وزارة التعليم العالي و البحث العلمي
جامعة مولود معمري – تيزي وزو
كلية الحقوق و العلوم السياسية
قسم الحقوق

الأمـــــــن السيبراني

مذكرة لنيل شهادة الماستر في الحقوق
تخصص القانون الجنائي و العلوم الجنائية

من إعداد الطالبين:

عيش موسى

خيمود محمد

تحت إشراف الأستاذ:

د/ براهيمي صفيان.

لجنة المناقشة:

- تاجر محمد أستاذ التعليم العالي، جامعة مولود معمري، تيزي وزو.....رئيسا
- براهيمي صفيان أستاذ محاضر " أ "، جامعة مولود معمري، تيزي وزو.....مشرفا و مقررا
- أوديع نادية أستاذة مساعد " أ "، جامعة مولود معمري، تيزي وزو ..... ممتحنا

تاريخ المناقشة : 26 /06 /2023

الشكر لله عز وجلا

الذي أنار لي الدرب، وفتح لي أبواب العلم و أمدني بالصبر
و الإرادة.

وفي هذا الإطار أتقدم بشكري الى الأستاذ المشرف
"**سفيان براهيمي** "الذي أمدني بإشرافه وتوجيهاته ونصحه السديد.

دون أن يفوتني أن أتقدم بالشكر الجزيل و التقدير والإحترام
الى كل السادة أعضاء لجنة المناقشة بدون إستثناء.

إلى كل الأساتذة الذين ساهموا بصدر رحب في تقديم
يد العون في هذا العمل وأخص بالذكر أستاذتي"
اوديع نادينة "بكلية الحقوق و العلوم السياسية بجامعة
"مولود معمري "تيزي وزو.

وفي الختام لا أنسى كل من ساعدني من قريب أو
بعيد ولو بكلمة طيبة، فجزاكم
الله خيرا.

إلى من كلله الله بالهيبة و الوقار

.....إلى من علمني العطاء بدون.....إنتظار.....

إلى من أحمل أسمه بكل إفتخار.....رحمة الله عليه...

الذي سوف تبقى كلماته.

نجوم اهتدي بها اليوم و في الغد و إلى الأبد" **والدي العزيز**"

إلى ملاكي في الحياة .....إلى معنى الحب و إلى معنى الحنان

و التفاني.....

إلى بسمة الحياة وسر الوجود .....إلى من كان دعائها سر

نجاحي و حنانها

بلسم جراحي إلى أغلى الحبايب "**أمي الحبيبة**"

إلى سندي وقوتي وملاذي" ..... **زوجتي العزيزة**"

الى ملائكة البيت الصغار إبنتي وإبني" **روان و محمد إليان**

"حفظهم الله

وشكر خاص الى الأخت" **عائشة نايلي**"

موسى

قائمة المختصرات

أولا: باللغة العربية

ج.ر: الجريدة الرسمية

ج.ج : للجمهورية الجزائرية

ع: العدد

ط: الطبعة

ص: صفحة

ق.ع: قانون العقوبات

ق.إ.ج: قانون الإجراءات الجزائية

ثانيا: باللغة الفرنسية

- SCLC : Service de lutte contre la cyber criminalité.

- CPLCIC : Centre de protection contre les crimes informatiques et la cyber criminalité.

- INCC : Institut national de la criminologie.

- CAGI : Conférence Africaine de gouvernance internet

- UIT : Union Internationale des Télécommunications

- UA : Union Africaine

- GCI : Global Cybersecurity Index

- CERIST : Centre d Recherche sur l'information Scientifique et Technique

- UNDOC : United Nations Office on Drugs and Crime

- INCC : Institut National de criminalistique et de Criminologie de la Gendarmerie Nationale.

مقدمة

مقـــدمة:

إن الأمن السيبراني قضية ناشئة في حقل العلاقات الدولية من خلال حداثة هذا المجال فهناك تاريخ طويل من التخمينات حول دور التكنولوجيا الرقمية في الدراسات الأمنية، و قد كان هناك تاريخ واسع من الإختبارات النظرية و الأخلاقية بشأن المخاوف المتعلقة بالأمن السيبراني.[1]

و مع نهاية الحرب الباردة، حدثت تحولات تدريجية، ظهرت على مستوى التفكير في الدراسات الأمنية لأن النظرة الضيقة المتمركزة حول الدولة كانت ستاتيكية ثابتة و دائما ما تؤدي إلى إنتقادات حول كيف كان الأمن دائماً مفهوما تقليديا.

و ضمن مجال الدراسات الأمنية النقدية، يمكن فهم دور الأمن السيبراني و هو ما تجلى في أعمال مدرسة كوبنهاغن و روادها أمثال: باري بوزان Barry BUZAN و أولي ويفر Ole WAEVER، حيث إكتسبت أعمالهم أهمية كبرى خاصة عند التفكير في الأمن السيبراني، لأن تركيزهم لم يقم على محاولة موضوعية لتصنيف ما هو التهديد أو ما هي الثغرة الأمنية، بل ما هي الشروط أو الحالة الراهنة التي يجب أن تباشرها جهات فاعلة محددة من أجل إظهار فعل ما بأنه تهديد و هو ما يعرف بعملية الأمنية "the process of securitization" و هي الإجراء الذي يحدد من خلاله المنظرين ما ينبغي و ما لا ينبغي تعريفه بأنه مشكلة أمنية، أي إضفاء الطابع الأمني على قضية معينة.[2]

1- فارس محمد العمرات، إبراهيم محمد الحمامصة: الأمن السيبراني، دار الخليج للنشر و التوزيع، ط.1، عمان، 2022، ص 9.

2- فريدة طاجين: تأثير القوة السيبرانية على الإستراتيجيات الأمنية للدول الكبرى، مذكرة شهادة الماستر، جامعة ورقلة، 2018، ص 11 .

و أصبح الأمن السيبراني مطلبا ضروريا لكل الدول دون إستثناء، لأنه يتعلق بالحماية من المخاطر المحتملة عن طريق مصادر خارجية من خلال الإنترنت، فهو إذن حماية الحواسيب المكتبية أو المحمولة من أي نوع من الإعتداءات أو الاختراقات و التهديدات التي تحدث عن طريق السيرفرات و الحواسيب الأخرى و شبكة الإنترنت بشكل عام، و يعمل مختصو الأمن السيبراني على ضمان عدم السماح لأحد غير مصرح له بالدخول و الوصول إلى المعلومات.[1]

فالذين يمارسون الجرائم الإلكترونية يقومون بنشر الفيروسات أو ينسخون المعلومات السرية و الهامة أو يعدلون و يحرفون في معلومات مهمة او حتى يبثوا معلومات غير صحيحة على مواقع مهمة، و ذلك عندما يكون الأمن السيبراني ضعيفا و يحتاج لتقوية بالتالي فإن مهمة هذا النوع من الأمن تكمن في حماية الحاسب كله من المصادر الخارجية، و أمن المعلومات ليس بعيدا عن الأمن السيبراني، فهو يهتم بحماية كل ما يتعلق بالمعلومات ضمن الحاسب او خارجه و ليس حماية الحاسب كله من أي خطر خارجي محتمل كالسرقة و الاختراق، و يمنع أي شخص غير مصرح له بالوصول إليها من ذلك، و من هنا و لأهمية هذا الجانب في حياة الدولة و حياة الأفراد جاءت هذه الدراسة ليستفيد منها الجميع[2].

و لقد كان لظهور الانترنت و الثورة المعلوماتية دورا في بزوغ العصر السيبراني، و خلق بيئة جديدة سميت بالفضاء السيبراني، و قد أصبح هذا الفضاء يؤثر في النظام الدولي، خاصة مع بروز شكل جديد من القوة السيبرانية، و التي توزعت و انتشرت بين عدد أكبر من الفاعلين على المستوى الدولي و المحلي، الأمر الذي جعل الفضاء السيبراني مجالا جديدا للصراع بين الدول.

1- منى عبد الله السمحان: متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية، مجلة كلية التربية، جامعة المنصورة، العدد 111 ، المملكة العربية السعودية، 2020، ص 56.

2- فريدة طاجين: المرجع السابق، ص 12.

و لقد أدى ظهور الفضاء الالكتروني و استخداماته في كثير من المجالات التي تغير شكل و طبيعة عمل النظام السياسي، حيث لعب دور المؤسسات الوسيطة و التواصل ما بين عملية صنع القرار و الرأي العام، إضافة إلى أنه ساعد على نقل النشاط السياسي الداخلي إلى ظاهرة عالمية، من خلال التواصل بين دول العالم المختلفة و الإنفتاح على التطورات الديمقراطية في العالم أجمع[1].

و يعد الهدف الأسمى للأمن السيبراني هو القدرة على مقاومة التهديدات المتعمدة و غير المتعمدة و الاستجابة و التعافي، و بالتالي التحرر من الخطر أو الأضرار الناجمة عن تعطيل أو إتلاف تكنولوجيا المعلومات و الإتصالات أو بسبب إساءة إستخدام تكنولوجيا المعلومات و الإتصالات و يتطلب حماية الشبكات و أجهزة الكمبيوتر، و البرامج و البيانات من الاعتداءات أو الضرر أو الوصول الغير المصرح به، و نتيجة لأهمية الأمن السيبراني في واقع مجتمعات اليوم فقد جعلته العديد من الدول على رأس أولوياتها، خاصة بعد الحروب الإلكترونية التي بدأت تظهر تجالياتها بين بعض الدول الكبرى، في إشارة صريحة إلى نهاية الحروب التقليدية التي كانت تستخدم فيها الأسلحة الثقيلة، و الإعلان عن بداية حروب جديدة هي الحروب الالكترونية[2].

إن إختيار موضوع الأمن السيبراني، جاء مدفوعا بجملة من الأسباب منها ما هو موضوعي و منها ما هو ذاتي، و التي يمكن حصرها في الأتي:

1- الأسباب الموضوعية:

- كون موضوع الدراسة يحوز على إهتمام بالغ الاهتمام لدى صناع القرار.

1- فارس محمد العمرات، إبراهيم محمد الحمامصة: المرجع السابق، ص 10.

2- المرجع نفسه، ص 10.

- الاهتمام بمعرفة و استكشاف الأمن السيبراني كونه موضوع حديث.

2- الأسباب الذاتية:

إن الميول الشخصي لمختلف القضايا التي تمس الأمن دفعني لإختيار هذا الموضوع ضمن قائمة المواضيع المقترحة من قبل الأستاذ المشرف و هذا بهدف الاطلاع المعمق عليه خاصة أنه موضوع حديث يعكس الوجه الأخر للتكنولوجيا و أخطارها إذا ما استعملت بطريقة غير مشروعة، و كذا من أجل إثراء الرصيد العلمي و المعرفي باللغة العربية في هذا الموضوع.

إن أهمية موضوع الأمن السيبراني من أهم الموضوعات التي تستدعي الغوص في عناصرها و تستحق البحث و الدراسة في إجراءاتها و ذلك كونها تندرج ضمن الدراسات الأمنية و الإستراتيجية و تبرز أهميته العلمية من خلال التعرف على الأمن السيبراني و أشكال تهديداته التي تخل بالأمن القومي للدول، و كذلك يعتبر الأمن السيبراني من المواضيع التي تعني بأهمية كبيرة لدى الدول، لمعرفة عناصر الأمن السيبراني و المعايير و المشاكل التي تواجه الأمن السيبراني.

تهدف دراسة هذا الموضوع إلى إبراز مجموع من المسائل و هي:

- التعرف على الأمن السيبراني من الناحية النظرية، و من خلال ضبط ماهية الأمن السيبراني، و تحديد عناصره، و كشف عن معاييره، و المشاكل التي تواجهه.
- المساهمة في خلق و تطوير الوعي الجماعي بشأن الظاهرة، فهي سلاح ذو حدين.
- معالجة الموضوع بأسلوب علمي و ذلك بالاستعانة بمناهج البحث العلمي، و مختلف النظريات التي اهتمت بالموضوع.

إن توسيع دائرة القوة السيبرانية في عدة مناطق من العالم، و عجز الدول عموما عن مواجهة التهديدات الناجمة عن ذلك، "الإعتداءات السيبرانية"، شكل أبرز ظواهر مشكلة البحث، و وفقا لذلك فإن مفهوم الأمن، و مقتضياته، أصبح في حاجة إلى المراجعة لا كمطلب سياسي، أو اقتصادي، أو اجتماعي، و إنما كخيار إستراتيجي بعيد المدى، فالنزاع لم يعد دوليا فقط، أو إقليميا، بل و محليا داخل الدولة.

عليه تقوم هذه الدراسة، بمعاجلة موضوع الأمن السيبراني و من هذا المنطلق يثار التساؤل الرئيسي حول:

صولا للإجابة عن هذه الإشكالية و عن هذه التساؤلات المتفرعة عنها فإنه إعتمادا على المنهج التحليلي بإعتباره يعمل على الجمع بين القانون و بين فهم الواقع، و ذلك من خلال شرح و تحلبل نصوص القانون هذا من جهة و نظرا لمستلزمات موضوع الدراسة فقد إعتمدنا من جهة أخرى على المنهج الوصفي على إعتباره يعد أسلوب من أساليب المنهج التحليلي من خلال وصف الحالة المراد دراستها و تفسيرها بموضوعية تنسجم و معطيات الدراسة و رغبة منا في الوصول إلى إنجاز عمل شامل و متكامل لهذا الموضوع.

يقتضي منا موضوع الدراسة شرح موضوع الأمن السيبراني الذي جعلنا نقسم هذا البحث إلى فصلين، حيث خصصنا لكل فصل مبحثين و هذا ما سيتم تبيانه من خلال الخطة التالية:

- تناولنا في الفصل الأول الإطار المفاهيمي للأمن السيبراني من خلال تقسيم هذا الفصل إلى مبحثين حيث خصصنا المبحث الأول ماهية الأمن السيبراني في حين خصصنا المبحث الثاني لأركان الجريمة بالإضافة إلى تقسم كل مبحث إلى مطالب.
- أما الفصل الثاني فتناولنا فيه المجال السيبراني إذ جعلنا من المبحث الأول خاص بأبعاد و مخاطر الأمن السيبراني و كيفية الردع و المبحث الثاني القوة السيبرانية و الإختراق.

- ثم نقوم في أخر المطاف بوضع حوصلة لهذه الدراسة من خلال عرض و تقديم مختلف النتائج المتوصل إليها و كذا المسائل المتفرعة عن الدراسة و ذلك بوضع خاتمة تجمع كل ما تحصلنا عليه من نتائج و ملاحظات و توصيات في دراستنا لهذا الموضوع.

الفصل الأول

الفصل الأول

الإطار المفاهيمي للأمن السيبراني

لقد أدت نهاية الحرب الباردة إلى بروز العديد من التحديات و التهديدات التي لم يشهدها المجتمع الدولي من قبل، و التي تعرف بالتهديدات اللاتماثلية أو اللاتناظرية العابرة للحدود التي لا تعترف بالحدود أو السيادة الوطنية أو فكرة الدولة القومية، الأمر الذي أدى إلى حدوث تحولات في حقل الدراسات الأمنية و الإستراتيجية و كذلك على مستوى الممارسة السياسية.

لقد أصبح الأمن السيبراني مطلبا ضروريا لكل الدول دون إستثناء، لأنه يتعلق بالحماية من المخاطر المحتملة عن طريق مصادر خارجية من خلال الإنترنت، فهو إذن حماية الحواسيب المكتبية أو المحمولة من أي نوع من الهجمات و الإختراقات و التهديدات التي تحدث عن طريق السيرفرات و الحواسيب الأخرى و شبكة الإنترنت بشكل عام، و يعمل مختصوا الأمن السيبراني على ضمان عدم السماح لأحد غير مصرح له بالدخول و الوصول إلى المعلومات، فالمارقون الذين يمارسون الجرائم الإلكترونية يقومون بنشر الفيروسات أو ينسخون المعلومات السرية و الهامة أو يعدلون و يحرفون في معلومات مهمة أو حتى يبثوا معلومات غير صحيحة على مواقع مهمة، و ذلك عندما يكون الأمن السيبراني ضعيفا و يحتاج لتقوية بالتالي فإن مهمة هذا النوع من الأمن تكمن في حماية الحاسب كله من المصادر الخارجية، و أمن المعلومات ليس بعيدا عن الأمن السيبراني، فهو يهتم بحماية كل ما يتعلق بالمعلومات ضمن الحاسب أو خارجه و ليس حماية الحاسب كله من أي خطر خارجي محتمل كالسرقة و الاختراق، و يمنع أي شخص غير مصرح له بالوصول إليها من ذلك، و لأهمية

هذه الحماية قامت الدولة بإستطلاع مدى الوعي المجتمعي بأهمية الأمن السيبراني و أمن المعلومات من خلال إجراء آراء عدد من المهتمين.[1]

لذلك فإن موضوع الدراسة يقتضي منا معرفة الإطار المفاهيمي للأمن السيبراني لذا سنخص لكل منها مبحثا مستقلا كالأتي:

- ماهية الأمن السيبراني كمبحث أول.
- أركان الجريمة كمبحث ثاني.

المبحث الأول

ماهية الأمن السيبراني

تعتبر مهمة ضبط المفاهيم و المصطلحات تحديا يواجه مختلف الباحثين و الدارسين في مختلف التخصصات، و ذلك لما يطرحه من إشكاليات تجعل من الصعوبة بمكان الاتفاق على تعريفات واضحة و شاملة و موحدة بين أعضاء المجتمع العلمي، و يعد الأمن السيبراني واحداً من المفاهيم المعقدة التي قدمت لها العديد من التعريفات المختلفة.

المطلب الأول

الأمن السيبراني

يشكل الأمن السيبراني جزءا أساسيا من أي سياسة أمنية وطنية فقد أصبحت الدول تصنف مسائل الدفاع السيبراني كأولوية في سياساتها الدفاعية كما خصصت أكثر من 130 دولة أقساما خاصة بالأمن السيبراني في فرقها الأمنية الوطنية، و يقصد بالأمن السيبراني مجموع الأطر القانونية و التظيمية و الهياكل التنظيمية و الوسائل التكنولوجية الوطنية

1- فارس العمارات، إبراهيم محمد الحمامصة، مرجع سابق، ص 11-12.

و الدولية التي تهدف إلى حماية الفضاء السيبراني الوطني كما تركز على حماية بيانات الأفراد و مؤسسات الدولة من الإستخدام الغير مصرح به أو أي أذى يلحق بشبكة البيانات[1].

الأمن السيبراني له 3 جوانب، حماية بيانات الأشخاص الإلكترونية و حماية الشركات و مؤسسات الدولة و بياناتها و عملائها ثم حماية الأمن القومي و سلامة المواطنين و رفاهيتهم و خصوصيتهم ألا تستخدم هذه البيانات بطرق غير شرعية أو ضد أصحابها.

يعتبر وجها لإحدى وجوه واقع العلاقات الدولية المعاصرة و التي وضعت مفهوم الأمن الوطني أو القومي كمحرك لهذه العلاقات و معيارا للسيادة الوطنية كما أصبح هاجسا لكافة الدول إعتبارا بهدفها الأسمى في حماية سلمها و أمنها و إلتزاما بإحترامها للأمن و السلم الدوليين بالموازاة مع محاربة الجريمة الإلكترونية و الإحتيال الإلكتروني و غيرها من المخاطر التي يأتي الأمن السيبراني على رأسه.[2]

الفرع الأول: مفهوم الأمن السيبراني:

يعرف الأمن السيبراني بأنه "مجموعة من الوسائل التقنية و التكنولوجية و العمليات التي يتم إستخدامها لحماية الشبكات و الأجهزة و البرامج و البيانات و من الإعتداءات أو التسلل الغير مسموح به و يعرف أيضا بأنه أمن تكنولوجيا المعلومات أو حماية المعلومات، كما يعرف أنه "النشاط الذي يؤمن حماية الموارد البشرية و المالية المرتبطة بتقنيات الإتصال كما يحد من

1- فيصل محمد عسيري، الأمن السيبراني و حماية أمن المعلومات، تاريخ الإضافة 02-2019، ص 1.
Application pdf http://www.kutub.info/librairy/book.21854

2- المرجع نفسه، ص 2.

الأضرار في حال حصول إعتداءات أو تهديدات سيبرانية و يعيد الوضع إلى ما كان عليه بأسرع وقت.[1]

أولا: الأمن السيبراني لغويا

مكون من لفظين "الأمن" و "السيبراني" و الأمن هو نقيض الخوف، أي بمعنى السلام، و الأمن مصدر الفعل أَمِنَ أَمْناً و أَمَاناً و أَمَنَةً: أي اطمئنان النفس و سكون القلب و زوال الخوف، و يقال أَمِنَ من الشر، أي سَلِمَ منه، و قد عرفه القاموس **بنغوين** للعلاقات الدولية بأنه مصطلح يشير إلى غياب ما يُهدد القيم النادرة.[2]

على الرغم من أن مصطلح الأمن القومي قد شاع بعد الحرب العالمية الثانية، إلا أن جذوره تعود إلى القرن السابع عشر، و خاصة بعد معاهدة **وستفاليا** عام 1648 التي أسست لولادة الدولة القومية أو الدولة **natio** و شكلت حقبة الحرب الباردة الإطار و المناخ اللذين تحركت فيهما محاولات صياغة مقاربات نظرية، و الأمة **state** و أطر مؤسساتية وصولا إلى إستخدام تعبير "إستراتيجية الأمن القومي"، و سادت مصطلحات الحرب الباردة مثل الاحتواء و الردع و التوازن و التعايش السلمي كعناوين بارزة في هذه المقاربات بهدف تحقيق الأمن و السلم و تجنب الحروب المدمرة التي شهدها النصف الأول من القرن العشرين.[3]

لقد تبنى آخرون مصطلح الحرب السيبرانية "cyber warfare" بالاستناد إلى أيديولوجية أمنية أو عسكرية تضع منهاجا لتحقيق الأهداف على الصعيد الأمني أو العسكري، تجاه " العدو المفترض".

1- فيصل محمد عسيري، المرجع السابق، ص 2.

2- محمود علي عبد الرحمن، "أسامة فاروق مخيمر، الفضاء الإلكتروني و أثره على مفاهيم القوة و الأمن و الصراع في العلاقات الدولية"، مجلة كلية السياسة و الإقتصاد، جامعة محمد البشير الإبراهيمي، برج بوعريريج، المجلد 6، العدد 5، الجزائر،2022، ص 438.

3- المرجع نفسه، ص 439.

أما البعض الأخر فاختار مصطلح الاعتداءات السيبرانية "Attacks cyber" كوصف واقعي يجمع بين فهو تصرف يدور في عالم افتراضي قائم على استخدام بيانات رقمية، و وسائل اتصال كل ما ذكر آنفا تعمل الكترونياً، و من ثم تطور ليتضمن مفهوما أوسع، يقوم على تحقيق أهداف عسكرية أو أمنية ملموسة و مباشرة، جراء اختراق مواقع الكترونية حساسة، عادة ما تقوم بوظائف تصنف بأنها ذات أولوية كأنظمة حماية محطات الطاقة النووية أو الكهربائية أو المطارات، و وسائل النقل الأخرى.[1]

لأن مصطلح الحرب هو مصطلح غير محبذ في وقتنا الراهن على مستوى التنظيم القانوني الدولي فيكون مصطلح الهجمات السيبرانية أكثر قربا للموضوع الذي تتناوله هذه الدراسة، و لاسيما أن تصرفات دولية عدة أشارت إلى مصطلح الهجمات، و عدتها بمثابة التصرف الذي يوضع في الحسابات أثناء النزاعات المسلحة، طبقا للقانون الدولي الإنساني.

السيبراني هي مصطلح السيبرانية إلا أن، و هو واحد من أكثر المصطلحات تردداً في معجم الأمن الدولي و تشير المقاربة الإبتيمولوجية لكلمة "cyber" إلى أنها لفظة يونانية الأصل مشتقة من كلمة "Norbert Kubernetes" بمعنى الشخص الذي يدير دفة السفينة، حيث تستخدم مجازا للمتحكم "Governor".

تجدر الإشارة إلى أن العديد من المؤرخين يرجعون أصلها إلى عالم الرياضيات الأمريكي و ذلك للتعبير عن التحكم الآلي، فهو الأب الروحي المؤسس للسبرنيتيقية من "1894-1964 wieners خلال مؤلفه الشهير:

"Cybernetics or control and communication the animal and the machine

أشار في كتابه إلى أن السبرنتيفيقة هي التحكم و التواصل عند الحيوان و الآلة و الإنسان، و الآلة ليستبدل مصطلح الآلة بعد الحرب العالمية الثانية بالحاسوب.[2]

1- فارس العمارات، إبراهيم محمد الحمامصة، المرجع السابق، ص 13-14.

2- نفس المرجع، ص 15.

