارات القانونية القاهرة، 2012.
20/ عليان ربحي مصطفى، اقتصاد المعرفة دار الصفاء النشر والتوزيع، عمان الأردن 2012،
21/ عيادة الهاشمي، الإرهاب الالكتروني، دار أمجد للنشر والتوزيع، 2019،
22/ فارس محمد العمارات الأمن السبيراني مفهوم وتحديات العصر، من الأولى، دار الخليج للنشر والتوزيع الأردن – عمان، 2022
23/ فرح يحي زعاترة، التهديدات السيبرانية علي الأمن القومي الأمريكي، العربي للنشر والتوزيع، مصر،2023
24/ فريد النجار، الاقتصاد الرقمي، الدار الجامعية لنشر والتوزيع، الاسكندرية، مصر، الطبعة الأولى، 2007.
25/ فريد راغب النجار، الاستثمار بالنظم الالكترونية والاقتصاد الرقمي، مؤسسة الشباب الجامعية، الإسكندرية، مصر،2004.
26/ مراد علة، جاهزية الدول العربية للاندماج في اقتصاد المعرفة دراسة نظرية تحليلية المؤتمر العالمي الثامن للاقتصاد والتمويل الإسلامي النمو المستدام والتنمية الاقتصادية الشاملة من المنظور الإسلامي، كلية الدراسات الإسلامية، الدوحة، قطر 2018 ديسمبر 2011.
27/ منال محمد عباس، الإرهاب الالكتروني والأمن الاجتماعي، دار المعرفة الجامعية، كلية الآداب، جامعة الإسكندرية 2019،
28/ منى الأشقر، الأمن السيبري: التحديات ومستلزمات المواجهة، اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني، بيروت 27-28 أغسطس 2012 القاهرة جامعة الدول العربية المركز العربي للبحوث القانونية والقضائية

29/الموسوي صفاء عبد الجبار، كاظم سعد الأعرجي، زينب هادي نعمة الاقتصاد الرقمي الأيام المنشر والتوزيع، عمان الأردن 2016
30/نجم عبود نجم، الإدارة الالكترونية الإستراتيجية، الوظائف والمشكلات دار المريخ، السعودية ،2004.
31/نسرين عبد الحميد نبيه الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف جلال حزي و شركاه 2008،
32/نسيمة سحواذ، الطموح لتوسيع دائرة الاعتماد المتبادل بإدراج طرق تحليلية لفائدة مخابر أخرى www.Dikanews.com ، تاريخ التصفح، 18 ماي 2024، 15:06
33/الهجمات السيبرانية الالكترونية والتأمين، تاريخ الاطلاع (2025/05/16) على الساعة: 13:05، متوفر على الموقع https://www.infegypLorg/NewsDetails.aspx ،
34/وفاء لطفي، الجهود الدولية في مجال مكافحة جرائم الإرهاب السيبراني التجربة الماليزية نموذجا، تاريخ الاطلاع متوفر على الرابط: http://jpsa.journals.ekb.eg/article ، تم الاطلاع بتاريخ 11/أفريل/2025، على 15:55

2. الرسائل الجامعية

- **رسائل دكتوراه:**

1/ بدري فيصل مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة لنيل شهادة دكتوراه علوم تخصص قانون عام. كلية الحقوق، جامعة الجزائر 1 بن يوسف بن خدة 2018
2/ بوكيشة محمد الأمن والدفاع السيبراني أولوية قصوى، مجلة الجيش، وزارة الدفاع الوطني الجزائر، العدد 651، 2017،
3/ التجار اخلاص باقر هاشم، الاقتصاد الرقمي والفجوة الرقمية في الوطن العربي، أطروحة دكتوراه جامعة البصرة 2007،

- **رسائل ماجيستير**

4/ النعيمي يوسف خليل إبراهيم، على انعكاس تكنولوجيا المعلومات والاتصالات في الاقتصاد المعرفي دراسة استطلاعية لشركتي آسيا سيل وزين العراق بمحافظة أربيل، رسالة ماجستير، جامعة تكريت 2015

5/ نور أمير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الإنسان، مذكرة ماجستير، الجامعة الافتراضية السورية 2021 ،

6/ الجبوري عدنان جاسم عبد، الآثار الاقتصادية لتطبيق الحوكمة في العراق دراسة تحليلية، رسالة الماجستير، جامعة تكريت 2014،

- **شهادات الماستر:**

1/ اسمهان بعيري، الهجمات السيبرانية وأثرها على تهديد الأمن والسلم الدوليين، مذكرة ماستر، قانون عام معمق، قسم الحقوق كلية الحقوق والعلوم السياسية، جامعة الشاذلي بن جديد، الطارف، 2022 .

