

كسب رهان الأمن السيبراني ضمان لتعزيز الأمن والدفاع الوطنيين في الجزائر Winning the cyber security bet is a guarantee to strengthen national security and defense in Algeria.

♦ معتوق أم الخير

الملحقة الجامعية قصر الشلالة - جامعة تيارت / الجزائر

مخبر البحث في تشريعات حماية النظام البيئي

oumelkheir.matoug@univ-tiaret.dz

تاريخ النشر: 2024/03/31

تاريخ القبول: 2024/03/14

تاريخ الإرسال: 2024/01/18

الملخص:

نظرا لسرعة التحول الرقمي الذي أصبح يعرفه العالم بأسره اليوم، أصبح العديد من الأشخاص والمؤسسات والمنظمات، أكثر ارتباطا بوسائل التواصل الاجتماعي، مما جعلهم معرضين للتهديدات السيبرانية التي قد تطل خصوصياتهم، ما نتج عنه ظهور نوع جديد من الإجرام ألا وهو الإجرام المعلوماتي، الذي أصبح يلقي بآثاره على الأمن القومي للدول وتهديده خصوصا في حالة عدم تفعيل اليقظة المعلوماتية، لذلك عمدت جل دول العالم على التخطيط من أجل اعتماد استراتيجيات لتحقيق الأمن السيبراني وجعله أولوية لكسب الرهان خصوصا أنه اضحى أمرا جد مهم وذلك بسبب الاعتماد المتزايد على الأنظمة الرقمية ما أدى إلى ازدياد حجم التهديد السيبراني.

والجزائر كغيرها من دول العالم، طالتها في الآونة الأخيرة العديد من الهجمات السيبرانية استهدفت العديد من المواقع الحكومية ومواقع مؤسسات خاصة، نظرا لكون مواقع التواصل الاجتماعي أضحت مجالا خصبا للإجرام المعلوماتي الأمر الذي من شأنه ضرب وتهديد أمن واستقرار الجزائر، وهذا دفع بالدولة الجزائرية إلى جعل تحقيق الأمن السيبراني وتعزيزه ضرورة حتمية لأن الأمر يتعلق بتحقيق منظومة أمنية متكاملة، ولا يكون ذلك إلا بتسليح استراتيجية وطنية متكاملة في المجال الرقمي تجمع بين الاستباقية والوقاية، ونشر ثقافة رقمية لدى كافة المؤسسات لتكون على أهبة الاستعداد للتصدي لكافة التهديدات التي قد تطل الجزائر، وبغية كسب رهان الأمن السيبراني والتجسيد الواقعي لهذه الاستراتيجية قامت باستحداث جملة من التشريعات من نصوص قانونية وتنظيمية تتلاءم وطبيعة هذا النوع من الإجرام للتصدي له وكسب حرب الغد، بالاعتماد على مؤسسات وهيكل عملياتية.

♦ المؤلف المرسل

الكلمات المفتاحية: الأمن السيبراني ، الفضاء السيبراني ، الجريمة السيبرانية ، التهديدات السيبرانية . الحرب السيبرانية .

Abstract:

Given the speed of digital transformation that the entire world now knows social media ", many people, institutions and organizations have become more connected to social media which has made them vulnerable to cyberthreats that may affect their privacy, The emergence of a new type of crime, namely information crime s national security and its threat, especially if information vigilance is not activated, Most of the world's nations have therefore planned to adopt strategies to achieve cybersecurity and make it a priority to win the bet, especially because it has become so important because of the increasing reliance on digital systems, which has led to an increase in the size of the cybersecurity threat.

Algeria, like other countries of the world, has recently been hit by numerous cyberattacks targeting many government sites and private institutions. As social media sites have become a fertile area of information criminality, which could strike and threaten Algeria's security and stability And this prompted the Algerian State to make the achievement and strengthening of cybersecurity imperative because it is about the achievement of an integrated security system, This can only be done by streamlining an integrated national digital strategy that combines proactiveness and prevention and the dissemination of a digital culture to all institutions in order to be ready to address all threats to Algeria; In order to gain the bet of cybersecurity and the realistic expression of this strategy, it has introduced a number of legal and regulatory texts adapted to the nature of this type of crime to address it and win tomorrow's war, using institutions and operational structures.

Keywords: Cybersecurity, cyberspace, cybercrime, cyberspace threats . Cyber war

مقدمة:

شهد العالم في السنوات الماضية الكثير من التطورات المتسارعة في الفضاء السيبراني ،ومازلنا نشهد رقمنة مختلف جوانب الحياة والخدمات وابتكار تكنولوجيات جديدة ومع كل مرحلة تطويرية في قطاع الاتصال وتكنولوجيات المعلومات نشهد كذلك ظهور تحديات جديدة.

دور الأمن السيبراني في مقاومة الدول للتهديدات الكامنة في الفضاء السيبراني (استراتيجية الجزائر نموذجاً)

لذلك أضحت قضية الأمن السيبراني محل اهتمام بشكل متزايد خلال الفترة الماضية لاسيما بعد جائحة كوفيد 19 التي اضطرت العديد من القطاعات إلى اعتماد على تكنولوجيا المعلومات والاتصالات بشكل أكبر من ذي قبل وبدأت تظهر العديد من الأبعاد في هذا السياق ، معظمها ذات طبيعة عابرة للحدود الجغرافية للدول ، كالأخبار المزيفة ، أخلاقيات الفضاء السيبراني والدبلوماسية السيبرانية والسيادة الرقمية ، دلالة على تنامي التحديات والتهديدات في هذا المجال .¹

مما أدى إلى بروز نوع جديد من الإجرام الإلكتروني خصوصا وأنها انتشرت - بسرعة في هذا العصر - ، باستخدام أسلحة تتلاءم ومقتضيات التطورات الجديدة في الميدان الرقمي منها : مواقع التواصل الاجتماعي ، البريد الإلكتروني ، والاعتماد على الخوارزميات في عملية صناعة البرمجيات الخبيثة وبرمجيات التجسس ، وتوظيف تقنيات الحوسبة السحابية ، وتقنيات الذكاء الاصطناعي ، في المساس بالأمن السيبراني للدول ، بذلك بات أمر مواجهتها صعب للغاية لكل دول العالم على حد سواء ، هذا نتيجة عدم تناسب التحولات الرقمية ونوعية وحجم مخاطر هذا النوع من الإجرام .²

لذا وجب اعتماد استراتيجية مبنية على آليات قانونية و أسس تنظيمية وإجرائية من أجل الحد من مخاطر التهديدات السيبرانية ، والعمل على التوعية منها خاصة المؤسسات والأفراد لما لها من نتائج وخيمة تلقي بظلالها على الحياة الخاصة للأفراد ، وأعمالهم .³ مع نشر ركائز الأمن السيبراني من أجل تأمين سلامة الممارسة الإلكترونية .

والجزائر على غرار دول العالم ، تولى أهمية خاصة لتحقيق الأمن السيبراني ، بالنظر إلى بعده الجيوستراتيجي في سياق حروب الجيل الجديد التي أضحت ضمن المخاطر التي تهدد سيادة الدول ، بذلك أصبح موضوع التهديدات في الفضاء السيبراني من أولويات السيد رئيس الجمهورية ، نظرا لمعرفته بأن تحقيق الأمن الوطني بكافة أبعاده لا يتم تحقيقه ، إلا بتحقيق الأمن السيبراني ، لذا وجب تسطير استراتيجية وطنية في المجال الرقمي أساسها الوقاية والاستباقية معا .⁴

¹ -الرؤية العربية للأمن السيبراني (الواقع -التحديات - الفرص) على الرابط الإلكتروني :

https://www.mtc.gov.tn/fileadmin/user_upload/livret_Aicto_Vf.pdf

اطلع عليه بتاريخ 2023/11/06 على الساعة 14:03.

² - أ.م.د. أميرة محمد محمد سيد أحمد ، استراتيجيات مكافحة الجرائم الإلكترونية في العصر المعلوماتي تعزيزا لرؤية مصر 2030 دراسة استشرافية ،

مجلة البحوث الإعلامية ، كلية الإعلام ، جامعة الأزهر ، الجزء الرابع ، العدد الثامن والخمسون ، تاريخ النشر :جويلية 2021 ، ص 1767.

³ - توصيات الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية ، رمز الوثيقة E_ESCWA_TDD_2015_1 منشور في موقع الأمم المتحدة اللجنة الاقتصادية والاجتماعية لغربي آسيا

<https://archive.unescwa.org/ar/publications> اطلع عليه بتاريخ 2023/11/06 على الساعة 14:20.

⁴ - لمزيد من التفصيل ينظر : افتتاحية مجلة الجيش الأمن السيبراني ضمن أولويات القوات المسلحة ، مقال على الرابط الإلكتروني :

<https://www.echoroukonline.com> / اطلع عليه بتاريخ 2023/11/06 على الساعة 16:01

معتوق أم الخير

ترتبط على ذلك فإن الدراسة البحثية في هذا الموضوع تهدف إلى تسليط الضوء على الاستراتيجية التي اعتمدتها الدولة الجزائرية لتعزيز وتحقيق الأمن السيبراني وكسب الرهان ، كونه يعد ضرورة حتمية للتصدي لكافة التهديدات السيبرانية التي قد تطل مؤسسات الدولة وأمنها .

ونظرا لهذه الاعتبارات وأهمية هذا الموضوع ما دفعت لدراسته ومعالجته . هذا ما يدعو إلى طرح الإشكالية التالية التي تتمحور فيما يلي : إلى أي مدى ستساهم الاستراتيجية المعتمدة من قبل الدولة الجزائرية في كسب الحرب الإلكترونية وتحقيق الأمن السيبراني ؟

وللوصول إلى أهداف الدراسة المسطرة والمتوخاة ، وللإجابة عن هذه الإشكالية المطروحة بدراسة قانونية علمية واضحة ، اتبعت منهجا علميا يناسب موضوع الدراسة وهو المنهج الوصفي مع اتباع أسلوب البحث العلمي المنهج التحليلي في بعض العناصر في إطار معالجة هذا الموضوع .

