استمارة المشاركة في الملتقى الوطني الموسوم ب:" الامن السيبراني و رهانات الامن الشامل في الجزائر " من تنظيم كلية العلوم الانسانية –جامعة "الشهيد حمة لخضر الواد بتاريخ 13–14 ماي 2024

1 –بيانات المتدخل:

الإسم و اللقب: محمد عدار

الدرجة العلمية: دكتوراه علوم في العلوم السياسية و العلاقات الدولية

الرتبة العلمية: أستاذ محاضر "أ"

المؤسسة المستخدمة: جامعة "امحمد بوقرة" بومرداس

البريد الإلكتروني:addar2001@yahoo.fr

رقم المحور: المحور الثالث

عنوان المداخلة: الهندسة الأمنية السيبرانية الجزائرية في مواجهة الجرائم الإلكترونية

الهندسة الأمنية السيبرانية الجزائرية في مواجهة الجرائم الإلكترونية

د.عدار محمد: جامعة بومرداس

ط.د: بوشقورة هيبة:جامعة تيزي–وزو

مقدمة:

لقد سمحت عبقرية الإنسان في مجال الإبداع التكنولوجي بإدماج سريع لكل أطياف المجتمع في بيئة تكنولوجية جديدة قوامها الحاسوب الإلكتروني ، الشبكة العنكبوتية، البيانات ، البرمجيات ، المنصات، و غيرها من الأدوات التكنولوجيا التي تعرف عليها الإنسان مع بداية الألفية الثالثة .

و قد شهدت الجزائر مع مطلع الألفية إنتشار للوسائط الإلكترونية المختلفة و انخراط كل مكونات المجتمع في مسار التحديث الإلكتروني من رقمنة إدارية و تواصل اجتماعي و تطبيقات إلكترونية للنقل و السفر و التعليم ، الأمر الذي يتطلب تجهيز هذه الأدوات الإلكترونية بمناعة سيبرانية صعبة الإختراق من جهة و الاستعداد الآني لكل محاولات التعطيل أو الإتلاف أو التجسس على بيانات هذه الأجهزة.

تفرض هذه التحديات ، هندسة أمنية سيبرانية متكاملة تمزج بين التشريعات القانونية و عمل المؤسسات العسكرية و المدنية المنشئة في هذا الشأن بهدف إحباط كل محاولات التوغل الداخلية و الخارجية.

أ–**إشكالية الدراسة:** تناقش الدراسة الإشكالية التالية:

فيما تتمثل السياسة الأمنية السيبرانية الجزائرية؟ و ما هي سبل نجاعتها؟

ب–**فرضيات الدراسة:** تعتمد الدراسة على الفرضيات التالية:

الفرضية الأولى: أدى تفوق الإنسان في مجال التقنية لإنتاج عدد هائل من الأدوات الإلكترونية المتناهية الدقة.

الفرضية الثانية: كلما زاد إنتشار تكنولوجيا المعلومات في مجتمع معين ، زاد معدل الإجرام الإلكتروني .

ج-**المناهج المتبعة:** تستأنس الدراسة بالمناهج العلمية التالية:

- **المنهج التاريخي:**
- **المنهج المقارن:**

1-**التقعيد المفاهيمي لمتغيرات الدراسة:** يكون من الأجدر مفاهيميا ، تحديد متغيرات الدراسة الأساسية التي تعتمد عليها في الإجابة على الإشكالية المطروحة ، و عليه، تعتمد الدراسة على المفاهيم التالية:

أ-تعريف الفضاء السيبراني: تنتسب كلمة " cyber" للفظ اليوناني"kybernetes" بمعنى الشخص الذي يدير دفة السفينة و تستخدم مجازا للمتحكم أو القائد،و يعد -في هذا السياق-عالم الرياضيات الأمريكي "روبرت وينرز"، "Robert, wienner's"المؤسس الأول لهذا الفضاء، صاحب كتاب: السيبرنيتقية أو التحكم و التواصل في عالم الحيوان و الآلة"،" cybernitics, or control and communication in the animal and the machine" الذي يعرفه:" أنه علم القيادة و التحكم".

وبانتشار الوسائل التكنولوجيا و التقنية ، ساعد ذلك في ظهور "بيئة افتراضية "([1]) و أضحت مكونات المجتمع المختلفة من فواعل رسمية و غير رسمية مندمجة في هذه البيئة الجديدة ، مما أضفى مرونة ، سهولة و سرعة في التعاملات بين فئات المجتمع المختلفة.

يمكن القول من خلال التعريف السابق أنه أقرب للإستراتجية الدولة في صناعة القوة و التفوق ، فمعاني القيادة و التحكم مرتبطة بالجيوش و القوة العسكرية ، و عليه ، هناك من يربط بين الفضاء السيبراني و الجيوش الحديثة ، فبعد البر ، البحر، الجو و الفضاء ، بدأت التصورات النظرية للإستراتجيات الحديثة للجيوش تأخذ بعين الإعتبار الفضاء السيبراني البيئة الجديدة للحروب المستقبلية([2]).

([1]) بوازدية ، جمال ، الأمن السيبراني محاضرات مقدمة لطلبة السنة الثانية ماستر (تخصص: دراسات إستراتيجية و أمنية)(الجزائر: كلية العلوم السياسية و العلاقات الدولية، 2021)ص 8.

([2]) عباس ، بدران ، الحرو الإلكترونية : الإشتباك في عالم متغير (بيروت: مركز دراسات الحومة الإلكترونية ، 2010) ص 4.

ومع تطور ابتكارات الإنسان في المجال التكنولوجي المادي ، أصبح الفضاء السيبراني مفاهيميا أقرب للجوانب المادية ، حيث عرفته:

تعريف الوكالة الفرنسية لأمن أنظمة الإعلام(anssi): تعرف الوكالة الفرنسية لأمن انظمة الإعلام ، الفضاء السيبراني على أنه "هو فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية." ([3]).

و في سياق آخر، و إن كان تعريف الوكالة الفرنسية يتطلب توفر العناصر المادية لإستحداث البيئة الإفتراضية ، فإن تعريف الإتحاد الدولي للإتصالات يشمل العناصر المادية و غير المادية في البيئة الرقمية ، حيث أصبحت البيانات ، البرمجيات ، المعلومات المحوسبة و المحتويات و غيرها من العناصر اللامادية التي تدخل ضمن مستلزمات البيئة الرقمية و على هذا الأساس نورد تعريف الإتحاد الدولي للإتصالات .

تعريف الإتحاد الدولي للاتصالات(int): يعرف الإتحاد الدولي للإتصالات ، الفضاء السيبراني على أنه " المجال المادي و غير المادي الذي يتكون و ينتج عن عناصر هي: أجهزة الكمبيوتر، الشبكات ، البرمجيات ، حوسبة المعلومات ، المحتوى ، معطيات النقل و التحكم و مستخدموا كل هذه العناصر." ([4])

و من التعريفين السابقين للفضاء السيبراني (تعريف الوكالة الفرنسية لأنظمة الإعلام/تعريف الإتحاد الدولي للإتصالات) نخلص إلى التعريف الإجرائي التالي :

تعريف الفضاء السيبراني: هو بيئة تفاعلية حديثة تتضمن عناصر مادية و غير مادية ، يشترك فيها كل أطياف المجتمع رسميين(مصالح حكومية، شركات ، قادة،.....) أو غير رسميين(افراد) استعمالا و تشغيلا.

([3])اسماعيل ، زروقة ، الفضاء السيبراني و التحول في مفاهيم القوة و الصراع، **مجلة العلوم القانونية و السياسية** ، المجلد 10، العدد01، أفريل 2019، ص 10174.

([4]) The International Telecommunication nion(int) , Tool kit for cybercrime ligeslation, Geneva, 2010, p12

ب-**<u>تعريف الجريمة الإلكترونية:</u>** على الرغم من إتاحة تكنولوجيا المعلومات فرصا هائلة للإنسان المعاصر ، فأصبحت يومياته أكثر سهولة، و ذلك من خلال توظيف البنية التحتية للوسائط الإلكترونية .

غير أن استعمالات الإنسان لهذه الوسائط لا يخلو من أخطار و تهديدات تطال الدول و الأفراد على حد السواء ، حيث أصبح السطو الإلكتروني و تعطيل أنظمة الشركات و المؤسسات و الابتزاز المالي للأفراد ، التجسس على بيانات حساسة لدولة ما من التهديدات الإلكترونية التي تتطلب الاستعداد أكثر من أي وقت مضى لها.

و تجدر الإشارة إلى أنه لا يمكن-إجرائيا-وضح تسمية مناسبة للتهديدات الناتجة عن استخدام الوسائل التكنولوجية ، فمن الباحثين من يوظف: مصطلح الجريمة الإلكترونية، الجريمة المعلوماتية، جرائم إساءة إستخدام تكنولوجيا المعلومات و الإتصال و جرائم الكمبيوتر و الإنترنيت.

و بإختلاف المصطلحات ، تتباين التعريفات([5]) المهتمة بالجريمة الإلكترونية ، حيث يمكن تناول تعريف الجريمة الإلكترونية من الزوايا العلمية التالية:

- **<u>التعريف الذي يركز على الجوانب التقنية:</u>** يمكن تعريف الجريمة الإلكترونية على أنها:"نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود"([6]).

يحصر هذا التعريف الجريمة الأكترونية في الأبعاد التقنية و إغفال باقي عناصر التجريم التي ياتي ذكرها لاحقا.

- **<u>التعريف الذي يركز على الجوانب القانونية:</u>** يرى أنصار هذا التعريف أن التعرف على الجريمة الإلكترونية مقرون بتوفر مجموعة من المفردات الضرورية المتعلقة بارتكاب جرائم الحاسب الآلي و هي: الحاسب الآلي ، برنامج الحاسب الآلي ، البيانات ، الممتلكات ، الدخول و الخدمات.

([5]) مجمع البحوث و الدراسات الأكاديمية السلطان قابوس لعلوم الشرطة ، الجريمة الإلكترونية في المجتمع الخليجي و سبل مواجهتها (الرياض: أكاديمية نايف للعلوم الأمنية ، 2016) ص20.

([6]) مرجع سابق، ص 20.

و منه يمكن تعريف الجريمة الإلكترونية على "أنها الجريمة التي تقع بواسطة الحاسب الآلي أو عليه أو بواسطة شبكة الأنترنيت."

يعتقد أصحاب الفقه القانوني أن الجريمة الإلكترونية قد تسارعت وتيرتها في الأونة الأخيرة ، فهي عابرة للحدود ، تعجز التشريعات الوطنية و الدولية في الإحاطة بحيثياتها و يفتقد فيها العنف المادي مقارنة بالجرائم التقليدية و أن أدلتها سهلة الإتلاف.