3. مقالات علمية

1/ أبو المعالي محمد عيسى الحاجة إلى تحديث آليات التعاون الدولي في مجال مكافحة الجريمة المعلوماتية، ورقة بحثية مقدمة في إطار المؤتمر العلمي المغاربي الأول حول المعلوماتية والقانون. أكاديمية الدراسات العليا، طرابلس، ليبيا، المنعقد في الفترة من 28 إلى 29 أكتوبر 2009

2/ خالد محمد البراهمه (2017)، التجارة الالكترونية كمدخل لهيكلة الاقتصاد الرقمي، مقالة منشورة عبر الموقع: http://www.academy-news.com/articles.php?action=show&id=597

3/ الزهيري طلال ناظم، تكنولوجيا المعلومات، مقالة عن الحكومة الالكترونية والحوكمة الالكترونية العدد 3 لسنة 2016، متاحة على الموقع: drtazzuhairi.blogspot.com

4/ يوسف نورة عبد الرحمن ، الاقتصاد الرقمي مقالة في جريدة العرب الاقتصادية الدولية الالكترونية ، متاحة على الموقع www.aleqat.com

4. مجلات علمية

1/ وفاء مطروح ابتسام أونيس، تداعيات جائحة كوفيد – 19 وتأثيرها على تحقيق الأمن السيبراني في الجزائر، المجلة الدولية للاتصال، الاجتماعي، المجلد 09، العدد 02،

2/ يوسف بوغرارة ، الأمن السيبراني، الإستراتيجية الجزائرية للأمن والدفاع في القضاء السيبيري، دراسة منشورة مجلة الدراسات الأفريقية وحوض النيل، المركز الديموقراطي العربي، العدد الثالث، 2018،

3/ إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري مجلة مصداقية، كلية الحقوق والعلوم السياسية جامعة العربي التبسي، تبسة الجزائر المجلد 01، العدد 01، 2019،

4/ إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مجلة مصداقية، كلية الحقوق والعلوم السياسية جامعة العربي التبسي، تبسة الجزائر، المجلد 01، العدد 01، 2019

5/ أستاذ شريف بسام واقع الحوكمة الالكترونية في الدول العربية مجلة العلوم الاجتماعية والإنسانية، جامعة الجزائر 3، العدد 06 2016،

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

7/ آمال بوجليدة، "للتوسع حول الاقتصاد الرقمي، الاقتصاد الرقمي التحول من الاقتصاد الصناعي إلى اقتصاد المعلومات"، مجلة الجيش العدد: 630 جانفي 2016

8/ ب – بوعلام، الجيش الوطني الشعبي ورهانات تداول المعلومة عبر شبكات التواصل الاجتماعي، مجلة الجيش، العدد 603، جانفي 2016

9/ بطاهر بختة، توجهات الاقتصاد الرقمي في البلدان العربية في ظل رغبتها في تطبيقه، مجلة منتدى للدراسات والأبحاث العلمية، جامعة زيان عاشور الجلفة الجزائر، العدد 02، 2020