و للإجابة عن هذه الإشكالية سندرسها في مبحثين ، نخصص المبحث الأول : الإطار المفاهيمي للأمن السيبراني والمبحث الثاني الجهود الوطنية لتحقيق الأمن السيبراني.

1- المبحث الأول : الإطار المفاهيمي للأمن السيبراني

أضحى تحقيق الأمن السيبراني ضروري لكافة دول العالم ، خصوصا أنه يحمي من المخاطر المحتملة وقوعها بواسطة المصادر الخارجية في فضاء الأنترنت، كحماية مختلف الحواسيب من أي نوع من الهجمات السيبرانية والتهديدات التي تحدث في هذا الفضاء ، لذلك يؤكد مختصو الأمن السيبراني على ضمان منع الدخول الغير المصرح والوصول إلى المعلومات ، خصوصا أن الأشخاص الذين يمارسون الإجرام الإلكتروني ينشرون ويزرعون الفيروسات الإلكترونية أو يقومون بنسخ المعلومات والبيانات السرية أو تعديلها أو بتحريفها، كما قد يقومون بنشر- معلومات مغلوبة في مواقع مهمة ، ينتج هذا كله نتيجة لضعف الأمن السيبراني ، لذا وجب تقويته .¹

وعلى ضوء ما سبق بيانه ، سنتطرق في هذا المبحث لماهية الأمن السيبراني (المطلب الأول)

و المصطلحات المرتبطة بالأمن السيبراني (المطلب الثاني).

1.1- المطلب الأول : ماهية الأمن السيبراني

لما أوضحت الحرب السيبرانية أهم الوسائل المستحدثة للحروب بين دول العالم ، بعيدا عن الحروب التقليدية ، أصبح تحقيق وتعزيز الأمن السيبراني أمرا ضروريا وسلاحا جديا هام لكسب حرب الغد .²

¹ -د/فارس محمد العمارات ، أ/ إبراهيم محمد الحماسة ، الأمن السيبراني (المفهوم وتحديات العصر) ، الطبعة الأولى ، دار الخليج للنشر والتوزيع ،

عان ، الأردن ، سنة 2022 ، ص 11-12.

² -الأمن السيبراني ، على الرابط الإلكتروني :

دور الأمن السيبراني في مقاومة الدول للتهديدات الكامنة في الفضاء السيبراني (استراتيجية الجزائر نموذجاً)

ويعد مجالاً من مجالات تكنولوجيايات الاعلام والاتصال يدعى بأمن المعلومات حيث يتم من خلاله حماية الأفراد والمؤسسات من التهديدات السيبرانية من اختراق رقمي أو دخول غير مصرح به مما يؤدي بالمساس بالمعلومات والبيانات وخصوصيتها .

الفرع الأول : مفهوم الأمن السيبراني

كلمة "سيبراني" تعني كل ماله علاقة بالفضاء السيبراني (Cyberspace) والشبكة العنكبوتية، وتطبيقات التواصل الاجتماعي، وجل الخدمات في جميع مجالات الحياة على مستوى العالم التي تقوم بتنفيذها (كالتجارة الالكترونية، تحويل الأموال عبر الانترنت).¹

أولاً : تعريف الأمن السيبراني لغة

الأمن السيبراني كلمة مكونة من لفظين الأمن والسيبراني

"الأمن" الأمان والأمانة بمعنى. وقد أُمِنْتُ فأنا أَمِينٌ، وآمَنْتُ غيري تعني الأمان والأمان. والأمنُ عكس الخوف. والأمانةُ عكس الخيانة).²

الأمن لغة هو نقص الخوف، و"أمن" بمعنى حقق الأمان، كما نجد هذا المفهوم في القرآن الكريم، في سورة "قريش" بقوله تعالى "فليعبدوا رب هذا البيت الذي أطعمهم من جوع وآمنهم من خوف".

السيبراني :إن مصطلح السيبرانية يرجعه بعض المؤرخين إلى عالم الرياضيات الأمريكي Wiener Norbert (1894-1964) وذلك للتعبير عن التحكم الآلي، في حين أن كلمة "cyber" اصلها يوناني مشتقة من كلمة "kybernetes" والتي تعني الشخص الذي يدير دفة السفينة ، حيث تستخدم مجازاً للتحكم "governor".³ "أما في الوقت الحالي أصبحت أكثر كلمة تداولاً في قاموس الأمن الدولي .

¹- د/مني عبد الله السمحان ، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود ، مجلة كلية التربية ، جامعة

المنصورة ، مصر ، العدد 111 ، تاريخ النشر : جويلية 2020 ، ص 9.

²- ابن منظور ، مُجَدِّد بن مكرم بن علي ، لسان العرب (الجزء 13) ، الطبعة 3 ، دار صادر ، بيروت ، لبنان ، 1414 هـ ، ص 21. فلا عن: د/ناصر سعيد على محسن الدحياني ، د/أمير عبد الولي مُجَدِّد الصنوي ، متطلبات تطبيق الأمن السيبراني في الجامعات اليمنية من وجهة نظر الخبراء، مجلة الجامعة الوطنية ، اليمن ، العدد 18، تاريخ النشر 2021 ، ص 98.

³- د/مني عبد الله السمحان ، المرجع السابق ، ص 9.

ثانيا : تعريف الأمن السيبراني اصطلاحا

الأمن السيبراني يعرف بأنه حماية للأنظمة المعلوماتية بما يتحقق معه أمن للمعلومات والبيانات ، بناء على إجراءات ، ومقاييس ، ومعايير وجب الالتزام بها ، من أجل مواجهة التهديدات السيبرانية ، والتخفيف من حدتها .¹

كما عرفه فريق العمل المشترك المعني بتعليم الأمن السيبراني في جامعة جورج واشنطن أنه "نظام يشمل جميع الجوانب القانونية والسياسية و العوامل البشرية والأخلاق وإدارة الأعمال حيث أنه يشمل التكنولوجيات والأفراد والأشخاص بالإضافة لإنشاء وتشغيل وتحليل اختبار أنظمة الكمبيوتر الآمنة".²

ثالثا : التعريف الإجرائي للأمن السيبراني

إذا ما تم تعريف الأمن السيبراني إجرائيا فنجد أنه مجموعة تدابير وإجراءات هدفها حماية أجهزة الحاسوب و برمجياته والشبكات والبيانات، وضمان منع الوصول الغير المصرح به إن كان نتيجة إتلاف بيانات أو أجهزة أو أي من الهجمات السيبرانية ، من خلال اعتماد التشفير ، التحكم في الوصول للبيانات والمعلومات بالإضافة إلى اعتماد خطة بغية الاستجابة للحوادث أو استعادتها .³

الفرع الثاني : عناصر الأمن السيبراني

لكي تتحقق أهداف الأمن السيبراني لابد من توافر جملة من العناصر والمحاور التي تعد ضرورية لكي يتم الحفاظ على أمن المعلومات ، من أهمها ما يلي :

أولا : التكنولوجيا التقنية (Technology):

إن للتكنولوجيا والتقنية ، دور جد هام سواء في بالنسبة للأفراد أو المؤسسات ، نظرا لما توفر من حماية أمام التهديدات والهجمات التي تطال الفضاء السيبراني ، خصوصا وأن هذه الحماية تشمل كافة أشكال الأجهزة الذكية والحاسوبية ، والشبكات .

¹ د/أمنة علي البشير نُجْم ، الأمن السيبراني في ضوء مقاصد الشريعة ، مجلة كلية الدراسات الإسلامية والعربية للبنات ، الإسكندرية ، مصر ، المجلد 01، العدد 37 ، بدون تاريخ نشر .

² د/خالد ظاهر عبد الله جابر السهيل المطيري ، دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي ، مجلة البحوث الفقهية والقانونية ، كلية الشريعة والفانون بدمنهور ، مصر ، العدد 38، تاريخ النشر:جويلية 2022 ، ص 994-995.

³ - ميار عادل فتحي عبد الحميد، تقى حامد معوض عبد الحميد ، دور القيادة السياسية الروسية في تعزيز الأمن السيبراني (2012-2023)،المركز الديمقراطي العربي للدراسات الاقتصادية ،الاقتصادية السياسية ، مقال منشور في موقع المركز بتاريخ 2023/6/22 ، على الرابط الإلكتروني : <https://democraticac.de/?p=90695> اطلع عليه بتاريخ : 2023/11/6 على الساعة 15:24.

دور الأمن السيبراني في مقاومة الدول للتهديدات الكامنة في الفضاء السيبراني (استراتيجية الجزائر نموذجاً)

لذا فهي تعد من أدوات الأمان اللازمة لحماية الأنظمة من الهجمات الإلكترونية المحتملة.¹

ثانياً: الأشخاص المنظّمات (People):

من اللازم على مستخدمي البيانات والأنظمة الاعتماد على أساسيات حماية البيانات الرسمية ، مثلاً اعتماد كلمة مرور قوية ، عدم فتح الروابط الخارجية والمرفقات مع البريد الإلكتروني ، مع ضرورة الإبقاء على نسخ للبيانات.²

ثالثاً: الأنشطة والعمليات (Process)

من أجل مواجهة الهجمات السيبرانية بكفاءة، لابد من الاعتماد على الأشخاص والتقنيات للقيام بجملة من العمليات والنشاطات تكون متوافقة وأسس الأمن السيبراني.³

2.1- المطلب الثاني: المصطلحات المرتبطة بالأمن السيبراني

يرتبط الأمن السيبراني بالعديد من المفاهيم ، من أهمها : الفضاء السيبراني ، الجريمة السيبرانية .

الفرع الأول : الفضاء السيبراني

الفضاء السيبراني (Cyberspace) ، هو ذلك العالم المادي والمفاهيمي الذي يشمل الحواسيب وكافة المعلومات والبيانات والبرمجيات التي بداخلها وشبكة الأنترنت ، ظهر هذا نتيجة التطورات الرقمية التي يعرفها العالم.⁴

أولاً : تعريف الفضاء السيبراني

إن أول من استخدم كلمة cyber مقترنة بكلمة space ، هو وليام جيبسون Gibson William لتظهر في مصطلح الفضاء السيبراني space cyber في كتابه الكلاسيكي عام 1984 ، وقد جاء استخدام

¹ /أمنة مُحمّد منصور ، تأثير الأمن السيبراني على الرقابة الداخلية وانعكاسها على الوحدة الاقتصادية (دراسة استطلاعية لأراء المدققين والمحاسبين في وزارة التعليم العالي والبحث العلمي) ، مجلة الإدارة والاقتصاد ، الجامعة المستنصرية ، بغداد ، العراق ، العدد 127 ، تاريخ النشر : مارس 2021 ، ص 226.