ثانيا: مفهوم الأمن السيبراني إصطلاحاً

هناك العديد من التعريفات التي قدمت لمفهوم الأمن السيبراني، حيث يعرف بأنه: " **مجموعة من الإجراءات المتخذة في مجال الدفاع ضد الاعتداءات السيبرانية و نتائجها التي تشمل تنفيذ التدابير المضادة المطلوبة".**

تعريف ريتشاردكمرر " Richard a kemmerr" على أنه عبارة عن وسائل دفاعية من شأنها كشف و إحباط المحاولات التي يقوم بها القراصنة، بينما يعرفه إدوارد أمورسو " Edward Amoroso" على أنه وسائل من شأنها الحد من خطر الاعتداء على البرمجيات أو أجهزة الحاسوب أو الشبكات، و تشمل تلك الوسائل الأدوات المستخدمة في مواجهة القراصنة، و كشف الفيروسات و وقفها و توفير الإتصالات المشفرة.[1]

الأمن السيبراني عبارة عن فن ضمان وجود و إستمرارية مجتمع المعلومات لأمة، و ضمان و حماية فضاء الإنترنت و المعلومات الخاصة به، و الأصول و البنية التحتية الخاصة به.[2]

كما يعرف الأمن السيبراني إنطلاقا من أهدافه بأنه النشاط الذي يؤمن حماية للموارد البشرية و المالية المرتبطة بتقنيات الإتصالات و المعلومات، و يضمن إمكانية الحد من الخسائر، و الأضرار التي تترتب في حالة تحقق المخاطر و التهديدات، كما يتيح إعادة الوضع إلى ما كان عليه بأسرع وقت ممكن بحيث لا تتوقف عجلة الإنتاج و بحث لا تتحول الأضرار إلى خسائر دائمة.[3]

1- بارة سميرة، "الأمن السيبراني في الجزائر"، المجلة الجزائرية للأمن الإنساني، العدد 4، جامعة قاصدي مرباح، ورقلة، الجزائر، 2017، ص 256.

2- المرجع مفسه، ص 257.

3- نسيب نجيب، الحرب السيبرانية من منظور القانون الدولي الإنساني، المجلة النقدية للقانون و العلوم السياسية، كلية الحقوق و العلوم السياسية، جامعة مولود معمري، تيزي وزو، المجلد 19، العدد 4، 2021، ص 222.

في التقرير الصادر عن الاتحاد الدولي للاتصالات حول اتجاهات الإصلاح في الاتصالات لعام 2010-2011 عرف الأمن السيبراني بأنه: **"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".**[1]

قدمت وزارة الدفاع الأمريكية "البنتاغون" تعريفا دقيقا لمصطلح الأمن السيبراني، فاعتبرته: **"جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية و الالكترونية، من مختلف الجرائم، الهجمات، التخريب، التجسس و الحوادث".**

كذلك الأمن السيبراني، يعرف بأنه أمن الشبكات و الأنظمة المعلوماتية، و البيانات و المعلومات و الأجهزة المتصلة بالإنترنت، فهو المجال الذي يتعلق بإجراءات و مقاييس، و معايير الحماية المفروض اتخاذها، أو الالتزام بها، و يرتبط هذا الأمن، ارتباطا وثيقاً، بأمن المعلومات، فالوصول إلى هذه الأخيرة، أو بثها أو الاطلاع عليها و المتاجرة بها، أو تشويهها و استغلالها، هو ما يقف غالب الأحيان، وراء عمليات الاعتداء على الشبكات و على الإنترنت بشكل أكثر.[2]

من هنا فإن الأنظمة الالكترونية تعتمد على المعلومة، الحقيقية، و التي تفرض اعتمادا على التي تعالجها و الحديث عن الأمن، يستدعي تعريف الخطر، أي التهديد الذي يتعرض له النظام، إضافة إلى نقاط الضعف، أو الثغرات التي تعتريه، و من ثم الإجراءات المفروض اتخاذها، لدفع الخطر، فالتهديد هو نوع من الأعمال العدائية، التي يمكن أن تمارس ضد النظام، بينما نقاط الضعف هي مستوى الانكشاف على التهديد في سياق معين، و الإجراءات

1- الحروب السيبرانية، ويكبيديا، http://ar.m.wikipedia.org/wiki/d8 0103

2- فارس العمارات، إبراهيم محمد الحمامصة، المرجع السابق، ص 15-16.

التي يفترض اتخاذها، و لا يمكن أن تقتصر في أي حال من الأحوال على التقنية، بل أنها تتناول بناء القدرات و التوعية و التدريس و نقل الخبرات.

و هنا تجدر الإشارة إلى أن الأمن السيبراني مفهوم أوسع من أمن المعلومات فالأمن السيبراني يهتم بأمن كل ما هو موجود على السايبر من غير أمن المعلومات، بينما أمن المعلومات لا يهتم بذلك، كما أن أمن المعلومات يهتم بأمن المعلومات الفيزيائية" الورقية بينما لا يهتم الأمن السيبراني بذلك.

ثالثا: مفهوم الأمن السيبراني إجرائيا

يمكن القول عن الأمن السيبراني هو مجموعة الآليات و الإجراءات و الوسائل و الأطر التي تهدف إلى حماية البرمجيات و أجهزة الكمبيوتر الفضاء السيبراني بصفة عامة من مختلف الإعتداءات و الاختراقات و التهديدات السيبرانية التي قد تهدد الأمن القومي للدول.[1]

الفرع الثاني: أهمية و أهداف الأمن السيبراني

للأمن السيبراني أهمية كبيرة لكل مجتمع و لكل دولة، فالأمن السيبراني مهم على مستوى الفرد في حماية البيانات الشخصية و الصور و الملفات و الفيديوهات و الحسابات الشخصية و كلمات المرور و الحسابات البنكية. و على مستوى المجتمع، من حيث حماية المجتمع من الهندسة الاجتماعية و استهداف السلوك الاجتماعي و البيانات المجمعة و الخصوصيات للمجتمع. و على مستوى الشركات و المؤسسات، في حماية الأصول الإلكترونية و البيانات و المعلومات و بيانات الموظفين و السيرفرات و المواقع الالكترونية. و على مستوى الدولة، في حماية أمنها الالكتروني و حماية الأنظمة المالية و الاقتصادية و العسكرية و التلفزيون و الراديو من الإعتداءات الإلكترونية و القرصنة و التعطيل.[2]

1- فارس العمارات، إبراهيم محمد الحمامصة، المرجع السابق، ص 17.

2- محمود علي عبد الرحمن، أسامة فاروق مخيمر، المرجع السابق، ص 437.

أولا: أهمية الأمن السيبراني

للأمن السيبراني أهمية بالغة في الفضاء السيبراني، خاصة ما تعلق بالجانب الوقائي للبيانات، و المعلومات، و الإتصالات المختلفة و تكمن هذه الأهمية في النقاط التالية:

- إستكشاف نقاط الضعف و الثغرات في الأنظمة و معالجتها.
- توفير بيئة عمل آمنة جدا خلال العمل عبر الشبكة العنكبوتية.
- الحفاظ على المعلومات و تجانسها و سلامتها و ذالك بكف الأيادي من العبث بها و تحقيق وفرة البيانات و جاهزيتها عند الحاجة إليها.
- يحمي الأمن السيبراني مختلف أنواع البيانات الحساسة و المهمة من تعرضها للسرقة أو الإتلاف.
- تعرض الأمن السيبراني للإختراق من بشأنه أن يحدث الكثير من الأضرار التي تلحق بسمعة الشركة أو المؤسسة و بالتالي تؤثر على مستوى التعاملات التي تقوم بها في الأسواق التجارية.[1]

ثانيا: أهداف الأمن السيبراني

- تعزيز حماية أنظمة التقنيات التشغيلية، على كافة الأصعدة و مكوناها من أجهزة و برمجيات و ما تقدمه من خدمات و ما تحويه من بيانات.
- التصدي للهجمات و حوادث أمن المعلومات التي تستهذف الأجهزة الحكومية و المؤسسات و القطاع العام و الخاص.
- توفير بيئة آمنة و موثوقة للتعاملات في مجتمع المعلومات.
- صمود البنية التحتية الحساسة للهجمات الإلكترونية.

1- مها دحام، متاح على الموقع، تاريخ الإطلاع 2023/04/09، www.stors.com

- توفير متطلبات الأزمة للحد من المخاطر و الجرائم الإلكترونية التي تستهدف المستخدمين.[1]
- سد الثغرات في أنظمة أمن المعلومات.
- مقاومة البرمجيات الخبيثة و ما تستهدفه من إحداث أضرار بالغة للمستخدمين.

المطلب الثاني

الجريمة السيبرانية

إن مخاطر السيبرانية قد تزداد كلما ازدادت هيمنة تكنولوجيا المعلومات و الاتصال على النسق العام للحياة، فأصبحنا أمام جرائم حقيقية و متكاملة الأركان، تتم عن طريق شبكة الإنترنت بأشكال مختلفة كسرقة الأموال و النصب و الاحتيال و التخطيط للعمليات الإرهابية، فضلا عن ترويج الأخبار المضللة و القرصنة بإعتبارها الجريمة الأكثر شيوعا في العالم الرقمي.

في هذا السياق، فإن البحث في مكنونات الأمن السيبراني و التحديات الأمنية في العصر الرقمي بحاجة إلى الغوص فيها من أجل بيان بيئة التهديدات، خاصة أن شبكة الإنترنت توفر لحوالي مليار و نصف مواقع الكترونية و صفحات لا عدد لها، و خاصة مع الإنتشار الواسع فيما بعد العام 2018، و إتصالا بموضوع التهديدات السيبرانية تشير تقارير عدة و إحصائيات إلى نحو حوالي 95٪ من الشركات الكبرى متعددة الجنسيات تعترف بتعرضها للقرصنة، حيث إتخذت أكثر من حوالي 135 حكومة في العالم إجراءات حازمة تخص العالم الافتراضي و الأمن الالكتروني، خاصة مع كثرة الإعتداءات الإلكترونية بين الدول.[2]

1- منى عبد الله السمحان، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية، مجلة كلية التربية، جامعة المنصورة، العدد111 ، المملكة العربية السعودية، 2020، ص 11-12.

2- فارس العمارات، إبراهيم محمد الحمامصة، المرجع السابق، ص 42.

يمكن إعتبار تحدي الأمن السيبراني أعلى تحديات يواجهها الأمن القومي في القرن الواحد و العشرين خاصة أن الأمن لا يقتصر فقط على الجوانب العسكرية، بل فإنه يواكب كل التهديدات و التحديات التي يمكن أن تشكل حجر عثرة أمام الإقتصاد الرقمي و تدفق المعرفة[1].

لم يتفق الفقهاء و الباحثين على تعريف موحد للجرائم السيبرانية منهم من ينظر إلى موضوع الجريمة و منهم من ينظر إلى الوسيلة المستعملة لارتكابها، فبالنظر إلى موضوع الجريمة يرى هذا الإتجاه أنها كل سلوك إيجابي أو سلبي يقع بإستخدام تقنية المعلومات على مصلحة مشروعة بالإعتداء، في حين ينظر آخرون إلى وسيلة إرتكاب الجريمة و يرون بأنها كل فعل إجرامي يستخدم الكمبيوتر كأداة رئيسية.[2]

تفاديا للقصور في التعريفات المضيقة ذهب البعض إلى القول بأن هذه الجرائم هي كل عمل أو إمتناع عن عمل يأتيه الإنسان إضرار بمكونات الحاسب المادية و المعنوية و شبكات الاتصال الخاصة به، بإعتبارها من المصالح و القيم المتطورة التي يحميها القانون.[3]

غير أن ما نلاحظه من خلال هذا التعريف أنه حدد نطاق هذه الجرائم و جاء واسعا لا يشمل الجانب البرمجي للنظم المعلوماتية فحسب، بل يدخل فيها كل ما تفرزه التطورات التكنولوجية من جديد.

الفرع الأول: خصائص الجرائم السيبرانية وتقسيماتها

إن طبيعة الجرائم السيبرانية و تميزها عن الجرائم التقليدية يرجع إلى الوسط الذي ترتكب فيه الجريمة و هي الآداة أو الوسيلة التي إستخدمها الجاني في إرتكاب فعله غير المشروع، و تتطلب توفر معرفة أو حد أدنى من الثقافة التقنية لدى الجاني، و هي لا تخرج عن كونها

1- فارس العمارات، إبراهيم محمد الحمامصة، المرجع السابق، ص 42.

2- رامي متولي القاضي، مكافحة جرائم المعلوماتية، دار النهضة العربية، مصر، 2011، ص 17.

3- محمد أمين الشوابكة، جرائم الحاسوب و الانترنت، دار الثقافة، الإمارات العربية المتحدة، 2011، ص 9.

سلوك إجرامي ينشأ بإرتكاب فعل جرمه القانون أو الإمتناع عن فعل أمر به القانون، و تتجه إرادة الجاني إليه رغم وجود نص قانوني يجرم السلوك.[1]

أولا: خصائص الجرائم السيبرانية

يمكن إجمال خصائص هذه الجرائم في عدة نقاط:

- جرائم تتم بإستخدام الحاسب الآلي كأداة لإرتكاب الجريمة، و تستخدم شبكة الإنترنت كوسيلة لذلك.[2]
- جرائم لا يتم في أغلب الأحيان التبليغ عنها، خاصة إذا تعلق الأمر بالمؤسسات و الشركات التجارية، تجنبا للإساءة للسمعة أو إهتزاز ثقة العملاء.[3]
- جرائم صعبة الإكتشاف لعدم تركها لآثار مادية يمكن من خلالها حل القضية و يطلق على هذه الآثار بالآثار المعلوماتية الرقمية.
- جرائم غامضة لصعوبة إثباتها و ذلك بسبب غياب الدليل المرئي و لأن أغلب البيانات عبارة عن رموز لا يمكن قراءتها.
- جرائم عابرة للحدود الوطنية تلحق أضرار جسيمة تمس عدة أقاليم.
- جرائم تستدعي إلمام مرتكبيها بالمعرفة التقنية و الخبرة الفائقة في مجال الحاسب الآلي.
- جرائم لا تمتاز بالعنف، لا يستخدم مرتكبيها القوة الجسدية أو العضلية للقيام بالجريمة.

أما التشريع الجزائري لم يستقر على إستخدام مصطلح واحد للدلالة على هذه الجرائم حيث سماها بموجب القانون رقم 04-15، المتضمن قانون العقوبات بجرائم المساس بأنظمة

1- أحمد طارق عفيفي صادق، الجرائم الإلكترونية، المركز القومي للإصدارات القانونية، القاهرة، 2015، ص 24.

2- نبيلة هروال، جرائم الإنترنت، دارسة مقارنة، رسالة الدكتوراه، كلية الحقوق و العلوم السياسية، جامعة بوبكر بلقايد، تلمسان، 2014، ص 37.

3- محمد الأسدي، مدى فاعلية الأحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، دار حام للنشر و التوزيع، عمان، الأردن، 2015، ص 25.

المعالجة الآلية للمعطيات، ثم بموجب القانون رقم 09-04، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها، إستخدم مصطلح الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال للدلالة على هذه الجرائم، و عرفها بأنها : جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أي جريمة أخرى ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية أو نظم الإتصالات الإلكترونية.[1]

ثانيا: تقسيمات الجرائم السيبرانية

وفقا للمفوضية الأوروبية فإن الجرائم السيبرانية تشمل ثلاث فئات من النشاط الإجرامي، و هي:

- صور الجرائم التقليدية مثل الإحتيال و التزوير المعلوماتي.
- نشر المحتوى الغير مشروع بالوسائل الإلكترونية منها المتعلقة بالعنف الجنسي ضد الأطفال و إنتهاك حقوق الملكية الفكرية.
- الإعتداءات الخاصة بالشبكات الإلكترونية كالقرصنة.[2]

هذا و قد قسمت **إتفاقية بودابست** هذه الجرائم إلى أربعة أصناف تشمل:

- جرائم تمس خصوصية و سلامة و توافر بيانات و نظم الكمبيوتر.
- جرائم متصلة بالكومبيوتر كالتزوير و الإحتيال عبر الكمبيوتر.
- جرائم متعلقة بالمحتوى كالجرائم المتعلقة بالمواد الإباحية ضد القصر.
- جرائم متعلقة بحقوق النشر و التأليف و الحقوق المجاورة.[3]

1- القانون رقم 09-04، المؤرخ في 14 شعبان 1430، الموافق لـ 5 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام و الاتصال و مكافحتها، ج.ر-ج.ج، ع. 47، الصادر في 16 أوت 2009.

2- يوسف مناصرة، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، دار الخلدونية، الجزائر، 2018، ص 48.

3- الإتفاقية الأوروبية المتعلقة بالجريمة الإلكترونية، بودابست، 2001، مجلس أوروبا، مجموعة المعاهدات الأوروبية، رقم 185، حرر في 23 نوفمبر/تشرين الثاني 2001.

عددت الإتفاقية العربية لمكافحة جرائم تقنية المعلومات هذه الجرائم و هي:

- جرائم الدخول الغير المشروع.
- جرائم الإعتراض الغير المشروع.
- الإعتداء على سلامة البيانات.
- جرائم إساءة إستخدام وسائل تقنية المعلومات.
- جرائم التزوير و الإحتيال.
- جرائم الإباحية و ما يرتبط بها.
- جرائم الإعتداء على الحياة الخاصة.
- الجرائم المتعلقة بالإرهاب الإلكتروني.
- الجرائم المتعلقة بالجرائم المنظمة و المرتكبة بواسطة تقنية المعلومات.
- الجرائم المتعلقة بإنتهاك حقوق المؤلف و الحقوق المجاورة.
- الإستخدام غير المشروع لأدوات الدفع الإلكتروني.[1]

الفرع الثاني: آليات و قوانين الحد من الجرائم السيبرانية

الواقع أن خاصية العالمية التي تميز جرائم المعلوماتية قد دفعت رجال القانون و الفقهاء إلى الدعوة لمواجهتها من خلال وضع قواعد اتفاقية تعبر عن تصور دولي موحد لتدارك النقائص و الثغرات التي تعتري منظومة القوانين الداخلية للدول و ذلك بهدف التقليل من حدة آثار هذه الجريمة. و في هذا الإطار تضافرت الجهود من أجل وضع إطار قانوني اتفاقي يسمح بمتابعة مرتكبي جرائم المعلوماتية و معاقبتهم، و هو الأمر الذي تجسد في إتفاقيات

1- الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، المصادق عليها من طرف الجزائر بموجب المرسوم رقم 14-252، الموافق لـ 8 سبتمبر 2014، ج.ر، ع. 57، الصادر بتاريخ 28 سبتمبر 2014، ص 26.

ثنائية و متعددة الأطراف متعلقة بالمسألة، سواء على المستويين الدولي أو الإقليمي، و من أجل بيان تلك الجهود من الأهمية بمكان الإشارة إلى بعضها بإيجاز فيما يأتي:

أولا: سبل مكافحة الجرائم المعلوماتية قبل صدور القانون 09-04

إعتبر المشرع الجزائري برامج الحاسوب الآلي من المصنفات الأدبية و الفنية، و في ذلك نصت المادة 04 من الأمر رقم 09-04 المتعلق بحقوق المؤلف و الحقوق المجاورة على إعتبار برامج الحاسوب الآلي كمصنف أدبي مكتوب محمي بهذا القانون، فالحقوق المادية أو المالية هي الإطار الذي يمكن صاحب الحق من إستغلال برنامجه بشتى الطرق من دون غيره أو لمن يخوله هو نفسه هذا الحق، و له في ذلك إبلاغه للجمهور بأية منظومة معالجة معلوماتية و يترتب على ذلك حقوق مادية للمؤلف صاحب البرنامج بالإستغلال التجاري له و لورثته بمختلف الطرق.[1]

قد حدد هذا الأمر أحكام جزائية تنص على جنحة التقليد و العقوبات المقررة لها بموجب المواد من 151 إلى 160 من هذا الأمر، و مع هذه البداية دخلت مجموعة تعديلات أخرى على قانون العقوبات الإجراءات الجزائية و هو ما سنتناوله:

1- تعديل قانون العقوبات:

بدأ المشرع الجزائري في مواكبة التطورات التكنولوجية من خلال إدخاله لمجموعة تعديلات على قانون العقوبات بإدراج قسم خاص يتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات بموجب القانون 04-15 المؤرخ في 10 نوفمبر 2004، ثم توالي التعديلات و إدراج بعض السلوكيات الإجرامية المتعلقة بذلك بموجب 06-23 المؤرخ في 20 ديسمبر2006، منها

1- زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري، الجزائر، دار الهدى، 2011، ص 88.

الدخول و البقاء عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات، أو الإدخال عن طريق الغش معطيات في نظام المعالجة الآلية أو الإزالة أو التعديل بطريق الغش لبعض المعطيات،أو في حالة تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية أو حيازة أو إفشاء أو نشر أو إستعمال المعطيات بطريق الغش، كما تشدد العقوبة في حالة حذف أو تغيير المعطيات، أو تخريب نظام إشغال المنظومة.

رغم نص المشرع الجزائري على هذه المواد إلا أنه لم يتطرق إلى جرائم القذف و السب الإلكتروني أو المطاردة عبر الإنترنت أو الغش المعلوماتي و إنما إكتفى بالنصوص العقابية التقليدية التي لا تتوافق مع طبيعة الجرائم السيبرانية و لا تتماشى مع مبدأ شرعية الجرائم و العقوبات و حظر القياس.[1]

2- تعديل قانون الإجراءات الجزائية:

إستحدث المشرع الجزائري بموجب قانون الإجراءات الجزائية مجموعة من الإجراءات الخاصة التي تتماشى مع العالم الإفتراضي و تتمثل في إعتراض المراسلات و إلتقاط الصور و تسجيل الأصوات، و إجراء التسرب[2]

حيث سمح المشرع الجزائري باللجوء إلى إعتراض المراسلات و إلتقاط الصور و تسجيل الأصوات لمقتضيات التحري و التحقيق في جرائم محددة حصرا و من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، و لا بد أن تراعي في ذلك شروط محددة قانونا، و المتمثلة في الإذن، و طبيعة الجريمة، و كتمان السر المهني، و تحرير محضر من طرف ضابط الشرطة القضائية المأذون له بالعملية و أشار المشرع بموجب المادة 03 من القانون 09-04

1- نبيلة هروال، مرجع سابق، ص388.

2- المرجع نفسه، ص 389.

إلى ضرورة إحترام سرية المراسلات، و عرف الإتصالات الإلكترونية في المادة 01 من نفس القانون بأنها أي تراسل أو إرسال أو إستقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة لأي رسالة إلكترونية.[1]

كإجراء آخر فقد أجاز المشرع اللجوء إلى التسرب بموجب المادة 65 مكرر 11 قانون الإجراءات الجزائية الجزائري، و ذلك إذا إقتضت ضرورة التحري و التحقيق ذلك في الجرائم المحدد حصرا و من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، حيث يجوز لوكيل الجمهورية أو لقاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب بإحترام الضمانات و الشروط المقررة قانونا، و المتمثلة في إحترام شرط الإذن المكتوب و المسبب و من ثم يمكن إستخدام هوية مستعارة للقيام بالتسرب في مدة زمنية محددة تقدر بأربعة أشهر قابلة للتجديد، و يحرر تقريرا يتضمن أهم العناصر الضرورية لمعاينة الجريمة.[2]

ثانيا: آليات مكافحة الجرائم السيبرانية على ضوء القانون09-04

كخطوة جديدة قام المشرع الجزائري بسن القانون 09-04 المتعلق بالوقاية من تكنولوجيا الإعلام و الإتصال و مكافحتها، و إن كان تجسيد بنوده على أرض الواقع مازال ضعيفا إلى حد الساعة نتيجة إهمال الجوانب التقنية الكفيلة بتصنيف هذه الجرائم و في تحديد العقوبة المناسبة في حق مرتكبيها، حيث تقتصر العقوبات في غالبية الأحيان على الغرامة المالية فقط.[3]

1- المادة 04 من القانون 09-04، مرجع سابق، ص 6.

2- أحمد بن خليفة، محفوظة الأمير عبد القادر، الجريمة الإلكترونية و آليات التصدي لها، الجزائر، 2017، ص 165.

3- المرجع نفسه، ص 166.

غير أنه وضع مجموعة من تدابير وقائية و إجرائية للوقاية من هذه الجرائم و مكافحتها، و أهمها:

1- تدابير الوقاية:

يهدف هذا القانون إلى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها.

أ- المراقبة الالكترونية:

حيث سمح بهذا الإجراء في حالات محددة حصرا[1] و تكون بموجب إذن مكتوب من السلطات القضائية المختصة، للوقاية من الأفعال الإرهابية أو التخريبية أو الجرائم الماسة بأمن الدولة، أو في حالة توفر معلومات عن إحتمال إعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، كما أنه لمقتضيات التحريات و التحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى هذا الإجراء، و يمكن الإستعانة بالمراقة الإلكترونية في إطار تنفيذ المساعدة القضائية الدولية المتبادلة.

ب- الإستعانة بمزودي الخدمات للوقاية من الجرائم السيبرانية:

يكون ذلك من خلال تقديم مزودي الخدمات المساعدة للسلطات المكلفة بالتحريات القضائية لجمع و تسجيل المعطيات المتعلقة بمحتوى الإتصالات في حينها و بوضع المعطيات تحت تصرف السلطات، و تشمل هذه المعطيات:[2]

- المعطيات التي تسمع بالتعرف على مستخدمي الخدمة.