10/ بلقاسم بن صابر و محمد حيدرة الهجمات السيبرانية ومواجهتها في ضوء القانون الدولي المعاصر"، مجلة حقوق الإنسان والحريات العامة، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس مستغانم العدد 4 جوان 2017،
11/ بورابحة سليمة، السياسات العامة الجزائرية في مجال السيبرانية الواقع والتحديات، مجلة دفاتر السياسة والقانون، المجلد 15، العدد 01 2023،
12/ تغريد صفاء مهدي لبني خميس مهدي، أثر السيبرانية في تطور القوة، مجلة حمورابي للدراسات، مركز حمورابي للبحوث، والدراسات الاستراتيجية، العددان 33-34 السنة الثامنة (شتاء ربيع)، 2020
13/ جمال بوازدية الإستراتيجية الجزائرية في مواجهة السيبرانية التحديات والأفاق المستقبلية"، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 01 أفريل 2019
14/ جمال بوازدية، الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية التحديات والافاق المستقبلية، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 01
15/ حياة حسين الفضاء الالكتروني وتحديات الأمن العالمي، مجلة العلوم القانونية والسياسية، مخبر الرقمنة والقانون في الجزائر، جامعة البليدة 02 المجلد 12 العدد 01 أفريل 2021،
16/ حياة حميدي، نسيمة طايلب مدخل مفاهيمي حول الأمن السيبراني، مجلة مدار للدراسات الاتصالية الرقمية، المجلد 02، العدد 02 نوفمبر 2022
17/ راشد محمد المري، الأمن السيبراني وحماية الأنظمة الإلكترونية (دراسة تحليلية تأصيلية)، مجلة الدراسات القانونية والاقتصادية، المجلد 09، العدد 01 مارس 2023
18/ سامية صديقي، المسؤولية الدولية المترتبة عن الهجوم السيبراني في منظور القانون الدولي، مجلة البحوث القانونية والاقتصادية، جامعة محمد البشير الابراهيمي برج بوعريريج، الجزائر، المجلد 06 ، العدد 01، 2023
19/ سعيد بن دنيدة، عامر بوعا كاز، سبل ووسائل حماية المستهلك الالكتروني من مخاطر الاقتصاد الرقمي، مجلة البناء الاقتصادي، جامعة الجلفة الجزائر، العدد 01 2018.

/20 طلال ياسين العيسى و عدي محمد عناب، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر"، مجلة الزرقاء للبحوث والدراسات الإنسانية، كلية الحقوق، جامعة عجلون الوطنية، الأردن، المجلد 19، العدد 01 2019

/21 عبد العزيز بن فهد بن محمد بن داود الجرائم السيبرانية: دراسة تأصيلية مقارنة مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 09، العدد 03، 2020، ص14

/22 علي محمد مدلول الاقتصاد الرقمي رؤى وآفاق دراسة حالة البلدان العربية مجلة جامعة بابل العدد (2) لسنة 2020،

/23 محمد أحمد سليمان عيسى، التعاون الدولي لمواجهة الجرائم الإلكترونية، المجلة الأكاديمية للبحث القانوني، كلية العلوم والدراسات الانسانية بالغاط، جامعة المجمعة، المملكة العربية السعودية، المجلد / 14 العدد 02، 2016

/24 محمد السعيد زناتي الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية، مجلة إيليزا للبحوث والدراسات، المركز الجامعي إيليزي، الجزائر، المجلد 02، العدد 01، ديسمبر 2017

/25 محمد جبار طاهر الشمري (2008)، دور اقتصاد المعرفة في تحقيق النمو الاقتصادي – مصر أنموذجا مجلة الغري للعلوم الاقتصادية المجلد 02، العدد 10، كلية الإدارة والاقتصاد جامعة الكوفة العراق، متاح على الرابط: http://www.uokufa.edu.iq/journals/index.php/ghjec/article/view/1727

/26 محمد مختار، هل يمكن أن تتجنب الدول مخاطر الهجمات الإلكترونية؟"، مجلة اتجاهات الأحداث. العدد 6، يناير 2015

/27 مراد مشوش الجريمة المعلوماتية في ظل قانون العقوبات وقانون الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، مجلة القانون المجلد 09، العدد 01، 2020.

28/ مني عبد الله السمحان، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية جامعة المنصورة، العدد 111 يوليو 2020

29/ هاجر ختال الوضع القانوني للحرب السيبرانية على ضوء القانون الدولي، مجلة التواصل في الاقتصاد و الإدارة و القانون، كلية الحقوق و العلوم السياسية، جامعة باجي مختار، عناية المجلد 25 العدد 03 سبتمبر 2019

30/ ورداني يوسف محمد، كيفية تنظيم السياحة الالكترونية ومردودها على صناعة السياحة مجلة التراث الثقافي 2008،

5. ملتقيات علمية

1/ الملتقى الدولي، الدفاع السيبراني مكون أساسي للأمن والدفاع الوطني، المنظم من طرف قيادة الاركان للجيش الوطني 2017 الشعبي بتاريخ 15-16/ 2017/05، وكذلك الندوة الدولية الخدمات الالكترونية والأمن العمومي، المنظمة من طرف قيادة الدرك الوطني، 2017/03/28، في طبعتها الثانية.