² - د/فارس مُحمّد العمارات ، أ/ إبراهيم مُحمّد الحمامصة ، الأمن السيبراني (المفهوم وتحديات العصر) ، المرجع السابق ، ص 36.

³ - د/سارة مُحمّد رويحي فتحي غزال ، المرجع السابق ، ص 581.

⁴ - علاء الدين فرحات ، الفضاء السيبراني تشكيل ساحة المعركة في القرن الحادي والعشرين ، مجلة العلوم القانونية والسياسية ، جامعة الوادي ، الجزائر ، المجلد 10 ، العدد 03 ، تاريخ النشر : 2019/12/28 ، ص 90.

معتوق أم الخير

الفضاء السيبراني كنمط من استخدام القوة عن طريق التأثير على عمل مصادر المعلومات وأنظمة الاتصالات عن طريق الهجوم السيبراني بما يؤدي ذلك إلى إرباك عمل البنية التحتية الحيوية.¹

عرفه (فريدريك مايور) أنه بيئة انسانية وتكنولوجية جديدة للتعبير والمعلومات والتبادل، فهو يتكون بالأساس من الأشخاص الذين ينتمون لكل الأقطار واللغات والأعمار والمهن التي ترتبط مع بعضها البعض عن طريق البنية التحتية الاتصالية التي تسمح بتبادل المعلومات ونقلها بطريقة رقمية، وعليه تستخدم كلمة Cyber مقترنة بكلمة Space لكي تشير إلى أشهر تعبير في عصر المعلومات، حيث أصبح مفهومها أشمل وأوسع من الأنترنت ليضم كل الاتصالات والشبكات وقواعد البيانات، ويشير كذلك لمجموعة المعلومات المتوفرة إلكترونية ويتم تبادلها وتشكيلها في مجموعات بناء على استخدامها.²

ثانيا : خصائص الفضاء السيبراني

يعتمد الفضاء السيبراني كجال افتراضي على نظم الكمبيوتر وشبكات الأنترنت ومخزون هائل من البيانات والمعلومات، بحيث يتم الاتصال بالشبكات غير الحواسيب أو الهواتف أو غيرها من دون تقييد بالحدود الجغرافية.³

ومن أبرز خصائصه انه أصبح ممكنا للتهديدات الإجرامية اللامتناهية من هجمات إلكترونية، وملاذبا للمتطرفين والإرهابيين، ومجالا حيويا لتنفيذ سياسات التجسس الإلكتروني وإلحاق الضرر بالغير في صورة الحروب السيبرانية، وذلك راجع أساسا إلى غياب سلطة عليا تتحكم فيه وآليات تسمح بحصر مجال الخطر الناتج عنه سواء من الناحية القانونية أو المؤسسية الآلية.⁴

الفرع الثاني : الجريمة السيبرانية

يشار إلى إساءة استخدام تكنولوجيا المعلومات والاتصالات من قبل المجرمين بالتبادل على أنها جرائم الإنترنت، أو إساءة استخدام الكمبيوتر، والجريمة المرتبطة بالحاسب الآلي، جريمة التكنولوجيا العالية، والجريمة الإلكترونية.⁵

¹ -/تفريد صفاء، أ د/لبنى خميس مهدي، أثر السيبرانية في تطور القوة، مجلة حمورابي، مركز حمورابي للبحوث والدراسات الاستراتيجية، العراق، العدد 33-34، تاريخ النشر سنة 2020.

² -/قاسمي صافية، الفضاء السيبراني والأغور الإلكترونية (إشكالية خلق فضاء عمومي افتراضي حسب المنظور الهابرماسي، مجلة الحكمة للدراسات الفلسفية، مؤسسة كنوز الحكمة للنشر والتوزيع، الجزائر، العدد 7، تاريخ النشر، جوان 2016، ص 66-67.

³ -د/نورة شلوش، القرصنة الإلكترونية في الفضاء السيبراني (التهديد المتصاعد لأمن الدول)، مجلة مركز بابل للدراسات الإنسانية، جامعة بابل، العراق، المجلد 8، العدد 2، تاريخ النشر: سنة 2018، ص 190.

⁴ -/أريبي حسين، أ/وسمر نمج، الحروب السيبرانية المخاطر واستراتيجيات تحقيق الأمن السيبراني الدولي والناخلي، المجلة الجزائرية للأمن الإنساني، جامعة باتنة 1 الحاج لخضر، الجزائر، المجلد 7، العدد 2، تاريخ النشر: جويلية 2022، ص 175.

⁵ -د/بارة سمير، الأمن السيبراني (Cyber Security) في الجزائر السياسات والمؤسسات، المجلة الجزائرية للأمن الإنساني، جامعة باتنة 1 الحاج لخضر، الجزائر، المجلد 2، العدد 2، تاريخ النشر: 2017/7/1، ص 259.

دور الأمن السيبراني في مقاومة الدول للتهديدات الكامنة في الفضاء السيبراني (استراتيجية الجزائر نموذجاً)

أولاً : تعريف الجريمة السيبرانية

الجريمة السيبرانية هي نوع جديد من الجرائم يعتمد على ضرورة المعرفة التامة والخاصة بتقنيات الحاسب الآلي لارتكابها أو التحقيق فيها ومقاضاة فاعليها ، فهي تصرفات غير قانونية يقوم بها المجرم في شبكة الانترنت أو أجهزة إلكترونية¹.

كما عرفها آخرون بأنها "هي التي تتم بواسطة الكمبيوتر أو أحد وسائل التقنية الحديثة على كمبيوتر آخر أو أحد وسائل التقنية الحديثة ، مع ضرورة توفر شبكة اتصال فيما بينهما ."

وتعرف كذلك بأنها : "ذلك السلوك الإجرامي الذي يعتمد فيه تقنية الحاسب الآلي مباشرة أو غير مباشرة كوسيلة أو هدف قصد تنفيذ الفعل الإجرامي المقصود ."²

ثانياً : خصائص الجريمة السيبرانية

تتسم الجريمة السيبرانية بجملة من الخصائص والمميزات تميزها عن الجرائم التقليدية حيث تمتاز بسهولة الوقوع في فخها، حيث إنّ غياب الرقابة الأمنية تساهم في انتشارها وتسهيل ذلك ، كما أن الضرر الناجم من الجريمة الإلكترونية غير قابل للقياس، لأنها تلحق أضراراً جسيمة.

ومن خصائص الجريمة السيبرانية (الإلكترونية) :

1. عدم القدرة على الكشف عن مرتكب الجريمة إلا بأساليب أمنية وتقنية عالية .
2. سلوك خارج عن المألوف وغير أخلاقي مجتمعي. ذات عنف ومهدد أقل من الجرائم التقليدية .
3. جريمة غير مقيدة بزمان ومكان، إذ تمتاز بالتباعد الجغرافي وعدم تقيدها بالتوقيت الزمن.³
4. فسرعة ارتكاب الجريمة قد تكون خلال جزء من الثانية ، وقد لا تتطلب الإعداد قبل التنفيذ .
5. يمكن للجاني تنفيذ جرمته وهو في دولة بعيدة كل البعد عن المجني عليه.
6. جرائم لا تعرف الحدود الجغرافية للدول ، نظراً لارتباط العالم بشبكة واحدة ، وهذا قد يسبب إشكاليات لدى الاختصاص القضائي من حيث التحقيق والمحاكمة ، وذلك تبعاً لتعقيد الإجراءات التي تحكمها الاتفاقيات والمعاهدات والعلاقات الدولية ، والتنازع فيما بينها على أي القانون الواجب التطبيق.

¹ د/هاني مُنجد خليل إبراهيم العزاري ، النظام القانوني الدولي لمكافحة المخاطر السيبرانية ، مجلة مصر المعاصرة ، الجمعية المصرية للاقتصاد السياسي، مصر ، العدد 549 ، تاريخ النشر :يناير 2023 ، ص 473.

² روان بنت عطية الله الصحفي ، الجرائم السيبرانية ، المجلة الإلكترونية الشاملة متعددة التخصصات ، الأردن ، العدد 24، تاريخ النشر :ماي 2020، ص 8.

³ د/عبد السلام مُنجد المايل، د/عادل مُنجد الشرجي ، د/ علي قابوسة ، الجريمة الإلكترونية في الفضاء الإلكتروني (المفهوم - الأسباب - سبل المكافحة مع التعرض لحالة ليبيا)، مجلة آفاق للبحوث والدراسات ، المركز الجامعي إليزي، الجزائر ، العدد 4 ، تاريخ النشر : 2019/6/4 ، ص 250-251.

7. جرائم صعبة الإثبات .
8. جرائم لا تمارس بالعنف ، و لا تحتاج إلى أدنى مجهود عضلي ، بعكس بعض الجرائم التقليدية.¹

المبحث الثاني : الجهود الوطنية لتحقيق الأمن السيبراني.

بالرجوع لواقع الأمن الدولي ، نجد ارتفاعا في الجهود المبذولة لتحقيق الأمن السيبراني من خلال تبني جل الفاعلين من الدول أو المؤسسات أو الأفراد لأنجع الطرق بغية الوصول للأهداف المرجوة من الأمن السيبراني خصوصا أن العالم الآن أصبح يشهد تزايدا مستمرا في حجم التهديدات التي تطل الفضاء السيبراني بكافة أنواعها وهذا نتيجة للتحويلات السريعة في الميدان الرقمي.²

نظرا لحجم التحديات والتهديدات التي أصبحت تواجه الجزائر في فضاءها السيبراني ، خصوصا من الهجمات السيبرانية، أضحي بذلك تحقيق الأمن السيبراني من صميم أولوياتها، حيث قامت بتسخير كافة الوسائل المتاحة لها من أجل مجابهة هذه الحرب من أجل حماية نفسها ،من خلال الوقاية أو اعتماد عمليات استباقية لوقف هذه الهجمات ما يتحقق معه حماية المنظومات المعلوماتية والمعطيات.³

وعلى ضوء ما سبق بيانه ، سنتطرق في هذا المبحث للآليات القانونية لتعزيز الأمن السيبراني

(المطلب الأول) و الآليات المؤسسية لتعزيز الأمن السيبراني (المطلب الثاني).