1- المادة 04 من القانون 09-04، المرجع سابق 6.

2- المادة 11 من القانون 09-04، المرجع سابق 7.

- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للإتصال.
- الخصائص التقنية و كذا تاريخ و وقت و مدة كل إتصال.
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة و مقدميها.[1]
- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الإتصال و كذا عناوين المواقع المطلع عليها.

يشترط إلتزام مقدمي الخدمات بحفظ هذه المعطيات و أطلق عليها : المعطيات المتعلقة بحركة السير، و لم يغفل تعريفها بموجب المادة 01 من القانون بأنها: أي معطيات متعلقة بالإتصال و الوجهة المرسل إليها و الطريق الذي يسلكه و وقت و تاريخ و حجم و مدة الإتصال و نوع الخدمة.

زيادة على ذلك أفرد المشرع الجزائري بمجموعة إلتزامات خاصة بمقدمي خدمات الإنترنت تشمل التدخل الفوري لسحب المحتويات المخالفة للقوانين و تخزينها أو حضر الدخول إليها، إضافة إلى الإلتزام بموضوع ترتيبات تقنية تحصر إمكانية الدخول إلى الموزعات التي تحتوي على معلومات مخالفة للنظام العام أو الآداب العامة.[2]

1- التدابير الإجرائية:

مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات و الإتصالات، يمكن لمقتضيات حماية النظام العام أو مستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية في هذا القانون، وضع ترتيبات تقنية لمراقبة

1- المادة 12 من القانون 09-04، المرجع السابق، ص 8.

2- المادة 03 من القانون 09-04، المرجع السابق، ص 6.

الإتصالات الإلكترونية و تجميع و تسجيل محتواها في حينها و القيام بإجرات التفتيش و الحجز داخل منظومات معلوماتية.[1]

أ- تفتيش و حجز المنظومة المعلوماتية:

فالمقتضيات حماية النظام أو مستلزمات التحريات أو التحقيقات القضائية الجارية، تم وضع مجموعة ترتيبات تقنية لمراقبة الإتصالات الإلكترونية، و تجميع و تسجيل محتواها في حينها، و القيام بإجراءات التفتيش و الحجز داخل المنظومة المعلوماتية.[2]

غير أن إجراء الحجز قد تصادفه عدة إشكالات لأسباب تقنية مما يتعين على السلطات التي تقوم بالتفتيش إستعمال تقنيات مناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية أو إلى نسخها الموضوع تحت تصرف الأشخاص المرخص لهم بإستعمال هذه المنظومة.[3]

جدير بالذكر أن هذا القانون أجاز اللجوء إلى التفتيش و لو عن بعد بسرعة إلى منظومة معلوماتية أو جزء منها و كذا المعطيات المعلوماتية المخزنة فيها، كما يمكن التفتيش عن بعد في منظومة تخزين معلوماتية.

يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها و تزويدها بكل معلومات ضرورية.[4]

1- المادة 03 من القانون 09-04، المرجع السابق، ص 6.

2- المرجع نفسه.

3- المادة 07 من القانون 09-04، المرجع السابق، ص 7.

4- المرجع نفسه.

ب- تمديد الإختصاص بهذه الجرائم:

حيث يؤول الاختصاص للمحاكم الجزائرية بالنظر للجرائم المتصلة بالتكنولوجيات الإعلام و الإتصال المرتكبة خارج الإقليم الوطني، في حالة إرتكاب الجريمة من أجنبي و كانت الجريمة تستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني.[1]

ت- تبادل المساعدة القضائية الدولية:

سمح المشرع الجزائري بإمكانية تبادل المساعدة القضائية الدولية لجمع الأدلة المتعلقة بالجريمة في شكلها الإلكتروني، و من الممكن الإستجابة لطلبات المساعدة الرامية إلى تبادل المعلومات أو إتخاذ أي إجراءات تحفظية وفقا للإتفاقيات الدولية أو وفقا لمبدأ المعاملة بالمثل.[2]

ث- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها:

إستحدثت هذه الهيئة بموجب القانون 09-04 و بقيت تشكيلتها و تنظيمها و كيفيات سيرها لتحدد عن طريق التنظيم و الذي توالت فيه التغيرات إبتداء من المرسوم الرئاسي لسنة 2015 ثم سنة 2019 ليأتي المرسوم الرئاسي لسنة 2020 ليعيد تنظيم الهيئة، و عرفها بأنها : سلطة إدارية مستقلة تتمتع بالشخصية المعنوية و الاستقلالية المالية توضع تحت سلطة رئيس الجمهورية، و يحدد مقرها في الجزائر العاصمة، و يمنكن نقله إلى أي مكان من التراب الوطني

1- المادة 15 من القانون 09-04، المرجع السابق، ص 8.

2- المادة 17 من القانون 09-04، المرجع السابق، ص 8.

بموجب مرسوم رئاسي، و تتكون الهيئة من مجلس توجيه و مديرية عامة يوضعان تحت السلطة المباشرة لرئيس الجمهورية و يقدمان عرضا عن نشاطاتهما.[1]

ثالثا: القوانين اللاحقة المتممة للقانون 09-04 للحد من الإجرام السيبراني

القوانين اللاحقة للقانون 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها و التي تنص على آليات و أساليب و طرق التصدي للجرائم السيبرانية و الحد منها و من بين هذه القوانين نذكر ما يلي:

1- القانون 18-04 المتعلق بالقواعد العامة المتعلقة بالبريد و الإيصالات الإلكترونية:

حيث إستحدث هذا القانون و وضع مجموعة آليات للتصدي للجرائم المتعلقة بالعالم الإفتراضي منها، استحداث سلطة ضبط من بين مهامها السهر على إحترام متعاملي البريد و الإتصالات الإلكترونية للأحكام القانونية و التنظيمية المتعلقة بالبريد و الإتصالات الإلكترونية و الأمن السيبراني.[2]

تجريم إنتهاك سرية المراسلات المراسلة عن طريق البريد أو الإتصالات الإلكترونية أو إفشاء مضمونها أو نشرها أو إستعمالها دون ترخيص من المرسل أو المرسل إليه أو الأخبار بوجودها، و تجريم محاولة فتح أو تخريب أو تحويل البريد أو المساعدة في إرتكاب هذه الجريمة، و سنت مجموعة من العقوبات ضمن المواد من 164 إلى 188 من هذا القانون.[3]

1- مرسوم رئاسي رقم 20-183، المؤرخ في 13 يوليو 2020، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها، ج.ر، ع 40، الصادر بتاريخ 18 يوليو 2020، ص 6.

2- المادة 13 من القانون 18-04، المؤرخ في 10 مايو 2018، الذي يحدد القواعد العامة المتعلقة بالبريد و الإتصالات الإلكترونية، ج.ر،عدد 7، الصادر في 13 مايو 2018، ص 10.

3- المرجع نفسه، ص 11.

2- القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي:

ضع المشرع الجزائري مجموعة من الآليات المتعلقة بالعالم الإفتراضي و التي يمكن إجازها في عدة نقاط:

- إستحداث سلطة وطنية لحماية المعطيات ذات الطابع الشخصي.
- وضع مجموعة إلتزامات ملقاة على عاتق المسؤول عن المعالجة الآلية للمعطيات ذات الطابع الشخصي.
- إتخاذ السلطة الوطنية لمجموعة إجراءات إدارية في حالة خرق أحكام القانون من طرف المسؤول عن المعالجة.
- يمكن للسلطة الوطنية القيام بالتحريات و معاينة المحلات و الأماكن التي تتم فيها المعالجة بإستثناء محلات السكن، كما يمكنها الولوج إلى معطيات المعالجة و جميع المعلومات و الوثائق التي كانت دعامتها.
- تأهيل أعوان رقابة للقيام ببحث و معاينة الجرائم المتعلقة بالمعطيات ذات الطابع الشخصي تحت إشراف وكيل الجمهورية.
- يمكن للمدعي المساس بحق من حقوقه المنصوص عليها في هذا القانون أن يطلب من الجهة القضائية إتخاذ أي إجراءات تحفظية للحد من التعدي أو الحصول على تعويض.
- تختص الجهة القضائية الجزائرية بمتابعة هذه الجرائم التي ترتكب خارج إقليم الجمهورية من طرف جزائري أو شخص أجنبي مقيم في الجزائر أو شخص معنوي خاضع للقانون الجزائري، كما تختص بمتابعة الجرائم المنصوص عليها في هذا القانون وفقا لقواعد الإختصاص المنصوص عليها في المادة 588 من قانون الإجراءات الجزائية.

– تجريم الإعتداء على المعطيات ذات الطابع الشخصي بإفراد عقوبات مالية و أخرى سالبة للحرية وفقا للمواد من 54 إلى 74 من هذا القانون.[1]

المبحث الثاني

أركان الجريمة

القاعدة العامة أن الجريمة تقوم على ركنين أساسيين، فالأول هو الركن المادي الذي يقر أنه "لا جريمة دون سلوك مادي" فلا عقاب لدينا في القانون الجنائي على النوايا "اما الثاني هو الركن المعنوي يتمثل في القصد الجنائي و هو اتجاه إرادة الجاني إلى تحقيق النتيجة الإجرامية مع علمه بأن ما هو مُقْدم عليه يوقعه في الإثم الجنائي، و لا تثير مسألة الوقوف على الركن المادي أي صعوبات بالنظر إلى خصائصه المادية المدركة بالحواس، غير أن ما يثير الكثير من المشاكل العملية هو كيفية الوقوف على الركن المعنوي، لاسيما أن مسألة الوقوف على توافر الركنين ترتبط بارتباط وجود أو عدم وجود الجريمة.[2]

لابد من وجود مسؤولية جنائية التي تعني إسناد الفعل إلى الجاني، كما يكون الجاني لحظة إرتكاب الجريمة متمتع بالوعي و الإرادة، فارتكاب الجريمة حتى و إن وصلت لحد القتل و ثبت أن الجاني غير مميز أو معدوم الإرادة فلا يسأل جنائيا.

إذا أنه من الصعب إسناد النتيجة الإجرامية لصاحب السلوك الذي أدى إليها دون معرفة طبيعة الإستعداد النفسي لدى الجاني في تقبل تلك النتيجة، و دون معرفة إن كان ذلك عن قصد أو عن طريق الخطأ، و هذا ما يؤسس أيضا إلى قاعدة لا جريمة بدون ركن معنوي لكن الملاحظ اليوم و مع تطور المجتمعات من كل النواحي خاصة الاقتصادية منها جعل

1– المادة 53 من القانون 18–07، المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات طابع شخصي، ج.ر، عدد 34، الصادر بتاريخ 10 يونيو 2018، ص 22.

2– الهادي كنزو، محاضرات في القانون الجنائي العام، كلية الحقوق و العلوم السياسية، تونس، 1988، ص 68.

التشريعات تتبنى أنواع جديدة من التجريم تتماشى و السرعة المطلوبة للفصل في مثل القضايا الاقتصادية ذات الطابع الجزائي و ذلك باللجوء إلى الاكتفاء بإثبات السلوك المادي دون الخوض في تعقيدات إثبات الركن المعنوي، باعتباره حالة نفسية تستوجب أساليب معقدة للكشف عن طبيعتها، بل أن قانون. العقوبات بنفسه يزخر أيضا بعدة نصوص تفترض هذا الركن بمجرد توافر العناصر المادية للجريمة.[1]

منه فإنه لا تختلف أركان الجريمة السيبرانية عن أركان أي جريمة أخرى فلابد من توافر الركن المادي و الركن المعنوي.

المطلب الأول

الركن المادي

القانون لا يعاقب الإنسان على مُجرد الأفكار و النوايا، و لا عن المشاعر و الأحاسيس الباطنية، و لا يتدخل إلا إذا تجسدت هذه الأفكار في العالم الخارجي في شكل مادي ملموس، يلُحق الضرر بالفرد أو المجتمع، و الركن المادي للجريمة هو كل العناصر التي يتطلبها النص الجنائي لقيام الجريمة فالركن المادي يمثل صلب كل جريمة لأن المشرع لا يجرم مجرد التفكير في الجريمة أو على مجرد الدوافع و النزاعات النفسية إنما يستوجب أن تظهر تلك النزاعات و العوامل في صورة واقعة مادية هي الواقعة الإجرامية فالمشرع لا يستطيع تفسير أعماق نفوس البشر و التفتيش في تفكيرهم المجرد ليعاقبهم على ذلك و قد اتفق الفقهاء على أن الركن المادي للجريمة هو مظهرها الذي يبرز إلى العالم الخارجي و أن القاعدة العامة هي أن لا

1- المادة 01 من الأمر رقم 66-156، المؤرخ في 8 يونيو1966، يتضمن قانون العقوبات، ج.ر.ج، عدد49، صادر بتاريخ 11 يونيو1966، المعدل و المتمم بالقانون رقم 16-02، المؤرخ في 19 يونيو2016، ج.ر-ج.ج، عدد 37، صادر بتاريخ 22 يونيو2016 .

جريمة بدون ركن مادي و كذلك و يعُرف الركن المادي بأنه: "النشاط المادي الذي يصدر عن الجاني متخذا مظهرا خارجيا يتدخل من أجله القانون بتقرير العقاب" و لذلك يشُترط لقيام الجريمة عناصر بناء الركن المادي و هي الفعل و النتيجة و العلاقة السببية بينهما.[1]

الفرع الأول : السلوك الإجرامي

هو ذلك النشاط المادي الخارجي للجريمة أو هو حركة الجاني الإختيارية التي يترتب عليها تغيير في العالم الخارجي، و إن النشاط أو السلوك المادي في جرائم السيبرانية يتطلب وجود بيئة رقمية و إتصال بالإنترنت و يتطلب معرفة بداية هذا النشاط و الشروع فيه و نتيجته، فمثلا يقوم مرتكب الجريمة بتجهيز الحاسوب لكي يحقق له إمكانية إرتكاب الجريمة، فيقوم بتحميل الحاسب ببرامج إختراق، أو أن يقوم بإعداد هذه البرامج بنفسه، و كذلك قد يحتاج إلى تهيئة صفحات تحمل في طياتها مواد مخلة بالآداب العامة و تحميلها على الجهاز المضيف، كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيداً لبثها[2].

كل جريمة تستلزم وجود أعمال تحضيرية فهي تتعلق بتهيئة الوسائل اللازمة لإتمام ما عقد الفاعل العزم عليه و هي الخطوات التي تعقب نشاطه نحو إرتكاب الجريمة، فتأتي بعد التفكير و العزم فتبرز ماديا في العالم الخارجي بأعمال مادية ملموسة، حيث يختار الفاعل الوسائل الضرورية لتنفيذ جريمته و الظروف المناسبة لذلك، فالأعمال التحضيرية تتعلق بتهيئة الوسائل لإتمام ما عقد الفاعل العزم عليه و هي خطوات تخرج عن نطاق التفكير في الجريمة و تقترب من مرحلة التنفيذ، و هذه المرحلة غير معاقب عليها مبدئياً و ذلك تشجيعاً للعدو

1- فريد روابح، محاضرات في القانون الجنائي العام، موجهة لسنة الثانية لسانس، كلية الحقوق و العلوم السياسية، قسم الحقوق، جامعة محمد لمين دباغين، سطيف، الجزائر، 2019، ص 52 -69.

2- المرجع نفسه، ص 71.

و عدم إتمام الجريمة، و في الحقيقة يصعب الفصل بين العمل التحضيري و البدء في النشاط الإجرامي في الجرائم السيبرانية و الإنترنت حتى و لو كان القانون لا يعاقب على الأعمال التحضيرية، إلا أنه في مجال تكنولوجيا المعلومات الأمر يختلف بعض الشئ، لكن المشرع المصري مع ذلك جرم بعض الأفعال التحضيرية و إعتبرها جرائم مستقلة مثل شراء برامج الإختراق، و معدات لفك الشفرات و كلمات المرور، فالتشريعات المقارنة أشارت صراحة إلى عنصر البدء في التنفيذ و إعتبرت أن مرحلة التجريم تبدأ عندما يصل الجاني إلى تلك المرحلة فقط، فالمادة 45 من قانون العقوبات المصري تنص على أن الشروع هو البدء في تنفيذ فعل بقصد إرتكاب جريمة[1].

إن السلوك الإجرامي هو النشاط المادي الخارجي الذي يصدر عن الجاني ليحقق النتيجة الجرمية التي يعاقب عليها القانون و هو عنصر ضروري في كل جريمة و لا يتدخل المشرع الجنائي بالعقاب قبل صدور النشاط المادي الخارجي المكون للجريمة حيث أن الجاني قبل أن يقدم على الجريمة يمر بمراحل من النشاط الذهني و المادي لا يناولها المشرع بالعقاب لأن الجريمة تبدأ بفكرة في ذهن الجاني قد يصرف النظر عنها أو قد يصمم على تنفيذها و إلى هذا الحد لا يباشر الإنسان نشاطا مجرما يستح العقاب لأن المشرع لا يعاقب على النوايا و المقاصد الشريرة مهما كانت واضحة ما لم تخرج إلى حيز الوجود في سلوك مادي ملموس تبقى خارج دائرة العقاب.[2]

إن السلوك الإجرامي المكون للركن المادي للجريمة إما أن يكون إيجابيا أو سلبيا، و الجريمة الإيجابية هي تلك الجريمة التي يكون السلوك المكون لركنها المادي إيجابيا أي

1- علي حسين الخلف، المبادئ العامة في قانون العقوبات، المكتبة القانونية، بغداد، العراق، 1991، ص 137.

2- علي راشد، القانون الجنائي، ط 2، دار النهضة العربية، 1974، ص 213. أنظر، محمد زكي أبو عامر، قانون العقوبات اللبناني، القسم العام، دار الجامعة، بيروت، 1984، ص 75.

إرتكاب. أما الجرائم السلبية فهي أي امتناع عن عمل يأمر القانون بالقيام به و يعاقب من يمتنع عن ذلك، و ليس للتفرقة بين الجرائم الإيجابية و الجرائم السلبية أهمية كبيرة من الناحية العملية إلا في موضوع الشروع حيث لا يتصور الشروع في الجرائم السلبية لأن هذه الجرائم إما أن تقع تامة أو لا تقع،[1] حيث أن السلوك الإجرامي هو كل حركة آو مجموعة حركات عضوية إرادية من شأنها أن تحدث تغييرا في العالم الخارجي سواء لدى المشرع التعبير عن الإرادة بحركة عضوية واحدة آو مجموعة حركات و إذا تحقق السلوك الإجرامي بصورة سلبية آو إيجابية لا عبرة بعدئذ بالقول في أي عنصر آخر في تشكيل السلوك الإجرامي فالأصل أنه لا يعد من الأفعال الإجرامية الوسائل المستخدمة آو مكان إتيان السلوك الإجرامي آو زمانه و تطبيقا لذلك فان المشرع يجرم فعل الإعتداء على الحياة لأنه يستهدف مصلحة جوهرية في حماية الحق في الحياة.[2]

أن تحقق الجريمة بالإمتناع تكون في أحوال إمتناع الشخص عن إتيان فعل ايجابي معين كان ينتظر منه في ظروف معينة فتحقق الجريمة بالإمتناع يتطلب توافر ثالث عناصر الأول هو ضرورة الإحجام عن إتيان فعل إيجابي معين و مثال ذلك جريمة الإمتناع عن إنشاء السلطة العامة عن جناية مخلة بأمن الدولة و العنصر الثاني هو ضرورة أن يكون الإمتناع من بأنه الإخلال بواجب قانوني لأن إمتناع المجرم يفترض إلزاما قانونيا سواء كان مصدر هذا الواجب قانون العقوبات أو القوانين المكملة له كما كان الجائز أن يكون مصدر الواجب عمال قانونيا كالعقد أو المبادئ القانونية العامة، و العنصر الثالث هو ضرورة توفر الصفة الإرادية

1- محمد إسماعيل المعموري، محاضرات في قسم القانون – الجرائم الايجابية و السلبية، كلية القانون، جامعة بابل، العراق، 2010، ص 65.

2- أحمد فتحي سرور، الوسيط في قانون العقوبات، القسم العام، دار النهضة، 1989، ص 247.

لالمتناع أي تكون الإرادة مصدر الإمتناع و أن تتوافر صلة السببية بين الإرادة و السلوك السلبي الذي إتخذه الممتنع.[1]

الفرع الثاني :النتيجة الجرمية

تثير مسألة النتيجة الإجرامية في الجرائم السيبرانية جدلا كبيرا بين أنصار المذهب المادي و أنصار المذهب القانوني حول تحديد الجريمة السيبرانية هل هي جرائم مرتكبة سلوكا أو كنتيجة في العالم الإفتراضي، أم أن هناك امتدادا للنتيجة لتحقيق وجودها المادي.[2]

هي العنصر الثاني من عناصر الركن المادي بعد السلوك الإجرامي و هي التغيير الذي يحدث في العالم الخارجي كأثر للسلوك الإجرامي فيتحقق عدوانا ينال مصلحة أو حقا قدر المشرع جدارته بالحماية القانونية مما يعني أنها مدلولين، مادي و هو التغير الناتج عن السلوك الإجرامي في العالم الخارجي و الأخر قانوني و هو العدوان الذي ينال مصلحة أو حقا يحميه القانون[3] و انقسم الفقه في بأن تعريف النتيجة الجرمية إلى إتجاهين الأول قانوني و الثاني مادي حيث إن الإتجاه القانوني هو العدوان الذي يصيب حقا أو مصلحة يحميها القانون سواء تمثل هذا العدوان في ضرر فعلي يصيب الحق أو المصلحة محل الحماية أو مجرد تعرض هذا المحل للخطر حيث هو التكييف القانوني للآثار المادية المترتبة على السلوك الإجرامي حيث ينتهي هذا الإتجاه إلى ان النتيجة شرط أو عنصر في كل جريمة، إما الإتجاه المادي فهو يصور النتيجة على أنها تغيير يطرأ في العالم الخارجي كأثر للسلوك الإجرامي أي يعتبر النتيجة حقيقة مادية لها كيانها في العالم الخارجي، و إن الإختالف واضح بين الإتجاهين حيث أن النتيجة وفقا للإتجاه القانوني عبارة عن تكييف أو وصف للسلوك الإجرامي الذي ينال من حق او مصلحة يحميها القانون أي أنها أمر معنوي غير محسوس و هي تدخل في علة

1- أحمد فتحي سرور، مرجع سابق، ص 237.

2- فريد روابح، مرجع سابق، ص 79.

3- محمود نجيب حسني، شرح قانون العقوبات، القسم العام، المكتبة القانونية، القاهرة، مصر، 1990، ص 277.

التجريم، إما وفقا للإتجاه المادي فهي منفصلة عن السلوك و لها كيان مادي ملموس في العالم الخارجي و النتيجة كعنصر من عناصر الركن المادي للجريمة لا يعتد بها إلا إذا كان يتجسد فيها صفات هذا الركن من مظهر خارجي أو كيان مادي ملموس في العالم الخارجي و بهذا ينفصل الإتجاه المادي عن الإتجاه القانوني.[1]

و تثير مسألة النتيجة الإجرامية في الجرائم السيبرانية مشاكل عدة فعلى سبيل المثال المكان و زمان تحقيق النتيجة الإجرامية، فلو قام أحد المجرمين في بلد ما بإختراق جهاز خادم server أحد البنوك في بلد أخر، و هذا المكان ، موجود في بلد ثالث فكيف يمكن معرفة وقت حدوث الجريمة هل هو توقيت بلد المجرم أم توقيت بلد البنك المسروق أم توقيت الجهاز الخادم، و القانون الواجب التطبيق في هذا الشأن، و هنا نظر المشرع المصري للإختصاص المكاني فقط.[2] و إن العلاقة بين مدلولين النتيجة حسب الفقه توجد رابطة تصل بين مدلولي النتيجة فالنتيجة بوصفها حقيقة قانونية هي تكييف قانوني للآثار المادية التي ينتجها السلوك الإجرامي و بالتالي يكون منطقيا أن يتحدد المعنى القانوني للنتيجة نطاق معناها المادي فالآثار التي ينتجها السلوك الإجرامي كثيرة و متنوعة حيث أن القانون لا يحفل بجميع هذه الآثار و إنما يحفل ببعضها الذي يتجسد فيه الإعتداء على المصلحة القانونية و بهذا يعتبر المعنى القانوني وسيلة لإستبعاد الآثار التي لا تعني المشرع عن تلك التي تتميز بأهمية قانونية، حيث أن الجرائم جميعها تنتج عنها نتيجة بالمعنى القانوني و بعض الجرائم تترتب عليها نتيجة بالمعنى المادي.[3]

1- علي حسين الخلف، المرجع سابق، ص 140.

2- المرجع نفسه، ص 145.

3- فخري عبد الرزاق الحديثي، شرح قانون العقوبات، (القسم الخاص)، الجرائم الواقعة على الأشخاص، ط 2، دار الثقافة للنشر و التوزيع، الأردن، 2009، ص 290.