2/ عبد الحميد بن بادة جريمة التجسس الالكتروني نمط جديد من التهديدات السيبرانية الماسة بأمن دول المنطقة، ورقة بحث قدمت ضمن فعليات الملتقى الدولي الأول الموسم بأمن المعلومات في القضاء السيبراني، المنظم من قبل كلية الحقوق و العلوم السياسية، جامعة غرداية، يومي 17 و 18 فيفري (2020)،

3/ متناوي محمد، الاقتصاد الرقمي واشكالية التجارة الالكترونية في الدول العربية، الملتقى الدولي الثاني حول المعرفة في ضل الاقتصاد الرقمي ومساهمتها في تكوين المزايا التنافسية للبلدان العربية، جامعة حسيبة بن بو علي بالشلف، يومي 4-5 ديسمبر 2007.

4/ الندوة الافريقية، حوكمة النترنت www.lemaghrebdz.com. CAG، 11 أفريل 2025، 12:07

5/ الندوة العالمية لمنظمي الاتصالات التوصيلية الشاملة، مستقبل التنظيم، بورت فيلا فانواتو، من 9 إلى 12 تموز 2019.

6.كتب ومجلات باللغة الأجنبية

1/ Agence nationale de la sécurité des systèmes d'information (ANSSI), CyberDico de P'ANSSI (FR/EN), Gouvernement français, 2020, disponible sur:

2/ Bukht, Rumana&Heeks, Richard, Defining, Conceptualising and Measuring the Digital Economy, University of Manchester, Arthur Lewis Building. Manchester M13 9PL, UK, 2017

3/ Djan-Ohene,J. (2008). Electronic commerce. London: University of London

http://arabic.people.com.cn /4

5/ https://www.info.gouv.fr/upload/media/content/0001/11/a5fcaf7ccf1f6058d70e3a17570037569b979d8

6/ Khazragui, h (2011). Export Promotion Of Small And Medium Sized Enterprises In Developing Countries: The Perceived Usefulness Of International Trade Points By Smes In Egypt, Thesis, Manchester: University Of Manchester.

7/ Neittaanmaki Pekka, Lehto Martti, Cyber Security: Analytics, Technology and Automation,

8/ Spnger international Publishing, volume 78, Inteellingent System, control and Automation Science and Enerineering, Switzerland, 2015.

9/ United Nation Conference On Trade And Development(UNCTAD), Digital Economy Report 2019

الفهرس

الفهـــــــــرس

2.شكر وعرفان

3.اهداء

مقدمة .....أ-ت

الفصل الأول: الإطار المفاهيمي للأمن السيبراني والاقتصار الرقمي

المبحث الاول: الامن السيبيراني.....5

المطلب الأول: تعريف الامن السيبيراني 6

الفرع الاول: التعريف اللغوي 6

الفرع الثاني: التعريف الاصطلاحي 7

الفرع الثالث: التعريف القانوني.....9

المطلب الثاني: أهداف وأهمية الأمن السيبيراني 10

الفرع الأول: أهداف السيبيراني 10

الفرع الثاني: أهمية الأمن السيبيراني.....11

المطلب الثالث: أبعاد الامن السيبراني.....12

الفرع الأول: البعد الاقتصادي 13

الفرع الثاني: البعد الاجتماعي.....13

الفهـــــــــرس

الفرع الثالث: البعد القانوني 14

الفرع الرابع: البعد السياسي 15

الفرع الخامس: البعد العسكري 15

المطلب الرابع: التدابير الموضوعية والإجرائية المتبعة لتحقيق الأمن السيبراني وفق التشريع الجزائري 16

الفرع الأول: التدابير الموضوعية والتقنية للأمن السيبراني 16

الفرع الثاني: التعاون الدولي والتدابير الهيكلية والفعالية الأمن السيبراني..... 19