1.2- المطلب الأول :الآليات القانونية لتعزيز الأمن السيبراني

يعتبر الأمن السيبراني عنصرا مستحدثا في أجندة تحقيق الأمن العالمي بما يحقق معه الأمن القومي للدول، لأنه يحمي الدول والمؤسسات والأشخاص ، من الاستعمال السيئ لشبكات الكمبيوتر لأهداف الإرهاب ، الحروب ، التجسس الاقتصادي .نظرا للتحول الذي عرفه مفهوم القوة والانتقال من القوة الذكية والسيبرانية ، بذلك أصبح الفضاء السيبراني مجالا خصبا للصراعات الدولية والإجرام ، كما كانت جائحة كوفيد 19 تحديا للأمن السيبراني نظرا لأنها أدت إلى تسارع التحول الرقمي .⁴ ، وهذا يعد تحديا حقيقيا للأمن السيبراني .¹

¹ - روان بنت عطية الله الصحفي ،المرجع السابق ، ص 12.

2 -د/محمد الكويتي ،الأمن السيبراني في 2023: تحولات وتحديات عصر الذكاء الاصطناعي ، على الرابط الإلكتروني :

<http://trendsresearch.org/research.php?id=17:12> اطلع عليه بتاريخ 2023/11/8 على الساعة 17:12.

³ -لمزيد من التفصيل ينظر : كلمة السيد رئيس الجمهورية عبد المجيد تبون في إطار ملتقى وطني الاستراتيجية الوطنية للأمن السيبراني من أجل جزائر صامدة سيبرانيا . على الرابط الإلكتروني :

<https://www.aps.dz/ar/algerie> اطلع عليه بتاريخ : 2023/11/8 على الساعة 17:42.

⁴ - وكالة الأمن العام للأمم المتحدة والممثل السامي لشؤون نزع السلاح السيدة إيزومي ناكاميتسو حذرت قبل أيام من الزيادة الكبيرة في الجرائم السيبرانية منذ تفشي وباء كورونا. وقالت أن الوباء الحالي وزيادة الاعتماد الرقمي أديا إلى زيادة نسبتها نحو 600 في المئة في رسائل البريد الإلكتروني الخبيثة، مشيرة إلى أن هجوماً إلكترونياً يقع كل 39 ثانية. وطالبت ناكاميتسو دول العالم بمزيد من الابتكار التكنولوجي والتعاون عبر الشبكة

دور الأمن السيبراني في مقاومة الدول للتهديدات الكامنة في الفضاء السيبراني (استراتيجية الجزائر نموذجا)

هذا ما يدعو إلى ضرورة مضاعفة الجهود على كافة الأصعدة من أجل مواجهة هذه التحديات وكذا الحد من المخاطر الإلكترونية .

وباعتبار الجزائر كغيرها من الدول التي أصبحت تتعرض لعدد من الهجمات السيبرانية الأمر الذي من شأنه المساس بالعناصر الحيوية للدولة ،وجب عليها الاعتماد على استراتيجية أساسها تحقيق سياسة أمنية وطنية ، تضمنها آليات وميكانيزمات من أجل كسب الحرب السيبرانية سواء بالوقاية أو بالردع خصوصا وأن الجزائر الآن لها من الإطارات البشرية والوسائل المادية التي من خلالها يتحقق الأمن السيبراني².

الأمر الذي دفع بالدولة الجزائرية إلى تكثيف جهودها بالكامل لمكافحة الإجرام السيبراني حيث سنت ترسانة تشريعية لتأطير كل ما هو مرتبط بتكنولوجيات المعلومات وتعزيز الأمن السيبراني .

الفرع الأول : مكافحة الجرائم الإلكترونية في القواعد العامة

بغية التصدي للإجرام المعلوماتي وما ينتج عنه من نتائج ضارة على الأفراد وعلى مؤسسات الدولة من جهة، ومحاولة منه للتدراك الفراغ التشريعي القائم في هذا المجال من جهة أخرى، عمد المشرع الجزائري منذ الألفية الثانية إلى تعديل العديد من القوانين الوطنية بما فيها التشريعات العقابية على رأسها قانون العقوبات لجعلها تتجاوب مع التطورات الإجرامية في مجال تكنولوجيات الإعلام و الاتصال، كما استحدث قوانين أخرى خاصة لضمان الحماية الجنائية للمعاملات الإلكترونية³.

حيث تجدر الإشارة على أن المشرع الجزائري، قد وضع النصوص التي تعاقب على الأفعال التي تشكل جرائم معلوماتية وكان ذلك سنة 2001، المادة 144 مكرر، ومكرر 1، ومكرر 2، والمادة 146 من قانون العقوبات ثم أصدر نصا تشريعيا سنة 2004، يشمل سبعة مواد "المادة 394 مكرر إلى غاية المادة 394 مكرر 7، من

الإلكترونية، لا سيما في ظل وجود تقارير عن هجمات يتم شنّها تستهدف أنظمة الرعاية الصحية ومرافق البحوث الطبية في دول عدة حول العالم. مقال بعنوان : أين العرب من الأمن السيبراني ، على الرابط الإلكتروني :

<https://www.independentarabia.com/node/1759> اطلع عليه بتاريخ 2023/11/8 على الساعة 17:59

¹ - أ/ إيمان غلاء الدين ، الأمن السيبراني المفهوم والتداعيات في السياسة العالمية ، مقال منشور في موقع الحضارة للدراسات والبحوث ، بتاريخ 2021/4/1 ، على الرابط الإلكتروني :

<https://hadaracenter.com/> اطلع عليه بتاريخ 2023/11/8 على الساعة 17:56.

² - د/ين مرزوق عنتر ، أ /حشاوي محي الدين ، الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية ، مقال منشور على الرابط الإلكتروني :

<https://dspace.univ-ouargla.dz/jspui/bitstream>

اطلع عليه بتاريخ 2023/11/8 على الساعة 18:16

³ - د/بوضياف اسمهان ، الجريمة الإلكترونية والاحداث التشريعية لمواجهتها في الجزائر ، مجلة الأستاذ الباحث للدراسات القانونية والسياسية ، جامعة محمد بوضياف المسيلة ، الجزائر ، المجلد 3، العدد 3، تاريخ النشر : سبتمبر 2018 ، 361-360.

معتوق أم الخير

قانون العقوبات خاصة بالمساس بأنظمة المعالجة الآلية للمعطيات¹، وأخيرا صدر القانون المتضمن القواعد الخاصة للوقاية من لجرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحتها².

أولا: تجريم المساس بأنظمة المعالجة الآلية للمعطيات المرتكبة من الشخص الطبيعي

في سياق مساعي الدولة الجزائرية لمكافحة الجريمة الإلكترونية ، قام المشرع الجزائري بمعاقبة الشخص الطبيعي في حالة ما إذا قام بالمساس بأنظمة المعالجة الآلية للمعطيات ، حيث أنه من خلال استقراء نص المادة 394 مكرر من قانون العقوبات الجزائري ، نجد أنه قد جرم فعل الدخول والبقاء أو محاولة فعل ذلك ، بطريقة غير مشروعة عن طريق الغش ، لكل أو جزء من منظومة للمعالجة الآلية للمعطيات³.

كما قام بتجريم فعل الدخول أو كل فعل من شأنه إزالة أو تعديل بطريق الغش المعطيات التي يتضمنها⁴.

حيث بين المشرع الجزائري من خلال المادة 394 مكرر (2) عن تجريم كل من يقوم عمدا بفعل نشر- أو تجميع أو حتى الاتجار بالمعطيات أو معالجة لمراسلة بواسطة منظومة معلوماتية ، وجرم فعل الحيازة العمدية للمعطيات المتحصل عليها ، أو نشرها واستعمالها مهما كان الغرض⁵.

تضاعف العقوبات المنصوص عليها في هذا القسم في حالة ما تم استهداف الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام من خلال هذه الجريمة ، دون الإخلال بتطبيق عقوبات أشد⁶.

ثانيا : تجريم المساس بأنظمة المعالجة الآلية للمعطيات المرتكبة من الشخص المعنوي

قام المشرع الجزائري بمعاقبة الشخص المعنوي بغرامة مالية تعادل خمس (5) مرات الحد الأقصى- للغرامة المقررة للشخص الطبيعي ، وذلك في حالة ما إذا قام بارتكاب الجرائم المنصوص عليها في هذا القسم⁷.

الفرع الثاني : مكافحة الجرائم الإلكترونية في القوانين الخاصة

نظرا لإدراك الجزائر لحجم المخاطر التي يمكن أن تتعرض لها المعلومات والبيانات في البيئة الرقمية خصوصا ما تعلق منها بخرق التوقيعات الرقمية من خلال بعض التقنيات المستعملة لفك الشفرات ، بالإضافة

¹ - القانون رقم 15/04 المؤرخ في 10/11/2004 المتضمن قانون العقوبات الجزائري المعدل والمتمم للأمر رقم 156/66 ، ج ر ع 71 ، المؤرخة بتاريخ 10 نوفمبر 2004 .

² - د/أحمد بن مسعود ، جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري ، مجلة الحقوق والعلوم الانسانية ، جامعة زيان عاشور الجلفة ، الجزائر ، المجلد 10 ، العدد 1 ، تاريخ النشر 2017/3/10 ، ص 483.

³ - القانون رقم 15/04 المؤرخ في 10/11/2004 المتضمن قانون العقوبات الجزائري ، مشار إليه سابقا .