النتيجة الإجرامية يقصد بها الآثار الذي يحدث في العالم الخارجي كأثر للسلوك الإجرامي، و هذا التغير لا يقصد به التغير الواقعي و إنما التغير القانوني، أي الذي يتطلبه المشرع في النموذج القانوني للجريمة.

قد تكتمل الجريمة و تحقق نتيجتها الإجرامية، و قد تختلف هذه النتيجة برغم استنفاذ الجاني سلوكه الإجرامي، كما أنه قد لا يكمل الجاني هذا السلوك نتيجة عامل مستقل، و في مثل هاتين الحالتين لا يكتمل الركن المادي للجريمة و يطلق على الجريمة المرتكبة مصطلح الشروع أو المحاولة.

إذا كان الشروع في الجريمة السيبرانية جريمة خاصة ناقصة النتيجة التي كان الجاني يسعى إليها بسبب خارج عن إرادته، فإن ذلك يغطي في تطبيقات الشروع ثلاثة فروض أساسية يجمع بينها عدم إفضاء نشاط الجاني إلى نتيجة يمكن إلقاء تبعتها عليه قانونا.[1]

- **الفرض الأول:** عدم إفضاء نشاط الجاني بالمرة إلى النتيجة الإجرامية المقصودة و لا إلى اي نتيجة إجرامية اقل جسامة، كإطلاق فيروس إختراق على بخص دون أن يصاب من جرائها بأذى لأنه إمتنع عن فتح رسالته لعطل في الجهاز المستهدف.
- **الفرض الثاني:** تتحقق فيه بعد نشاط الجاني ذات النتيجة الإجرامية التي كان يسعى إليها دون أن يمكن قانوناً نسبتها إلى فعله، لإنقطاع علاقة السببية بينهما، فثمة في هذا الفرض تحقق مادي للنتيجة النهائية المقصودة دون ان تعتبر الجريمة تامة في مواجهة الجاني.[2]

1- أسامة مهمل، الإجرام السيبراني، رسالة ماجستير، كلية الحقوق و العلوم السياسية، جامعة محمد بوضياف، المسيلة، 2018، ص 83.

2- خالد حسن أحمد لطفي، الدليل الرقمي و دوره في إثبات الجريمة المعلوماتية، دار الفكر الجامعي، الإسكندرية، مصر، 2020، ص 96.

كذلك ثمة صورتان أساسيتان للشروع:

- **الشروع التام:** و يعرف كذلك" بالجريمة الخائبة"، و فيها يستنفد الجاني نشاطه الإجرامي كاملا و تختلف النتيجة لسبب خارج عن إرادته، مثل أن يقوم بخص بإنشاء حساب إلكتروني بقصد نشر الاباحية و التحريض على قتل أو إيذاء بخص و يقوم مدير الموقع بحذف المنشور او الحساب قبل إنتاج جريمته.
- **الشروع الناقص:** و يعرف بالجريمة الموقوفة و هو الصورة الثانية للشروع، و فيها لا يستنفذ الجاني نشاطه الإجرامي حتى نهايته، و إنما يوقفه أو يحبطه عامل خارجي فلا يستكمل النشاط و لا تتحقق النتيجة، مثلا أن يقوم الشخص بإنشاء فيروس لإختراق موقع و يوقفه نظام الحماية الجدار الناري الموجود على النظام فلا تتم جريمته.[1]

لا مجال للشروع في الجريمة إلا إذا قطع الجاني، على طريق الجريمة، مسافة يمكن معها القول بأنه قد بدأ في تنفيذها، و لكن تحديد ذلك ليس بالأمر اليسير و يرجع هذا إلى أن المشروع الإجرامي، في الجرائم الكبرى على وجه الخصوص، يمر بمسار طويل يبدأ بالمرحلة النفسية الخالصة، ثم التحضير لإرتكاب الجريمة، ثم البدء في تنفيذها، ثم تنفيذها كاملة.[2]

أما المرحلة النفسية، ففيها تتولد فكرة الجريمة و تتبلور تدريجيا حتى تنقلب إلى عزم و تصميم على إرتكابها، و القاعدة أنه لا تجريم و لا عقاب على ما يدور داخل النفس مهما بدا العزم قاطعاً، و القول بغير ذلك مؤداه تدخل سافر في مكنون الأنفس، و مطاردة قانونية لمجرد النوايا، و فتح لباب التعسف على مصراعيه فضلا عن أنه لا خطورة من التصميم الإجرامي المجرد، لأنه يجوز لصاحبه أن يعدل عنه دون عائق قبل التنفيذ، و من حسن السياسة

1- أسامة مهمل، مرجع سابق، ص 85.

2- المرجع نفسه، ص 86.

التشريعية تشجيعه على ذلك، و قد أكد المشرع هذا المعنى بوضوح في الفقرة الثانية من المادة 45 بقوله "لا يعد شروعاً في الجناية أو الجنحة مجرد العزم على إرتكابها..."[1]

مع ذلك يتدخل المشرع أحيانا و يجرم عزما او تصميما إجراميا متبلورا، و ذلك حينما يقدر أن تصميم الجاني قد أقترن بفعل خارجي يعبر عن خطورة ملموسة، فيخلق حينئذ من هذا الوضع جريمة قائمة بذاتها، و من ذلك أن يتخذ العزم صورة تهديد شفوي او مكتوب بإرتكاب قتل، او يعبر عن التصميم بالإنضمام إلى عصابة إجرامية او بتأمر بين عدة أشخاص لإرتكاب جريمة ماسة بأمن الدولة.

تنقسم النتيجة الإجرامية إلى قسمين:

1- جرائم الضرر: هي التي يطلب القانون في ركنها المادي حصول ضرر معين، و ذلك مثل حصول الضرر في الجرائم السلبية و الإيجابية.

2- جرائم الخطر: فهي جرائم السلوك المجرد حتى لو لم تقع النتيجة الإجرامية و كذلك كما في جرائم المشروع و التي تعاقب عليها الأنظمة في حالة كونها جناية، و ذلك لما يمثله السلوك الإجرامي من خطر دون النظر في نتيجة ذلك الفعل.[2]

بينما يختلف الأمر في الجنح و المخالفات فلا يعاقب عليها القانون بصفة عامة نظرا لقلة خطورة الدافع الإجرامي في نفس الفاعل.

1- محمد إسماعيل المعموري، مرجع سابق، ص 79.

2- علي عبد القادر القهوجي، شرح قانون العقوبات، القسم العام، ط 1 ، منشورات الحلبي الحقوقية، 2008، ص 55.

الفرع الثالث: العلاقة السببية

يراد بها الصلة التي تربط ما بين السلوك الإجرامي و النتيجة الجرمية الضارة ك رابطة العلة بالمعلول، بحيث تثبت ان السلوك الإجرامي الواقع هو الذي أدى إلى حدوث النتيجة الضارة. و السببية هذه أهميتها فهي التي تربط بين عنصري الركن المادي فتقيم بذلك وحدته و كيانه و بالتالي فمن دونها لا قيام فان مرتكب السلوك لا يسال إلا عن شروع في الجريمة إذا كانت الجريمة عمدية مقصودة، أما إذا كانت غير عمدية، فلا يسأل إطلاقا لأنه شروع في الجرائم غير العمدية[1] أما معيار تحقق العلاقة السببية تظهر أهمية وضع معيار لمعرفة تحقق قيام علاقة السببية عندما تساهم مع سلوك الجاني في أحداث النتيجة الجرمية عوامل أخرى حيث يثور التساؤل عما إذا كان تدخل هذه العوامل ينفي علاقة السببية او يتركها قائمة[2].

تعد السببية من أعقد المسائل و أدقها في التشريع الجنائي فرابطة السببية في تحديد المسؤولية الجنائية للفاعل لها أهمية بالغة تظهر على وجه الخصوص في الجرائم السيبرانية بإعتبارها أكبر الجرائم إثارة لمشاكل السببية، إن جرائم الحاسبات بإعتبارها من الجرائم ذات النتيجة لا تقوم مسؤولية الفاعل عنها لمجرد إسناد الفعل المادي للجاني و إنما يتوجب فوق ذلك إسناد النتيجة إلى الفعل للمساءلة عن الجريمة، فإذا لم تتوافر رابطة السببية بين الفعل و النتيجة تقف مسؤوليتها الفاعل عند حد الشروع، إذا كان الفعل مقترنا بقصد الأضرار أما في الخطأ غير المقصود عندما يقترن الفعل بالخطأ، فلا يكفي أن يقع خطأ من الفاعل و تحدث الجريمة، بل لا بد أن تستند الجريمة السيبرانية إلى خطأ الفاعل، و عند إنتفاء الرابطة السببية بينهما،[3] لا يسأل الفاعل عن جريمته، و السؤال الذي نطرحه حول رابطة السببية بينهما هو

1- السعيد مصطفى السعيد، الأحكام العامة في قانون العقوبات، ط 1، مؤسسة المعارف للطباعة و النشر، مصر، 1962، ص 80.

2- سلطان عبد القادر الشاوي، المبادئ العامة في قانون العقوبات، المكتبة القانونية، بغداد، العراق، 1991، ص 138.

3- محمد إسماعيل المعموري، مرجع سابق، ص 80.

الآتي: إذا تعددت العوامل التي ساهمت في إحداث الجريمة السيبرانية فإلى أي مدى يعتبر فعل الجاني سبباً في إحداث الضرر؟ لقد خلا التشريع المصري من أي تنظيم لنظرية السببية، و بالرغم من الموضوعات الشائكة التي تطرحها هذه النظرية مما فتح الباب واسعاً للإجتهاد و الإختلاف على مستوى الفقه و القضاء، بالمقابل نجد أن المشرع السوري قد نظم نظرية السببية و قننها بنص صريح في قانون العقوبات موفراً على الفقه و القضاء عناء إيجاد حلول للإشكاليات التي تطرحها مسألة السببية، و قد أخذ أحكام هذا التشريع من المادة 41 من قانون العقوبات الإيطالي، و من تلك المادة نجد أن علاقة السببية كي تعتبر متوفرة لا يشترط أن تكون في الجرائم المقصودة فقط و إنما يجب توفرها في الجرائم المقصودة و غير المقصودة، فهي لا غنى عن توفرها في القتل قصداً و القتل عن طريق الخطأ.[1]

فلا يكفي لقيام الجريمة السيبرانية أن يكون هناك فعل و نتيجة ضارة لهذا الفعل، و إنما يجب أن يكون هناك علاقة سببية تربط بين هذا الفعل و تلك النتيجة، فيجب أن يتصل الفعل بالنتيجة صلة العلة بالمعلول و المسبب بالسبب، و ذلك كي يتحمل الفاعل عبء النتيجة التي أفضى إليها فعله، و إذا لم يتوافر عنصر السببية فلا يكتمل الركن المادي للفعل و تكون العلاقة السببية بين الفعل و النتيجة متوفرة متى كان هذا الفعل صالحاً في الظروف التي إرتكب فيها لإحداث تلك النتيجة وفقاً لمجرى الأمور العادي.[2]

يقصد برابطة السببية ضرورة توافر رابطة بين سلوك الجاني و النتيجة الإجرامية بحيث يمكن القول أن النتيجة حدثت بسبب سلوك الجاني لا غيره، فالسلوك الإجرامي يتنوع إلى سلوك إيجابي و سلوك سلبي.

1- محمود عمر محمود، الجرائم المعلوماتية و الإلكترونية، خوارزم العلمية، 2015، ص 145.

2- علي عبد القادر القهوجي، مرجع سابق، ص 57.

1- السلوك الإيجابي: و هو كل حركة عضوية إرادية تصدر عن الجاني و يتوصل بها إلى إرتكاب الجريمة.[1]

2- السلوك السلبي: و هو إمتناع عن القيام بعمل يفرضه القانون مثل إمتناع مدير الموقع الإلكتروني عن الحفاظ على بيانات العملاء بعدم إتباعه تعليمات أمان المواقع و بناء الحوائط النارية و برامج الحماية من الفيروسات و الإختراقات و تحديثها.[2]

لم يحدد القانون الجنائي معيارا لتحديد الرابطة السببية، فناقش علماء القانون و إستقر رأيهم على ثلاث نظريات:

1- نظرية تعادل الأسباب: و هي تساوي جميع العوامل التي تساهم في إحداث النتيجة الإجرامية، فهي متعادلة من حيث قوة أثرها في حصول النتيجة.[3]

2- نظرية السبب الأقوى أو السبب المباشر: فهي لا تساوي بين الأسباب المساهمة في حصول الجريمة، بل تنظر إلى السبب الأقوى سواء كان هو سلوك الجاني أو غيره، و هذه النظرية حصرت النتيجة في عامل واحد هو أقوى الأسباب، و هذا يؤدي بالجاني إلى الإفلات من العقاب.

1- محمد حميد المزمومي، الوسيط في شرح نظام الإجراءات الجزائية السعودي، ط 2، مركز النشر العلمي بجامعة الملك عبد العزيز، جدة، السعودية، 2019، ص 182.

2- خالد حسن أحمد لطفي، الدليل الرقمي و دوره في إثبات الجريمة المعلوماتية، ط 1، دار الفكر الجامعي، الإسكندرية، مصر، 2021، ص 94.

3- سلطان عبد القادر الشاوي، مرجع سابق، ص 140.

3- نظرية السببية الملائمة: و مضمونها أن الجاني يسأل عن النتائج المحتملة أو المتوقعة لفعله و ذلك حسب المجرى العادي للأمور، ما لم يتدخل لقطع تلك العلاقة بسب شاذ أو غير مألوف، و قد تكون هذه النظرية هي أنسب النظريات ظن فلو أرسل الجاني فيروسا إلى بريد المجني عليه الإلكتروني مما تسبب في تلف الجهاز بالكامل لدى فتح المجني عليه بريده الإلكتروني، فهذا سبب مباشر يسأل الجاني عنه، بينما لو كان المجني عليه قد أُرسلت له عدة فيروسات من عدة أشخاص و تسببت. بمجموعها بتلف الجهاز، فإن القضاء حينئذ يعمل إحدى النظريات السابقة.[1]

المطلب الثاني

الركن المعنوي

من المعروف قانونا أن كل شخص يصدر عنه فعل من الأفعال المجرمة في القانون تقوم في حقه المسؤولية الجنائية باعتبار أن الشخص يمس أمن و مصلحة المجتمع بكامله و ليس فقط الأفراد. و قيام الجريمة في القانون لا يتوقف فقط على إرتكاب الواقعة المادية من طرف الجاني إنما يستلزم رابطة نفسية تصل بين الجاني و الفعل المادي الذي يقوم بارتكابه.[2]

هذه الرابطة النفسية تتمثل في الركن المعنوي الذي هو الحلة النفسية للجاني، التي تربط بين ماديات الجريمة و شخصية الجاني، فهو في الحالة النفسية و الذهنية للفاعل أثناء إقترافه للجريمة فلم تعد التشريعات الجنائية تكتفي بوجود فعل مادي مجرم لقيام المسؤولية الجنائية بحق الفاعل بل لابد من التعرف على الحالة النفسية للفاعل المرافقة لإقترافه الجرم و التي من خلالها يستطيع القاضي التعرف على مدى خطورة الفاعل و العقوبة المناسبة للحد من خطورته

1- السعيد مصطفى السعيد، مرجع سابق، ص 82.

2- سمير عالية، أصول قانون العقوبات القسم العام (معالمه، نطاق تطبيقه، الجريمة، المسؤولية، الجزاء)، ط 1، المؤسسة الجامعية للدراسات و النشر و التوزيع، بيروت، لبنان، 1996، ص 234.

إصلاح حاله إن أمكن، و قد تنقل المشرع الأمريكي في تحديد الركن المعنوي للجريمة بين مبدأ الإرادة و مبدأ العلم، فهو تارة يستخدم الإرادة كما هو الشأن في قانون العلامات التجارية في القانون الفيدرالي، و يعرف بأنه العلم بالجريمة و إرادة إرتكابها و بالتالي يتكون هذا الركن من عنصرين هما العلم و الإرادة.[1]

1- العلم: هو إدراك الأمور على نحو مطابق للواقع، يسبق الإرادة، و يشمل على عدة عناصر:

- العلم بالوقائع.
- العلم بموضوع الجريمة.
- العلم بحقيقة الفعل و خطورته و أنه يلحق ضرار بالحق المعتدى عليه.

لا يشترط شرط العلم في القانون الجنائي أن يكون الجاني عالما بأن الفعل الذي يقدم عليه هو فعل مجرم يعاقب عليه القانون.[2]

2- الإرادة: فهي إتجاه لتحقيق السلوك الإجرامي، و قوة نفسية و نشاط نفسي يوجه لتحقيق هدف معين بوسيلة معينة، فهي ظاهرة نفسية يصدر عن وعي و إدراك، و تقوم الإرادة على عنصرين.[3]

- **إرادة الفعل:** و هي إثبات بأن الجاني قد إتجه إلى عمل يمثل فعله خطر على الحق الذي يحميه القانون.
- **إرادة النتيجة:** فلا يكتفى بإرادة الفعل بل لابد من إرادة النتيجة، ليكتمل القصد الإجرامي بالركن المعنوي.[1]

1- سمير عالية، مرجع سابق، ص 235.

2- محمد حميد المزمومي، مرجع سابق، ص 189.

3- محمود أحمد القرعان، الجرائم الإلكترونية، ط 1، دار وائل للنشر و التوزيع، عمان، الأردن، 2017، ص 75.

برزت تلك المشكلة في قضية **موريس** الذي كان متهما في قضية دخول غير مصرح به على جهاز حاسوب فيدرالي و قد دفع محامي موريس على إنتفاء الركن المعنوي، الأمر الذي جعل المحكمة تقول "هل يلزم أن يقوم الإدعاء بإثبات القصد الجنائي في جريمة الدخول غير المصرح به، بحيث تثبت نية المتهم في الولوج إلى حاسوب فيدرالي، ثم يلزم إثبات نية المتهم في تحدي الحظر الوارد على إستخدام نظم المعلومات في الحاسب و تحقيق خسائر، و مثل هذا الأمر يستدعي التوصل إلى تحديد أركان جريمة الدخول دون تصريح و بذلك ذهبت المحكمة إلى تبني معيارين هنا هما الإرادة بالدخول غير المصرح به و كذا معيار العلم بالحظر الوارد على إستخدام نظم معلومات فيدرالية دون تصريح أما بالنسبة للقضاء الفرنسي فإن منطق سوء النية هو إلا علم في بأن جرائم الإنترنت، حيث يشترط المشرع الفرنسي وجود سوء نية في الإعتداء على بريد إلكتروني خاص بأحد الأشخاص.[2]

هذا يمكن القول أيضا يتوافر الركن المعنوي في جرائم الإنترنت في المثال التالي، قيام أحد القراصنة بنسخ برامج كمبيوتر من موقع على شبكة الإنترنت، و القيام بفك شفرة الموقع و تخريبه للحصول على برمجيات و لإيقاع الأذى بالشركة.[3]

القصد الجنائي يتخذ عدة صور منها القصد العام و القصد الخاص و هي كالآتي:

الفرع الأول: القصد الجنائي

لم يتم تعريف القصد الجنائي في قانون العقوبات الجزائري صراحة بل تم الإشارة إليه بشكل ضمني في كثير من مواده، و ذلك من خلال إشتراط توافر العمد لدى الجاني عند إرتكابه الجريمة و قد ترك المجال للفقه للقيام بتعريف القصد الجنائي فأعطاه تعريفات عديدة

1- خالد حسن أحمد لطفي، مرجع سابق، ص 122.

2- محمود نجيب حسني، مرجع سابق، ص 280.

3- خالد حسن أحمد لطفي، مرجع سابق، ص 125.

يتمحور مضمونيا حول نقطتين تتمثلان في إتجاه إرادة الجاني إلى إرتكاب الجريمة مع ضرورة العلم بكافة أركانه القانونية، و إذا تحقق العلم و الإرادة لدى الجاني قام القصد الجنائي و إذا إنتفى أحدهما أو كليهما إنتفى قصد الجاني.[1]

أولاً: مفهوم القصد الجنائي

القصد الجنائي هو الصورة الأصلية الأساسية للركن المعنوي في الجريمة و يعتبر شرطًا ضروريًا لكي تقوم المسؤولية الجنائية في حق الجاني حيث يترأس قمة الهرم في الجريمة العمدية بإعتباره ينطوي على إنصراف إرادة الجاني للفعل المجرم و إلى النتيجة المرغوب تحقيقيا، و هو يختلف بإختلاف نوع الجريمة، و لا يشترط تحقيق النتيجة لكي يتوافر القصد الجنائي و إنما يتحقق كذلك في حالة بروع الجاني في جريمته دون الوصول إلى الهدف المطلوب.[2]

كما سبق الذكر أن المشرع الجزائري لم يعرف القصد الجنائي بشكل صريح في القانون إنما إكتفى بالإشارة إليه ضمنيا فقط و ذلك من خلال إدراج كلمة العمد في كثير من النصوص القانونية الدالة على قصد و نية الجاني التي تنعكس مباشرة على الجريمة التي يرتكبها الجاني و إرادة تحقيق النتيجة[3] و قد أشار المشرع الجزائري إلى العمد في نصوص القانون في أمثلة كثيرة نذكر منها ما هو وارد في المادة 254 من قانون العقوبات الجزائري التي خصصها المشرع للقتل العمدي و التي نص فيها على ما يلى **"القتل هو إزهاق روح إنسان عمدًا"**،

1- عبد الله سليمان، شرح قانون العقوبات الجزائري (الجريمة القسم العام)، ديوان المطبوعات الجامعية، الجزائر، 2005، ص 249.

2- المرجع نفسه، ص 250.

3- خلفي عبد الرحمان، القانون الجنائي العام (دراسة مقارنة)، دار بلقيس للنشر، الجزائر، 2016، ص 15.

و كذلك المادة 264 من قانون العقوبات الجزائري التي خصصت للضرب و الجرح العمدي و التي تنص على ما يلي: **"كل من أحدث عمداً جروحاً للغير أو ضربة".**[1]

فالقصد الجنائي عرفه الفقه بأنه: **"القوة النفسية التي تقف وراء النشاط المجرم الذي إستهدف به الفاعل إراديا الإعتداء على مصلحة من المصالح المحمية من طرف المشرع الجنائي".**[2]

ثانيا: توجه إرادة الجاني إلى إرتكاب الواقعة الإجرامية:

فمن يقوم بنشر فيروس على الشبكة العامة مخالفا بذلك قانون الإتصالات و تقنية المعلومات فيدمر أحد أجهزة الحاسوب الخاصة لشخص معين يتوفر لديه القصد الجنائي لأنه يوجه إرادته لتحصيل النتيجة التي هي تدمير أحد الأجهزة الإلكترونية للآخرين و لا يكفي أن يواجه الجاني لإتيان النشاط مادي مجرم حتى و لو تصور إمكانية حدوث الواقعة المكونة للجريمة و إنما ينبغي أن يكون كل ذلك من أجل تحقيق نتيجة إجرامية كواقعة بذاتها و يقدر القاضي العقوبة في حدود سلطته التي تتمثل في الحدين الأدنى و الأقصى للعقوبة في ظروف التخفيف المسموح بها قانونا.[3]

ثالثا: العلم بحقيقة الوقائع الإجرامية من الناحيتين الواقعة و القانونية

لا يكفي لتوافر القصد الجنائي توجيه إرادة الجاني فهو تحقيق الوقائع المكونة للجريمة من الناحية القانونية بل يلزم إضافة إلى ذلك أن يكون عالما بتلك الوقائع تمام العلم و محيطا بها

1- بلعليات إبراهيم، أركان الجريمة و طرق إثباتها في قانون العقوبات الجزائري (أركان الجريمة، أهمية الإثبات الجنائي، طرق الإثبات الجنائية)، دار الخلدونية للنشر و التوزيع، الجزائر، 2004، ص 119.

2- بلعليات إبراهيم، المرجع السابق، ص 120.

3- عبد الله سليمان، المرجع السابق، ص 251.

إحاطة تامة و لا هذا العلم كاملا إلا إذا كان ملما بعناصر الجريمة واقعية كانت هذه العناصر أو قانونية و معنى هذا أن القصد الجنائي لدى الفاعل ينتفي مبدائيا إذا وجه إرادته نحو تحقيق الواقعة أو الوقائع المكونة للجريمة و لكن عن جهل أو غلط في أحد عناصرها سواء من الناحية القانونية أو الواقعية.[1]

رابعا: أنواع القصد الجنائي

1- القصد العام و القصد الخاص:

- **القصد العام:** هو توجيه الجاني لإرادته نحو تحقيق الوقائع المكونة للجريمة الإلكترونية مع إحاطته أي علمه بعناصرها كما يحددها القانون في النص الجنائي المجرم إحاطته تامة سواء من الناحية القانونية أو الواقعية و لا يمكن أبدا قيام جريمة عمدية دون وجود قصد عام لدى الجاني لا فرق في ذلك بين الجناية أو الجنحة أو المخالفة.