المبحث الثاني: الاقتصاد الرقمي..... 23

المطلب الأول: مفهوم الاقتصاد الرقمي 23

الفرع الأول: تعريف الاقتصاد الرقمي 24

الفرع الثاني: خصائص الاقتصاد الرقمي 25

المطلب الثاني: مكونات وملامح الاقتصاد الرقمي 27

الفرع الأول: مكونات الاقتصاد الرقمي 27

الفرع الثاني: ملامح الاقتصاد الرقمي 31

المطلب الثالث: متطلبات الاقتصاد الرقمي ومؤشراته 33

الفرع الأول: متطلبات الاقتصاد الرقمي 33

الفرع الثاني: مؤشرات الاقتصاد الرقمي 34

المطلب الرابع: تطبيقات الاقتصاد الرقمي 36

الفرع الأول: التجارة الالكترونية: Electronic Commerce..... 36

الفرع الثاني: الحوكمة الالكترونية: Electronic Governance..... 39

الفرع الثالث: السياحة الالكترونية : Electronic Tourism 40

الفرع الرابع: الصيرفة الالكترونية: Electronic Banking..... 40

الفرع الخامس: الاستثمار الرقمي: Digital Investment 41

ملخص الفصل 42

الفصل الثاني: اليات تفعيل الامن السيبراني من اجل حماية الاقتصاد الرقمي في الجزائر

المبحث الأول: الهيئة الوطنية لتفعيل الامن السيبراني 44

المطلب الأول: من الناحية القانونية والعملية 45

الفرع الأول: من الناحية القانونية 45

الفرع الثاني: من الناحية العملية 46

المطلب الثاني: من الناحية الإدارية والتقنية 47

الفرع الأول: من الناحية الإدارية 48

الفرع الثاني: من الناحية التقنية..... 50

الفهـــــــــرس

المطلب الثالث: من الناحية العلمية 51

المبحث الثاني: الهجمات السيبرانية 51

المطلب الأول: مفهوم الهجمات السيبرانية 52

الفرع الأول: تعريف الهجمات السيبرانية وتمييزها عن المفاهيم المختلفة 52

الفرع الثاني: خصائص الهجمات السيبرانية و أنواعها 57

المطلب الثاني: مخاطر وأبعاد الهجمات السيبرانية 64

الفرع الأول: مخاطر الهجمات السيبرانية..... 64

الفرع الثاني: القانون الواجب التطبيق علي الهجمات السيبرانية..... 67

ملخص الفصل 68

الخاتمة 71

المصادر والمراجع 74

ملخص 90

Abstract..... 91

ملخص

تتناول هذه المذكرة العلاقة الجدلية والمعقدة بين متطلبات تعزيز الأمن السيبراني وديناميكيات نمو الاقتصاد الرقمي في السياق الجزائري. ففي ظل التحول الرقمي العالمي المتسارع، تبرز أهمية الاقتصاد الرقمي كرافعة استراتيجية للتنمية المستدامة في الجزائر، إلا أن هذا التوجه يواجه تحديات متزايدة مرتبطة بتصاعد التهديدات السيبرانية. تسعى الدراسة إلى استكشاف كيف يمكن للجزائر الموازنة بين ضرورة تأمين فضائها الرقمي وتحفيز نمو اقتصادها الرقمي الواعد.تنطلق الدراسة من إشكالية محورية تتمثل في فهم طبيعة التفاعل بين الأمن السيبراني ومختلف مكونات الاقتصاد الرقمي الجزائري، وتشخيص التحديات الأمنية النوعية التي تواجه الطموحات الرقمية الوطنية. اعتمدت الدراسة على منهج وصفي تحليلي، مستعينة بتحليل وثائقي معمق للتقارير الرسمية، والأطر القانونية، والأدبيات الأكاديمية ذات الصلة، بالإضافة إلى استقراء البيانات والمؤشرات المتاحة لواقع الاقتصاد الرقمي والأمن السيبراني في الجزائر.