⁴ - ينظر نص المادة 394 مكرر (1) من القانون رقم 15/04 المؤرخ في 10/11/2004 المتضمن قانون العقوبات الجزائري ، مشار إليه سابقا .

⁵ - ينظر نص المادة 394 مكرر (2) من القانون رقم 15/04 المؤرخ في 10/11/2004 المتضمن قانون العقوبات الجزائري ، مشار إليه سابقا .

⁶ - ينظر نص المادة 394 مكرر (3) من القانون رقم 15/04 المؤرخ في 10/11/2004 المتضمن قانون العقوبات الجزائري ، مشار إليه سابقا .

⁷ - ينظر نص المادة 394 مكرر (4) من القانون رقم 15/04 المؤرخ في 10/11/2004 المتضمن قانون العقوبات الجزائري ، مشار إليه سابقا .

دور الأمن السيبراني في مقاومة الدول للتهديدات الكامنة في الفضاء السيبراني (استراتيجية الجزائر نموذجا)

للجرائم الإلكترونية في البيئة الرقمية والهجمات السيبرانية التي تستهدف المؤسسات الوطنية القائمة على معالجة المعطيات والبيانات المتعلقة بالأفراد .

ونظرا لذلك كله ، بذل المشرع الجزائري جهودا تشريعية معتبرة وذلك من أجل مواجهة هذه المخاطر والتهديدات التي يمكن أن تتعرض لها الأنظمة الرقمية ، بداية من القانون 04/09 المتعلق بالوقاية من الجرائم المتصلة بالتكنولوجيات الحديثة ،¹ الذي تضمن إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الحديثة ، إلى غاية صدور المرسوم الرئاسي تحت رقم 05/20² المتعلق برسم ووضع منظومة وطنية لأمن الأنظمة المعلوماتية .³

أولا : مكافحة الجريمة الإلكترونية في القانون المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها .

بغية وضع قواعد خاصة تعنى بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها قام المشرع الجزائري باستصدار القانون رقم 04-09 ، حيث ضمنه كل ما يتعلق بمراقبة الاتصالات الإلكترونية ، وجملة القواعد الإجرائية فيما يخص تفتيش المنظومات المعلوماتية ، التزامات مقدمي الخدمات مساعدة السلطات ، إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها أما الفصل الأخير فقد نص على التعاون والمساعدة القضائية الدولية ، الاختصاص القضائي.

ثانيا : مكافحة الجريمة الإلكترونية في القانون المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي .⁴

نظرا لاستعمال تكنولوجيات الإعلام والاتصال الحديثة في ميادين عديدة ، خاصة مجال المعالجة الآلية للمعطيات ، وفي ظل العولة وسهولة الحصول على البيانات وتداولها ، هذا ما مكن كل من الشركات الخاصة أو العامة من المتاجرة بالبيانات الشخصية للأفراد واستغلالها بغرض الدعاية والإعلام لأهداف اقتصادية أو سياسية ، هذا ما دفع بالمشرع الجزائري لإصدار القانون 07/18 الذي يهدف على حماية الأفراد إزاء استعمال

¹ - القانون رقم 04/09 المؤرخ في 05/8/2009 المنظم القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ، ج ر ع 47 المؤرخة بتاريخ 2009/8/6

² - المرسوم الرئاسي 05/20 المؤرخ في 10/12/2020 المنظم وضع منظومة وطنية لأمن الأنظمة المعلوماتية ، ج ر ع 4 المؤرخة بتاريخ 2020/1/26

³ - د/حزام فتحة ، الحماية المؤسساتية للأنظمة الرقمية في الفترة التشريعية الممتدة من 2009-2020 ، مجلة الأكاديمية للدراسات الاجتماعية والإنسانية ، جامعة حسينة بن بوعلي الشلف ، الجزائر ، المجلد 13 ، العدد 2 ، تاريخ النشر : 2021/1/18 ، ص 274.

⁴ - القانون 07/18 المؤرخ في 10/6/2018 المنظم حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي ، ج ر ع 11 المؤرخة بتاريخ 2018/6/10.

معتوق أم الخير

تقنيات المعلومات والاتصال ، كما نص على إنشاء السلطة الوطنية لحماية المعطيات الشخصية والجزاءات المقررة في حالة مخالفة قواعد هذا القانون ¹.

كذلك وجوب أن تتم معالجة المعطيات الشخصية ، بغض النظر عن شكلها أو مصدرها ، دون المساس بالكرامة الإنسانية أو التعدي على الحياة الخاصة والحريات العامة أو بحقوق الأشخاص. ² في حين خصص الباب الثاني للمبادئ الأساسية لحماية المعطيات ذات الطابع الشخصي ، أما الباب الثالث فقد تضمن النص على إنشاء السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي ، حيث نص المشرع على استحداث سلطة إدارية مستقلة لحماية المعطيات ذات الطابع الشخصي- لدى السيد رئيس الجمهورية ، مع ضرورة تمتعها بالشخصية المعنوية والاستقلال المالي والإداري ، ³ وأما تشكيلتها فقد نصت عليها المادة 23 من نفس القانون ⁴.

كما تمت الإشارة على معالجة المعطيات ذات الطابع الشخصي المرتبطة بخدمات التصديق والتوقيع الإلكترونيين في الفصل الثاني ⁵ ومعالجة المعطيات في مجال الاتصالات الإلكترونية في الفصل الثالث من الباب الخامس من هذا القانون ⁶.

ثالثا: الحماية المقررة للأنظمة الرقمية بموجب المرسوم الرئاسي 05/20 المتضمن وضع منظومة وطنية لأمن الأنظمة الرقمية .

أصدر المشرع الجزائري مرسوما رئاسيا تحت رقم 05/20 المتعلق برسم ووضع منظومة وطنية لأمن الأنظمة المعلوماتية موكلة لوزارة الدفاع الوطني ، لتشكيل أداة للدولة في مجال أمن الأنظمة المعلوماتية ، وآلية تنظيمية من شأنها إعداد استراتيجية الوطنية لأمن المنظومة ⁷.

¹-مشتة نسرين ، بن عبید إخلاص ، الحماية القانونية للمعطيات الشخصية في ظل القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي ، المجلة الجزائرية للحقوق والعلوم السياسية، جامعة تيسمسيلت ، الجزائر ، المجلد 6، العدد 1 ، تاريخ النشر : 2021/6/1، ص 2.

² - ينظر :نص المادة 2 من القانون 07/18 المؤرخ في 2018/6/10 المتضمن حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، مشار إليه سابقا .

³ - ينظر :نص المادة 22 من القانون 07/18 المؤرخ في 2018/6/10 المتضمن حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، مشار إليه سابقا .

⁴ - ينظر :نص المادة 23 من القانون 07/18 المؤرخ في 2018/6/10 المتضمن حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، مشار إليه سابقا .

⁵ - ينظر :نص المادة 42 من القانون 07/18 المؤرخ في 2018/6/10 المتضمن حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، مشار إليه سابقا .

⁶ - ينظر :نص المادة 43 من القانون 07/18 المؤرخ في 2018/6/10 المتضمن حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، مشار إليه سابقا .

⁷ -د/حزام فتحة ، المرجع السابق ، ص 274.

دور الأمن السيبراني في مقاومة الدول للتهديدات الكامنة في الفضاء السيبراني (استراتيجية الجزائر نموذجا)

تشكل هذه المنظومة الوطنية الموضوعة لدى وزارة الدفاع الوطني ما يأتي :

1. مجلس وطني لأمن الأنظمة المعلوماتية ، دوره الموافقة على إعداد استراتيجية وطنية من أجل أمن المعلومات ، وتوجيهها .
2. وكالة لأمن الأنظمة المعلوماتية دورها تنظيم وتنفيذ الاستراتيجية الوطنية لأمن أنظمة المعلومات .¹

2.2- المطلب الثاني : الآليات المؤسساتية لتعزيز الأمن السيبراني

تعد الجزائر من بين الدول التي تواجه التهديدات السيبرانية ، حيث تعرضت لعدد من الهجمات الإلكترونية في الآونة الأخيرة ، حيث صنفت الأولى عربيا وال 14 عالميا ، حسب وزارة الاتصال الجزائرية . هذا الأمر الذي من شأنه إدراك أهمية الأمن السيبراني ، خصوصا وأن الدولة الجزائرية تتوجه نحو التحول لإحداث نقلة نوعية في مجال تسيير الشأن العام ، من خلال اعتماد استراتيجية مثلى للرقمنة ، في إطار تحقيق تنمية من شأنها الرفع من جودة المؤسسات ، حتى تصبح الجزائر بهذا قادرة على أن تكون ضمن الدول المتقدمة . وهذا ما أكدّه السيد رئيس الجمهورية عبد المجيد تبون ، وقيادة الجيش على أولوية الدولة الجزائرية الشديدة لمهمة الحفاظ على أمن الأنظمة المعلوماتية الوطنية بشقيها العام والخاص ، إضافة إلى تحقيق ما يُعرف بالسيادة الإلكترونية²

لذلك من أجل تجسيد ذلك على أرض الواقع ، قامت الدولة الجزائرية بتسخير مجهودها كاملة لاعتماد استراتيجية متكاملة لتعزيز الأمن السيبراني من خلال اعتماد آليات تشريعية كما سبق بيانه ، بالإضافة إلى مؤسسات وهيكل عملياتية مختلفة خصوصا على مستوى وزارة الدفاع الوطني ، ومديرية الأمن الوطني .

الفرع الأول : الآليات والمؤسسات التابعة لوزارة الدفاع الوطني للتصدي للجريمة الإلكترونية

نظرا للتحديات التي تواجه الجزائر على مستوى الفضاء السيبراني فرض عليها ضرورة ضمان أمن سيبراني ولا يكون ذلك إلا من خلال سن نصوص قانونية ذات صلة ، واستحداث مؤسسات وهيئات من أجل مواجهة الهجمات السيبرانية . ولما كان الأمن السيبراني أمرا أساسيا لبناء منظومة أمنية متكاملة عليه وجب على الدفاع الوطني من خلال أجهزته كالدرك الوطني الجزائري التصدي للإجرام المعلوماتي .