- **التعريف الذي يركز على بيئة وقوع الجريمة:** يتمثل القصور الذي وقع فيه أنصار الجوانب القانونية في تجاهل و إهمال مكان أو بيئة وقوع الجريمة و هي "الشبكة العالمية للمعلومات"، حيث يعد الفعل الالكتروني إجراميا لما يتعلق الأمر" بتعطيل الشبكة أو العمل على إبطاء سرعتها أو إتلاف المواقع عليها"([7]).
- **التعريف الذي يركز على الوسيلة:** حيث يعرف الفقيه الألماني "تاديمان" ([8])الجريمة الألكترونية على أنها:" كل أشكال السلوك غير المشروع أو الضار بالمجتمع و الذي يرتكب بإستخدام الحاسب الآلي".
- **التعريف الذي يركز على الجوانب الموضوعية:** بمعنى وقوع الجريمة الالكترونية داخل نظام الحاسب الآلي ، و عليه ، يمكن تعريفها على أنها"نشاط غير مشروع لنسخ أو تغيير أو حذف أو الوصول إلى

المعلومات المخزنة داخل الحاسوب أو التي ترسل عن طريقه.([9])"

- **التعريف الذي يركز على الجوانب المعرفية و الفنية للجريمة الإلكترونية:** تعرف الجريمة الأكترونية على أنها أية "جريمة يكون متطلبا لإقترافها أن تتوفر لدى فاعلها معرفة بتقنية الحاسب الآلي"([10]) .
- **التعريف الذي يركز على المعلومات:** يقصد بالجريمة الإلكترونية "كل فعل أو إمتناع عمدي ينشأ غن الإستخدام غير المشروع للتقنية المعلوماتية و يهدف إلى الإعتداء على الأموال المادية أو المعنوية.

([7]) مرجع ، سابق، ص 20 .

([8]) مرجع سابق ، ص 21.

([9]) مرجع سابق ، ص 22.

([10])عبد الفتاح بيومي، حجازي، مكافحة جرائم الكمبيوتر و الإنترنيت في القانون العربي النموذجي (القاهرة: دار الفكر الجامعي ، 2006) ص 25.

نستنتج مما سبق أن الدراسة توظف مصطلح "الجريمة الإلكترونية" باعتبار أن وقوع الفعل الإجرامي يتم بالإستعانة بالعناصر الالكترونية المادية و التي مقدمتها الحاسب الآلي أو أي أداة الكترونية أخرى أفرزتها الثورة المعلوماتية، إضافة إلى أن الفعل الإجرامي يطال التطبيقات المتضمنة في الحاسب الآلي كتعطيل البيانات أو التجسس عليها أو إتلافها .

ينم الفعل الإجرامي عن تدريبات أو توصيات يكون مخربوا هذه التطبيقات قد اطلعوا عليها و حاولوا تطبيقها على الشبكة المعلوماتية .

- **<u>أنواع الجرائم الإلكترونية</u>:** تتمثل الجرائم الإلكترونية في النشاطات الرقمية التالية:

التعدي على الأنظمة المعلوماتية /الجرائم الواقعة على الأموال/التعدي على الملكية الفكرية للأعمال الرقمية/البطاقات المصرفية و النقود الإلكترونية/جرائم تمس المعلومات الشخصية /جرائم ضد الإنسانية بوسائل معلوماتية و الجرائم المعلوماتية ضد الدولة و السلامة العامة.

تمثل هذه الأنواع مجمل الجرائم التي هي موضوعات للمواجهة في إطار الأمن السيبراني ، حيث تعمل الفواعل الرسمية (الدول، الشركات،....) و غير الرسمية (أفراد) على الحد من استفحال ظاهرة الإجرام الإلكتروني عبر العالم.

<u>ج-خصائص الجرائم الألكترونية</u>: تتميز الجرائم الإلكترونية عن الجرائم التقليدية بالمكان الذي ترتكب فبه هذه الجرائم و الأدوات المستعملة في تنفيذ الجريمة ن فالبيئة الإفتراضية و الحواسيب هما من أركان الفعل الإجرامي أضافة لتوفر حد أدنى من الثقافة التقنية للجاني .

و تتميز الجرائم الإلكترونية ب([11]):

- تتم الجرائم بواسطة الحواسيب كأدوات لارتكاب الجريمة أما الانترنيت فهي وسيلة الفعل.
- لا يتم في العادة التبليغ عن الجرائم الإلكترونية تفاديا للإساءة أو الإحراج.
- جرائم صعبة الإدراك بحكم صعوبة تحديد الجاني و عدم تركها لآثار مادية.
- جرائم غامضة تفتقد للإثبات المرئي.

([11])مهدي، رضا، الجرائم السيبرانية و آليات مكافحتها في التشريع الجزائري ، **مجلة إيليزا للبحوث و الدراسات** ، المجلد06 ، العدد02 ، 2021، ص 114.

- جرائم عابرة للحدود و نتائجها تمس عدة أقاليم.
- جرائم تتطلب قدر من الإلمام بقواعد التقنية.
- جرائم تفتقد لتوظيف العنف المادي–الجسدي.

د–**تعريف الأمن السيبراني:** تتطلب مواجهة الجريمة الإلكترونية ، الإحاطة بمتطلبات تحقيق سياسة أمنية قائمة على تفعيل وسائل الحماية ، حيث يعد الأمن السيبراني المدخل الجوهري لمواجهة اخطار الجريمة الإلكترونية.

فالأمن السيبراني هو مصطلح مركب من كلمتين : أمن و سيبراني

- **التعريف اللغوي للأمن:** الأمن هو نقيض الخوف، و مصدر للفعل أمن ،أمنا و أمانا و يعني اطمئنان النفس و سكون القلب و زوال الخوف و يقال: أمن من الشر أي سلم منه.
- **التعريف اللغوي لكلمة سيبراني:** يمكن تعريف تشير كلمة سيبراني لغويا للعناصر التالية:

العناصر المادية مثل: الحاسوب ، لوحات الكترونية ، هواتف محمولة أجهزة نانوية و غيرها من الأدوات الإلكترونية التي اخترعها ضمن مسيرة التفوق و العبقرية و التي تساهم في تسهيل مناحي الحياة.

كما تشتمل الكلمة على العناصر غير المادية كالانترنيت ، البرمجيات و التطبيقات المختلفة المعروفة في التواصل كالواتساب و الفيسبوك و غيرها من التطبيقات .

ينتج عن العلاقة بين العناصر المادية و اللامادية توفر خدمات إلكترونية كالدفع الآلي ، الشراء الآلي ،. التحويل الآلي للمعطيات و البيانات و غيرها من الخدمات التي توفرها الشبكة العنكبوتية لمستعمليها.

- **التعريف الإصطلاحي للأمن السيبراني:** يمكن القول في البداية أنه بالنظر لأهمية مصطلح الأمن السيبراني ، فقد كان محل تعريف من قبل هيئات رسمية تابعة لدول و مؤسسات عالمية ، كما ساهم كتاب في وضع تعاريف متباينة مرتبطة من زاوية النظر أو الرأي التابعة لمفكر أو آخر.
  - **تعاريف الهيئات الرسمية:** من الهيئات الرسمية التي ساهمت في وضع تعريف للأمن السيراني ، نجد:

- **تعريف وزارة الدفاع الأمريكية :** عرفت وزارة الدفاع الأمريكية مصطلح الأمن السيبراني على أنه:"جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية و الإلكترونية من مختلف الجرائم : الهجمات ، التخريب، التجسس و الحوادث.

نسنتنج من تعريف وزارة الدفاع الأمريكية أنه يركز على ضرورة مجابهة التهديدات السيبرانية المختلفة التي قد تطال المعلومات من تخريب و تجسس و غيرها عن طريف اتخاذ جميع الإجراءات من دون الإشارة إلى نوعها، و يتقارب تعريف وزارة الدفاع الأمريكية مع تعريف الإعلان الأوروبي الذي يركز على التصدي لكل حاولات الإختراق التي تستهدف بيانات و معلومات الشركات و الأشخاص.

- **تعريف الإعلان الأوروبي:** عرف الإعلان الأوروبي، الأمن السيبراني على أنه :" قدرة النظام المعلوماتي على مقاومة محاولات الاختراق التي تستهدف البيانات.
  - **تعاريف الهيئات الدولية:** عرف الإتحاد الدولي للإتصالات في تقريره الصادر في 2010-2011، الأمن السيبراني على أنه : مجموعة من المهمات : مثل تجميع وسائل و سياسات و إجراءات أمنية و مبادئ توجيهية و مقاربات لإدارة المخاطر و تدريبات و ممارسات فضلى و تقنيات يمكن استخدامها لحماية البيئة السيبرانية و موجودات المؤسسات و المستخدمين."

يركز الإتحاد الدولي للاتصالات في تعريفه للأمن السيبراني على العناصر التالية:

-**عناصر موجهة للأفراد(الكادر المستخدم):** تدريب الأفراد و مستخدمي الأنترنيت على كيفيات التعامل مع بيئة المخاطر الجديدة .

- **عناصر أكاديمية:** ضرورة التزود بالمقاربات النظرية و المبادئ التوجيهية لضمان سلامة البيانات، موجودات المؤسسات و المستخدمين.

-**عناصر أمنية**:الاستنجاد بالإجراءات الأمية الضرورية لحماية البيئة الافتراضية.

  - **التعاريف الأكاديمية للكتاب:** من التعاريف الأكاديمية للكتاب و الباحثين ، نورد مايلي:

- **<u>تعريف أدوارد اموروزو :</u>** يعرف أموروزو الأمن السيبراني على أنه :" وسائل ممن شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات و تشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة و كشف الفيروسات ووقفها و توفير الاتصالات المشفرة"([12]).

يركز أمروزو على وسائل المجابهة من خطر الجريمة السيبرانية و الأدوات التي من شأنها كشف الفيروسات و مواجهة القرصنة و توفير الإتصالات المشفرة.

<u>تعريف الكاتبان:</u> **<u>" Martti Lahto, Pekka, Neittaanmaki</u>** ":" مجموعة من الإجراءات التي إتخذت للدفاع ضد هجمات قراصنة الكمبيوتر و عواقبها و يتضمن تنفيذ التدابير المضادة المطلوبة"([13]).

يركز الكاتبان على جملة الإجراءات المتكاملة التي تتسلح بها الدول و الشركات للدفاع عن قراصنة الكمبيوتر.

<u>تعريف Richard ; A.kemmerer</u>: عبارة عن وسائل دفاعية من شأنها كشف و إحباط المحاولات التي يقوم بها القراصنة."

يرى ريتشارد كامرر على ضرورة إعداد وسائل دفاعية ذات منشأ تقني لإحباط كل محاولات القرصنة التي بات مرتكبوها (القراصنة) يوظفونها لتهديد مستخدمي و مستعملي الشبكة العنكبوتية.