يعرف كذلك بأنه الهدف الفوري و المباشر للسلوك الإجرامي و يتحصر في حدود تحقيق الغرض من الجريمة أي لا يمتد لما بعدها.[2]

- **القصد الجنائي الخاص:** يتأثر الجاني بعوامل مختلفة كالحاجة و اللذة و الرغبة في الانتقام و الطمع و تولد عنده عادة حالة من الحالات الإنفعالية بحيث تكون محركاً للنشاط الإجرامي لديه فيندفع إلى إرتكاب الجريمة و ذلك بهدف تحصيل النتيجة التي يعتقد بأنها تتحقق في نفس الوقت إشباعا للرغبة التي حركتها إحدى العوامل المؤثرة في إتجاه منحى الإجرام عند الفرد عموما فيأتي النشاط المجرم و هو تحت تأثيرها في جرائم محددة حيث إعتبرها عنصرا في الجانب الشخصي للجريمة، فالقصد الجنائي الخاص هو

1- السعيد مصطفى السعيد، المرجع السابق، ص 83.

2- خالد حسن أحمد لطفي، المرجع السابق، ص 69.

ما يتطلب توافره في بعض الجرائم دون الأخرى فلا يكتفي الفاعل بإرتكابه الجريمة، بل يذهب إلى التأكد من تحقيق النتيجة.[1]

هو أيضا ما يتطلب توافره في بعض الجرائم فلا يكفي بمجرد تحقيق الغرض من الجريمة، بل هو أبعد من ذلك أي أنه يبحث في نوايا المجرم.

إن المجرم السيبراني يتوجه من أجل إرتكاب فعل غير مشروع أو غير مسموح مع علم هذا المجرم بأركان الجريمة، و بالرغم من أن بعض المخترقين يبررون أفعالهم بأنهم مجرد فضوليون، و أنهم قد تسللوا صدفة، فلا إنتفاء العلم كركن للقصد الجنائي، كان يجب عليهم أن يتراجعوا بمجرد دخولهم، و لا يستمروا في الإطلاع على أسرار الأفراد و المؤسسات، لأن جميع المجرمين و الأشخاص الذين يرتكبون هذه الأفعال يتمتعون بمهارات عقلية و معرفية كبيرة تصل في كثير من الأحيان إلى حد العبقرية.[2]

فالقصد الجنائي متوافر في جميع الجرائم السيبرانية دون أي إستثناء، و لكن هذا لا يمنع أن هناك بعض الجرائم السيبرانية تتطلب أن تتوافر فيها القصد الجنائي الخاص مثل جرائم تشويه السمعة عن طريق الإنترنت، و في كلا الحالات فإن المنظم هم من يختص بتحديد الحالات التي يشترط فيها توافر القصد الجنائي الخاص.

منه فإن القصد الجنائي العام متوافر في جميع الجرائم السيبرانية دون أي إستثناء و لكن هذا لا يمنع أن بعض الجرائم السيبرانية لابد أن يتوافر فيها القصد الجنائي الخاص مثلا جرائم

1- علي نعمة جواد الزرفي، الجريمة المعلوماتية الماسة بالحياة الخاصة دراسة مقارنة، ط 1، المكتب الجامعي الحديث، 2019، ص 93.

2- سمير عالية، مرجع سابق، ص 132.

تشويه السمعة عبر الإنترنت و جرائم نشر الفيروسات عبر الشبكة، و في كل الأحوال يرجع الأمر للسلطة التقديرية للقاضي.[1]

2- القصد المباشر و القصد غير المباشر:

- **القصد المباشر:** يكون عندما تتجه إرادة الجاني إلى المساس المباشر بالمصلحة التي حماها المشرع في نص جنائي و تستهدف تحقيق النتيجة الإجرامية.
- **القصد الغير مباشر:** هذا النوع من القصد كفكرة قانونية لم تعرف الإستقرار بعد في الفقه، فالبعض ينكرها من أساسها و البعض الأخر يقول بها و الظاهر أن الخلاف في المواقف نشأ نتيجة لطبيعة القصد الإحتمالي فهو كفكرة يحوطها الغموض.[2]

3- القصد المحدود و القصد غير المحدود:

- **القصد المحدود:** يكون القصد الجنائي محدودا فيما تتجه إرادة الفاعل إلى إرتكاب جريمة بنتائج محددة و كما كان يقدرها أو يتصورها عند إرتكابه لها فهذا النوع من القصد يشكل الصورة المألوفة للقصد الجنائي، إذ المألوف أن الفاعل عندما يرتكب جريمة بقصد تحقيق موضوع الجريمة في حدود النتائج التي قدر أو تصور الوصول إليها مسبقا.[3]

- **القصد غير المحدود:** يعتبر القصد غير محدودا عندما تنصرف إرادة الجاني إلى إرتكاب جريمة ما لكنه يعجز فلا يستطيع لحظة إرتكابه لها تحديد ما يمكن أن يترتب عنها من نتائج و بعبارة أخرى فإن القصد الجنائي يكون غير محدود إذا إنصرفت إرادة الجاني إلى

1- غازي حنون خلف الدراجي، المرجع السابق، ص 32.

2- حلفي عبد الرحمان، المرجع السابق، ص 22.

3- طباش عز الدين، النظام القانوني للخطأ غير العمدي في جرائم العنف، رسالة لنيل درجة الدكتوراه في العلوم، كلية الحقوق و العلوم السياسية، جامعة مولود معمري، تيزي وزو، 2014، ص 92 .

تحقيق واقعة إجرامية و لكنه دون تحديد تام لنتائجها مثال ذلك أن يضع إرهابي مادة إعلامية على ببكة الإنترنت لكي يثير الإنتباه لحركته أو لمطالب غير مشروعة أو يحرض على إثارة الفتنة فيستجيب له أحد الأشخاص و يقوم بتصنيع أو تجهيز أو إستعمال قنبلة فتنفجر تلك المادة أو القنبلة و تقتل عددا كبيرا من الأبرياء هنا القصد غير موجود لدى الجاني إلا أنه يكون مسؤولا كقاتل عمد لتوافر القصد الجنائي المطلوب لتحقق هذه الجريمة، ان الجريمة المتعدية القصد ينتج عنها نتيجة بسيطة قصدها الجاني إبتدأً، كما تحدث بنتيجة[1] أبد جسامة من إلا أن هذه الجرائم تجمع القصد الجنائي الذي إنصرفت إليه إرادة الجاني بسلوكه الإجرامي لتحقيق النتيجة الإجرامية البسيطة و الخطأ يتسع ليشمل الجرائم ذات النتيجة المتعدية كافة، أن أغلب الجرائم ذات النتيجة المتعدية الواردة في قانون العقوبات العراقي يترتب عليها وفاة المجني عليه في أكثر الأحيان و المساس بسلامة جسمه في حالة حدوث عاهة مستديمة، أو لم يقصدها الجاني و قد يكون لم يتوقعها.[2]

فسلوك الجاني يتضمن قرار واحداً هو إرادته في إحداث النتيجة البسيطة إلا أن قراره ينتج عنه نتيجة أشد من النتيجة التي قصدها، و بهذا فإن الجريمة المتعدية القصد هي الجريمة التي تتصف بإتجاه إرادة الجاني إلى إحداث نتيجة إجرامية معينة قصدها الجاني، إلا أن فعله أحدث نتيجة أشد جسامة من إرادته.[3]

1- نظام توفيق المجالي، شرح قانون العقوبات، القسم العام (دراسة تحليلية في النظرية العام)، ط 3، دار الثقافة للنشر و التوزيع، الأردن 2016 ، ص 369 .

2- المرجع نفسه، ص 341.

3- عبد الله سليمان، المرجع السابق، ص 229.

4- القصد الفجائي و القصد المقرون بسبق الإصرار:

- **القصد الفجائي:** كمن يرتكب الجريمة العمدية ساعة أو فور تقريره إتيانها فيوصف القصد الجنائي عند إذ بذلك، كمن يثور تحت تأثير إهانة أو عنف أو غيض فيسب و يقذف الغير على الإنترنت[1].

- **القصد المقرون بسبق الإصرار:** عرفه المشرع **"بأنه العزم المصمم عليه قبل وقوع الجريمة على الإعتداء على بخص معين أو على أي شخص قد يوجد أو يصادف حتى و لو كان هذا العزم معلق على ظرف أو شرط"** مما سبق يتبين أن مرتكب الجريمة مع سبق الإصرار لإرتكابها إلا بعد العزم عليها و إتخاذ قرار في شأنها و لا يكون ذلك إلا بعد تفكير عميق قد يطول و قد يقصر (العنصر الزمني في هذا الظرف) و تقليب الأمر من جميع أوجهه و التخلص مما يكون قد وارده من تردد (العنصر النفسي) فيهيئ الوسائل المادية التي يستخدمها في التنفيذ و ينفذها في الأخير فيكون مرتكبا للجريمة بقصد مقترن بسبق الإصرار، إذن هناك خطورة إجرامية تهدد أمن و سلامة المجتمع لذلك وجب التشدد معه في العقاب مادام التصميم على إرتكاب الجريمة التي عزم عليها لم يلينه الوقت الفاصل بين إتخاذ القرار بشأنها و تنفيذه له.[2]

الفرع الثاني: الخطأ غير العمدي

نكون أمام جريمة الخطأ الغير عمدي عندما يأتي الفاعل سلوكا خاطئاً عن إرادة و إختيار دون أن يستهدف النتيجة الجرمية التي قد تترتب على هذا السلوك فالخطأ غير العمد يتحقق كلما أتى الفاعل سلوكاً لم يلتزم فيه بما يلتزم به الكافة و نحرص على حقوق المحمية قانونا

1- محمود نجيب حسني، مرجع سابق، ص 162.

2- عبد الله سليمان، مرجع سابق، ص 229.

كمن يقوم بتجاوز حق الدخول لموقع معين على شبكة غير مصرح بالدخول عليها بخطأ منه غير عمدي بالضغط على زر معين.[1]

أولا: الإهمال

يظهر في الموقف السلبي لشخص في مواجهة بعض الأوضاع التي تفرض عليه الحذر و مثال ذلك في الجرائم السيبرانية كالشخص الذي يسئ استخدام أساليب و وسائل الإتصال و يقوم بتوزيع خدمة الإنترنت بشكل عشوائي على جيرانه دون أن يتخذ الوسائل الإحترازية لحماية حق الدخول للخدمة التي يملكها مما قد يستخدمه مجرم أخر لإرتكاب الجريمة السيبرانية.

ثانيا: عدم التبصر

أي عدم قيام بعض الأشخاص بعملهم كما يجب أو جهلهم بقواعد عملهم مثال الأمي الذي لا يستطيع القراءة و الكتابة و الذي يقوم بعمل حساب إلكتروني على أحد مواقع التواصل الإجتماعي لتصفح الصور الموجودة ثم يقوم بعمل عملية إلكترونية معينة دون قصد فينشر صور لإحدى السيدات و المحتفظ بها على هاتفه المحمول فيكون قد إرتكب جريمة إفشاء أسرار خاصة و إنتهاك حرمة الحياة الخاصة.[2]

ثالثا: عدم مراعاة النظم أو القوانين

يقصد بالنظم و القوانين كل ما يصدر من تشريعات سواء عن السلطة التشريعية أو التنفيذية في الحدود المخولة لها و تمتد لتشمل تنظيمات المعامل، و الخطأ الغير العمدي يعبر عنها البعض بالخطأ الخاص بسبب أن القاضي لا يلتزم بتقييم سلوك المتابع للقول بثبوت

1- خلفي عبد الرحمان، مرجع سابق، ص 52.

2- المرجع نفسه.

الخطأ في جانبه من عدمه على إعتبار أن مجرد مخالفته للقانون أو الأنظمة يؤدي بذاته و مباشرة إلى مسائلته عن المخالفة أو الجنحة و هذا له عن الخطأ العام الذي يطلق على باقي الصور الأخرى للخطأ.[1]

1- خلفي عبد الرحمان، مرجع سابق، ص 230.

الفصل الثاني

الفصل الثاني

المجال السيبراني

تعتبر تسمية الفضاء السيبراني تسمية غير دقيقة، لأنه حقا مساحة غير ملموسة على الإطلاق إنه بلا شكل، و لا حدود له بطبيعته، و يعتمد هذا الفضاء على البنية التحتية المادية الخوادم و الكابلات و أجهزة الكومبيوتر لوجوده لكن النقطة المهمة هي أن مفهوم الإنترنت ينتشر و يحل محل المفاهيم التقليدية للأراضي و الملكية في ظل غياب أي حدود إقليمية في هذا الفضاء الجديد، كما أن تكلفة و سرعة إنتقال الرسائل في هذا الفضاء يكون بصورة مستقلة تماما عن المواقع المادية،[1] فمستخدم الإنترنت لا يعيش في المواقع على الإنترنت، و لا يمكن بذلك المطالبة بالحقوق في جزء معين من المواقع الإلكترونية.

يفرض نطاق الإنترنت فوق الوطني بطبيعته و المستخدمين على حد سواء مشاكل كبيرة للردع في الفضاء الإلكتروني، لتحقيق أهدافه، يعتمد الردع التقليدي على مفاهيم الدولة بما في ذلك الإقليم و الموطنين بإعتبارهم مظاهر مادية، لكن في الفضاء الإلكتروني يصعب تحديد هذه المظاهر، مثل تحديد ماهي أراضي بلد الإنترنت، و من هم مواطنوها على الإنترنت.

النقطة المهمة هي أنه من دون فهم دقيق للغاية لما يتم حمايته، فمن المستحيل معرفة متى تم إختراق الحدود و المعالم، خلال الحرب الباردة، تم ردع القوى العظمى عن مهاجمة بعضها البعض من خلال وضع الأسلحة الفتاكة خلف الخطوط، إما مادية(الحدود) أو مجازية (السياسة) بقصد إستخدام هذه الأسلحة إذ تم عبور الخط لكن في الفضاء الإلكتروني لا يوجد خط، على الأقل ليس خطأ سهل التعريف و التطبيق، إذ بدون مثل هذا الخط، يصبح من الصعب للغاية ردع الخصم، لأن قواعد اللعبة ليست واضحة للعيان.[2]

1- Johnson, D, R. and Post, D, G. (May 1996). Law and borders: the rise of law in cyberspace. Stanford Law Review (48), 1367-1402.

2- Schelling, T. (1994). The threat that leaves something to chance. in : Freedman, L. War. Oxford :Oxford University Press,

المبحث الأول

أبعاد و مخاطر الأمن السيبراني و كيفية الردع

لقد صنف الفضاء السيبراني بمثابة ميدان للمواجهة، كغيرة من الميادين إلا أنه يتطلب نوعا خاص من العدة و العتاد، و ذالك لخصوصيته التي تحتم على المتصارعين الإلتزام بإستراتيجيات و تقنيات تعتمد على القوة التكنولوجية، و الكفاءة البشرية المتمكنة في المجال، مع توفر عنصر السرعة و المباغتة، و لأن الإعتداءات في هذا الفضاء قائمة أساسا على الإعتداء أكثر مما هي قائمة على الدفاع، فلا بد من وضع خطط إستباقية لرصد مختلف التهديدات المحتملة، و كذا تحديد الأبعاد التي يمكن أن تصلها مختلف الإعتداءات السيبرانية للعدو.[1]

المطلب الأول

أبعاد ومخاطر الأمن السيبراني

إذا سلمنا أن الأمن هو قدرة الدولة على حماية مصالحها و شعبها في مختلف مجالات حياته اليومية و مسيراته نحو التقدم بكل طمأنينة على إعتبار أن هذه الحماية لها علاقة مباشرة و مرتبطة إرتباطاً وثيقاً بسلامة مصادر الثورة و الحياة في العصر الحالي (البيانات و المعلومات) التي تشكل جسر الإتصال و التواصل و القدرة على الإنتاج و الإبداع و المنافسة، فهذا معناه أن الأمن السيبراني يطال جميع المسائل العسكرية و الإجتماعية و السياسية و الإقتصادية و القانونية، حيث أن هناك مخاطر و تهديدات تمس بالأمن السيبراني و إنما هي بداية التساؤل حول التهديدات، نقاط الضعف و أخيراً وسائل الوقاية المناسبة للتعامل مع التهديدات و وسائل منع نقاط الضعف و التخطيط للمواجهة.[i]

الفرع الأول: أبعاد الأمن السيبراني

1- منى عبد الله السمحان، مرجع سابق، ص 85.

للأمن السيبراني إمتدادات و أبعاد إستراتيجة، بحيث يمكن أن يؤدي أي خلل، في إحدى هذه الأبعاد إلى نتائج وخيمة لا تعد و لا تحصى، خاصتا في فضاء يتسم بالسرعة في التخطيط و التنفيذ، إذ لابد من قوة و أسلحة سيبرانية رادعة تكون في مستوى الهجوم الإلكتروني، و من الأبعاد التي تتأثر بالأمن السيبراني، نجد البعد العسكري، و البعد الإقتصادي، و البعد الإجتماعي و القانوني و السياسي:

أولا: البعد العسكري

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

سرعة إتخاد القرارات العسكرية، و من ثمة تحقيق الأهداف عن بعد و من دون شك فإن عدم إستغلال هذه التقنية، و التسلح بها، أو تأمينها بشكل جيد من أي إختراق خارجي، سيؤدي بالضرورة إلى شن هجمات إلكترونية مضادة على شبكات القوات العسكرية و من ثم تدمير قواعد البيانات.

ثانيا: البعد الإقتصادي:

إن إستخدام الكمبيوتر و شبكة الإنترنت في تطوير الصناعات و تحريك الإقتصاد، و معالجة كل المعاملات الإقتصادية و المالية ، زاد من أهمية ضرورة توفير الأمن السيبراني لضمان حماية هذه المعلوم.[1]

1- بارة سمير، مرجع سابق، ص 160.

ثالثا: البعد الإجتماعي:

تعتبر الشبكة الدولية للمعومات مجالا مفتوح لجميع الأفراد حيث يمكن لجميع المتعاملين السيبرانين أن يستفيدو من البنية التحتية و الخدمات المتاح لهم دون تحمل المخاطر الأمنية و هنا يجب التمويه إلى ضرورة التحسيس بأخلاقيات الأمن السيبراني.

رابعا: البعد السياسي:

لقد أصبح بإمكان المواطن أن يتحول إلى لاعب أساسي و أصبح بإمكانه الإطلاع على خلفيات القرارات السياسية عبر الكم الهائل من المعلومات التي سهل عليه الوصول لها عن طريق الإنترنت و هنا نشير إلى التسريبات للوثائق الحساسة مثلا و التي تثير مشكلات عويصة، و أيضا دور شبكات التواصل الإجتماعي في تنظيم الدعايات السياسية و الإنتخابية و تنظيم التظاهرات الإفتراضية و إفتعال الإحتجاجات الإلكترونية... إلخ، و أصبح الفضاء السيبراني ملاذا للتجنيد من طرف التنظيمات الإرهابية و العديد من الإيديولوجيات و الدعايات الدينية.

خامسا: البعد القانوني:

أساليب ممارستية عديدة في إستخدام تقنية المعلومات، كإنشاء المدونات، و التجمعات على الإنترنت و الحق في حماية ملكية البرامج المعلوماتية و الإبلاغ عن المخالفات و الجرائم السيبرانية و هذا ما أدى إلى ظهور ترسانة قانونية تتوافق مع التغيرات الحاصلة.[1]

1- حنين جميل أبو حسين، "الإطار القانوني لخدمات الأمن السيبراني (دراسة مقارنة)"، رسالة مقدمة لإستكمال متطلبات الحصول على درجة الماجستير، تخصص قانون خاص، كلية الحقوق، جامعة الشرق الأوسط، الأردن، 2021، ص 18.

الفرع الثاني: مخاطر الأمن السيبراني

قبل التطرق إلى مخاطر حوادث الأمن السيبراني لابد أن نتطرق لأهم التهديدات التي قد تحول دون تحقيق الأمن في الفضاء السيبراني، و الذي لا يتأتى دون قوة سيبرانية تكون رادعة لمختلف الإعتداءات و التهديدات.

أولا: تهديدات الأمن السيبراني

1- العرضية للكابلات البحرية Submarine Cable: تعد الكابلات جزء هام لتوفير خدمة الإتصالات بين دول العالم في مجال الإنترنت، و شبكات الكمبيوتر و غيرها، فمنذ عام 2005 أصبحت الكابلات البحرية مأهولة على مجال الإتساع و الإنتشار، كما تعرضت تلك الكابلات إلى عدد من المشاكل التي تؤثر سلبا على أعمال البنية التحتية بالضرر، حيث تقع في مياه المحيط العميق.

2- التجسس الإلكتروني Cyber Espionage : يعد أحد أنواع التجسس التقليدي، بإستخدام وسائل التكنولوجيا الفائقة، و معظم الهجمات السيبرانية المتطورة التي تقع ضمن هذه الفئة حيث يتم الحصول على معلومات سرية بطرق غير مشروعة بهدف الحصول على أفضلية إقتصادية، أو إستراتيجية أو عسكرية بإستخدام تقنيات إلكترونية أو الشبكات السلكية أو الأقمار الإصطناعي.[1]

3- الإرهاب السيبراني Cyber Terrorism: و المقصود بالإرهاب السيبراني هو ذاك الإستخدام للموارد المعلوماتية، و أجهزة الحاسوب و شبكة الإنترنت، و الفضائيات من أجل أغراض التخويف و الإرغام لأغرض سياسية أو الإقناع الفكري و التثقيف السلبي و العدواني.

1- عنترة بن مرزوق، محي الدين حرشاوي، الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية، قسم الحقوق و العلوم السياسية، جامعة ورقلة، 2017، ص 20.

4- الحروب السيبرانية Cyber Warfae : و تعتمد على فريق من المختصين في الحروب الإلكترونية، حيث كل منهم يتميز بمسؤولياته و مهاراته الخاصة لترسيخ القدرة على القتال و التحكم بها و إبرازه ضمن الفضاء السيبراني و يقوم مشغلو الحروب السيبرانية بالتخطيط للنشاطات الهجومية و الدفاعية و إدارتها و تنفيذها عبر الفضاء السيبراني.[1]

ثانيا: المخاطر التي تهدد الأمن السيبراني

الدخول على الأنظمة و ما تحتويه من بيانات و معلومات دون إذن و التجسس على الإتصالات و الحد من سلامة المعلومات، نتيجة التلاعب، و التعديل عليها، و إتلافها، و هذا يعد إعتداء بحد ذاته على الحريات و الحقوق الشخصية و الجرائم العادية التي يتم إستخدام الإنترنت في تنفيذها كالسرقة و الغش، و الترويج لنشاطات مخالفة للقانون، و بالتالي إجمالي المخاطر المحتمل التعرض لها على شبكة ألنت، يهدف إلى التخريب المتعمد لأهداف سياسية، عسكرية و إقتصادية و غيرها[2] و عموما فإن التهديدات السيبرانية أو الهجمات السيبرانية هي التي تهدد أمن المجتمع و أمن الإقتصاد الوطني و الجانب الأمني و العسكري للدول، كما أن للتهديدات السيبرانية أهداف مسطرة حيث تمس كلا من الجانب المعنوي و الجانب المادي و على جميع الأصعدة، و لكن ما يتوجب على الدول المعرضة لتلك التهديدات وضع خطط إستراتيجية من أجل مكافحتها و التخلص منها و يمكن التوضيح أكثر من خلال الجدول الآتي

1- إدريس عطية، مرجع سابق، ص 110

2- إيمان محمد الشورة، الأمن السيبراني في البنوك الإسلامية الأردنية، مذكرة بكالوريوس، كلية الشريعة، الجامعة الأردنية، 2018 ، ص 111.