ومن بين مؤسسات وزارة الدفاع الوطني التي أعطيت لها مهمة حماية وتعزيز الأمن السيبراني نجد مركز يعني بالوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني ، المعهد وطني خاص بالأدلة الجنائية

¹ - ينظر نص المادة 3 المرسوم الرئاسي 05/20 المؤرخ في 2020/12/10 المتضمن وضع منظومة وطنية لأمن الأنظمة المعلوماتية ، مشار إليه سابقا .

² - الرئيس الجزائري يحذر من مخاطر هجمات إلكترونية محتملة ، مقال منشور بتاريخ 2023/6/7 على الرابط الإلكتروني :

<https://www.alaraby.co.uk/politics/> اطلع عليه بتاريخ 2023/11/9 على الساعة 10:06 .

معتوق أم الخير

وعلم الإجرام، وأخيرا استحداث المنظومة الوطنية لأمن الأنظمة المعلوماتية الموضوعة لدى وزارة الدفاع الوطني.

أولا : مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني

في سياق اتجاه الدولة الجزائرية لمكافحة الإجرام المعلوماتي ، وتحقيق الأمن السيبراني وتعزيزه ، من خلال تأمين منظومة المعلومات قامت بإنشاء مركز مقرر بئر مراد رايس تابع للدرك الوطني ، مهمته تحليل المعطيات والبيانات المرتبطة بالجرائم الإلكترونية المرتكبة ، والعمل على تحديد هوية مرتكبها سواء كانوا أشخاصا فرادى أو عصابات ، بهدف تأمين والحفاظ على أنظمة المعلومات خصوصا بالنسبة للمؤسسات والبنوك والبيوت ، كما يهدف إلى مساعدة أجهزة الأمن في التصدي لهذا النوع من الإجرام.¹

يعنى هذا المركز بمهام عديدة منها : مراقبة شبكة الانترنت بانتظام واستقرار ، و مراقبة الاتصالات الإلكترونية في إطار حدود القانون ، التحري والتسرب في بيئة الأنترنت لفائدة وحدات الدرك الوطني والجهات القضائية، التعاون بين مختلف المصالح الأمنية والهيئات الوطنية من أجل مكافحة الجريمة الإلكترونية ، كما يعمل بمساعدة الوحدات الإقليمية للدرك الوطني على التحقيق في الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال والبحث عن الأدلة.²

حسب تصريح لواء الدرك الوطني، "فإن المركز في إطار مساعدة الوحدات الإقليمية للدرك الوطني قد قام سنة 2017 بمعالجة حوالي ألف جريمة رقمية بنسبة تقارب 68 بالمائة مقارنة بالسنة السابقة".³

ثانيا :المعهد الوطني للأدلة الجنائية وعلم الإجرام

في إطار تدعيم قدرات الدرك الوطني في مجال مكافحة الجريمة بكافة أنواعها ، تم إنشاء المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني مقره بوشاوي ، من خلاله اعتماد التقنيات الحديثة التي من شأنها دعم قدرات هذا المركز في مجابهة هذا النوع من الإجرام بأساليب متطورة تعتمد على وسائل تكنولوجية حديثة وإدراج العلوم في العدالة الجنائية.⁴

¹ -د/بارة سمير ، المرجع السابق ،ص270.

² - أ/سميحة بلقاسم ، أ/حميد بوشوشة ، الجريمة الإلكترونية بعد جديد للإجرام في الجزائر ... واقعها وآليات مجابهتها ، مجلة العلوم الإنسانية ، جامعة أم البواقي ، الجزائر ، المجلد 10 ، العدد 1 ، تاريخ النشر :2023/6/15 ،ص552.

³ -كلمة اللواء قائد الدرك الوطني مناد نوبة خلال افتتاحه لأشغال الندوة الدولية حول الأمن السيبراني المنظمة بالنادي الوطني للجيش .على الرابط الإلكتروني :

⁴ -2023/11/10 <https://www.aps.dz/ar/algerie/54821-2> اطلع عليه بتاريخ 2023/11/10 على الساعة 13:19.

⁴ -موقع وزارة الدفاع الوطني https://www.mdn.dz/site_cgn/sommaire/presentation/unit_spe/incc/incc_ar.php

اطلع عليه بتاريخ 2023/11/10 على الساعة 13:32.

دور الأمن السيبراني في مقاومة الدول للتهديدات الكامنة في الفضاء السيبراني (استراتيجية الجزائر نموذجاً)

أنشئ هذا المعهد بموجب المرسوم الرئاسي رقم 183/04 المؤرخ في 26 جوان 2004 وعدل نظامه الأساسي بموجب المرسوم الرئاسي رقم 118/09 المؤرخ في 14 أفريل 2004.

يتكون هذا الجهاز من 11 دائرة متخصصة في مجالات مختلفة ، لتقديم المساعدات في المجال التقني العمل على معالجة وتحليل وتقديم كافة الأدلة الرقمية التي من شأنها مساعدة العدالة أو المحققين من خلال دائرة للإعلام الآلي، بالإضافة إلى محطة خاصة بالأجهزة المعطلة ، محطة محمولة وثابتة خاصة بخبرات الإعلام الآلي الشبكات ، كما يحتوي على قاعات هي :مكتب يعنى بالتوجيه ، فصيلة الأنظمة المشحونة ،الهواتف وأخرى خاصة بتحليل المعطيات و اقتناء المعطيات ، بقاعات للموزع والتخزين.¹

من مهام المركز :

1. إجراء الخبرات والفحوص العلمية في إطار التحريات الأولية والتحقيقات القضائية وهذا بغرض إقامة الأدلة التي تسمح بالتعرف على مرتكبي الجنايات والجحج .
2. ضمان المساعدة العلمية أثناء القيام بالتحريات المعقدة باستخدام مناهج الشرطة العلمية .
3. العمل على القيام بدراسات وتحليل بهدف الوقاية والتقليل من الجريمة .
4. إنشاء بنوك خاصة بالمعطيات
5. العمل على المشاركة في اعتماد سياسة جنائية واضحة المعالم لمكافحة الجريمة
6. الاعتماد على التكنولوجيات الدقيقة فيما يخص عملية إجراء البحوث الخاصة بكل ما يتعلق بالإجرام.²

ثالثا : المنظومة الوطنية لأمن الأنظمة المعلوماتية الموضوعة لدى وزارة الدفاع الوطني

حاول المشرع الجزائري التدخل من جديد ، وذلك من خلال استحداث آليات تحت رعاية وزارة سيادية وهي وزارة الدفاع الوطني كون قضايا الأمن السيبراني تمس سيادة الدولة الجزائرية ، كل ذلك بناء على أحكام المادة 03 المرسوم الرئاسي 05/20 ، هذه الآلية هي المنظومة الوطنية لأمن الأنظمة المعلوماتية الموضوعة لدى وزارة الدفاع الوطني التي تشمل كل من المجلس الوطني لأمن الأنظمة المعلوماتية ، والوكالة الخاصة بأمن الأنظمة المعلوماتية .³

¹ د-عائشة عبد الحميد ، الإطار القانوني والتشريعي للرقمنة والذكاء الاصطناعي ، المجلة الدولية للتعليم بالإنترنت ، جمعية التنمية التكنولوجية والبشرية ، مصر ، المجلد 19 ، العدد 1 ، تاريخ النشر : 2020/7/1 ، ص 99-100.

² د-بارة سمير ، المرجع السابق ، ص 271-272.

³ د-حزام فتيحة المرجع السابق ، ص 280.

معتوق أم الخير

الفرع الثاني: آليات المديرية العامة للأمن الوطني في التصدي للجرائم الإلكترونية

تعد الجرائم الإلكترونية ظاهرة مستحدثة أفرزها الاستعمال المتزايد لتكنولوجيات الإعلام والاتصال، حيث يتصف فاعليها بالدهاء والمكر والقدرة على إخفاء هويتهم، كما يتسمون بدقة اختيارهم للضحايا الذين يملكون وعيا منخفضا بخطورة الجريمة عبر الانترنت، وهي تختلف بذلك عن الجرائم التقليدية، ومن صور هذه الجرائم نجد الترويج للإرهاب والمخدرات، الاحتيال المعلوماتي، تزيف الوثائق والمستندات إلكترونيا والابتزاز

في هذا الإطار وأكبت وطورت المديرية العامة للأمن الوطني آليات التصدي للجرائم المتعلقة بالمعلوماتية التي عرفت انتشارا واسعا في السنوات الأخيرة، على غرار استحداث دائرة الأدلة الرقمية، التي تضمن استغلال مختلف الأجهزة الرقمية لكشف ملابسات الجرائم¹.

أولا: المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة للأمن الوطني

أمام البعد الخطير الذي تتخذه الجريمة الإلكترونية، لم تدخر المديرية العامة للأمن الوطني أي جهد من أجل تطوير آليات مجابهتها الأمر الذي من شأنه تعزيز مجهودات تحقيق الأمن السيبراني، فقامت سنة 2011 بإنشاء مصلحة مركزية على مستوى المديرية العامة للأمن الوطني شكلت نواة لتشكيل أمني كفاء بغية محاربة التهديدات الأمنية الناتجة عن هذا الإجرام المعلوماتي، كما قام المدير العام بإصدار قرار للأمن الوطني في جانفي 2015 من أجل استحداث مصلحة مركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال تابعة للهيكل التنظيمي لمديرية الشرطة القضائية².

ثانيا : المصالح والفرق المتخصصة التابعة للمصلحة المركزية لمكافحة الإجرام المتعلقة بتكنولوجيات الإعلام والاتصال .