يمكن القول في الأخير أن الأمن السيبراني هو مجموعة الآليات و الإجراءات و الوسائل و الأطر الهادفة لحماية أجهزة الكمبيوتر و البرمجيات من مختلف التهديدات السيبرانية التي تقوض نشاط الفواعل.

<u>2-المصطلحات المتقاطعة مع الأمن السيبراني:</u> يتقاطع مصطلح الأمن السيبراني مع المصطلحات التالية ذات العلاقة:

<u>الردع السيبراني:</u> منع الأعمال الضارة ضد الأصول الوطنية في الفضاء السيبراني.

([12])منى عبد الله ، السمحان، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود ، مجلة **كلية التربية**،العدد111، جويلية2020، ص 10.

([13]) بن مرزوق، عنترة، الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية ،**مجلة العلوم الإجتماعية** ، المجلد 19، العدد01، 2018، ص66.

الهجمات السيبرانية: هو سلوك يقوض من قدرات شبكات الكمبيوتر لغرض قومي أو سياسي من خلال استعمال نقطة ضعف معينة تمكن المهاجم من التلاعب بالنظام.

الجريمة السيبرانية: مجموعة الأعمال و الأفعال غير القانونية التي تتم عبر معدات أو اجهزة إلكترونية.

3-أهمية الأمن السيبراني: تكمن أهمية الأمن السيبراني في النقاط التالية:

-الحفاظ على المعلومات و سلامتها.

-حماية الأجهزة و الشبكات من الإختراقات و التعطيل .

-إكتشاف نقاط ضعف الأنظمة و معالجتها.

-توفير بيئة سيبرانية آمنة خلال استخدام الشبكة العنكبوتية.

4-**أهداف الأمن السيبراني:** تتمثل أهداف الأمن السيبراني في:

-صمود البنى التحتية الحساسة للهجمات الإلكترونية.

-الحد من التجسس و التخريب الإلكتروني على مستوى الحكومة و الأفراد.

-سد الثغرات في أنظمة امن المعلومات.

-تدريب الأفراد على آليات و إجراءات مواجهة الإختراقات المتعلقة بأجهزتهم سواء بالإتلاف أو بالسرقة.

-الحد من التجسس و التخريب الإلكتروني على مستوى الحكومة و الأفراد.

4-مكان الفرد في الفضاء السيبراني: مع الاعتماد المتزايد في الحياة اليومية على الأنظمة المعلوماتية و الأجهزة المتصلة بالشبكة الدولية للمعلومات و تشعب طبيعة هذه الأجهزة من هواتف خلوية و أجهزة حوسبة فردية ، و يزداد عدد المتعاملين بالفضاء السيبراني لدرجة الارتباط العضوي بين الفرد و الأداة الإلكتروني.

و تشير التقديرات أنه في الفترة الممتدة من 2014إلى 2018 ، انتقل عدد مستخدمي الإنترنيت من 2.8 مليار مستخدم إلى 3.8 مليار مستخدم ([14])، و سيعرف المزيد من حالات اندماج الأفراد في البيئة الافتراضية بحكم أن ممارسة نشاطات الإنسان الأساسية ، أصبحت تأديتها من خلال الفضاء السيبراني و عليه، يمثل الفرد داخله حلق أساسية باعتباره مستخدم يستفيد من المرونة و السهولة التي توفرها الإنترنيت في تحقيق أهداف الإنسان المختلفة ، كما تمثل في نفس الوقت تحديا للإنسان ذاته مع تزايد معدلات الجريمة الإلكترونية من قذف، ابتزاز ، احتيال و انتحال الشخصية و غيرها من التعاملات السلبية التي قد يتعرض لها الإنسان.

5-أبعاد الأمن السيبراني : تتمثل أبعاد الأمن السيبراني في:

أ-البعد السياسي: لقد أصبحت مختلف أجهزة الدولة معتمدة على التكنولوجيا في تصريف نشاطاتها و صارت "البيئة الرقمية" هي الفضاء الجديد في التعامل الإداري، الاقتصادي ، القضائي و حتى الاتصالي ، إذ بات العديد من قادة العالم يخاطبون شعوبهم عن طريق منصات التواصل المختلفة : فيعبرون عن نشاطات معينة تهم إقليم الدولة التي ينتمون إليها أو حتى انشغالات عالمية عن طريق استخدام شبكات الاتصال و الإعلام .

إن التحول الرقمي الحاصل في العالم ، بقدر ما سهل التنسيق و الإنسجام بين مؤسسات الدولة المختلفة و أضفى مرونة في طريقة تسيير المرافق المختلفة ، بدأت العالم يتجه نحو تهديدات جديدة تفوق التهديدات التقليدية أين أصبح "الفضاء السيبراني" هو ميدان المعركة الخامس([15]) الذي قد يقوض كيانات الدول و يجعل مؤسساتها خارج الخدمة أو تدمير لبيتها التحتية و غيرها من الهجمات السيبرانية التي قد تكون الدولة عرضة لها.

و عموما ، يمكن ذكر مجموعة من العوامل ، ساهمت في بروز الحروب السيبرانية :

([14]) حسين قوادرة ، منى كحلوش ، التداعيات الاقتصادية لحرب المعلومات السيبرانية ، **مجلة الناقد للدراسات السياسية** ، المجلد 05، العدد 01 ، 2021، ص207.

([15]) شريفة كلاع ، الأمن السيبراني و تحديات الجوسسة و الاختراقات الإلكترونية للدول عبر الفضاء السيبراني ، **مجلة الحقوق والعلوم الإنسانية** ، المجلد15 ،العدد01، 2002، ص 299.

–تزايد ارتباط دول العالم بالفضاء السيبراني ، مما يجعل البنية التحتية للدول أكثر عرضة للهجمات السيبرانية.

–تراجع دور الدولة في الجوانب الإقتصادية ، وبروز الشركات، خاصة تلك العاملة في المجال الإلكتروني كفاعل مؤثر في البيئة السيبرانية.

–قلة تكلفة الحروب السيبرانية مقارنة بنظيرتها التقليدية ، حيث أن الحروب السيبرانية لا تتطلب الوقت الكثير لتنفيذها.

–توظيف الفضاء السيبراني في تعظيم دور الدولة من خلال العمل على إبراز التفوق في إعداد الإستراتيجية السيبرانية للدولة.

–اتساع نطاق مخاطر الأنشطة التي يقوم بها الفاعلون سواء من الدول أو من غيرهم ، فقد تشن الهجمات السيبرانية عبر الأجهزة الأمنية السيبرانية التابعة للدولة أو عبر قراصنة أو عملاء لاستهداف بيانات الخصوم .

أدت هذه العوامل لجعل الدول عرضة لهجمات سيبرانية ، خاصة إذا اعتبرنا كل دولة تملك قدرات و إمكانيات المواجهة تختلف عن تلك الموجودة لدى دولة أخرى ، غير أن ذلك لا يمنع في جعل الهجمات السيبرانية على الدول تشترك في العناصر التالية:

استهداف البنية التحتية للدول: تكون البنى التحتية للدول و المرافق الحيوية فيها ، مدنية و عسكرية،عرضة لهجمات سيبرانية ، فتشل أنظمتها و يتعطل نظام تشغيلها ، فتضطرب يوميات المواطن و تسود الفوضى في إقليم الدولة ([16]).

و من أمثلة الهجوم الالكتروني الذي يستهدف الدول ما تعرضت له شبكة المياه الأوكرانية و الذي سبب في بقاء أوكرانيا لساعات في الظلام ، مما يوحي أن الهجمات الإلكترونية قد تخطت حاجز البيانات و المواقع الإلكترونية لتشمل البنية التحتية و الأنظمة الحيوية للدولة كالمفاعلات النووية ، أنظمة الكهرباء، الأنظمة الطبية و غيرها من البنى الحيوية للدولة.

([16]) أميرة عبد العظيم محمد ، عبد الجواد، المخاطر السيبرانية و سبل مواجهتها في القانون العام ، **مجلة الشريعة و القانون** ، ج3 ، العدد 35، 2020، ص 415.

كما وقعت الحكومة الإستونية في 2007م ضحية لهجمات سيبرانية من قبل مجموعات روسية نتيجة قيام الحكومة بإزالة تمثال الجندي البرونزي و جثث جنود روس سقطوا أثناء الحرب العالمية الثانية من حديقة عامة في "العاصمة تالين".

استهدف الهجوم السيبراني في الأول و تحت مسمى"الحرمان من الخدمة"،"DDoS"الوزارات الحكومية ، البنوك و مقرات الأحزاب السياسية و في موجة ثانية تم تعطيل الخوادم الخاصة و الصحف . فتأثر الإقتصاد الإستوني و تعطلت يوميات السكان و أصبحت الأنظمة المعلوماتية للبنية التحتية لإستونيا في يد هذه المجموعات ، مما يؤثر على علاقة الأفراد بنظامهم السياسي و ارتهان سيادة الدولة.

من أشهر الهجمات السيبرانية التي استهدفت البنى التحتية للدول ، ما تعرض له خط أنابيب النفط التركي بتاريخ 05أوت 2008م حيث اشتعلت النيران من دون انذار مبكر عن الحادث من طرف المستشعرات الإلكترونية الموضوعة لذلك .

يندرج هذا الهجوم السيبراني من زاوية العلاقات الدولية ضمن معارضة روسيا لإنشاء خط أنبوب للغاز يضم الثلاثي:باكو–تبليسي–جيهان ، بحكم أن هذا المشروع الجديد يقع خارج الدائرة الروسية و بالتالي تقويض قدرتها في التحكم في تدفق الطاقة لأوروبا([17]).

كما كانت محطات التزود بالكهرباء–في 2008– في البرازيل عرضة لهجمات سيبرانية ، حيث تمكن القراصنة من الدخول إلى الموقع الشبكي للحكومة و السيطرة عليه لمدة تزيد عن أسبوع ن حيث أن الإنقطاعات المتكررة للكهرباء في البرازيل هي نتيجة لهجوم سيبراني، و نفس المشهد، تعرضت له شركة الكهرباء في الولايات المتحدة الأمريكي.

شهدت السعودية هجوما سيبرانيا عنيفا ، في 2017م نفذه سيبرانيون إيرانيون يدعى "الصخرة الدوارة"،"Stone , Drill" حيث أحدث تأثيرات كبيرة على شركات الطيران و البيتروكيمياويات السعودية ، كما مارس–في نفس السياق–قراصنة إيرانيون هجمات سيبرانية متقدمة تحمل اسم:A.P.T ، إستهدفت بنى تحتية لدول الخليج .

([17]) شريفة ، كلاع، **مرجع سابق**، ص 301.

و شهدت إيران سلسلة من الهجمات السيبرانية ، طالت البنية التحتية لهذا البلد بهدف تقويض لقدراته الصناعية و اتجاهه نحو امتلاك السلاح النووي و تمثلت الهجمات السيبرانية في:

-هجوم سيبرانا بتاريخ 2 جويلية 2020م استهدف مفاعل "نتانز" النووي.