	الدفاع المجتمعي السيبراني	الدفاع الإقتصادي السيبراني	الدفاع العسكري السيبراني
القيم المهددة	الدين – الشباب الثرات – الأخلاق	الجودة – السرعة –التنافسية –الإختراعات التنموية– المعاملات المالية	العقيدة العسكرية– ميزان الرعب– ثقة الشعب بالجيش و الأمن
أهداف التهديدات السيبرانية	نشر الإنحراف لتشكيل خلايا إلكترونية مشوشة للدولة – الحصول على معلومات من الأفراد –التحريض على العنف. تشكيك الشعب بقدراته	تدمير التنمية الإقتصادية الإلكترونية –سرقة الأموال –تدبير التجارة الإلكترونية. –إيقاف التصدير و الإستراد. –إلحاق الخسائر المادية الإقتصادية.	الحصول على معلومات تخص التسليح. –التجسس على الإستخبارات. –إمكانية إعادة توجيه القتال والصواريخ الذكية. –التجسس على البيانات الرقمية.
إستراتيجية الدفاع الوطني	توصية الجهات الشخصية و الأجهزة الأمنية المختصة الوطنية و توجه و تركيز الدفاع الشعبي الإلكتروني	–ضرورة توعية الخبراء و المختصيين بمخاطر التهديدات السيبرانية الحرص على إستمرار عدم إنقطاع الإتصال بالإنترنت.	الهجوم الإلكتروني المضاد –محاكات عملية الإختراق الأمني العملياتي. –ولاء المسؤولين و

			الأجهزة الأمنية.
أدوات الدفاع السيبراني	-الشبكات الإجتماعية الإلكترونية. -البريد الإلكتروني. -مواقع وسائل الإعلام. -تقنيات الحماية الإلكترونية	مواقع الحماية من الفيروسات. -إدخال نشاط أمن المعلومات إلى الشركات. -تحفيز مواقع الإنترنت الإحتياطية وتجهيز البريد الإلكتروني.	-توفير برامج الحماية. -تجهيز منشآت الهجوم الإلكتروني. -توظيف الأنظمة الإلكترونية في الهجوم على مواقع العدو.
المسؤول عن الدفاع	كل من لديهم القدرة على عمل السلاح الرقمي.	مديرية المعلومات في المؤسسات	وحدات خاصة بتقييم إحداثيات داخل الجيش و المخابرات تكون مهمتها الدفاع و الهجوم

جدول رقم 01 : يوضح طرق إستخدام التهديدات السيبرانية و كيفية التعامل معها

المطلب الثاني

الردع السيبراني

يعرف الردع Deterrence على أنه ممارسة تثبيط أو كبح شخص ما في السياسة العالمية و عادة ما تكون دولة قومية – من إتخاذ إجراءات غير مرغوب فيها مثل الإعتداء المسلح كما أنه ينطوي على محاولة لوقف أو منع أي إجراء على عكس مفهوم الإرغام Compellence المرتبط بيه إرتباطا وثيقا و لكنه مختلف عنه، فهو محاولة لإجبار الفاعل على فعل شيء ما.[1]

فكرة الردع بطبيعة الحال ليست جديدة، إلا أن الإحاطة يفهم فكرة الردع الحديثة أمر ضروري من أجل صياغة الحوار السيبراني، و يعتبر الباحث الإطالي**"جيليو دوهيت" Guilio Douhet** من المهتمين بموضوع القوة الجوية من خلال كتابه " the Command of the air" الذي أشار من خلاه أن القيادة الجوية شكلت إتجاها جديدا في الفكر الاستراتيجي في القرن العشرين فظهور القوة الجوية قدم بعدا جديدا للصراع، إذ توقع **دوهيت** أن القوة التدميرية بالمعنى المادي و كذلك المعنى المحبط للحرب الجوية، سوف تمنع الدول في النهاية من شن الحرب على بعضها البعض، و أضاف بأن مثل هذا التقييد سوف ينبع من طائرة وحيدة يمكنها أن تحقق تجميد كل هذه الموارد و الطاقات بمجرد وجودها المحتمل، دون الحاجة إلى الإقلاع و الطيران على الإطلاق.[2]

الفرع الأول: إستراتيجية الدفاع السيبراني

أولا: إستراتيجة الدفاع السيبراني

1- يوسف بوغرارة، الإستراتيجية الجزائرية للأمن و الدفاع في الفضاء السيبراني، مجلة الدراسات الإفريقية و حوض النيل، ط 3، المركز الديمقراطي العربي، جامعة مستغانم، الجزائر، 2018، ص 107.

2- المرجع نفسه، ص 109.

أدوات الدفاع السيبراني مثل الفيروسات و البرامج الضارة و غيرها تندرج تحت وصف أدوات الدفاع، باعتبارها أسلحة. و السؤال هنا: ما أدوات الدفاع السيبراني، أو ما أسلحته؟ تقسم[1] Afroditi الأسلحة السيبرانية إلى ثالث فئات رئيسة:

الأولى: البرمجيات الخبيثة Malware، الثانية : هجمات منصات الخوادم Platform Attacks، و الثالثة: هجمات رفض الخدمة الموزعة DDOS distributed denial of service و في حين أن الفئة الأولى تندرج تحت وصف أدوات الحرب، فإن الفئة الثانية و الثالثة تندرجان تحت وصف أسلوب الحرب، أو الكيفية التي يتم بها إستخدام أسلحة الحرب.

الفئة الأولى: البرمجيات الخبيثة Malware: تحتوي هذه الفئة على البرامج الضارة مثل الفيروسات و أكواد معينة مصممة لإفساد أو تدمير البيانات، و برامج النسخ الذاتي، و البرامج المصممة؛ ليتم تشغيلها عند إستيفاء ظروف معينة، و الجذور، worms و الديدان فتبدو غير ضارة، إلا أنها تحتوي على horses trojan و هذه البرمجيات تحتوي على rootkits الخفية برمجيات ضارة يتم تفعيلها في وقت معين.

1- الفيروسات: و هي برامج تم تصميمها لإلحاق الضرر بقواعد البيانات، أو سرقتها و تخريبها أو قطع الإتصال بالشبكة، علما أنه يصعب التعرف أو إكتشاف هذه الأسلحة، و هي برامج صنعت عمدا لتغيير خصائص الملفات الغرض منها هو إلحاق الضرر بالحاسوب أو الهاتف أو السيطرة عليه، و كتابتها تكون بطريقة معينة، و قد تستخدم الفيروسات لتعطيل

1- فريدة طاجين، مرجع سابق، ص 24.

شبكات الخدمات و البنية التحتية للطرف المستهدف كإحداث فشل في شبكة الإتصالات لدولة ما.[1]

2- الديدان: هي برامج صغيرة تتكون من الشبكات و هي لا تعتمد على غيرها، غايتها قطع الإتصال عن الشبكة أو سرقة البيانات و ذالك أثناء تصفح المستخدمين للإنترنت، و من أشهر هذه الديدان، دودة **ميليسا** التي إنتشرت في 1999، و تم نشرها بواسطة البريد الإلكتروني، و دودة **ستكسنت** التي إنتشرت في 2010 عبر أجهزت USB.2.[2]

3- أحصنة طروادة Trojan Horse: هي شفرة صغيرة يتم تحميلها مع برنامج رئيسي من البرامج ذات الشعبية العالية، و يقوم ببعض المهام الخفية غالبا ما يرتكز على إضعاف قوى الدفاع لدى الضحية أو إختراق جهاز و سرقة بياناته، و في كثير من الأحيان ما يعتمد على الأبواب الخلفية أو الثغرات الأمنية التي تتيح الوصول الغير مصرح للجهاز المستهدف.

4- القنابل المنطقية Logic Bombs: قد تكون أحد أنواع أحصنة طروادة، بحيث تعمل عند حدوث أحداث معينة أو تحت ظروف معينة، أو لدى تنفيذ أمر معين و تؤدي إلى تخريب أو مسح البيانات أو تعطيل النظام.

5- الأبواب الخلفية Backdoors: هي ثغرة تترك عمد من قبل مصمم النظام لكي يستطيع الدخول عند حاجته لذالك، و تجدر الإشارة إلى أن كل البرامج و النظم التي تنتجها الولايات

1- نور أمير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، رسالة ماجستير، الجامعة الإفتراضية السورية 2021.

2- للمزيد حول فيروسات الحاسوب الآلي، راجع الرابط التالي : https://mawdoo3.com

المتحدة الأمريكية تحتوي على أبواب خلفية و تستخدمها عند الحاجة و هو ما يمكن هيئات و أركان حرب. المعلومات من التجوال الحر داخل أي نظام لأي دولة أجنبية[1].

الفئة الثانية Attacks Platform Server-Client:

هي هجمات مصممة لإستغلال ثغرات نظام تشغيل Windows و التلاعب في أنظمة الأمان، بواسطة وسائل إختراق برامج أمن الكمبيوتر الشخصي، و لا يؤدي مثل هذا الهجوم دائما إلى تدمير شبكة الكومبيوتر أو ملف البنية التحتية التي يسيطر عليها، و تتم هذه الهجمات عادة بإستخدام برامج التسلل، فبمجرد أن يتسلل المهاجم إلى شبكة كمبيوتر آمنة، يمكنه تنفيذ مجموعة متنوعة من الإجراءات، قد تتضمن تعطيل العمل. فعلى سبيل المثال، هجوم Stuxnet إستهدف شبكات الكمبيوتر الآمنة في إيران لغرض تعطيل عمل المنشأة النووية و قد يتضمن برنامج التسلل إرسال معلومات كاذبة بغرض تحقيق نتائج عسكرية معينة، ففي عام 2003، قبل غزو العراق، إخترقت الولايات المتحدة نظام البريد الإلكتروني لوزارة الدفاع العراقية للاتصال بضباط عراقيون و إعطائهم تعليمات باستسلام سلمي، و قد نجحت هذه الرسالة في توجيه الجيش العراقي للاستسلام، و قد تم هذا الهجوم بإستخدام ملف هجوم القيادة و السيطرة و هو ملف يقصد به التدخل في قدرة العدو على قيادة قواته و السيطرة عليها.[2]

تثبت هذه الأمثلة أن الهجمات لا تتم بالضرورة عبر الإنترنت، و لكنها قد تتضمن بدلا من ذلك من خالا التسلل إلى شبكات منفصلة و آمنة. هذه الشبكات التي تضم فقط أجهزة

1- فريدة طاجين، مرجع سابق، ص 24.

2- انظر، جريمة إتلاف و تدمير المعطيات و البيانات بواسطة الإنترنت، أفريل 2009، متاح على الرابط التالي: https://www.startimes.com/

الكمبيوتر المكتبية و المحمولة، بل تشمل كل شبكة تتضمن أنظمة الحوسبة، مثل أنظمة التحكم الصناعية.[1]

الفئة الثالثة: هجمات رفض الخدمة الموزعة ddos distributed denial of service:

هي الأكثر إستخداما في الأونة الأخيرة للتسلل إلى البنية التحتية لشبكة العدو، حيث يتم فيها إستخدام أدوات مؤتمتة لتحويل أجهزة الكمبيوتر إلى "زومبي" أو"روبوتات"، و التي بدورها تلوث دون علم أجهزة الكمبيوتر الأخرى المتصلة بها، في هذه الهجمات المنسقة يتم السيطرة على مجموعات من ألاف أجهزة الكمبيوترات بفيروسات ترهق الخوادم عن طريق زيارة مواقع ويب المعينة بشكل متكرر، مما يؤدي في النهاية إلى تعطيل النظام المستهدف و إغلاقه في النهاية.[2]

مثال هذه الهجمات، الهجوم السيبراني على إستونيا في أفريل 2007، حيث تم باستخدام هجوم DDOS، من قبل مجموعة من المتسللين، و قد أصابت الهجمات الإقتصاد، و الحكومة، و خدمات الطوارئ الإستونية بالشلل لفترة من الزمن، لكنها لم تسبب أي آثار جسدية مباشرة[3]، و لم ينسب الهجوم رسميا إلى أي دولة، بالرغم من الإشارة إلى تورط روسيا، بسبب تعقيد و حجم الهجوم، و بالرغم من أن آثار هذه الهجمات غالباً ما تسبب مجرد إزعاج، إلا أن هذا الهجوم كان مهددا للحياة تقريباً حيث كان خط الطوارئ لإستدعاء سيارة إسعاف أو سيارة إطفاء

1- طلال ياسين العيسى، وعدي محمد عناب،" المسئولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر"، مجلة الزرقاء للبحوث و الدارسات الإنسانية، المجلد 19، العدد 1، 2019، ص 86.

2 -Jeffrey T. G. Kelsey, Note, Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare, op.cit., p.1429.

3 - Ido Kilovaty, Cyber Conflict and The Thresholds Of War, (June 22, 2021). Forthcoming, Is the International Legal Order Unraveling? (David . Available 9Sloss, ed.) Oxford University Press (2022), p. at: https://ssrn.com/abstract=3871931 or http://dx.doi.org/10.2139/ssrn.3871931

خارج الخدمة لمدة ساعة،[1] كذلك، في يوليو 2009، تم إغلاق عدد من المواقع الحكومية و التجارية في الولايات المتحدة و في كوريا الجنوبية بهجوم DDOS، و بالرغم من أن كوريا الجنوبية ألقت باللوم على كوريا الشمالية، إلا أن الولايات المتحدة لم تتهم أي دولة[2]، و في ديسمبر 2015، عانت المناطق الغربية و العاصمة في أوكرانيا من انقطاع التيار الكهربائي بسبب عملية سيبرانية يزعم أنها مرتبطة بروسيا،[3] و في عام 2019، ذكرت صحيفة واشنطن بوست أن عملية سيبرانية تسببت في تعطيل عمليات الشبكة الكهربائية في غرب الولايات المتحدة، مما أدى إلى إغراق الشبكة بهجوم رفض الخدمة[4]، و قد تم التصدي لهذا الهجوم، إلا أن الخبراء يعتقدون أنه في حالة نجاح العملية السيبرانية ضد الشبكة الكهربائية يمكن أن تتسبب في خسائر في الطاقة في أجزاء كبيرة من الولايات المتحدة يمكن أن تستمر أيام في معظم الأماكن، و حتى عدة أسابيع في أماكن أخرى.[5]

---

1 - Newly Nasty: Defences Against Cyberwarfare Are Still Rudimentary. That's Scary, ECONOMIST (May 24, 2007), available at: http://www.economist.com

2 - Officials anonymously leaked qualified reports of U.S. suspicions that the attack emerged in North Korea. U.S. Eyes N. Korea for 'Massive' Cyber Attacks, MSNBC.COM (July 9, 2009, 3:31 AM), available at: http://www.msnbc.msn.com/id/31789294/ns/technology_and_

3 - Ellen Nakashima, Russian Hackers Suspected in Attack That Blacked Out Parts of Ukraine, WASH. POST, Jan. 5, 2016. Available at: https://www.washingtonpost.com/world/national-security/russian-hackerssuspectedin-attack-that-blacked-out-parts-ofukraine/2016/01/05/4056a4dc-b3de-11e5-a842- 0feb51d1d124_story.html

4 - Robert Knake, A Cyberattack on the U.S. Power Grid, COUNCIL ON FOR. REL. (Apr. 3, 2017), available at: https://www.cfr.org/report/cyberattack-us-power-

5- و يقدر تأثير مثل هذه العملية على الإقتصاد الأمريكي بما يتراوح بين 250 مليار دولار و تريليون دولار، وفقا لتقرير صادر عن جامعة كامبريدج.

Lloyd's & University of Cambridge Centre For Risk Studies, Business Blackout: The

ثانيا: الإستراتيجية الجزائرية في الدفاع السيبراني

تتفق العديد من الدوائر العلمية أن الجرائم المستحدثة في الفضاء السيبراني، أصبحت لا تعرف حدود فقد ألغت عنصر الزمان و المكان و أفقدت الدول إمكانية التحالف لمواجهتها، فالدقة المتناهية في تنفيذ الإختراقات جعلت الإنتصار شبه محقق حتى على المؤسسات العسكرية و ان لم تفعل اليقظة المعلوماتية المراقبة المستمرة لهذا الميدان حتى يتم الإستباق في وضع الآليات الكفيلة للتأقلم مع التحديات التي تفرزها التطورات التكنولوجية، فإن هذا الخطر من شأنه المساس بالأمن.

بالنسبة للجزائر فإن موقعها الجغرافي جعل منها فضاء مفتوح مغاربيا، متوسطيا و أفريقيا لتلاقي و تقاطع التهديدات اللاتماثلية التي تركت أثارها على مسألة الأمن الوطني و اذا أطفنا إلى ذلك المخاطر السيبرانية، فإن الجزائر كغيرها من الدول أصبحت إحدى ضحايا هذه التحديات و أصبحت في حاجة أمنية متعددة التخصصات الجوانب التشريعية، التنظيمية، البشرية، المالية، التقنية، و المعلوماتية حتى يتسنى لها تأمين الثورة الرقمية للأفراد و المؤسسات و بالتالي التصدي لخطر في هذا الإطار، توجهت الجزائر إلى طرح تصورات و رسم سياسة أمنية مزدوجة الأمن السيبراني للتحكم في أنظمة المراقبة لحماية المنظومة المعلوماتية للمؤسسات و المواطنين من جهة، و مواجهة الأخطار من جهة ثانية، و لتدارك النقائص تجتهد الجزائر على المستوى الخارجي من خلال التعاون المتعدد التخصصات، للإستفادة من تجارب غيرها من الدول.

Insurance Implications of A Cyber Attack on The Us Power Grid, (2015). Available at: https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-lloydsbusiness-blackout scenario. Pdf.

من هذا المنطلق، و في إطار رسم السياسة الأمنية العامة طرحت السلطات في الجزائر مخطط وطني لتفادي الوقوع في مأزق امني جديد إختراق أنظمة المعلومات الحساسة لرئاسة الجمهورية، وزارة الدفاع الوطني، أجهزة الأمن أخذين بعين الإعتبار من جهة، الأزمة الأمنية التي تحاصر البلاد في شقها المتوسطي، المغاربي و الساحل الإفريقي، و من جهة ثانية، الحفاظ على الحقوق الشخصية و الحريات الفردية وفق ما تضمنته المواثيق الدولية و القوانين الوطنية، و سوف نطرح تصور أو مقاربة الجزائر للموضوع من خلال النقاط التالية.[1]

1-على المستوى الوطني:

أدرج الأمن السيبراني كإحدى الأولويات في برنامج المواجهة ضد الجريمة الإلكترونية و الإرهاب الإلكتروني، بل أصبح يشكل جزء لا يتجزأ من إستراتيجيات الدفاع، لأن الدروس المستخلصة من الدول التي لها تجربة في هذا المجال، أثبتت أن النجاعة في التطبيق و فعالية المعايير و الوسائل المستعملة لا يمكن لها أن تتجسد ما لم يكون هناك تخطيط محكم وتنسيق بين الفاعلين في الميدان، و عليه توجهت الجزائر إلى رسم إستراتيجياتها مركزة على النقاط التالية:

أ- من الناحية القانونية:

إعتمد المشرع الجزائري في سن الأحكام القانونية لمواجهة الإعتداءات الإلكترونية على ثلاثة معايير متفق عليها إلى حد ما لدى الفقهاء و التشريعات المقارنة.[2]

1- علي نعمة جواد الزرفي، الجريمة المعلوماتية الماسة بالحياة الخاصة دراسة مقارنة، المكتب الجامعي الحديث، 2019، ص 38.

2- Le législateur algérien a pris en considération certaines dispositions de la législation rançaise de 1988, voir à ce sujet, André Lucas, Jean Devrèze, Jean Frayssinet, Droit de l'informatique et de l'Internet, édition Dalloz, collection Thémis (Droit Privé), Novembre 2001, (France), page 679.

و يهدف المشرع من هذه الخطوة إلى تحديد النطاق الذي تنشط فيه الجريمة الإلكترونية حتى يتسنى للفاعلين التحكم في الموضوع، و من خلال القراءة التحليلية لمواد القوانين المستحدثة أو المعدلة، يتضح أن المشرع الجزائري قد طرح تصور يتوفر على العلاج الوقائي و الردعي لمواجهة الإعتداءات السيبرانية من الجوانب التالية.

تم تعريف الجريمة الإلكترونية إدراجها ضمن الأعمال المعاقب عليها قانونا في المادة 02 من القانون رقم 09-04 المؤرخ في 2009/05/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها، كما تبني القانون النقاط الأساسية المذكورة في المعيار الأول او الثاني، أما المعيار الثالث، فقد تناوله المشرع من خلال إدراج المادة 323 من القانون 05-10 الصادر في 2005/06/20 المتضمن الدليل الإلكتروني (أنظر القانون المدني طبعة 2014)، كما تم تعديل المواد 720.238.212.156.143.79.65 من قانون الإجراءات الجزائية، و المواد 396.394.333.303 من ق.ع المتضمنة تجريم وتسليط العقاب على كل من يثبت في حقه إختراق أنظمة معلومات المؤسسات أو الأفراد بطريقة غير شرعية، كما جاءت المادة 87 من نفس القانون صريحة في تجريم و تسليط العقاب على كل من يثبت تورطه في أعمال الإشادة و التجنيد لصالح الجماعات الإرهابية (الإرهاب الإكتروني) بالإظافة إلى ذلك تدعمت الإجراءات القانونية بآلية تقنية جديدة تتمثل في:

- صدور القانون 16-03 المؤرخ في 2016/06/19 المتضمن البصمات الجنائية في الإجراءات الجزائية لتحديد هوية الأشخاص، كما تم تعزيز الجهات القضائية على المستوى الوطني بأربعة محاكم خاصة الجزائر، قسنطينة، وهران و ورقلة (لتسهيل عمليات البحث و التحري لذوي الإختصاص من الأجهزة الأمنية و البث في القضايا المعروضة دون الرجوع إلى الوصاية، كما شمل التشريع بعض المجالات التي يحتمل أن

تشملها الجريمة و التي لها صلة بمجال الحريات الخاصة على غرار قانون الملكية الفكرية، الثقافية، حقوق المؤلف، 05-01 الصادرين بتاريخ 2005/02/05، و قانون الوقاية و مكافحة المخدرات 04-18 الصادر بتاريخ 2004/12/25.

- تم مطابقة التشريع الداخلي مع ما جاء في التشريعات الدولية و خاصة الإتفاقية الدولية المبرمة في عاصمة المجر بودابيست بتاريخ 2001/11/02 المتضمنة الجرائم السيبرانية و تعتبر هذه الإتفاقية بمثابة المرجعية القانونية لكل التشريعات الدولية الصادرة في هذا المجال، و من بين النقاط التي شملتها المطابقة.
- إستعمال المصطلحات المعمول بها في مجال الإعلام الآلي و تكنولوجيات الإتصال معطيات الإعلام، معطيات متعلقة بالإختراق، ممول الخدمات،(أنظر المادة 01 من الإتفاقية و مقدمة القانون 09-04 الجزائري)، ليبقى الهدف، تسهيل عمل المختصين في الإعلام الآلي من قراءة صحيحة للعمل المطلوب أو الملف المطروح.
- الدخول الغير شرعي للأنظمة المعلوماتية، (أنظر المادة 02 من الإتفاقية و المادة 394 مكرر ق.ع الجزائري) أهمية تجريم هذا العمل هو تحديد نقاط الضعف للنظام المستهدف مع إمكانية تحديد هوية الجاني.
- الإعتراض الغير شرعي للمكالمات و المعطيات المتبادلة سواء في إطار خاص أو مهني (الإتفاقية و المادة 303 من ق.ع الجزائري).[1]
- المساس بنزاهة أو إستماتة المعطيات(أنظر المادة 04 من الإتفاقية و المادة 394 مكرر ق.ع الجزائري)، لأن الحصول على المعطيات بطريقة غير شرعية من شأنه أن يحول من مسار المعلومة في جانبها المهني أو الشخصي، و هذه الخطوة من أخطر التهديدات الإلكترونية.

1- طلال ياسين العيسى، وعدي محمد عناب، مرجع سابق، ص88.

- المسؤولية المعنوية للجهات المكلفة بتسيير مجالات تكنولوجيا الإعلام تبقى قائمة، لأنهم في نظر القانون الضامن الوحيد على حسن و سلامة الأنظمة المعلوماتية (أنظر المادة 12 من الإتفاقية و المادة 394 مكرر ق.ع الجزائري).
- التعاون الدولي من أجل سلامة الإجراءات القانونية (الإنابة القضائية، تسليم المجرمين) و هي من أهم العناصر التي ركزت عليها الإتفاقية في الباب الثالث و المواد 614-713، من ق.إ.ج و المادة 15 من القانون 09-04 لأن هذه الخطوة تبقى السبيل الأمثل بالنسبة للخبراء للحد من الجريمة الإلكترونية، كما تشكل عائق لحسن سير المتابعة القضائية إذا كانت طلبات الإنابة أو التسليم تمس بسيادة الدولة، بالرغم من المجهودات المبذولة من طرف الدولة، إلا أن المختصون يرون أن البنية التنظيمية و التشريعية مازالت في طور التشكيل حتى تكتمل المعادلة، على إعتبار أن القوانين التي تحوي قواعد ملزمة، و رادعة أخذت حصة الأسد في التشريع في حين هناك العديد من الجوانب لم يتم تطويرها بما يتوافق مع البيئة الوطنية، كالمقاييس الدولية للحماية، المواصفات التقنية للمعلومات، البيانات، الأنظمة، البرامج و الأجهزة.[1]

لإستدراك هذه النقائص، تجتهد الجزائر من خلال الهيئات المختصة على التحسين المستمر لآليات المواجهة و تعزيز الإطار القانوني، لمواكبة المتغيرات و التحولات الطارئة في هذا المجال، و من بين أهم النقاط التي تعتزم السلطة التشريعية القيام بها، إصدار قانون لحماية المعطيات الخاصة بالمواطن من الإعتداءات الإلكترونية، تماشيا مع ما جاء في دستور 2016 الذي أوصى بإحترام و حماية الحقوق الخاصة المواد 46-50-51.

1- جوزيف س. ناي الابن، المنازعات الدولية: مقدمة للنظرية و التاريخ، ترجمة: أحمد أمين الجمل، و مجدي كامل) القاهرة : الجمعية المصرية لنشر المعرفة و الثقافة العالمية، 1994، ص 82.