في ذروة الاجتياح الإلكتروني والتطور الهائل الذي تشهده تكنولوجيات الإعلام والاتصال والتي أصبحت مرتعا لبعض الأطراف الإجرامية لارتكاب مختلف الجناح والجرائم والهجمات الإلكترونية وبيئة خصبة لنشر الأخبار المغلوطة والمضللة، وأمام البعد الخطير الذي يتخذه هذا النوع من الجرائم، لم تدخر المديرية العامة للأمن الوطني جهدا لتطوير ميكانيزمات التصدي للجرائم المعلوماتية، من خلال تسخير تشكيل أمني مؤهل وكفاء، مهمته جمع الأدلة والقيام بعمليات استباقية لوقف القرصنة ومختلف الجرائم الرقمية، ويصبو إلى تحقيق التوازن بين ثنائية الردع والوقاية، مع الحرص الدائم على التكيف مع كافة التحولات السريعة للفضاء السيبراني، حيث تركز محام المصالح المختصة وفرقها العملياتية التابعة للشرطة القضائية، على اتخاذ مجموعة

¹ -دائرة الأدلة الرقمية للأمن الوطني دعم تقني احترافي بامتياز، مجلة الشرطة، مديرية الأمن الوطني، العدد 149، تاريخ النشر: أكتوبر 2021،

ص 36.

² - أ/سميحة بلقاسم، أ/حميد بوشوشة، المرجع السابق، ص 548.

دور الأمن السيبراني في مقاومة الدول للتهديدات الكامنة في الفضاء السيبراني (استراتيجية الجزائر نموذجا)

من التدابير الوقائية لتجنب وقوع هاته الجرائم ، وفي حال حدوثها ، تعتمد الأساليب الردعية من خلال التحريات وتقني مجرمي المنصات الافتراضية وتسليمهم إلى الجهات القضائية المختصة من أجل تطبيق الإجراءات القانونية اللازمة¹.

ومن مهام المصالح المختصة لمكافحة الجرائم المعلوماتية ورفقها العملياتية التابعة للشرطة القضائية ما يلي :

1. قيام مصالح الشرطة القضائية المختصة للأمن الوطني بدعم المشاركة وتنسيق التحقيقات والتحريات والنشاطات المتعلقة بالوقاية المباشرة و مكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال .
2. المشاركة في تأمين وحماية الأنظمة المعلوماتية والفضاء السيبراني الوطني .
3. التعاون والمشاركة في التحقيقات والتحريات ذات البعد الوطني والدولي في مجال مجابهة الجرائم الإلكترونية .
4. مباشرة اليقظة المعلوماتية والبحث عبر الشبكات المفتوحة عن كل محتوى غير شرعي عبر الانترنت ، يشكل في حد ذاته جريمة في قانون العقوبات .
5. المشاركة في التكوين المتخصص لعناصر الشرطة المتواجدة على مستوى فرق مكافحة الجريمة المعلوماتية بأمن الولايات².

وبالنظر لحصيلة القضايا التي عالجتها المديرية العامة للأمن الوطني بخصوص جرائم تكنولوجيات الإعلام والاتصال خلال مدة 7 أشهر من سنة 2021 ، نجد أنه عالج ما يقارب نسبة 82.59% من قضايا جرائم المساس بالأشخاص عبر الانترنت ، ونسبة 15.64% من قضايا جرائم النصب والاحتيال ، وكذا نسبة 1.75% بالنسبة لقضايا جرائم المساس بالقصر عبر الانترنت³.

ثالثا :دائرة الأدلة الرقمية للأمن الوطني

استحدثت المديرية العامة للأمن الوطني في شهر أفريل 2009 دائرة متخصصة في استغلال الأدلة الرقمية من أجل توفير الدعم التقني والفني الخاص بتحليل واستغلال العتاد الرقمي وكل ذلك للمساهمة في محاربة الجرائم المعلوماتية والجرائم التقليدية التي تستخدم تكنولوجيات الإعلام و الاتصال .

¹ - الشرطة الجزائرية تتصدى لصناع الكراهية عبر المنصات الرقمية ، مجلة الشرطة ، مديرية الأمن الوطني ، العدد 149 ، تاريخ النشر : أكتوبر

2021 ، ص 32.

² - المرجع نفسه ، ص 33.

³ - لمزيد من التفصيل ينظر :حصيلة القضايا المعالجة حول جرائم تكنولوجيات الإعلام والاتصال ، مجلة الشرطة ، المرجع نفسه ، ص 38.

معتوق أم الخير

تتكون الدائرة المختصة في استغلال الأدلة الرقمية من ثلاث فرق عملياتية تسهر على السير الحسن للمهام الموكلة لها .

أ/ قسم الإعلام الآلي : يتم من خلاله استغلال أجهزة الإعلام الآلي من جميع الأنواع وبمختلف

مكوناته من أقراص صلبة داخلية وخارجية ، دعامات التخزين ، بطاقات الذاكرة ، الأقراص المضغوطة وغيرها بالإضافة إلى آلات التصوير والكاميرات الرقمية واستخراج محتوى الدعامات الرقمية ، كما يتوفر القسم على وسائل وتجهيزات جد حديثة وخبرات شرطية في استخراج الكلمات السرية واسترجاع الملفات .

ب/ قسم استغلال دعائم الاتصالات النقالة : يسمح القسم في حالة توقيف مشتبه فيهم كانوا قد استعملوا تكنولوجيا الهواتف النقالة ، من استخراج جميع المعطيات الظاهرة والمحدوفة منها ، معرفة مختلف شرائح "سيم" التي تم وصلها أو استعمالها وكذا بطاقات الذاكرة ، بالإضافة إلى تشخيص المعطيات التي لها على علاقة مع القضايا المعالجة ، كما يوفر القسم دعما في تحليل المعطيات ، قائمة الاتصالات ، الرسائل النصية ، الرسائل المرئية ، الإيميلات ، سجل المكالمات الهاتفية ، الملتيميديا ، الإنحار عبر الأنترنت .

ج/ قسم معالجة الصور والفيديوهات : يعتبر هذا القسم سندا ودعما تقنيا في معالجة وتحسين نوعية الصور والفيديوهات المحزنة في الدعائم الإلكترونية ، والرقمية كالمسجلات الرقمية ، الأقراص الصلبة ، ودعامات التخزين.¹

خاتمة:

في ختام الدراسة نجد أن موضوع الأمن السيبراني أصبح يشغل العديد من دول العالم في الآونة الأخيرة ، لاسيما في ظل التطور التكنولوجي والتحولات الرقمية ، وازدياد الاتصال الإلكتروني ، والتبادل المالي ، والتجارة ، وغيرها من المجالات بالاعتماد على التكنولوجيا ما أدى إلى احتمالية ازدياد وتيرة الهجمات السيبرانية بشكل متسارع ، خصوصا بعد ما بعد جائحة كورونا التي كانت المساهم الأكبر في ذلك ، لذا كان لزاما على الدول تسطير استراتيجية لتفادي الوقوع في مصيدة جرائم الانترنت وخسارة الحرب الإلكترونية .

الجزائر من بين الدول التي باتت طرفا في هذه الحرب التي أصبحت تدعى بحرب الغد ، حيث طالبتها العديد من الهجمات السيبرانية مست منظومتها الإلكترونية وأضحت تهدد أمنها القومي ، لذلك اعتمدت استراتيجية أساسها اليقظة الشاملة ، لمجابهة هذه التحديات الرقمية ، والأن هي في طريقها لتعلم كيفية نشر- البيانات المنشورة في المواقع الإلكترونية وتأمينها ، وبناء أمنها السيبراني ، وفي السياق نفسه قررت السلطات الجزائرية تعزيز قدرتها في مجال نظم الحماية السيبرانية وذلك من خلال إنشاء مدرسة عليا للأمن السيبراني بهدف تعليم وتكوين إطارات الدفاع والأمن في المجال الإلكتروني ، والإجرام المعلوماتي .

كما توصلت هذه الدراسة إلى مجموعة من التوصيات نلخصها في النقاط الآتية :

¹ - دائرة الأدلة الرقمية للأمن الوطني دعم تقني احترافي بامتياز ، المرجع السابق ، ص 37.

دور الأمن السيبراني في مقاومة الدول للتهديدات الكامنة في الفضاء السيبراني (استراتيجية الجزائر نموذجاً)

- ✓ الوعي التام بمصدر التهديد وطبيعته لمعرفة العدو في هذا الفضاء الافتراضي .
- ✓ اعتماد اجراءات احترازية للوقاية من الهجمات السيبرانية .
- ✓ توظيف وتعبئة كافة القدرات في الدولة ، لمواجهة كافة المخاطر السيبرانية .
- ✓ ضرورة تطبيق الأمن السيبراني على كافة المستويات
- ✓ ضرورة تطوير الدولة الجزائرية للأنظمة والبحث عن كل ما هو أحسن كل 3 أشهر أو 6 أشهر .
- ✓ اعتماد نظام التراسل الذي يساعد على التراسل المشفر بين الدول .
- ✓ عدم اعتماد البريد الالكتروني الغير المؤمن .
- ✓ الاعتماد على تجارب الدول التي كسبت رهان الأمن السيبراني من أجل حماية الأمن القومي .

قائمة المصادر والمراجع:

1. النصوص القانونية :

- القانون رقم 15/04 المؤرخ في 10/11/2004 المتضمن قانون العقوبات الجزائري المعدل والمتمم للأمر رقم 156/66 ، ج ر ع 71 ، المؤرخة بتاريخ 10 نوفمبر 2004 .
 - القانون رقم 04/09 المؤرخ في 05/08/2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ، ج ر ع 47 المؤرخة بتاريخ 06/08/2009
 - القانون 07/18 المؤرخ في 10/06/2018 المتضمن حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر ع 11 المؤرخة بتاريخ 10/06/2018
- المراسم :

- المرسوم الرئاسي 05/20 المؤرخ في 10/12/2020 المتضمن وضع منظومة وطنية لأمن الأنظمة المعلوماتية ، ج ر ع 4 المؤرخة بتاريخ 26/01/2020.

2. الكتب :

- الكتب المتخصصة :

- د/فارس محمد العمارات ، أ/ إبراهيم محمد الحماسة ، الأمن السيبراني (المفهوم وتحديات العصر-) ، الطبعة الأولى ، دار الخليج للنشر والتوزيع ، عمان ، الأردن ، سنة 2022 .

3. المقالات :

- أم د . أميرة محمد محمد سيد أحمد ، استراتيجيات مكافحة الجرائم الإلكترونية في العصر- المعلوماتي تعزيزاً لرؤية مصر- 2030 دراسة استشرافية ، مجلة البحوث الإعلامية ، كلية الإعلام ، جامعة الأزهر ، الجزء الرابع ، العدد الثامن والخمسون ، تاريخ النشر : جويلية 2021 .