- هجوم آخر بتاريخ 4 جويلية ، حدث انفجار في محطة "شهيد مدح زرقان".

- هجوم الكتروني في 7 جويلية تعرض مصنع الأوكسجين في بلدة"باقر" .

-هجوم سيبراني استهدف منشأة صواريخ تابعة للحرس الثوري الإيراني في 9 جولية 2020.

-انفجار غاز مبنى سكني في طهران بتاريخ 11 جويلية.

-شهد" مصنع توند جويان" للبتروكيمياويات الإيراني تفجيرات مرعبة سببها هجمات سيبرانية.

-عرف مجمع صناعي ايراني انفجار في 13 جويلية و حريق في مصنع الالمنيوم في بلدة "لامرد" الإيرانية و انفجار في خط انابيب نفط في "الاهواز" في 18 جويلية و انفجار في محطة توليد الطاقة في "اصفهان" .

وقد قامت مجموعة من القراصنة "المنتقمون"الايرانية بهجوم سيبراني استهدف شبكة المياه و الكهرباء الاسرائلية في 16 جويلية2020.

يمكن القول أن البنى التحتية لمختلف الدول تمثل الأهداف المثلى للهجمات السيبرانية نظرا لما تخلفه هذه الاعتداءات من انكشاف أمني للدولة من جهة و قلق و خوف لدى الساكنة.

-**<u>فقدان الثقة بين أجهزة الدولة:</u>** تؤدي الهجمات السيبرانية التي تقوم بها الدفاعات الأمنية للدولة ضد البنى التحتية لدولة مناوئة لتدني درجة الوثوقية لدى أجهزة و مصالح الدولة المختلفة .

معروف على الدولة قوة أداء نظامها السياسي و التزامها القانوني بتعهداتها تجاه مواطنيها في المجال الداخلي حيث تلتزم بتوفير الحماية والسكينة و الأمن للأفراد داخل اقليم الدولة، فبتعرض أحد منشآت الدولة للتخريب الأرهابي أو الالكتروني يكون عى عاتق تلك الدولة صد تلك الهجمات من جهة و ضمان عودة نشاط تلك الأجهزة للخدمة في وقت وجيز و ذلك حتى تحافظ الدولة على درجة الوثوقية بينها و بين مواطنيها و حتى بين الدولة و الشركاء الأجانب لاسيما في المجال الاقتصادي. و نظرا لتفاوت مستوى

التصدي للهجمات السيبرانية ، قد يتعرض النظام السياسي لدولة ما لفقدان الثقة بينه و بين مواطنيه إذا أظهر عجزا في مواجهة تلك التهديدات ، و عليه ، يقع على عاتق الدولة تحديث أجهزتها الإلكترونية بانتظام لتفادي اي طعن في مشروعية النظام السياسي.

ب-البعد الإقتصادي لقد أضحت الأسواق المالية -بفضل أنظمة حماية الشبكات الإلكترونية-أكثر اتصالا ببعضها البعض من ذي قبل ، فللمؤسسات المالية قدرة على تبادل رؤوس الأموال الكترونيا و في ظرف وجيز.

غير أنه و في نفس السياق ، تعتبر القطاعات الاقتصادية و المالية أكثر عرضة للهجمات السيبرانية التي من المحتمل تزايدها في المستقبل، فالمصاريف المالية ، قطاع التأمين ، شركة الطيران،مؤسسات الفندقة هي عبارة عن أهداف سيبرانية لما وصفته الحكومة الأمريكية "هجوم الفدية "،"ransom war"، ووفقا لتقديرات مكتب التحقيقات الفيدرالي الأمريكي فإنه يرى أن مبلغ الفدية يقترب من مليار دولار سنويا و ان الشركات التجارية تقع ضحية هجومات سيبرانية كل 14 ثانية خاصة إذا إعتبرنا أن عام 2018 هو عام الإختراقات الإلكترونية.

لقد أصبحت الهجمات السيبرانية أكثر تكلفة بالنسبة للمؤسسات المصرفية والمالية ، ففضلا عن الخسائر المالية التي تعدت 80 مليار دولار خلال الهجمة السيبرانية الواحدة، تتسبب هذه الهجمات في فقدان الثقة لدى العملاء مما قد يؤدي لسحب الودائع و حصول أزمة سيولة .

أصبح الاقتصاد العالمي يتكبد نتيجة الهجمات السيبرانية ما يتجاوز 230 مليار دولار، بمعدل 1000 هجمة كل دقيقة ، أين تكون المؤسسات المالية هي الهدف الأول لهذه الهجمات ن مما يتطلب تجديد و تفعيل لبرامج الكشف المبكر عن الهجمات و استباق حدوثها من قبل الدول ، و من التجارب ، يمكن ذكر([18]):

-التجربة الإفريقية: تم تأسيس "اتفاقية الأمن الإلكتروني و حماية البيانات الشخصية" أو "اتفاقية مالابو" التي بموجبها تم وضع الحد الأدنى من المعايير و الإجراءات لبناء بيئة رقمية موثوقة بهدف ضمان احترام الخصوصيات على الأنترنيت.

([18])دراعو ، عزالدين،الآثار الإقتصادية و المالية للهجمات السيبرانية في ظل بالتحول الرقمي : النتائج ، التجارب و الحلول -مع الإشارة لحالة الجزائر-**مجلة التكامل الإقتصادي**، المجلد10 ، العدد02، جوان2022، ص119.

-**التجربة الصينية:** تبنى البرلمان الصيني في 2016م القانون الجديد الأمن السيبراني الذي دخل حيز النفاذ في 2017م الذي يحدد مهام القطاعات الحكومية تجاه تأمين الشبكات و البيانات ، كما تضمن القانون كيفيات ضبط و مراقبة مزودي الأنترنيت ، كما يجبر القانون-تحت اسم" الجدار الناري العظيم- مختلف الشركات و المؤسسات بوضع برامج حماية ضد الهجمات السيبرانية إلى مستوى قد يصل إلى حجب بعض المواقع المتسللة إلى الكيانات الإقتصادية الصينية.

-**التجربة الأمريكية:** قامت الولايات المتحدة الأمريكية في 2014م بإطلاق "برنامج العمل لتحسين الأمن السيبراني للبنية التحتية الحساسة" الذي يقوم على الجانب التطوعي-موجه للشركات و المؤسسات المالية- من أجل حماية ممتلكاتها المعلوماتية من أي إختراق سيبراني ، و حسب الإحصائيات ، فإن 30% من المؤسسات الأمريكية قد انخرطت في هذا البرنامج.

وفي ماي2020م تم إصدار أمر رئاسي لتحديث الخدمات السحابية لمختلف الوكالات الفيدرالية و تطوير برنامج تدريب متخصصين يقضي بمراجعة تقنيات السلامة السيبرانية و الكشف المبكر عن الثغرات الأمنية.

-**التجربة الأوروبية:** تعمل المفوضية الأوروبية -ضمن برنامج توجيه الشبكات و أمن المعلومات-على تحديث قواعدها للأمن السيبراني عبر العناية بالقطاعات الحساسة كالصحة و الدفاع.

و على صعيد الدول ، تمكنت بريطانيا من إحباط 250 هجوم سيبراني بفضل يقظة مكتب الاتصال الإلكتروني ووزارة الدفاع البريطانية ، في حين قامت ألمانيا بتحديث أنظمة حماية الشبكات و صيانتها.

ج-البعد العسكري: إن لجوء الدولة إلى الشبكة الإلكترونية من أجل خلق بيئة افتراضية يسهل التعامل من خلالها بين مختلف المصالح و الهيئات من جهة و ضمانا لخدمة نوعية و عصرية و سريعة لمختلف البيانات و المعلومات التي ترد إلى هذه الهيئات غير أنه أحيانا ، قد تقع هذه البيانات فريسة لقراصنة إلكترونيين يعملون على تعطيلها، التلاعب بها أو إتلافها ن الأمر الذي يصنع تحديات أمام الدولة من الجانب العسكري ، تتمثل في:

التجسس الألكتروني: يعني التجسس الإلكتروني([19]) تلك المحاولات المتعمدة لاختراق أجهزة الكمبيوتر التابعة لدولة خصم بهدف سرقة معلومات سرية في ميادين سياسية ، اقتصادية ، اقتصادية و أمنية – عسكرية .

يعمل التجسس على تسريب معلومات سرية لدى دولة ما و استغلالها لمصلحة دولة معينة ، فمثلا استطاع "هاكرز مجهول الهوية من النفاذ لجهاز معلومات أحد متعاقدي الجيش الأمريكي و سرقة آلاف الملفات الخاصة بالمقاتلة "أف–35"، كما أن سرقة المعلومات الاقتصادية لدولة ما قد تؤثر على مواقفها التفاوضية بين الدول ، و قامت وكالة الأمن القومي الأمريكي بالتجسس على أجهزة معلومات أكثر من 35 شخصية سياسية بارزة عبر العالم و تحصلت على معلومات ، نتيجة تجسسها على أكثر من 60 مليون مكالمة عبر العالم الأمر الذي يوحي بأنة عملية التجسس لا تشمل فقط رعايا الدولة المناوئين بل تتجاوز حدود الدولة لتشمل أفراد في العالم و الدليل ما خلفه "برنامج بيقاسوس"،"pigasus project"

من جو عدم الثقة و تقويض الأمن و السلم العالميين ، فللعلم أن هذا البرنامج طورته شركة" groupe NSO "الإسرائلية التي تقوم على اختراق مليارات الهواتف التي تعمل بنظام تشغيل الأندرويد أو ios و تزداد قوة هذا البرنامج عند اعتماده على هجمة "صفر نقرة" فحتى أذا لم يشغل المستخدم جهازه ، يستطيع هذا البرنامج اختراقه، حيث تعرض ألاف الصحافيين و النشطاء و حتى قادة دول للإختراق عن طريق هذا البرنامج .

السيطرة على الانظمة العسكرية و تعطيلها أو اتلافها: كأن يقوم قراصنة محترفين أو جيوش نظامية بشن هجوم سيبراني يهدف للسيطرة على نظم القيادة و السيطرة العسكرية التابعة لدولة ما و اخراجها عن دائرة تحكم القيادة المركزية و إعادة توجيهها نحو اقليم الدولة أو ضد دول صديقة ، كما تستهدف الهجمات :طائرات بدون طيار ، الغواصات النووية و حتى الأقمار الصناعية العسكرية يمكن اخراجها– عن طريق هجمات سيبرانية–من مداراتها و تحكم الدول التابعة لهاو استغلال معلوماتها .

و من الأمثلة التي تدل على سرقة تصميمات عسكرية للدول ما تعرضت له شركة "لوكهيد–مارتين" الأمريكية من سرقة لبرامج تصميم المقاتلة "اف–35" لتستفيد منها الصين في تصميم المقاتلة"تي20".