كما تعكف لجنة من الخبراء على تحضير الأرضية لقانون ينظم مهام سلك البريد و الإتصالات الإلكترونية و جعلها من أولويات سلطة الضبط، لأن أغلبية الأخطاء المهنية المؤدية إلى هذا النوع من الجرائم، نفس الطرح تعمل وزارة العدل على تجسيده من خلال[1] مشروع القانون الجديد المتضمن تنظيم كل ما يتعلق بخصوصية المعلومات و سريتها، للمحافظة عليها في ظل التعاملات الإلكترونية عبر شبكات الإتصالات.

ب- من الناحية العملية:

لضمان التنفيذ الفعلي و الجدي لمختلف التدابير الهادفة لتحقيق الأمن السيبراني، أوكلت السلطات العليا للدولة هذه المهمة إلى هيئات متخصصة ضمن أسلاك الأمن، و أوصت بإحترام الحريات في إطار الشرعية الدستورية و المواثيق الدولية، من بين الهيئات، نذكر ما يلي:

- **المصلحة المركزية لمكافحة الجريمة المعلوماتية(SCLC)** : التابعة لمديرية الأمن الوطني، و تعتمد هذه المصلحة على موارد بشرية لها من الكفاءة المهنية ما يؤهلها لتنفيذ مهامها على المستوى الدولي من خلال التعامل مع المصالح المختصة) **أنتربول، أفريكوم** (أو مصالح الشرطة لكبرى الدول، و على المستوى الوطني تتواصل هذه الهيئة مع الشرطة العلمية و المكاتب اللامركزية المختصة في الإجرام (الشرطة القضائية).

- **مركز الوقاية من جرائم الإعلام الآلي و الجرائم المعلوماتية CPLCIC**: التابعة للقيادة العامة للدرك الوطني، لا تختلف كثيرا في مهام التحقيق و التحريات في هذا المجال عن نظيرتها التابعة للأمن الوطني سواء محليا أو وطنيا، بل بالعكس يتم التنسيق بينهما تحت المسؤولية المباشرة للنائب العام على مستوى دائرة الإختصاص.

1- جوزيف س. ناي الإبن، المرجع نفسه، ص 83.

- المعهد الوطني للأدلة الجنائية و علم الإجرام للدرك الوطني (INCC) : التابعة للقيادة العامة للدرك الوطني، يعتمد المعهد في أداء مهامه على الخبرة العلمية و التجارب المخبرية الدقيقة لكل الأدلة المتحصل عليها من مكان إرتكاب الجريمة عامة، من أجل تنوير العدالة و توجيه الجهات الأمنية كلما تعلق الأمر بإستكمال التحقيق.[1]

من بين النتائج المتوصل إليها من طرف هذه المصالح، إتضح أن الجرائم الإلكترونية بالجزائر تتضاعف بطريقة سريعة جدا، و هذا ما كشفت عنه الأرقام المسجلة التي تم البحث فيها، حيث سجلت سنة 2017 أكثر من 2500 جريمة و يتعلق أبرزها ٪70 إنتهاك الحريات الشخصية، و التهديد عبر الإنترنت، و نشر صور فاضحة، الإبتزاز، و القرصنة الإلكترونية و غيرها.

حسب تقدير نفس الأجهزة، فإن هذه الأرقام لا يمكن تسجيلها لو لا الممارسات الغير عقلانية التي جسدها الإستعمال المفرط و الغير منتظم لوسائل الإتصال و تكنولوجيات الإعلام، فقد تم إحصاء أكثر من حيث 28 مليون مستعمل للإنترنت، 18 مليون[2] لهم حسابات و مواقع فايس–بوك و 13 مليون متفحص يومي لشبكة التواصل الإجتماعي، كما طالت عمليات الإختراق وزارة الدفاع الوطني، فحسب المسؤولين، فإن المؤسسة تجهض يوميا ما يقارب 3500 محاولة إختراق لمواقع قيادات قواتها و مديرياتها المركزية، بمعدل 130 ألف محاولة إختراق في السنة، من قبل عصابات" **الهاكرز**" من مختلف دول العالم، في إطار ما يعرف بـ "الحرب الإلكترونية".

1- شريف بسام، " واقع الحوكمة الالكترونية في الدول العربية "، مجلة العلوم الاجتماعية و الإنسانية، جامعة الجزائر 3 ، العدد 6، جوان 2016، ص 157.

2- هذه الأرقام تم الحصول عليها من الوزارة الوصية حصيلة سنة 2017 ، و تمثل حسب الخبراء زيادة 64٪ بالنسبة لسنة 2016، هذا إذا أخذنا بعين الاعتبار عدد السكان الذي يقارب 41 مليون نسمة، مع الإشارة أن معدلات إستعمال تكنولوجية الاتصال بالجزائر في زيادة مستمرة و الدليل أن نسبة إستعمال الهاتف عموما(الثابت، الخلوي) قد وصلت إلى نسبة 115٪ لتخصم منها نسبة 39 ٪ موجها للإستغلال في شبكات التواصل الاجتماعي.

ج- من الناحية الإدارية:

لتفادي الوقوع في تداخل الصلاحيات بين مختلف الأجهزة الفاعلة في مسائل الأمن و الدفاع الوطني، حرص المشرع الجزائري على وضع ضوابط الإحترام الإطار الإداري المنظم لصلاحيات الهيئات المدنية، العسكرية و التقنية في إدارة الإستراتيجية الجزائرية للأمن السيبراني، و يمكن قراءة ذلك من النقاط الآتية:

- **الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها:** التي أنشئت سنة 2009، و وضعت تحت السلطة المباشرة لوزير العدل حافظ الأختام، و لم تدخل حيز التنفيذ إلا بعد صدور المرسوم الرئاسي رقم 261-15، المؤرخ في 2015/10/08، من أبرز المهام المنوطة بها:
  - تعزيز التنسيق بين مختلف الفاعلين في الميدان و التشديد على ضرورة التعاون بين القطاعين العام و الخاص و المجتمع المدني، من أجل نشر ثقافة المواجهة لكل الممارسات التي تخالف القانون في الفضاء السيبراني و حماية الحقوق و الحريات الأساسية.[1]
  - التنسيق و التعاون بين مختلف الأجهزة الأمنية، المالية و الإدارية التي لها علاقة مباشرة بأنشطة تكنولوجيا الإعلام، من أجل تحديد المسؤوليات لفرض مراقبة صارمة بعد حصر المجالات المستهدفة من طرف محترفي الجريمة الإلكترونية، مع العلم أن الدولة متوجهة إلى تحقيق الحوكمة الإلكترونية التي تعتمد في أعمالها على المعاملات الإلكترونية في جميع مجالات الحياة، و يمكن إعتماد المعايير التي ذكرها البنك الدولي للحوكمة الإلكترونية، التي تستطيع من خلالها المؤسسات الحكومية في إستخدامها

1- خلال الندوة الإفريقية حول حوكمة الإنترنت CAGI، المنعقدة بالجزائر بتاريخ 2007/02/21، بحضور 27 دولة إفريقية و العديد من المنظمات الجهوية BAD, UIT, UA، ذكرت ممثلة الحكومة الجزائرية وزيرة البريد و تكنولوجيات و الاتصال، أن البلاد متمسكة بالمبادئ العامة التي نصت عليها هيئة الأمم المتحدة، للمزيد من المعلومات، انظر الرابط تاريخ 2017/02/22 ، www.lemaghrebdz.com

لتكنولوجيا المعلومات التي لديها القدرة على تغيير و تحويل العلاقات مع المواطنين و رجال الأعمال و المؤسسات الحكومية و زيادة قناعة المواطن بدور المؤسسة الحكومية في حياته.[1]

- إقتراح الأرضية اللازمة لتجسيد الإستراتيجية الوطنية للوقاية و محاربة الجرائم الإلكترونية (حسب ما جاء في المادة 04 من المرسوم أعلاه)، و تعتبر هذه الخطوة من الصلاحيات الدالة على أهمية إدارة الأمن السيبراني بالنسبة للدولة.
- بالعودة إلى الدراسات العلمية و الميدانية التي تجمع أن الجانب التوعوي يلعب دور مهم للحد من الجرائم المعلوماتية، فإن الجهات المختصة (الهيئة الوطنية) إذا أرادت النجاح في تحقيق و تطوير الأمن السيبراني، عليها بالعناية الكافية بتوعية كل من له صلة مباشرة أو غير مباشرة بمجال المعلومات، و متى تحقق ذلك، فإن التوعية تستحق أن تكون من العناصر المكملة للجوانب الأخرى على غرار، تفعيل القوانين، التنسيق و التعاون و توفر الأدوات التقنية اللازمة لتحقيق الأمن و التعاون الدولي[2] ، لتجسيد هذه الفكرة، سطرت الدولة كذلك برنامج إعتمدت في تطبيقه على أجهزة السمعي البصري، اللقاءات العلمية، الدورات التكوينية داخل المؤسسات، توزيع مطويات و ألواح إشهارية، و أشتركت في ذلك جميع الوسائط (مؤسسات الدولة و المجتمع المدني).

1- مصلحة الدفاع السيبراني و مراقبة أمن الأنظمة:

بالنظر لحساسية قطاع الدفاع الوطني، أستحدث بتاريخ 2015/06/11، هذه المصلحة على مستوى دائرة الإستعمال و التحضير لأركان الجيش الوطني الشعبي و أوكلت لها مهمة،

1- شريف بسام، المرجع السابق، ص 159.

2- الاتحاد الدولي للاتصالات، " تأمين شبكات المعلومات و الاتصالات، أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني"، لجنة الدراسات، التقرير النهائي الفترة 2014-2017، جنيف، سويسرا، افريل 2017.

حماية المنظومات و المنشأت الحيوية للبلاد ضد كل أنواع الجريمة السيبرانية، و من بين المحاور التي تناولتها الأرضية العملياتية لهذه المصلحة، نذكر ما يلي:

- توجيه، تنفيذ و تأطير الأعمال في هذا المجال لا يجب أن يتعدى الإطار الوظيفي أو التنظيمي
- تطوير و تعزيز المنظومة القانونية لتفادي التجاوزات أثناء إستخدام التكنولوجيا و ضمان حماية منظومات الإعلام.
- إعتماد التكوين التقني و العلمي لإنتاج الكفاءات و المهارات القادرة على خلق نظام الدفاع السيبراني في كافة أنشطة المؤسسة العسكرية و بالتالي تفادي الأخطار الإجرامية.
- غرس ثقافة الإستعمال الكيفي لهذا العنصر الحيوي " تكنولوجيات الإعلام و الإتصال " من خلال حملات تحسيسية لكافة مستخدمي المؤسسة بغض النظر عن الرتبة أو الوظيفة.[1]
- فتح مجال التعاون الدولي مع المؤسسات العسكرية الأجنبية، خاصة تلك التي لها رصيد في المجال لتبادل الخبرات و الإستفادة من تجاربهم في هذا المجال.[2]

أصدرت العديد من الوزارات على غرار وزارة البريد و الإتصال، المالية، التعليم العالي، الداخلية، تعليمات و توجيهات إلى مصالحها التنفيذية تتضمن الآليات و الكيفيات الواجب تطبيقها من الناحية العملية لتفادي الوقوع في الأخطاء، نلخصها فيما يلي:

1- ب. بوعلام، "الجيش الوطني الشعبي و رهانات تداول المعلومة عبر شبكات التواصل الاجتماعي"،... مجلة الجيش، العدد 603، جانفي 2016.

2- الهام غازي، " الوقاية و مكافحة الجريمة المعلوماتية في التشريع الجزائري"، مجلة الجيش، العدد 603 ، جانفي 2016 .

- عدم السماح لأي كان من الحصول على معلومات من الأنظمة المعلوماتية الموصولة بشبكة الإنترنت، ما لم يكن هناك إذن أو موافقة من المصلحة المؤهلة قانونا، كما لا يمكن إستخدام الحسابات الخاصة للأفراد أو تداول أرقامهم السرية.
- إحترام المقاييس المعمول بها في تداول المعلومات المشفرة" " إرسالا و إستقبالا " ، سواء تعلق الأمر بالأنظمة المعلوماتية الداخلية للشبكات الوطنية أو الدولية.

ما يلاحظ في هذا العنصر، أن المجهودات التي تبذلها الجزائر للإلمام بأهم العناصر الكفيلة بتحقيق الأمن السيبراني، مازالت بعيدة، لأن الإجراءت الإدارية المتخذة لحد الأن من طرف الهيئات المذكورة أعلاه للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها تبقى غير كافية و تتطلب المزيد و الإستمرارية في الموقف و النهج.

ت- من الناحية التقنية:

الحصول على أفضل الوسائل التكنولوجية، الإعتماد على الكفاءات و الإطلاع على أفضل طرق الحماية تعتبر حلقة وصل صلبة لتفادي الثغرات و مقاومة الإختراقات، و لتحقيق هذه المهمة، أصبح من الضروري على السلطات الإستثمار في الجانب التقني و تشجيع المبادرة الهادفة لتطوير سياسات أمن و حماية البنية المعلوماتية، خاصة إذا علمنا، أننا على عتبة تجسيد مشروع الحكومة الإلكترونية التي أصبحت مطلب للمواطن لتحسين الخدمات.

لكن ما يعاب من هذه الناحية، أن النقائص التي تم حصرها من طرف الخبراء[1]، أضعفت مجالات الأمن المعلوماتي و جعلت منه فضاء مفتوح للتهديد و الإختراق و من النقائص المذكورة، أن الكيفيات المستعملة في التوظيف غير مطابقة أو غير ملائمة للمواصفات الدولية

1- الإتحاد الدولي للإتصالات، " تقرير حول الأمن السيبراني للدول النامية"، مكتب تنمية الإتصالات، جنيف، سويسرا، أفريل 2001.

لأمن الأنظمة المعلوماتية[1] التي أقرتها علامات كما يشير الخبراء إلى عدم تفعيل و تطوير مختلف تقنيات الأمن السيبراني التي أكد عليها الإتحاد الدولي و يمكن تفحص جميع المعطيات من خلال الإطلاع على تقرير الإتحاد الدولي ITU للإتصالات[2] السنوي (نوفمبر 2017) الذي خلص في النهاية إلى تصنيف دول العالم في مجال الأمن السيبراني معتمدا في ذلك على مقياس "مدى إلتزام الدول في جميع أنحاء العالم بتفعيل و تطوير مختلف تقنيات الأمن السيبراني"، و قسمها إلى ثلاث فئات، دول متخلفة، الناضجة و المتقدمة، و بين التصنيف و التقسيم إحتلت الجزائر المرتبة الثامنة و الستون 68 عالميا من مجموع 164 دولة شملها التقرير و المرتبة التاسعة 21 من مجموع 22 دولة عربية[3] كما يمكن قراءة نفس الإستنتاجات السلبية من خلال تحليل المقاييس العالمية لمستويات التأهب في مجال الأمن السيبراني المستعملة من طرف المؤسسات المتخصصة في هذا المجال القوانين، الإجراءات التقنية اللوائح تنظيمية، بناء القدرات و التعاون أين وجدت الجزائر نفسها في مؤخرة القائمة، حيث إحتلت المرتبة الثالثة و العشرون (23) عالميا من أصل 29 دولة بمؤشر 0.176 مقارنة بالولايات

1- في إطار الشراكة لمحاربة الجريمة الإلكترونية، نظم بالجزائر العديد من اللقاءات مع خبراء و مختصون أجانب، خاصة من دول الإتحاد الأوروبي، و حسب النتائج المتوصل إليها، تبين أن المصالح المركزية لوزارة البريد و التكنولوجيات الإتصال، تفتقر إلى مصلحة التحليل البيانات ذات المقاييس العالمية التي بفضلها يمكن لأجهزة الأمن تحديد الوجهة لمعرفة مرتكبي الجرم، و إذا كان مركز البحث حول المعلومات العلمية و التقنية هو القائم بمهمة التحليل، فهذا لا يعني حسب الخبراء الإستغناء عن فكرة خلق CERIST التابع لوزارة التعليم العالي و البحث العلمي مصلحة التحاليل في أقرب وقت، لأن التهديد الذي تواجهه الجزائر مطابق لما تعيشه الدول المتقدمة.

2- أُنشئ الإتحاد الدولي للإتصالات في 1865 في باريس تحت إسم الإتحاد الدولي للبرق ثم أخذ إسمه الحالي سنة 1939، ليصبح وكالة متخصصة تابعة للأمم المتحدة إبتداءا من سنة 1947، يقوم الإتحاد الدولي للإتصالات منذ نشأته على الشراكة بين القطاعين العام و الخاص، و يبلغ عدد الأعضاء فيه حاليا 193 بلدا و ما يزيد على 800 هيئة من القطاع الخاص و المؤسسات الأكاديمية

3- الدول الرائدة في مجال الحماية الإلكترونية هي: سنغافورة، الولايات المتحدة الأمريكية، ماليزيا، سلطنة عمان، إستونيا، أستراليا، (جورجيا، فرنسا و كندا، أما عربيا، فالدول التي إحتلت المراتب الثمانية الأولى هم: سلطنة عمان (04) عالميا، جمهورية مصر (14) عالميا، قطر (25) عالميا، تونس(40) عالميا، المملكة العربية السعودية (46) عالميا، الإمارات العربية المتحدة (47) عالميا، المملكة المغربية (49) عالميا، و أخيرا البحرين (65) عالميا.

المتحدة الأمريكية صاحبة المرتبة الأولى، بمؤشر 0.824 ، و المرتبة العاشرة (10) عربيا بمجموع 0.1765 مقارنة بالمملكة الأردنية الهاشمية صاحبة المرتبة الأولى بمجموع 0.7643[1]

ث- من الناحية العلمية:

حتى تتمكن الهيئات من السيطرة على مختلف الجوانب المتعلقة بعملية تحقيق الأمن السيبراني وفق ما تم ترسيمه في الإستراتيجية الوطنية، توجهت المؤسسات السيادية رئاسة، و يقع مقر الإتحاد في جنيف، سويسرا، و يضم 10 مكتباً من المكاتب الإقليمية و مكاتب المناطق في جميع أنحاء العالم، و يمثل أعضاء الإتحاد مجموعة واسعة من قطاع تكنولوجيا الإتصالات في العالم من شركات التصنيع و شركات التشغيل، بالإظافة إلى مؤسسات البحوث و التطوير الرائدة و الدوائر الأكاديمية.

ج- الجمهورية، وزارة الدفاع، المؤسسات الأمنية، الوزارات إلى تنظيم دورات تكوينية و سخرت لها كافة الوسائل المادية و البشرية، كما إستنجدت الجزائر بخبراء دوليين لتمكين الإطارات الناشطة في المجال من جميع الأسلاك لمعرفة أفضل الممارسات في تكنولوجيا الأمن و السياسات العامة للأعمال الإلكترونية المعمول بها في الخارج، كما تم إرسال بعثات للحضور و المشاركة في المؤتمرات الدولية للإستفادة من الخبرات التي تهدف إلى إصدار التوصيات المناسبة لأمن و سلامة المعلومات في الفضاء السيبراني.[2]

1- مرزوق عنترة، حرشاوي محي الدين، " الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية"، تاريخ الفحص 2018/04/04، أنظر كذلك المؤشر العالمي للأمن السيبراني، النسخة الثانية الصادرة عن وكالة الأمم المتحدة للإتصالات GCI 2017.07.05

2- الملتقى الدولي الموسوم بعنوان " الدفاع السيبراني مكون أساسي للأمن و الدفاع الوطني"، المنظم من طرف قيادة الأركان للجيش الوطني، 15-2017/05/16 و كذلك الندوة الدولية المنظمة من طرف قيادة الدرك الوطني بتاريخ 27-2017/03/28 في طبعتها الثانية تحت عنوان "الخدمات الالكترونية و الأمن العمومي".

كما ساهمت الجامعات و مؤسسات البحث العلمي من خلال تنظيم أيام دراسية و ملتقيات الأكاديمية، نذكر على سبيل المثال، الملتقى الدولي الذي نظمته كلية الحقوق، جامعة برج بوعريريج بتاريخ 2017/04/12 تحت عنوان "الإجرام السيبراني، المفاهيم و التحديات"، و كذا الملتقى الدولي الذي نظمه كل من الجيش الوطني الشعبي و قيادة الدرك الوطني في الفترة الممتدة بين شهر مارس و ماي 2017. كل التوصيات التي إنتهت إليها اللقاءات العلمية تجتمع حول نقاط مشتركة يمكن إستخلاصها في العناصر التالية:

- تنسيق الجهود، الإعتماد على الكفاءات، إنشاء هيئة مديرة، تعزيز الجانب المادي و البشري، إطلاق مشاريع بحثية، تشجيع المهارات، تعزيز التعاون الدولي.

هذه المطالب و إن لم تكن جديدة الطرح، إلا أن المختصون يعتبرونها بمثابة جسر للتواصل بين الباحثين و الأكاديميين و المهنيين لتعزيز الهياكل الوطنية و تقييم الإنجازات التي تم تجسيدها من طرف الهيئات المدنية أو العسكرية المعنية بمكافحة الجريمة السيبرانية و ذلك في إطار التحول التكنولوجي و الرقمي الكبير الذي تشهده الجزائر.

2- على المستوى الخارجي:

أمام هذه التحديات، لجأت الجزائر في بداية الأمر إلى التعامل مع هذه الجريمة من خلال تفعيل المبادئ العامة المتعارف عليها عالميا في مجال مكافحة الجريمة تبادل المعلومات، تبادل الخبرات و المساعدة الفنية، و مع التطور المذهل لثورة المعلومات و تزايد نسبة الجرائم.

3- السيبرانية، سارعت إلى توقيع العديد من الإتفاقيات الثنائية و المتعددة الأطراف مع الدول العربية في إطار الإتفاقية العربية لمكافحة الإرهاب لسنة 1998 الإتفاقية العالمية لمكافحة الجريمة المنظمة العابرة للحدود لسنة 2000، كما عززت التعاون بين الدوائر المختصة لوضع مقاييس و معايير مطابقة لبرامج الأمن و السلامة المعلوماتية العالمي لضمان الأمن السيبراني الوطني من جهة و تحضير الأرضية لسن تشريع خاص بالجرائم السيبرانية، كما دعمت كل

المبادرات المطروحة لمواجهة الظواهر الإجرامية عامة و الجريمة الإلكترونية خاصة، و من بين الإسهامات المحسوبة للجزائر "المشاركة بفريق من خبراء القانون في العديد من الدورات لأشغال مركز البحوث التابع للجامعة العربية لمناقشة مشاريع القوانين و الإتفاقيات المطروحة للتكيف مع التطورات المتسارعة، لاسيما في المجال التكنولوجي، و من بين المشاريع المنجزة الإتفاقية العربية لضمان أمن و سلامة الفضاء السيبراني[1]. كما عملت أيضا على تجسيد مبدأ الشراكة الأوروبية متوسطية و ذلك بالتوقيع على إتفاق مع الدول الأعضاء في الإتحاد الأوروبي بتاريخ 2002/04/22 المتضمن التعاون في المجال الأمني و القضائي لمحاربة مختلف الجرائم، و كذا الإتفاق المبرم مع فرنسا بتاريخ 2003/10/25 المتضمن التعاون في مجال الأمن و مكافحة الإجرام المنظم، إنطلقت الجزائر في خطوة جديدة بعنوان "التعاون لمواجهة الجرائم السيبرانية في الضفة الجنوبية" للإستفادة من التجربة الأوروبية، و عقدت في هذا الشأن، عدة لقاءات في الجزائر جمعت فريق من الخبراء من مختلف المؤسسات الفاعلة في هذا المجال و خبراء جانب، و أنتهت المشاورات بمجموعة من التوصيات، من بينها:

- تعزيز المنظومة القانونية و مطابقتها للتشريعات الدولية **إتفاقية بودابست**[2] للرد على تحديات الإجرام السيبراني سواء على المستوى الوطني، الجهوي أو الدولي مع إحترام مبدأ السيادة الوطنية و حقوق الإنسان.
- تعزيز الإمكانيات المادية و البشرية للمؤسسات الأمنية المكلفة بمواجهة الإجرام السيبراني، و كذا التنسيق بين ذات المصالح و الهيئات المشرفة.

1- أنظر محتوى الاتفاقية العربية لبناء الثقة في الفضاء السيبراني، و كذلك التوصيات الصادرة عن المؤتمر الرابع للمتخصصين في الأمن و سلامة الفضاء السيبراني (الإنترنت)، المنعقد في مقر المركز العربي للبحوث القانونية (الجامعة العربية)، بيروت، لبنان (2015/08/19).

2- إتفاقية بيدابيست الأوروبية حول الإجرام المعلوماتي المصادق عليها من طرف المجلس الأوروبي بتاريخ 2001/11/23، دخلت حيز التنفيذ سنة 2004 ، تعتبر بمثابة الأرضية القانونية التي أعطت دفعا للدول الأوروبية خاصة و دول العالم عامة، للإسراع في سن قوانين و فرض إجراءات قانونية و إدارية لمحاصرة الإجرام السيبراني، خاصة و أن أهم معضلة تواجه التعاون الدولي تسليم المجرمين و الإنابة القضائية، قد تم الفصل فيها.