كشفت الدراسة عن وجود جهود معتبرة لتطوير البنية التحتية الرقمية في الجزائر، إلا أنها لا تزال تواجه تحديات تتعلق بجودة الخدمة، والفجوة الرقمية، وتكلفة النفاذ. كما أظهرت نموًا في قطاعات الاقتصاد الرقمي كالتجارة الإلكترونية والتكنولوجيا المالية، لكن بوتيرة تحتاج إلى تسريع، مع وجود عوائق تنظيمية ولوجستية ومتعلقة بالثقة. وعلى صعيد الأمن السيبراني، بينت الدراسة تزايدًا في حجم ونوعية التهديدات التي تستهدف الجزائر، مع وجود استراتيجية وطنية ومؤسسات متخصصة، لكنها تواجه تحديات في بناء القدرات التقنية والبشرية، ونقص الوعي العام، والحاجة إلى إطار قانوني أكثر شمولية وتكاملًا. أكد التحليل على أن ضعف الأمن السيبراني يشكل عائقًا حقيقيًا أمام تبني الخدمات الرقمية ويؤثر سلبًا على ثقة المستهلكين والمستثمرين، مما يتسبب في خسائر اقتصادية مباشرة وغير مباشرة. في المقابل، يُعد الاستثمار في الأمن السيبراني عاملاً ممكّنًا لبناء الثقة وتعزيز المعاملات

ملـــــــــخص

الآمنة وزيادة جاذبية البيئة الرقمية للاستثمار والابتكار. خلصت الدراسة إلى مجموعة من التوصيات الاستراتيجية، أهمها ضرورة تحديث وتفعيل الأطر القانونية والتنظيمية، والاستثمار المكثف في بناء القدرات الوطنية التقنية والبشرية في مجال الأمن السيبراني، وإطلاق حملات توعية وطنية شاملة ومستدامة، وتفعيل الشراكة بين القطاعين العام والخاص، وتعزيز التعاون الدولي لتبادل الخبرات ومواجهة التهديدات العابرة للحدود. كما أوصت بتبني مقاربة استباقية للاستفادة من التكنولوجيات الناشئة كالذكاء الاصطناعي والحوسبة السحابية في تعزيز كل من الاقتصاد الرقمي والأمن السيبراني.

Abstract

This thesis examines the complex and dialectical relationship between the requirements of strengthening cybersecurity and the growth dynamics of the digital economy within the Algerian context. Amidst the accelerating global digital transformation, the digital economy emerges as a strategic lever for sustainable development in Algeria. However, this trajectory faces increasing challenges linked to the rise of cyber threats. The study seeks to explore how Algeria can balance the necessity of securing its digital space with stimulating the growth of its promising digital economy. The research stems from a central problem: understanding the nature of the interaction between cybersecurity and the various components of the Algerian digital economy, and diagnosing the specific security challenges facing the nation's digital ambitions. The study employed a descriptive-analytical methodology, relying on an in-depth documentary analysis of official reports, legal frameworks, and relevant academic literature, in addition to interpreting available data and indicators on the state of the digital economy and cybersecurity in Algeria. The study revealed significant efforts to develop digital infrastructure in Algeria, yet challenges persist regarding service quality, the digital divide, and access costs. Growth was observed in digital economy sectors like e-commerce and fintech, but at a pace needing acceleration, hindered by regulatory, logistical, and trust-related obstacles. On the cybersecurity front, the research indicated an increase in the volume and sophistication of threats targeting Algeria. While a national strategy and specialized institutions exist, challenges remain in building technical and human capacities, addressing low public awareness, and the need for a more comprehensive and integrated legal framework.

The analysis confirmed that weak cybersecurity acts as a genuine barrier to the adoption of digital services, negatively impacting consumer and investor confidence, and causing direct and indirect economic losses. Conversely, investing in cybersecurity is identified as an enabler for building trust, promoting secure transactions, and enhancing the digital environment's attractiveness for investment and innovation. The study concludes with

a set of strategic recommendations, primarily emphasizing the need to update and enforce legal and regulatory frameworks, invest heavily in building national technical and human cybersecurity capacities, launch comprehensive and sustained national awareness campaigns, activate public-private partnerships, and enhance international cooperation for expertise exchange and combating transborder threats. It also recommends proactively leveraging emerging technologies like AI and cloud computing to bolster both the digital economy and cybersecurity. The thesis underscores that achieving sustainable digital development in Algeria requires an integrated approach that considers cybersecurity an intrinsic part of the digital transformation strategy, not merely a separate technical component. Building a strong and prosperous digital economy inevitably involves constructing a secure, trustworthy, and resilient cyberspace.