([19]) ربيعي ، حسين ، سمر محمود ، الحروب السيبرانية: المخاطر و استراتيجيات تحقيق الأمن السيبراني الدولي و الداخلي ، **المجلد الجزائرية للأمن الإنساني**، المجلد 07، العدد02 ، السنة السابعة ، جويلية2022، ص 182.

كما تعرض مقاولون تابعون لوزارة الدفاع الأمريكية يعملون في مجال تصنيع طائرات بدون طيار للإختراق بهدف سرقة برامجهم المتعلقة بكيفيات تطوير هذا النوع من الطائرات.

سرقة المعلومات و البيانات العسكرية أو التلاعب بها: تكون البيانات الخاصة بتصميمات المعدات أهدافا مثلى للهجمات السيبرانية ، فقد شنت أقوى الهجمات على حواسب الجيش الأمريكي ،سنة 2008م عن طريق وصلة(u.s.b)كانت متصلة بمحمول تابع للجيش الأمريكي ، فتم تسريب لآلاف البيانات من الملفات العسكرية إلى خوادم خارجية.

كما تعرض العراق في سبتمبر 2019م لهجوم سيبراني تمثل في سرقة معلومات بيانات وزارات حساسة على غرار الداخلية و الدفاع الوطني و الخارجية و الصحة ،و على الرغم من تصدي الحكومة العراقية لهذه الهجمات و النجاح في استرجاع معلومات بعض المصالح إلا أن تحقيق الأمن السيبراني الشامل يبقى هدف بعيد المنال.

جمع معلومات اقتصادية استخباراتية: لطالما كانت قواعد بيانات الشركات و البنوك مطمعا لقراصنة و عملاء و حتى أجهزة تجسس تابعة لدول ، و في هذا الإطار ، اصدر الرئيس السابق الأمريكي "باراك أوباما " في فترة إداراته الثانية أوامر بوقف التنصت على مقري المؤسسات المالية العالمية و ذلك عقب تسريبات كشف عنها المتعاقد السابق في الجيش الأمريكي "ادوارد سنودن" بخصوص وجود برامج تنصت أمريكية تستهدف جمع معلومات حول حلفاء و أعداء الولايات المتحدة الأمريكية و حتى بعض الأمريكيين كما قامت كوريا الشمالية بهجمة سيبرانية استهدفت شركة "سوني"،" sony pictures entertaiment"

مما جعل آلاف الحواسيب خارج الخدمة و تم تسريب آلاف البيانات الحساسة بخصوص موظفي هذه الشركة و شخصيات عالمية شهيرة كانت تتعامل معها الأمر الذي يجعل تفوق الهجمات على برامج الحماية و يجعل من مستلزمات تطبيق الأمن السيبراني تحديا يساور الكثير من المهندسين و الخبراء .

د-البعد الاجتماعي: قد لا نختلف إذا اعتبرنا أن البيئة الافتراضية لم تعد آمنة ، فالغزو الثقافي الرقمي ، الجريمة الألكترونية و التنمر و الابتزاز الإلكترونين ، كل هذه الحالات هي نتائج لانتشار المعدات

الإلكترونية في المجتمع، فوفقا لقائمة جدول أعمال علم الاجتماع المعاصر و التي أعدها"أولريش بك"، uilrich, beck " حيث يرى أن المجتمع الإنساني المعاصر بانتقاله إلى عصر المعلوماتية يشهد "حالة من الفوضى " و عدم الأمان و فقدان اليقين و غيرها من التوصيفات التي ضمنها الكاتب في مؤلفه:"مجتمع المخاطر العالمي: بحثا عن الأمان المفقود"([20]) و ذلك نتيجة لتعاظم التهديدات السيبرانية.

و من التحديات التي تخلفها الجريمة الإلكترونية في أبعادها الاجتماعية ما تعلق ([21]):

-**تهديد القيم و الأخلاق:** لقد بات المجتمع مع انتشار الوسائل الإلكترونية أكثر عرضة للمحتويات السلبية غير المرغوب فيها قد تؤثر على سلوكيات الأفراد في جانبها الأخلاقي فالتنمر و الحث على التجنيد و الإنتساب لجماعات ارهابية في الفضاء السيبراني من الجرائم الإلكترونية التي بات من الضروري إدراك مخاطرها و التجند لمحاربتها من خلال زيادة الوعي الاجتماعي في توظيف هذه الوسائط في التدريب و التربية و اكتساب المعارف.

-**ضياع الهوية:** لقد تكرست رابطة الإنسان مع بيئته و مجتمعه منذ ولادته، فيتفاعل مع الآخرين في إطارها ، فتنشأ تلك الرابطة الهوياتية بينه و بين بيئته ، غير أنه بعد انتشار التقنية ، بدأ زوال الرابطة باتجاه الإنسان نحو الكسموبوليتالية و ظهور اهتمامات عالمية للإنسان جعلته يفتقد هويته المحلية و يذوب في هوية العالم السائلة الأمر الذي يؤثر على منظومة القيم التي كونها نتيجة اتصاله ببيئته المحلية.

هـ-البعد القانوني: يمثل القانون أداة لضبط المجتمع عن طريق مجموعة القوانين و الأوامر ، و طبيعي أيضا أن يحمل نفس الوظيفة فيما يتعلق بالفضاء السيبراني ،فالجريمة على المستوى الإفتراضي تفتقر للصرامة و عليه ، بات من الواجب على الدول تكريس منظومة قانونية لتنظيم نشاط الفواعل على مستوى البيئة الإفتراضية .

([20]) اسلام، فوزي، الأمن السيبراني:الأبعاد الاجتماعية و القانونية: تحليل سوسيولوجي ، **المجلة الإجتماعية القومية**، المجلد السادس و الخمسون ، العدد الثاني ، مايو2019، ص 109.

([21]) فايزة أحمد الحسيني، مجاهد ، الوعي بالأمن السيبراني ترف أم ضرورة في عصر المعلوماتية ، **مجلة بحث و تربية**، المجلد 13، العدد 02، ديسمبر2023، ص 63.

لقد أصبح حق النفاذ إلى هذه البيئة و ما يترتب عنها من حقوق المستحدثة كحق إنشاء المدونات الإلكترونية ، الحق في حماية البرامج الإلكترونية من التحديات التي تنتظر التشريع للاجتهاد بخصوصها و إثرائها([22]).

5-الهندسة الامنية السيبرانية الجزائرية: لقد سارعت الجزائر في إطار تطويق انتشار الجريمة الإلكترونية لهندسة سياسة أمنية متكاملة و متناسقة لردع كل محاولات لإختراق المؤسسات الرسمية كالمصالح الحكومية و الهيئات الرسمية و البنوك و المؤسسات الإقتصادية و حتى حسابات رجال السياسة و المال و الإقتصاد ، و من ثم تتمثل ركائز السياسة الأمنية السيبرانية في الأركان التالية:

أ-التشريعات القانونية: مع بروز الإجرام الإلكتروني كشكل جديد من التهديدات ، و إعتماده على التطور التكنولوجي كأدوات لتنفيذ الجريمة ، بادر المشرع الجزائري لإتخاذ جملة من التدابير و الإجراءات القانونية من أجل ردع أساليب الجرائم المختلفة الحديثة منها و التقليدية.

- **نظرة المشرع الجزائري لبرامج الإعلام الآلي:** اعتبر المشرع الجزائري ، وفقا **للمادة 4 من الأمر 03-05**([23]) المتعلق بحقوق المؤلف و الحقوق المجاورة برامج الحاسب الآلي مصنفا أدبيا مكتوبا و محميا ، حيث يمكن لصاحبها الحق في إستغلال برنامجه و إبلاغه لجمهوره تحت أية منظومة معلوماتية ، فيترتب عن ذلك حقوقا مادية للمؤلف صاحب البرنامج .

و أمام التهديدات المتزايدة للجريمة الإلكترونية ، تم تعديل **قانون رقم 04-15** المؤرخ في 10 نوفمبر 2004 و **المتمم للأمر رقم56-156** المتضمن قانون العقوبات، حيث تم إدراج قسم خاص يتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات الإلكترونية ، إذ جرم المشرع الجزائري -بموجب قانون العقوبات-الأفعال التالية:

([22]) شويرب جيلالي ، محروب السيبرانية و الأمن السيبراني ، **مجلة الحقوق و الحريات** ، المجلد11 ، العدد01، 2023 ص 167.

([23]) سميحة بلقاسم و حميد بوشوشة، الجريمة الإلكترونية بعد جديد للإجرام في الجزائر .....واقعها و آليات مجابهتها، **مجلة العلوم الإنسانية لجامعة أم البواقي** ، المجلد1 ، العدد1 ، جوان 2023، ص 536.

أولا: المعاقبة بالحبس–بموجب المادة 394 مكرر– من ثلاثة أشهر إلى سنة و بغرامة مالية من 50.000دج إلى 100.000دج ، عن فعل الدخول و البقاء غير المشروع لمنظومة معلوماتية ، و تضاعف العقوبة أذا ما ترتب على فعل الدخول تغيير أو حذف لمعلومات تلك المنظومة

ثانيا: المعاقبة بالحبس–بموجب المادة394 مكرر1– من ستة أشهر لثلاث سنوات و بغرامة مالية من 500.000دج إلى 2000.000دج كل من أدخل عن طريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها(التزوير المعلوماتي).

ثالثا: المعاقبة بالحبس–بموجب المادة 394 مكرر2–من شهرين إلى ثلاث سنوات و بغرامة مالية من 1.000.000دج إلى 5.000.000دج كل من يقوم عمدا أو عن طريق الغش بتصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية ، بمعنى آخر ، جرم المشرع الجزائري فعل الإستيلاء على المعطيات المعلوماتية أو إفشائها أو الإتجار بها لأي غرض كان ، إضافة إلى جريمة الإحتيال المعلوماتي عن طريق تصميم و تجميع معطيات المنظومة المعلوماتية عن طريق الغش.

رابعا: مصادرة الأجهزة ن البرامج و الوسائل الإلكترونية المستخدمة –بموجب المادة394 مكرر6–مع إمكانية إغلاق المحل مكان الإستغلال إذا كان حدوث فعل الجريمة بعلم صاحبها.

خامسا: شدد المشرع الجزائري العقوبة –بموجب القسم السابع من قانون العقوبات 04–15–على الجرائم التي تستهدف جهاز الدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام.

سادسا: نص المشرع –بموجب المادة394 مكرر5–على تجريم الإشتراك في مجموعة أو إتفاق لغرض الإعداد لجريمة من الجرائم الماسة بأنظمة المعالجة الألية للمعطيات.

سابعا: و قد شملت المادة 394 مكرر 4 العقوبة التي تطال الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في القسم السابع من قانون العقوبات ، حيث تشمل العقوبة غرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

و اعتبرت المادة 394 مكرر7 أن الشروع في الجريمة المعلوماتية يعاقب عليها بالعقوبة المقررة للجريمة ذاتها.