معتوق أم الخير

- د/مني عبد الله السمحان ، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود ، مجلة كلية التربية ، جامعة المنصورة ، مصر ، العدد 111 ، تاريخ النشر : جويلية 2020.
- د/ناصر سعيد على محسن الدحاني ،د/أمير عبد الولي نُجْد الصنوي ، متطلبات تطبيق الأمن السيبراني في الجامعات الجنية من وجهة نظر الخبراء ،مجلة الجامعة الوطنية ، النين ، العدد 18، تاريخ النشر 2021 .
- د/أمنة علي البشير نُجْد ،الأمن السيبراني في ضوء مقاصد الشريعة ، مجلة كلية الدراسات الإسلامية والعربية للبنات،الإسكندرية ، مصر ، المجلد01، العدد 37 ، بدون تاريخ نشر .
- د/خالد ظاهر عبد الله جابر السهيل المطيري ، دور التشريعات الجزائرية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي ، مجلة البحوث الفقهية والقانونية ، كلية الشريعة والقانون بدمهور ، مصر ، العدد 38، تاريخ النشر:جويلية 2022 .
- د/سارة نُجْد روجي فتحي غزال ، الأمن السيبراني ودرجة وعي المؤسسات بأهميته ، المجلة العربية للنشر العلمي ، الأردن ، العدد47، تاريخ النشر 2 سبتمبر 2022 ،ص 581.
- أ/ أمنة نُجْد منصور ، تأثير الأمن السيبراني على الرقابة الداخلية وانعكاسها على الوحدة الاقتصادية (دراسة استطلاعية لأراء المدققين والمحاسبين في وزارة التعليم العالي والبحث العلمي) ،مجلة الإدارة والاقتصاد ، الجامعة المستنصرية ،بغداد ، العراق ، العدد 127، تاريخ النشر : مارس 2021 .
- علاء الدين فرحات ، الفضاء السيبراني تشكيل ساحة المعركة في القرن الحادي والعشرين ، مجلة العلوم القانونية والسياسية، جامعة الوادي ، الجزائر ، المجلد 10 ، العدد 03 ، تاريخ النشر :2019/12/28 .
- أ/تغريد صفاء ، أ د/لبنى خميس مهدي ، أثر السيبرانية في تطور القوة ،مجلة حمورابي ، مركز حمورابي للبحوث والدراسات الاستراتيجية، العراق ، العدد 33-34 ، تاريخ النشر سنة 2020.
- أ/قاسمي صافية ، الفضاء السيبراني والأغور الإلكترونية (إشكالية خلق فضاء عمومي افتراضي حسب المنظور الهابرماسي ، مجلة الحكمة للدراسات الفلسفية ، مؤسسة كنوز الحكمة للنشر والتوزيع ، الجزائر ، العدد 7 ، تاريخ النشر ،جوان 2016 .
- د/نورة شلوش ،القرصنة الإلكترونية في الفضاء السيبراني (التهديد المتصاعد لأمن الدول) ،مجلة مركز بابل للدراسات الإنسانية ،جامعة بابل ، العراق ، المجلد 8، العدد 2 ، تاريخ النشر: سنة 2018 .
- أ/ربيعي حسين ، أ/وسمر نُجْد ، الحروب السيبرانية المخاطر واستراتيجيات تحقيق الأمن السيبراني الدولي والداخلي ، المجلة الجزائرية للأمن الإنساني ،جامعة باتنة 1 الحاج لخضر ، الجزائر ، المجلد 7، العدد2، تاريخ النشر:جويلية 2022 .
- د/بارة سمير ، الأمن السيبراني (Cyber Security) في الجزائر السياسات والمؤسسات ،المجلة الجزائرية للأمن الإنساني ، جامعة باتنة 1الحاج لخضر ، الجزائر ، المجلد2، العدد 2 ، تاريخ النشر: 2017/7/1 .
- د/هاني نُجْد خليل ابراهيم العازي ، النظام القانوني الدولي لمكافحة المخاطر السيبرانية ،مجلة مصر المعاصرة ،الجمعية المصرية للاقتصاد السياسي ،مصر ، العدد549 ، تاريخ النشر :يناير 2023 .
- روان بنت عطية الله الصخفي ، الجرائم السيبرانية ، المجلة الإلكترونية الشاملة متعددة التخصصات ،الأردن ، العدد 24،تاريخ النشر :ماي 2020.

دور الأمن السيبراني في مقاومة الدول للتهديدات الكامنة في الفضاء السيبراني (استراتيجية الجزائر نموذجا)

-د/عبد السلام مُحمَّد المايل، د/عادل مُحمَّد الشربجي، د/علي قابوسة، الجريمة الإلكترونية في الفضاء الإلكتروني (المفهوم – الأسباب – سبل المكافحة مع التعرض لحالة ليبيا)، مجلة أفاق للبحوث والدراسات، المركز الجامعي إليزي، الجزائر، العدد 4، تاريخ النشر: 2019/6/4.

- د/بوضياف اسمهان، الجريمة الإلكترونية والاجراءات التشريعية لمواجهةها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة مُحمَّد بوضياف المسيلة، الجزائر، المجلد 3، العدد 3، تاريخ النشر: سبتمبر 2018.

-د/أحمد بن مسعود، جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري، مجلة الحقوق والعلوم الانسانية، جامعة زيان عاشور الجلفة، الجزائر، المجلد 10، العدد 1، تاريخ النشر 2017/3/10.

-د/حزام فتiche، الحماية المؤسسية للأظمة الرقمية في الفترة التشريعية الممتدة من 2009- 2020، مجلة الأكاديمية للدراسات الاجتماعية والإنسانية، جامعة حسيبة بن بوعلي الشلف، الجزائر، المجلد 13، العدد 2، تاريخ النشر: 2021/1/18.

-مشتة نسرين، بن عبید إخلاص، الحماية القانونية للمعطيات الشخصية في ظل القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المجلة الجزائرية للحقوق والعلوم السياسية، جامعة تسميسيلت، الجزائر، المجلد 6، العدد 1، تاريخ النشر: 2021/6/1.

- أ/سميحة بلقاسم، أ/حميد بوشوشة، الجريمة الإلكترونية بعد جديد للإجرام في الجزائر ... واقعها وآليات مجابته، مجلة العلوم الإنسانية، جامعة أم البواقي، الجزائر، المجلد 10، العدد 1، تاريخ النشر: 2023/6/15.

-د/عائشة عبد الحميد، الإطار القانوني والتشريعي للرقمنة والذكاء الاصطناعي، المجلة الدولية للتعليم بالإنترنت، جمعية التنمية التكنولوجية والبشرية، مصر، المجلد 19، العدد 1، تاريخ النشر: 2020/7/1.

4 - الموريات :

- مجلة الشرطة، مديرية الأمن الوطني، العدد 149، تاريخ النشر: أكتوبر 2021، ص 36.

5. الروابط الإلكترونية :

-الرؤية العربية للأمن السيبراني (الواقع -التحديات - الفرص) على الرابط الإلكتروني :
https://www.mtc.gov.tn/fileadmin/user_upload/livret_Aicto_Vf.pdf

-توصيات الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية ،رمز الوثيقة
E_ESCWA_TDD_2015_1 منشور في موقع الأمم المتحدة للجنة الاقتصادية والاجتماعية لغربي أسيا

<https://archive.unescwa.org/ar/publication>

-الأمن السيبراني، على الرابط الإلكتروني :

<http://www.tra.gov.lb/Cybersecurity-AR>

-ميبار عادل فتحي عبد الحميد، تقى حامد معوض عبد الحميد، دور القيادة السياسية الروسية في تعزيز الأمن السيبراني (2012-2023)،المركز الديمقراطي العربي للدراسات الاقتصادية،الاقتصادية السياسية، مقال منشور في موقع المركز بتاريخ 2023/6/22،.على الرابط الإلكتروني :

<https://democraticac.de/?p=90695>

-د/مُحمَّد الكويتي، الأمن السيبراني في 2023: تحولات وتحديات عصر الذكاء الاصطناعي، على الرابط الإلكتروني :

معتوق أم الخير

<http://trendsresearch.org/research.php?id=>.

-لمزيد من التفصيل ينظر : كلمة السيد رئيس الجمهورية عبد المجيد تبون في إطار ملتقى وطني الاستراتيجية الوطنية للأمن السيبراني من أجل جزائر صامدة سيبرانيا . على الرابط الإلكتروني :

<https://www.aps.dz/ar/algerie>.

- مقال بعنوان : أين العرب من الأمن السيبراني ، على الرابط الإلكتروني :

<https://www.independentarabia.com/node>

- أ/ إيمان علاء الدين ، الأمن السيبراني المفهوم والتداعيات في السياسة العالمية ، مقال منشور في موقع الحضارة للدراسات والبحوث ، بتاريخ 2021/4/1 ، على الرابط الإلكتروني :

<https://hadaracenter.com/>

- د/بن مرزوق عنتر ، أ/ حرشايي محي الدين ، الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية ، مقال منشور على الرابط الإلكتروني :

<https://dspace.univ-ouargla.dz/jsui/bitstream>

-الرئيس الجزائري يحذر من مخاطر هجمات إلكترونية محتملة ، مقال منشور بتاريخ 2023/6/7 على الرابط الإلكتروني :

<https://www.alaraby.co.uk/politics/> .

-كلمة اللواء قائد الدرك الوطني مناد نوبة خلال افتتاحه لأشغال الندوة الدولية حول الأمن السيبراني المنظمة بالنادي الوطني للجيش . على الرابط الإلكتروني :

<https://www.aps.dz/ar/algerie/54821-2>

-موقع وزارة الدفاع الوطني

https://www.mdn.dz/site_cgn/sommaire/presentation/unit_spe/incc/incc_ar.php

افتتاحية مجلة الجيش الأمن السيبراني ضمن أولويات القوات المسلحة ، مقال على الرابط الإلكتروني :

<https://www.echoroukonline.com>