قانون 06-23 المؤرخ في 20 ديسمبر 2006([24]): مع تزايد خطورة الإجرام المعلوماتي ن ادخل المشرع الجزائري تعديلات أخرى بموجب قانون 06-23 المؤرخ في 20 ديسمبر 2006 حيث مس التعديل القسم السابع مكرر الخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

جرم المشرع كل أنواع المساس بحرمة الحياة الخاصة بإستخدام الوسائل التكنولوجية الحديثة ، فقد حددت المواد 303 مكرر إلى 303 مكرر3 الجرائم التي تقع على حرمة الحياة الخاصة و هي : جريمة إلتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بدون إذن صاحبها.

تعديل قانون الإجراءات الجزائية([25]): مواكبة للتطور الرقمي الحاصل في المجتمع ، أقر المشرع الجزائري جملة من الإجراءات الخاصة بالإعراض على المراسلات ، التفتيش ، تسجيل الأصوات و التقاط الصور.، حيث نصت المواد 65 مكرر5 إلى المادة65 مكرر10 على أمكانية اللجوء للإعتراض على المراسلات ، التقاط الصور و تسجيل الأصوات و ذلك لمقتضيات التحري و التحقيق في جرائم المخدرات الجريمة العابرة للحدود و **الجرائم الماسة بأنظمة المعالجة الألية للمعطيات** ، مع مراعاة ، طبعا، كتمان السر المهني ، تحرير محضر من طرف الضابط المحقق ، حيث يمكن لوكيل الجمهورية أن يأذن ب:

-إعتراض المراسلات التي تتم عن طريق وسائل الإتصال السلكية و اللاسلكية.

-وضع الترتيبات التقنية-دون موافقة المعنيين-من أجل التقاط ، تثبيت، بث ، تسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص واحد أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.

و في نفس السياق، أقر المشرع إجراءات توقيف النظر في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ، حيث تنص المادة 51 من قانون الإجراءات الجزائية المعدل على "إذا رأى ضلبط الشرطة القضائية ، لمقتضيات التحقيق ، أن يوقف للنظر شخصا لاأو أكثر ، أشير إليهم في المادة 50، فعليه أن يطلع فورا وكيل الجمهورية المختص بذلك مع إعداد تقرير عن دواعي التوقيف للنظر.

كما قد يخضع التوقيف للنظر للتمديد مرة واحدة- بإذن من وكيل الجمهورية ، إذا كانت موضوع الجرائم متعلق بالمساس بأنظمة المعالجة الآلية للمعطيات.

([24]) مرجع ، سابق، ص 541.

([25]) مرجع ، سابق، ص541.

قانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام و الإتصال:

المراقبة الالكترونية([26]): تضمن هذا القانون أحكام جديدة متعلقة بكيفيات معالجة الجريمة الإلكترونية و مستلزمات التحريات و التحقيقات القضائية ، حيث تطرقت المادة الثالثة من قانون 09-04 لتدابير الوقاية من الجرائم الإلكترونية و المتمثلة في:

-**المراقبة الالكترونية:** تتمثل حالات المراقبة الإلكترونية بموجب المادة 4 من قانون 09-04 في :

-الوقاية من الأفعال الموصوفة بجرائم الإرهاب ، التخريب أو الجرائم الماسة بأمن الدولة .

-عند توفر معلومات مفادها احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام ، الدفاع الوطني، مؤسسات الدولة أو الاقتصاد الوطني.

-إذا كان من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية لما تقتضيه التحريات و التحقيقات الجارية.

-في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

-**التفتيش:** يعد من أدق الصلاحيات الممنوحة للمحقق، و ذلك على حساب الحريات الفردية المكفولة دستوريا و عليه ، فقد أحاطها المشرع بضوابط متعلقة بالسلطة التي تأذن بمباشرة التفتيش ، السلطة التي تقوم بالتفتيش و الأحوال التي يجوز فيها التفتيش.

أشارت المادة 3 من قانون 09-04 أنه لمقتضيات حماية النظام العام و لمستلزمات التحريات ن يمكن وضع ترتيبات تقنية لمراقبة الإتصالات الإلكترونية و القيام بإجراءات التفتيش و الحجز داخل المنظومة المعلوماية.

و تنص المادة 05 من قانون 09-04 على أنه يجوز للسلطات القضائية و ضباط الشرطة القضائية و في الحالات المنصوص عليها في المادة4 من قانون09-04 الدخول بغرض التفتيش و لو عن بعد في حالتين:

([26]) مرجع ، سابق، ص543.

الحالة الأولى: تفتيش منظومة معلوماتية أو جزء منها أو معطيات معلوماتية مخزنة فيها .

الحالة الثانية: تفتيش منظومة تخزين معلوماتية.

كما منح المشرع الجزائري للسلطات المكلفة بالتفتيش إمكانية الإستنجاد بأي شخص له دراية بعمل المنظومة المعلوماتية محل البحث

الحجز: يعني الحجز وضع اليد على شيء مرتبط بجريمة تمت ، و يتم الحجز بموجب المادة6 و المادة7 من قانون09-04 في حالتين:

الحالة الأولى: حجز المعطيات المعلوماتية: يمكن للسلطة التي تباشر التفتيش في منظومة معلوماتية حجز المعطيات المخزنة التي تكون مفيدة في الكشف عن الجرائم أو مرتكبيها و ليس ضروريا حجز كل المنظومة و ذلك من خلال نسخ المعطيات محل البحث .

و الجدير بالملاحظة في هذا السياق ، أوجب المشرع على ذات السلطة السهر على سلامة المعطيات في المنظومة المعلوماتية مجيزا في ذلك استعمال كل الوسائل البتقنية الضرورية من أجل تشكيل أو إعادة تشكيل المعطيات المتحصل عليها قصد جعلها قابلة للإستغلال لغرض التحقيق من دون المساس-طبعا- بمحتوى المعطيات.

الحالة الثانية: الحجز عن طريق منع الوصول إلى المعطيات: إذا استحال حجز المعطيات المعلوماتية لأسباب تقنية ، فإنه، حسب المادة7 ، يتعين على السلطة التي تقوم بالتفتيش بإستعمال التقنيات المناسبة لمنع الوصول إلى المعطيات المتضمنة في المنظومة المعلوماتية أو نسخها ، كما يمكن منع الإطلاع على المعطيات المحجوزة التي يشكل محتواها جريمة بموجب المادة8 ، عن طريق تكليف شخص مؤهل و بإستعمال الوسائل التقنية المناسبة لذلك.

القوانين الموالية لقانون09-04 ذات الصلة بالجرائم الإلكترونية: تماشيا مع التطور الحاصل على مستوى التقنيات الإلكترونية و تطبيقات التواصل المختلفة و قصد وضع حد للإنتشار الرهيب لجرائم انتهاك المراسلات ، المساس بالحريات العامة ، القذف، التشهير،الإبتزاز المالي و الإحتيال بإستخدام الأساليب التقنية ، فقد أقر المشرع الجزائري:

قانون رقم 18-04 المحدد للقواعد العامة المتعلقة بالبريد و الإتصالات الإلكترونية([27]) لقد تم تجريم -بوجب قانون 18-04 لاسيما المواد 164-188 منه المرسلات المرسلة عن طريق الإتصالات الإلكترونية أو إفشاء مضمونها أو نشرها أو إستعمالها دون ترخيص من المرسل أو المرسل إليه، كما تجرم كل محاولة لفتح أو تخريب للبريد الإلكتروني للأشخاص الطبيعيين أو المعنويين أو المساعدة على هذه الجريمة.

و في نفس السياق ، يكون المقصود بالاتصالات -حسب المادة10 من قانون18-04 :"كل إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو بيانات أو معلومات مهما كانت طبيعتها عبر الأسلاك أو الألياف البصرية أو بطريقة كهرومغناطسية."

قانون18-07 المتعلق بحماية الأشخاص الطبيعيين فير مجال معالجة المعطيات ذات الطابع الشخصي([28]): يكون المقصود بمعالجة المعطيات ذات الطابع الشخصي-بموجب قانون18-07 :"كل عملية أو مجموعة عمليات منجزة بطرق أو وسائل آلية أو بدونها على معطيات ذات طابع شخصي مثل: الجمع، التسجيل ، التنظيم، الحفظ ، الملاءمة، التغيير، الإطلاع، الإستخراج، الإستعمال، الإيصال عن طريق النشر أو الإرسال أو أي شكل من أشكال الإتاحة أو التقريب أو الربط البيني وكذا الإغلاق أو التشفير أو المسح أو الإتلاف".

و قد سن المشرع الجزائري مجموعة من الآليات و الضوابط تتمثل في:

استحداث سلطة وطنية لحماية المعطيات ذات الطابع الشخصي مكلفة بضمان عدم انطواء استعمال تكنولوجيات الإعلام و الاتصال على أية أخطار تجاه حقوق الأشخاص و الحريات العامة و الخاصة و أن كل محاولة الاعتداء على المعطيات ذات الطابع الشخصي تكون بإقرار عقوبة مالية و أخرى سالبة للحرية مع إمكانية مصادرة محل الجريمة(الفصل الثالث من قانون 18-07 لاسيما المواد من 54الى 74).

([27]) مرجع سابق، ص545

([28]) مرجع ، سابق ، ص 546.

قانون 08-01 المتعلق بالتأمينات الإجتماعية([29]): لم يكتف المشرع الجزائري بمحاصرة الجرائم الإلكترونية المتعلقة بإفشاء أسرار و محتويات المراسلات و إتلاف المعطيات ذات الطابع الشخصي أو الإطلاع عليها ، بل عالج الجريمة الإلكترونية التي تطال الهيئات الوطنية كالضمان الاجتماعي، إذ تطرق قانون 08-01 للعقوبات التي تخص البطاقة الإلكترونية للشفاء و التي تسلم للمؤمن اجتماعيا بسبب العلاج ، فوردت العقوبات -وفق المادة 93 مكرر2 و المادة 93 مكرر3-كما يلي:

- تسليم او أستلام بهدف الإستعمال غير المشروع أو القيام عن طريق الغش بتعديل أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية.

-إعداد أو تعديل أو نسخ بطريقة غير شرعية للبرمجيات التي تسمح بالوصول أو استعمال للمعطيات المدرجة في البطاقة الإلكترونية للمؤمن له اجتماعيا أو في المفتاح الإلكتروني لهيكل العلاج أو المفتاح الإلكتروني لمهني الصحة.

توضح التشريعات القانونية السابقة إرادة المشرع في محاربة الجريمة الإلكترونية باستخدام الأدوات التقنية فكل معالجة آلية للمعطيات ، تخالف التشريع الوطني ، تكون عقوبتها سلب الحرية لمرتكبها مع إقرار مخالفة مالية ، كل ذلك من أجل حماية المجتمع من الإخطار الإلكترونية المتزايدة و التي باتت تفرضها نزوع الإنسان نحو الرقمنة .

ب-الجوانب التقنية: إن الانتشار اللافت للجريمة الإلكترونية و اتصافها بصعوبة تحديد هوية المستخدم و زوال الحواجز الجغرافية في الفضاء السيبراني ، جعل من الضروري على الدول الاستنجاد بأحدث التكنولوجيا من أجل إفشال الاعتداءات الإجرامية على الساكنة من خلال تزويد القائمين على عملية التأمين بما يلي:

-تنمية و تعزيز و تأهيل القدرات البشرية المكلفة بعمليات التحقيق في الجرائم الإلكترونية.

-توفير المعدات التكنولوجية المتقدمة و الدقيقة المرتبطة بالإعلام الآلي و الاتصالات.

-إنشاء قاعدة بيانات واسعة و محينة بإستمرار.

-القدرة على تصميم البرامج المعلوماتية و تطويرها.

([29]) مرجع ، سابق ، ص547.

ج-المؤسسات العملياتية : عمدت الجزائر و بغية تنفيذ سياسة سيبرانية فعالة ، على إنجاز مجموعة من المؤسسات العلمية و العملياتية ، تقوم بمسؤولية الحماية و كشف مختلف أنواع الجرائم ، و في مقدمة تلك الجرائم ما تعلق بالتهديدات السيبرانية .

- **المؤسسات العلمية لتحقيق الأمن السيبراني:**

تحقيقا لمتطلبات الأمن السيبراني و خلق بيئة أمنية آمنة ، و في مخرجات اجتماع لمجلس الوزراء للدولة الجزائرية بتاريخ 12 سبتمبر 2023م تم استحداث مدرسة وطنية عليا للأمن السيبراني بالتنسيق مع وزارة الدفاع الوطني ، لضمان توحيد الجهود و مضاعفة الفعالية في هذا المجال الحساس من أجل تحصين الأمن الوطني القومي.

- **المؤسسات التنفيذية لتحقيق الأمن السيبراني:** تتمثل في :
  - **مؤسسات ذات الوصاية الأمنية:** يندرج تحتها ما يلي:
- **مصلحة الدفاع السيبراني و مراقبة أمن الأنظمة:** تم استحداثها بتاريخ 11-06-2015، تابعة لدائرة الإستعمال و التحضير لأركان الجيش الوطني الشعبي، تضطلع بمهمة حماية المنظومات الحيوية للبلاد ضد كل أنواع الجريمة الإلكترونية.

من بين أهم أهدافها:

-اعتماد التكوين التقني و العلمي لإنتاج الكفاءات و المهارات القادرة على خلق دفاع سيبراني يشمل كافة أنشطة المؤسسة العسكرية لتفادي الأخطار الإجرامية.

-غرس ثقافة "الإستعمال كيفي لتكنولوجيات الإعلام و الإتصالé من خلال حملات تحسيسية لكافة مستخدمي المؤسسة.

-الإعتماد بطريقة مستمرة على البحث العلمي لتطوير وسائل الدفاع استجابة للتطورات الحاصلة في مجال التكنولوجيا.

- **مركز الوقاية من جرائم الإعلام الآلي و الجرائم الإلكترونية التابعة للدرك الوطني:** هو جهاز تابع لسلاح الدرك الوطني ، يتواجد ببئر مراد رايس ، أنشئ في 2008 و يعد الجهاز الوحيد المختص في جرائم الإعلام الآلي و الجريمة المعلوماتية.

يقوم المركز بالمهام التالية:

-تحليل معطيات و بيانات الجرائم المعلوماتية المرتكبة و تحديد هوية أصحابها .

-تأمين الأنظمة المعلوماتية و الحفاظ عليها لاسيما تلك التابعة للمؤسسات الرسمية و البنوك.

-تقديم المساعدة الأمنية للأجهزة الأخرى في مجال محاربة الجريمة الإلكترونية.

و طبقا لإحصائيات متعلقة بالجرائم الإلكترونية في الجزائر ، يمكن التأكيد على إنتقال الجريمة إلى العالم الإفتراضي ، حيث سجلت قيادة الدرك الوطني ما مجموعه 1362 جريمة سيبرانية تورط فيها 1028 شخص خلال 2020م .

و الجدير بالملاحظة ، و طبقا لتحليل معطيات الجريمة الإلكترونية : تحتل جرائم القذف و السب الصدارة عبر الفضاء السيبراني بنسبة55%يليها جرائم ضد الأمن العمومي ثم الأعمال الماسة بالحياة الخاصة و إفشاء الأسرار و أخيرا الابتزاز و الاحتيال و الإستغلال الجنسي و الأفعال المخالفة للآداب العامة.

و في سياق التعاون الدولي ، أحبطت" شركة كسبرسكي"،"kasparsky" المختصة في محاربة الجريمة السيبرانية 95000 هجمة إلكترونية كانت موجهة ضد الجزائر.

- **<u>المعهد الوطني للأدلة الجنائية و علم الإجرام التابع للدرك الوطني:</u>** هي مؤسسة عمومية ذات طابع إداري ، تعمل تحت الوصاية المباشرة لوزير الدفاع الوطني.

يضم المعهد العديد من الأقسام و المعاهد ، أهمها:

<u>أ-مصلحة الإعلام الآلي</u>: تعد مصلحة أساسية بالنظر لجمل المهام الموكلة لها و هي :

-رصد و تتبع و مراقبة عملية الإختراق و القرصنة المعلوماتية .

-اكتشاف المعلومات المسروقة.

-تفكيك البرامج المعلوماتية.

ب–مصلحة البصمات: يتم على مستوى هذه المصلحة التعرف على الجثث ، مع العلم أن سلاح الدرك الوطني مجهز بنظام التعرف الآلي على البصمات (the automated fingerprint identification system).

ج–مصلحة الوثائق : يتم التأكد في هذه المصلحة من :

–صحة الإمضاءات .

–التحقق من النقود المزورة و الوثائق السرية.

د–مصلحة البيئة: تبحث هذه المصلحة في أسباب تلوث المياه و التربة و الكشف عن المواد السامة المتواجدة في المحيط وة أماكن العمل.

هـ –قسم التحليل الدقيق: و هو قسم مجهز بأحدث وسائل المسح الإلكتروني و يقوم بمقارنة المعطيات الدقيقة التي يتم العثور عليها في مسرح الجريمة.

و –قسم السيارات: أين يتم التعرف على السيارات ذات الترقيم المزور من خلال تتبع عملية تغيير او تحريف الأرقام التسلسلية للمركبة.

وبوجود المصالح الحيوية للمعهد ، فإنه يضطلع بالمهام التالية:

أ–المشاركة في تحديد سياسة جنائية مثلى لمكافحة الإجرام.

ب–إجراء الخبرات و الفحوصات الأولية في إطار التحريات بهدف التعرف على مرتكبي الجرائم و الجنح.

ج–المبادرة باجراء بحوث تطبيقية متعلقة بالإجرام عن طريق اللجوء إى التكنولوجيا الدقيقة.

د–العمل على ترقية البحوث التطبيقية ذات العلاقة بالتهديدات السيبرانية.

كما يحتوي المعهد على : قسم الحرائق و الإنفجارات ، قسم الطب الشرعي ، قسم علم الإنسان و الأسنان الشرعيين ، قسم علم البواعث المؤدية للموت ، مصلحة بصمة الأصبع، مصلحة الإشارة و مصلحة الإلكترونيك ، كما يضم المركز زمرة من المهندسين و التقنيين من ذوي الخبرة و التجربة للتصدي لكافة أنواع الجريمة و تهديداتها.

- **المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني:** تماشيا مع استفحال الجريمة الإلكترونية و إستجابة لمطلب تحقيق مستلزمات الأمن السيبراني ، قامت المديرية العامة للأمن الوطني بإستحداث المصلحة المركزية للجريمة الإلكترونية التي عمدت منذ إنشائها على تدريب التشكيل الأمني على مهارات ردع كل محاولات الإختراق أو التجسس أو غيرها من الأفعال الإجرامية ، فتم في 2011 بتشكيل النواة الأمنية الأولى لمحاربة الجريمة و بقرار من المدير العام للأمن الوطني ، في 2015، تم إنشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال([30]).
- **نيابة مديرية الشرطة العلمية و التقنية التابعة للمديرية العامة للأمن الوطني:** أوكلت المديرية العامة للأمن الوطني مهمة محاربة الجريمة الإلكترونية لنيابة مديرية الشرطة العلمية و القنية مزودة إياها بالوحدات التالية:

–المخبر المركزي للشرطة العلمية، مقره ابن عكنون –الجزائر العاصمة.

–المخبر الجهوي للشرطة العلمية ، مقره قسنطينة.

–المخبر الجهوي للشرطة العلمية ، مقره وهران .

يتولى كل مخبر (مركزي–جهوي) مهام البحث و التحقيق و التحري بشأن الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ، عن طريق

- **الدائرة العلمية:** تقوم بمهام البحث و التحقيق و تحليل الأدلة المتصلة بالمجال البيولوجي ، الكيميائي و الطب الشرعي و تلك المتعلقة بالتسمم ، الحرائق و المتفجرات.
- **الدائرة التقنية:** تتولى مهام البحث و تحليل الأدلة الناتجة عن الجرائم المتصلة بإستعمال الأسلحة و القذائف إضافة لمعالجة الجرائم المعلوماتية.

و في سياق آخر ، و فضلا عن الدوريات الروتينية للمراقبة الفيزيائية للأفراد و المركبات قصد ضمان السكينة و الأمن العام في المجتمع ن تقوم الشرطة في مجال التصدي للجريمة الإلكترونية بالمهام التالية:

- تنشيط عمل خلايا اليقظة الإلكترونية من خلال رصد أي تصرف مشبوه.
- تتبع الأثر الإلكتروني/التوعية و التحسيس.

([30]) بارة ، سمير ، الأمن السيبراني في الجزائر: السياسات و المؤسسات ، المجلة الجزائرية للأمن الإنساني ، العدد الرابع ، جويلية 2071، ص 272.

- العمل على تجفيف مصادر التمويل و التجنيد عبر الفضاء السيبراني.

تقوم المديرية العامة للأمن الوطني بمساعي حثيثة داخل الوطن و خارجه لشل كل محاولات تنفيذ السلوك الإجرامي ، حيث تم إنشاء فرق متخصصة عبر 58 مقر أمن ولائي، تتمحور مهامها في:

استقبال شكاوي المواطنين في مجال الجرائم المرتكبة في الفضاء السيبراني .

البحث و التحري في الجرائم المعلوماتية تحت إشراف السلطات القضائية.

توعية و تحسيس المواطنين بمخاطر الانترنيت خاصة على الأطفال.

و في مجال تعقب الجريمة الإلكترونية خارج الحدود و في إطار التعاون الدولي للجزائر في المجال السيبراني كانت الجزائر من الدول التي انضمت سريعا للمنظمة الدولية للشرطة الجنائية و تعد عضو مؤسس للمنظمة الإفريقية للشرطة الجنائية مما يدل على تصميم قيادة جهاز الشرطة على محاربة كل ما يهدد السلامة الترابية من تهديدات تقليدية و مستحدثة.

- **مؤسسات ذات وصاية مدنية:** إنطلاقا من كون عملية محاربة الجريمة الإلكترونية ليست مسؤولية المؤسسات الأمنية وحدها ، قامت السلطات العليا الجزائرية بإنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها.

- **الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها:** تشكلت هذه الهيئة بمقتضى المرسوم الرئاسي رقم 15-261 المؤرخ في 8 اكتوبر 2015 و هي سلطة إدارية مستقلة تابعة لوزير العدل .

تضم أعضاء من الحكومة ممن تتقاطع مهامهم بتكنولوجيا الإعلام و الإتصال . إضافة لمسؤولي مصالح الأمن المختلفة و قاضيين من المحكمة العليا يعينهما المجلس الأعلى للقضاء.

و يتواجد أيضا ضمن أعضاء الهيئة : قضاة ن ضباط و أعوان من الشرطة القضائية تابعين لمختلف المصالح و الهيئات العسكرية و المدنية في الدولة و ذلك وفقا لأحكام قانون الإجراءات الجزائية.

- **مهام الهيئة:** تساهم الهيئة في :
- اقتراح الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال.
- تنشيط و تنسيق عمليات الوقاية منها.
- تقديم المساعدة للسلطات القضائية و مصالح الشرطة القضائية في مجال مكافحة الجرائم الإلكترونية.
- ضمان المراقبة الوقائية للإتصالات الإلكترونية.

- **<u>القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال:</u>** أنشئ بموجب الأمر رقم 11/21 المؤرخ في 25 أوت 2021 المعدل و المتمم لقانون الإجراءات الجزائية ، يتواجد على مستوى مجلس قضاء العاصمة.

يعرف –بداية –الأمر رقم 11/21 الجريمة المتصلة بتكنولوجيات الإعلام و الاتصال كونها أي جريمة ترتكب أو يسهل ارتكابها باستعمال منظومة معلوماتية أو نظام للاتصالات الإلكترونية أو أي وسيلة أخرى أو آلية ذات صلة بتكنولوجيا الإعلام و الإتصال.

يقوم هذا القطب الجزائي بمهمتين أساسيتين:

–المتابعة و التحقيق في الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال.

الحكم في الجرائم المنصوص عليها في الباب السادس من الأمر 11/21 إذا كانت تشكل جنحا.

و قد فصلت المادة211مكرر24 في الجرائم المتعلقة بتكنولوجيات الإعلام و الإتصال و الجرائم المرتبطة بها و التي يتعين على السادة:

وكيل الجمهورية لدى القطب

قاضي التحقيق

رئيس القطب

المختصين حصريا بالمتابعة و التحقيق و الحكم فيها ، إذا كانت الجرائم تمثل:

- الجرائم التي تمس أمن الدولة و الدفاع الوطني.
- جرائم نشر و تحرير اخبار كاذبة بين الجمهور من شأنها المساس بالأمن و السكينة العامة و استقرار المجتمع.
- جرائم نشر و ترويج أخبار مغرضة تمس بالنظام و الأمن العموميين.
- جرائم الإتجار بالأشخاص ، الأعضاء البشرية و تهريب المهاجرين.
- جرائم التمييز و خطاب الكراهية (الأمر 11/21 ص8).

لقد أصدرت العديد من الوزارات على غرار وزارة الداخلية ،البريد ، الإتصال ، التعليم العالي ، المالية تعليمات لمصالها التقنية ، تتضمن الكيفيات العملية الواجب إتخاذها لتفادي أي تسريب سيبراني ، و تتمثل هذه الكيفيات في :

-عدم السماح لآي كان من الحصول على معلومات من الأنظمة المعلوماية الموصولة بشبكة الأنرنيت ، ما لم يكن هناك موافقة من المصلحة المؤهلة قانونا ، كما لا يمكن إستخدام الحسابات الخاصة بالأفراد أو أرقامهم السرية.

-احترام المقاييس المعمول بها أثناء تداول المعلومات المشفرة -أرسالا و استقبالا.

الخاتمة:

نستنتج مما سبق أن الهندسة الأمنية السيبرانية الجزائرية تقوم على العناصر التالية:

-استفحال ظاهرة الجريمة الإلكترونية بعد انتشار الأدوات التكنولوجية المختلفة من حواسيب و حواسيب ذكية و هواتف ذكية ووصل مسار التكنولوجيا إلى إنتاج أدوات إلكترونية متناهية الدقة و تقوم بتخزين أو إرسال أحجام كبيرة من المحتويات و البيانات و المعلومات.

-ظهور محتويات رقمية تتخذ من الأدوات التكنولوجية وسيلة لتسهيل حياة البشرية ، فمضامينها تختلف ما بين الاقتصادي المرتبط بالتمويل البنكي و تسديد الأقساط و معرفة سعر السعر و غيرها و منها ما هو اجتماعي-تثقيفي يهدف لنشر الوعي و المعرفة بين مكونات المجتمع المختلفة.

-انخراط الإنسان في الفضاء السيبراني مكونا بيئة افتراضية و التي أصبحت نواة التعامل و التفاعل ، فصار أكثر بهذه البيئة (الإنسان الرقمي) إلى درجة الانصهار في العالم الافتراضي.

- يمكن التأكيد أن البيئة الإفتراضية لا تخلو من تهديدات سسيبرانية تستهدف البنى التحتية للدول و تحاول تخريبها أو إتلافها ، فحروب الجيل الخامس تتخذ من هذه البيئة مسرحا لها و أن الحواسيب ما هي إلا أسلحة للمعارك المستقلية و بياناتها هي اهداف للقراصنة و العملاء و حتى الدول.

-تفرض البيئة السيبرانية جملة من التحديات تواجه من خلالها الدول و الشركات و حتى الأفراد اختراقات و عليه ، يكون من الضروري تحيين ادوات التصدي و المجابهة لكل هجوم سيبراني.

-تعمل الجزائر من خلال جملة من اجراءات الأمن السيبراني على التصدي لكل انواع الهجومات ، حيث تم ارساء نصوص قانونية ردعية ضد من يعدل أو يعطل أو يغش في أنظمة المعلومات الوطنية ، كما تمتلك منظومة تنفيذية لابطال كل محاولات الإختراق ن فهما أبدى هؤلاء القراصنة تفوقا تكنولوجيا ، إن السياسة الأمنية الجزائرية تظل بالمرصاد لكل محاولتهم و بارمجهم السيبرانية التي لن تصمد أمام اصرار و عزيمة العقول الأمنية الجزائرية.

قائمة المراجع:

1-الكتب:

– عبد الفتاح بيومي، حجازي، مكافحة جرائم الكمبيوتر و الإنترنيت في القانون العربي النموذجي (القاهرة: دار الفكر الجامعي ، 2006).

-مجمع البحوث و الدراسات لأكاديمية السلطان قابوس لعلوم الشرطة ، الجريمة الإلكترونية في المجتمع الخليجي و كيفية مواجهتها (الرياض: أكاديمية نايف للعلوم الأمنية ، 2016).

2-المجلات:

بارة ، سمير ، الأمن السيبراني في الجزائر: السياسات و المؤسسات ، **المجلة الجزائرية للأمن الإنساني** ، العدد الرابع ، جويلية2017.

دراعو ، عزالدين،الآثار الإقتصادية و المالية للهجمات السيبرانية في ظل بالتحول الرقمي : النتائج ، التجارب و الحلول –مع الإشارة لحالة الجزائر–**مجلة التكامل الإقتصادي**، المجلد10 ، العدد02، جوان2022.

ربيعي ، حسين ، سمر محمود ، الحروب السيبرانية: المخاطر و استراتيجيات تحقيق الأمن السيبراني الدولي و الداخلي ، **المجلد الجزائرية للأمن الإنساني**، المجلد 07، العدد02 ، السنة السابعة ، جويلية2022.

منى عبد الله ، السمحان، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود ، مجلة **كلية التربية**،العدد111، جويلية2020.

([1]) بن مرزوق، عنترة، الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية ،**مجلة العلوم الإجتماعية** ، المجلد 19، العدد01،

اسلام، فوزي، الأمن السيبراني:الأبعاد الاجتماعية و القانونية: تحليل سوسيولوجي ، **المجلة الإجتماعية القومية**، المجلد السادس و الخمسون ، العدد الثاني ، مايو2019.

فايزة أحمد الحسيني، مجاهد ، الوعي بالأمن السيبراني ترف أم ضرورة في عصر المعلوماتية ، **مجلة بحث و تربية**، المجلد 13، العدد 02، ديسمبر2023.

حسين قوادرة ، منى كحلوش ، التداعيات الاقتصادية لحرب المعلومات السيبرانية ، **مجلة الناقد للدراسات السياسية** ، المجلد 05، العدد 01 ، 2021.

شريفة كلاع ، الأمن السيبراني و تحديات الجوسسة و الاختراقات الإلكترونية للدول عبر الفضاء السيبراني ، **مجلة الحقوق والعلوم الإنسانية** ، المجلد15 ،العدد01، 2002.

مهدي، رضا، الجرائم السيبرانية و آليات مكافحتها في التشريع الجزائري ، **مجلة إيليزا للبحوث و الدراسات** ، المجلد06 ، العدد02 ، 2021.

أميرة عبد العظيم محمد ، عبد الجواد، المخاطر السيبرانية و سبل مواجهتها في القانون العام ، **مجلة الشريعة و القانون** ، ج3 ، العدد 35، 2020.

شويرب جيلالي ، محروب السيبرانية و الأمن السيبراني ، **مجلة الحقوق و الحريات** ، المجلد11 ، العدد01، 2023 ص 167.

سميحة بلقاسم و حميد بوشوشة، الجريمة الإلكترونية بعد جديد للإجرام في الجزائر .....واقعها و آليات مجابهتها، **مجلة العلوم الإنسانية لجامعة أم البواقي** ، المجلد1 ، العدد1 ، جوان

اسماعيل ، زروقة ، الفضاء السيبراني و التحول في مفاهيم القوة و الصراع، **مجلة العلوم القانونية و السياسية** ، المجلد 10، العدد01، أفريل 2019،

3-محاضرات:

بوازدية ، جمال ، الأمن السيبراني محاضرات مقدمة لطلبة السنة الثانية ماستر (تخصص: دراسات إستراتيجية و أمنية)(الجزائر: كلية العلوم السياسية و العلاقات الدولية، 2021).

Books in forein languges

The International Telecommunication nion(int) , Tool kit for cybercrime ligeslation, Geneva, 2010.