- إستعمال الدليل الإلكتروني كمعيار للقيام بالإجراءات القضائية الصحيحة.
- الديمومة في تكوين الإطارات الأمنية و القضائية وفق المناهج العلمية المعتمدة دوليا لتسهيل عملية التأقلم مع التطورات الحاصلة في الميدان.
- الإسراع في رسم إستراتيجية فعالة تتضمن كل الجوانب التنظيمية، العملية و التقنية لتدارك الأخطار الناجمة عن هذه الجرائم.

كان المجلس الأوروبي قد أقر معاهدة مكافحة الجريمة السيبيرية، التي دخلت حيز التنفيذ، سنة 2004،[1] داعيا جميع الدول إلى التوقيع عليها، منذ تاريخ إقرارها في العام 2001. و تعتبر أحكام هذه المعاهدة، منسجمة مع متطلبات مكافحة الجريمة السيبرانية، لاسيما و أنها تطلب من الدول الأعضاء، إنشاء مراكز إتصال تعمل بحسب مبدأ إستمرارية الخدمة، أي تأمين متابعة على إمتداد ساعات اليوم، بحيث تكون دائمة الإستعداد، للتجاوب مع الطلبات القادمة من خارج الحدود الجغرافية، و للتعاون مع القوات المعنية بمكافحة الجريمة، بسرعة و فعالية.

يأتي في هذا السياق، أيضا، إلتزام الدولة، في حال كونها مصدر الفعل الجرمي الملاحق، الإحتفاظ بالبيانات الخاصة بحركة الإتصالات، و الكشف عنها، إلى الدولة التي تطلب ذلك، نتيجة وقوع نتائج الجرم فيها، و يعني ذلك عمليا، ضرورة سن التشريعات الخاصة، التي تسمح بتسهيل عمليات البحث، و الإستقصاء، و المتابعة، و وضع اليد، على معلومات الإتصالات، و إدخال التعديلات اللازمة على القوانين الجزائية، بحيث تأتي منسجمة، مع متطلبات تسليم المطلوبين من العدالة، و تبادل المعلومات.

1- http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG

أما على مستوى العالمي و أمام تصاعد الإهتمام العالمي بهذا العالم الإفتراضي، و أمام تزايد النشاط التجاري، و المالي، إزداد حجم دفق البيانات و المعلومات، عبر الشبكة العالمية للمعلومات، و توسعت حركة المبادلات التجارية، و التحويلات المالية على الإنترنت[1]، في المقابل، توسعت حركة التشريع و التنظيم في البلدان التي تعي أهمية إقتصاد الإنترنت حول مسائل: حماية المستهلك، و حماية البيانات، و سلامة التحويلات، و السلطات القضائية المختصة، و حماية الملكية الفكرية، و الخصوصية، و غيرها الكثير مما يتعلق بالمسؤولية عن الخدمات، و نوعيتها.

كما تبرز في هذا المجال أيضا: القضايا المتعلقة بحوكمة الإنترنت، و الحماية من الجريمة السيبرانية و تداعياتها، على تطور المعاملات الإلكترونية، و إستخدام تقنيات المعلومات و الإتصالات، و من المتوقع في هذا المجال، بروز القضايا التي ترتبط بإستخدام المال الإلكتروني، أو المال الجوال، و طرق الدفع الآمنة، و آلياته، و تخزين المال الإلكتروني، و إستخدامه كبطاقات دفع إفتراضية، أو كبطاقات هدايا. و يضاف إلى هذا، إزدياد نزاعات العمل، التي يمكن أن تنشأ في إطار نماذج العمل عن بعد، و إستخدام تقنيات المعلومات و الإتصالات، كالشبكات الإجتماعية، و الشبكات الداخلية، في أماكن العمل، و تندرج هنا أيضا، قضايا حماية خصوصية العامل، و حقوقه.

1- J.P. Morgan: Global E-Commerce Revenue To Grow By 19 Percent In 2011.
http://techcrunch.com

تبذل الهيئات الدولية، و في مقدمها، الإتحاد الدولي للإتصالات[1] ، جهودا حثيثة، تؤكد على حتمية الأمن السيبراني. و يخصص الإتحاد هذا الأخير، بجزء أساسي من برامجه و خطط عمله المختلفة.

قد تعاملت الأمم المتحدة، مع تقنيات المعلومات و الإتصالات، لاسيما فيما يتعلق بالإنترنت، من منطلق كونها، أداة للتنمية الإجتماعية و الإقتصادية[2]، و وسيلة ناجعة في السعي إلى تحقيق أهداف الألفية. و عليه، فقد أو كل المجلس الإقتصادي الإجتماعي، لمتابعة قضايا التنمية المتعلقة بالإنترنت. في المقابل، تهتم اللجنة الخاصة بالعدالة الجنائية و منع

1- أُنشئ الاتحاد الدولي للاتصالات في 1865 في باريس تحت اسم الاتحاد الدولي للبرق. و يرجع اسمه الحالي إلى 1934، و في 1947 أصبح وكالة متخصصة تابعة للأمم المتحدة. يقوم الاتحاد الدولي للاتصالات منذ نشأته على الشراكة بين القطاعين العام والخاص، و يبلغ عدد الأعضاء فيه حالي 193 بلدا و ما يزيد على 800 هيئة من القطاع الخاص و المؤسسات الأكاديمية. و يقع مقر الاتحاد في جنيف، سويسرا، و يضم 12 مكتباً من المكاتب الإقليمية و مكاتب المناطق في جميع أنحاء العالم. و يشمل أعضاء الاتحاد مجموعة واسعة من قطاع تكنولوجيا المعلومات و الاتصالات في العالم، من أكبر شركات التصنيع و شركات التشغيل في العالم إلى الأطراف الفاعلة الصغيرة المبتكرة التي تستعمل تكنولوجيات جديدة أو ناشئة إلى جانب مؤسسات البحوث و التطوير الرائدة و الدوائر الأكاديمية، يضم مجتمع به أكثر من 20000 مهني، يعتبر المكان الوحيد في العالم الذي يحتوي شبكة غنية و متنوعة من الخبراء و القادة في النظام الإيكولوجي العالمي لتكنولوجيا المعلومات و الاتصالات، من مهامه:

- تسهيل التوصيلية الدولية لشبكات الاتصالات و توزيع الطيف الراديوي و المدارات الساتلية في العالم.
- وضع المعايير التقنية التي تضمن سلامة التوصيل بين الشبكات العالمية و إختيار أفضل الممارسات من أجل المساعدة على ضمان انتشار النفاذ إلى خدمات تكنولوجيا المعلومات و الاتصالات و التكنولوجيات،
- تحسين النفاذ إلى تكنولوجيات المعلومات و الاتصالات لفائدة المجتمعات المحلية التي تعاني من نقص الخدمات في جميع أنحاء العالم.
- دعم و حماية الوسائل التكنولوجية الكفيلة بضمان حق كل فرد في الاتصال. و الاتحاد هو منصة فريدة للشراكات العالمية بين القطاعين العام و الخاص. و بالانضمام إلى الاتحاد، يمكنك أن تصبح جزء اً من
- ضمان التعاون بين القطاعات الحكومية و الهيئات الأكاديمية سواء في القطاع العام أو الخاص، لتحديد ملامح البيئة السياساتية و التنظيمية لتكنولوجيا المعلومات و الاتصالات في المستقبل.

2 - Resolution 60/252 , 27 April 2006, adopted by the General Assembly –World Summit on the Information Society.

الجريمة، الموكلة بمتابعة الجهود الدولية في مكافحة و منع الجرائم الوطنية و العابرة للحدود[1]، بالقضايا المتعلقة بجرائم الإنترنت.

في سياق عينية، هناك تعاون بين المكتب المعني بالمخدرات و الجريمة (UNDOC) في الأمم المتحدة و الإتحاد الدولي للإتصالات، لمساعدة الدول الأعضاء في الإتحاد، للحد من المخاطر التي تشكلها الجريمة السيبرانية، و ذلك بموجب مذكرة تفاهم موقعة بين المنظمتين، في منتدى القمة العالمية لمجتمع المعلومات.[2]

كذلك تلعب **الآيكان**، دورا هاما على مستوى أمن الفضاء السيبراني، من خلال إدارتها لأسماء النطاقات، و البرامج التي تطورها في هذا المجال.

على خط مواز، إتجهت معظم الدول المتقدمة، إلى إقرار سياسات وقائية و دفاعية، ضد الهجمات السيبرانية، و خصصت الدول الكبرى، مثل الولايات المتحدة الأميركية[3]، أستراليا، و المملكة المتحدة، مبالغ طائلة، لمعالجة مسائل الأمن السيبراني، و إستقرار الفضاء السيبراني و ليست هذه الحقيقة، سوى مؤشر، إلى مدى الإهتمام الذي توليه هذه الدول، لإرساء الثقة

1- Economic and Social Council Resolution 1992/22: Implementation of General Assembly Resolution 46/152 concerning operational activities and coordination in the field of crime prevention and criminal justice, E/1992/92, 30 July 1992.

2- UN and ITU team up to fight Cybercrime By Messaging News staff On May 19, 2011 the ITU , the United Nations agency for information and communications technologies, cemented new global partnerships designed to make cyberspace a safer, more secure place to be for consumers, businesses, and – most crucially – children and youth. A Memorandum of Understanding (MoU), signed between ITU and the United Nations Office on Drugs and Crime (UNODC) at this year's WSIS Forum event in Geneva will see the two organizations collaborate in assisting ITU and UN Member States mitigate the risks posed by cybercrime.
http://www.messagingnews.com/short-takes/un-and-itu-team-fight-cybercrime

3 - PricewaterhouseCoopers, Cyber Security M&A: Decoding Deals in the Global Cyber Security Industry (Nov. 2011)

و الإستقرار، كما السلامة و الأمن في هذا الفضاء. فالإقتصاد العالم، كما حياتنا اليومية، متصلان إتصالا وثيقا بالفضاء السيبراني، و الخدمات الحيوية، كالأمن، و الدفاع، و العلاقات الدولية، مهددة في كل لحظة، نتيجة الإختراقات، و الإعتداءات على الشبكة العالمية للمعلومات، و على الأنظمة المعلوماتية، و قواعد المعلومات.

مع بروز الحوسبة السحابية، تستعد الشركات الكبرى، كما الحكومات، لنقلة نوعية، تتمحور حول النماذج الجديدة، في تخزين و معالجة البيانات، و المعلومات، و إنتقالها في الفضاء السيبراني، و تواجدها في أماكن بعيدة عن سيطرتها المباشرة، كما تتمحور حول الكلفة، و نوعية الخدمات و سلامة المعلومات، و قد بدأ البعض منها، في وضع بنود على موازنتها، خاصة بالخدمات المرتبطة بهذه التقنية، كما بالسياسات و الإستراتيجيات التي لا بد من وضعها، بحيث تؤمن الأطر الصحيحة، و آليات التعاقد و البنية الإدارية الضرورية لذلك.

كان قادة القطاعات الصناعية و التجارية، قد وجهوا طلبا إلى لجنة الإتحاد الأوروبي، لإيجاد الإطار التشريعي المناسب لخدمات الحوسبة السحابية[1]، فبعد إنتقال الخدمات الكلاسيكية، كالبريد الإلكتروني، و الرسائل القصيرة، و شبكات إدارة العمل، إلى الإفادة من خدمات الحوسبة السحابية، ستنتقل دون أدنى شك، إدارة المحفظة الإلكترونية، و الخدمات المالية و المصرفية، و النشاطات الحكومية، من نقل و موارد طاقة و غيرها. و بالتالي، يصبح ملحا، تقرير الموجبات و الحقوق، بما يضمن، الأنسياب السهل للمعلومات و تفادي ممارسات مزودي الخدمات التي تمنحهم أرباحا غير محقة، كما يبدو ضروريا، إستيعاب الحاجة إلى مقاربة جديدة لحماية المعلومات تبعا لحساسيتها إنطلاقا، من الإعتماد على المعايير و المقاييس الدولية في هذا المجال. و هنا أيضا، يطرح المختصون، أهمية سياسات الوصول إلى المعلومات و حماية البيانات، لاسيما مع البلبلة التي مازالت تتحكم في هذا الموضوع، و مع

1- PricewaterhouseCoopers, Cyber Security M&A: Decoding Deals in the Global Cyber Security Industry (Nov. 2011)

إنعدام الإنسجام بين القواعد التشريعية الوطنية. فمع إنتقال المعلومات، عقود و نوعية خدمات، و صيانة، لا بد من إيجاد نماذج جديدة، تأخذ كل هذه العناصر بعين الإعتبار.

فمع التزايد المطرد في نسبة الجريمة و إستغلال المنظمات الإجرامية للمناخ الدولي المتسم بالمرونة لتوسيع مجال عملياتها الإجرامية عبر الحدود – إما بطريق مباشر من خلال مد نشاطها الدولي، أو بطريق غير مباشر عن طريق إنتشار شبكات دولية للمنظمات الإجرامية تتعاون فيما بينها، كان من الضروري التفكير في تقييم آداء أجهزة العدالة الجنائية الدولية، و خلق أجهزة نوعية متخصصة، و رفع كفاءة الأجهزة المختصة بملاحقة الجريمة.

لا تزال الجريمة عبر الوطنية من الموضوعات المطروحة للنقاش في المحافل– العلمية الدولية و الإقليمية – لغرض التوصل إلى فهم مشترك لهذه الظاهرة، و خصائصها، بوصفها – غالبا – جريمة فاعلين متعددين، يرتكبها أفراد منتمون إلى مجموعة إجرامية تتجاوز حدود الدولة الواحدة الأمر الذي دفع بالمجتمع الدولي إلى البحث عن آليات جديدة تتلاءم و طبيعتها، و تطوير الوسائل التقليدية بما يكفل تضامن جهود الدول، و أجهزتها القائمة بمهمة مكافحة الجرائم عموما و الجريمة المنظمة على وجه الخصوص و ذلك لتحقيق خلق مؤسسات أكثر ديناميكية، إستجابة لسرعة ظهورها و تطورها.

ذلك أن المكافحة المثلى للجريمة قد تتجاوز الوسائل التقليدية إلى وسائل أكثر جرأة تدعم التعاون رسمي المتخصص، سواء أكان ثنائيا أم متعدد الأطراف، بحيث يسمو على الخلافات السياسية و الهيكلية التي تواجهها الحكومات، حيث لا يزال مبدأ السيادة من المبادئ الجوهرية التي تحد من فعالية التعاون الدولي، و يعيق الأسس العلمية للتعاون الدولي اللازم و الملائم لمكافحة الجريمة.

فالتعاون القضائي الدولي هو الآلية الرئيسية للكفاح ضد الجريمة بأبعادها المختلفة، مثل : الإرهاب الدولي، و الإتجار غير المشروع بالأسلحة، و المخدرات، و الأشخاص، و غسيل

الأموال، و تزييف العملات، و غير ذلك من الجرائم التي ترتكبها منظمات إجرامية أو أشخاص طبيعية أو إعتبارية عن الأغراض التي أنشئت لأجلها.

يقصد بالتعاون في هذا المقام: ما تقدمه سلطات دولة لدولة أخرى من مساعدة و عون في سبيل ملاحقة الجناة بهدف عقابهم على جرائمهم، و ذلك من خلال تدابير وقائية تستهدف مواجهة الصيغة غير الوطنية للجريمة، و تستجمع الأدلة بمختلف الطرق، و هو ما يستغرق وقتا، و يتطلب إمكانات لا تملكها سلطات قانونية لدولة واحدة ما لم تدعمها و تساندها جهود السلطات القانونية في الدول الأخرى.

لم تتأخر الإدارة الأميركية، عن إستحداث قيادة عسكرية جديدة، مختصة بأمن الفضاء السيبيري[1]، و تتولى مروحة من النشاطات العسكرية، تشمل إلى الحماية، القيام بمناورات سيبرانية، سواء لتحديد مدى فاعلية الحماية، أو مدى القدرة على الرد، أو للتعرف إلى مكامن الضعف، و التدريب على آليات الرد. و يتم ذلك، في إطار إستراتيجية أعدتها وزارة الدفاع في العام 2011 حول كيفية العمل في الفضاء السيبراني[2]، و كان رئيس الوزراء الإنكليزي، **غوردن براون**، قد أعلن هو أيضا، عن إنشاء وحدة خاصة، لمكافحة الجريمة السيبرانية[3].

كل التوجهات التي إعتمدتها الهيئات المتخصصة سواء على المستوى الدولاتي (الشركات المتعددة الجنسيات) أو على المستوى الأممي (الإتحاد الدولي للإتصالات) لوضع مقاييس

1- Les USA se dotent d'un commandement militaire pour le cyberspace. …porte-parole du pentagone : « les risques lies au cyber sécurité figurent parmi les défis économiques et de sécurité nationale les plus sérieux du XXIe siècle ».http://www.elwatan.com/Les-USA-se-dotent-d-un

2- www.defense.gov/news/d20110714cyber.pdf

3- Le cyberspace anglais désormais protégé par d'anciens pirates informatiques. http://techno.branchezvous. com/actualite/2009/06/le_cyberspace_anglais_desormais

و ضوابط لحماية البيانات، سلامة التحويلات الإلكترونية في جميع المجالات، حوكمة الإنترنت، إنخرطت فيها الجزائر و تعاملت معها بإيجابية من خلال وضع مناهج و آليات للحماية من الجريمة السيبرانية و تداعياتها المستقبلية، هذه الخطوات و غيرها أعطت دفعا للإستراتيجية الجزائرية التي تفاعلت مع كل صور التعاون الدولي بمختلف مظاهره خاصة و أن معدل الإختراقات على الشبكة العالمية للمعلومات، و على الأنظمة المعلوماتية الوطنية بلغ درجات من الخطورة المهددة للأمن الوطني، القومي و العالمي.

الفرع الثاني: الإعتداءات السيبرانية

تعرف الإعتداءات السيبرانية على أنها أفعال يقوض من قدرات وظائف الشبكة المعلوماتية من خلال إستغلال " Marshall" أحد نقاط الضعف ما يمنح المعتدي القدرة على التلاعب بالنظام، أما **جونيد و مارشال** فيعرفه على أنه عملية الإستغلال المتعمد لأنظمة الكمبيوتر و الشبكات المعتمدة على التكنولوجيا "junaidu" من خلال البرمجيات الضارة، و تتعدد مابين الأساليب الممكنة أو العشوائية، فقد تستخدم من طرف الرسمسسن، أو أساليب ضغط بشكل عشوائي من طرف محترفين لتحقيق النفع الذاتي أو المصالح الشخصية أو إعتداءات منظمة من طرف جماعات مارقة.

الإعتداء السيبراني في دليل العمليات السيبرانية و الإرهاب السيبراني للجيش الأمريكي بأنه: " الإستخدام المتعمد للأنشطة التخريبية أو التهديد بها ضد أجهزة الكمبيوتر أو الشبكات، بقصد إحداث ضرر أو تحقيق أهداف إجتماعية، أو إيديولوجية، أو دينية، أو سياسية، أو

أهداف مماثلة، أو لتخويف أي شخص من أجل تحقيق هذه الأهداف[1] " و تتضمن منهجية الهجوم السيبراني إجراء متعمدا بغرض " تغيير، أو تعطيل، أو خداع، أو إهانة، أو تدمير أنظمة، أو شبكات الكمبيوتر المعادية أو المعلومات أو البرامج المقيمة في هذه الأنظمة، أو الشبكات أو التي تمر عبرها"[2] و يعرف البعض الإعتداء السيبراني بأنه" أي إجراء يتم إتخاذه لتقويض وظائف شبكة الكمبيوتر. لأغراض سياسية، أو أمنية وطنية[3] و يلاحظ في هذه التعريفات أنها تقصر الإعتداء السيبراني على ما يؤدي إلى تبعات غير عنيفة في الواقع المادي، و تقتصر آثاره على الفضاء السيبراني، في حين يعرف دليل **تالين** الإعتداء السيبراني بأنه عملية سيبرانية، هجومية أو"دفاعية من المتوقع – بشكل معقول أن تتسبب في إصابة أو وفاة الأشخاص، أو تلف، أو تدمير الأشياء[4] و بالتالي، على عكس التعريفات السابقة، يقصر الإعتداءات السيبرانية على ما تؤدي إلى تبعات عنيفة في الواقع المادي مثل: التسبب في إصابة، أو وفاة الأشخاص، أو تلف، أو تدمير الأشياء.

1 –The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or to further social, ideological, religious, political or similar objectives. Or to intimidate any person in furtherance of such objectives". U.S. Army Training & Doctrine Command, Dcsint Handbook No. 1.02, Critical Infrastructure Threats and Terrorism, at Vii-2 (2006).

2- Gervais, Cyber Attacks and the Laws of War (October 1, 2011). Michael Available at: https://ssrn.com/abstract=1939615

3- Hathaway, et al. "The Law of Cyber-Attack", op.cit., pp. 817.

4- Tallinn Manual, op.cit., p.415.

المبحث الثاني

القوة السيبرانية و الإختراق

يعتبر العصر الحديث عصر التكنولوجيا التي سيطرت على جميع نواحي الحياة والتي تتطور يوما بعد يوم بسرعة كبيرة حتى أصبح الفضاء الإلكتروني عصب الحياة المعاصرة للأفراد والدول وأصبحت شبكة الإنترنت مجالا خصبا للتواصل و الإتصال و وسيلة ربط للحياة الإجتماعية و السياسية و الإقتصادية على المستوى الدولي، و أصبح عمل جميع قطاعات الدولة يختزل في مجموعة بيانات و معلومات مسجلة على الحواسيب و الأمر نفسه بالنسبة لبيانات الأفراد، و على هذا الأساس تحولت العلاقات الدولية خاصة النزاعات بين الدول إلى هذا الفضاء الإلكتروني و أصبحت أداة للهجوم و للدفاع بما يسمى بالهجمات السيبرانية و كذا إجراءات حماية المعلومات التي تتبناها كل دولة حماية لمصالحها، أو الحروب السيبرانية في حالات أشد خطورة تغير فيها المفهوم التقليدي للحروب، و إكتسى النزاع الدولي صبغة إلكترونية لم تعد تلتفت إلى المفاهيم التقليدية للصراع.[1]

عليه فإن من يملك المعلومة يملك القوة كما أن حرب اليوم هي حرب المعلومة ما يستلزم دراسة الموضوع لمعرفة واقع اليوم و مدى تأثير التكنولوجيا الحديثة في قوة الدول وأمنها المعرض للإختراق الذي لم يعد يقتصر على دولة معادية فقط و إنما قد يحدث من طرف فرد أو جماعة أفراد أو هيئات في شكل أداة ضغط و في كثير من الأحيان أداة تدمير للأخر، و قد شهد العالم الحديث مثل هذا النوع من الصراعات الذي أدى إلى دمار شامل بسرعة مرعبة.[2]

1- خالد بن سلمان الغثبر، محمد بن عبد الله القحطاني، أمن المعلومات بلغة ميسرة، مركز التميز لأمن المعلومات، جامعة الملك سعود، الرياض، السعودية، 2009، ص 23.

2- محمد سعد محمود، الحرب السيبرانية أدواتها، وقودها و خسائرها، تاريخ الإطلاع 2003/05/11سا :0- /28/ 10:31 11، Noor-book.com2020

المطلب الأول

القوة السيبرانية

يعد الهدف الأسمى للأمن السيبراني هو القدرة على مقاومة التهديدات المتعمدة و غير المتعمدة و الاستجابة و التعافي، و بالتالي التحرر من الخطر أو الأضرار الناجمة عن تعطيل أو إتلاف تكنولوجيا المعلومات و الاتصالات أو بسبب إساءة استخدام تكنولوجيا المعلومات و الاتصالات و يتطلب حماية الشبكات و أجهزة الكمبيوتر، و البرامج و البيانات من الهجوم أو الضرر أو الوصول غير المصرح به، و نتيجة لأهمية الأمن السيبراني في واقع مجتمعات اليوم فقد جعلته العديد من الدول على رأس أولوياتها، خاصة بعد الحروب الإلكترونية التي بدأت تظهر تجلياتها بين بعض الدول الكبرى، في إشارة صريحة إلى نهاية الحروب التقليدية التي كانت تستخدم فيها الأسلحة الثقيلة، و الإعلان عن بداية حروب جديدة هي الحروب الإلكترونية[1] كذلك تعتبر إحدى الوسائل التي تعاظمت بفضل الفضاء السيبراني حيث أصبح التفوق في هذا المجال عنصرا حيويا في تنفيذ عمليات ذات فاعلية في الأرض، و البحر، و الجو، و الفضاء، و إعتماد القدرة القتالية في الفضاء الإلكتروني على نظم التحكم والسيطرة التكنولوجية، بغية إعادة تشكيل خريطة الموازين في العلاقات الدولية.

هذا الوضع أدى إلى تغيير في مفهوم القوة الوطنية للدولة، فبات بالإمكان تعريفها بأنها مجموعة الوسائل، و الطاقات، و الإمكانيات المادية و غير المادية المنظورة و غير المنظورة التي بحوزة الدولة، و يستخدمها صانع القرار في فعل مؤثر يحقق مصالح الدولة و تؤثر في سلوك الوحدات السياسية الأخرى.

1- فارس قرة، الأمن السيبراني، تاريخ النشر 2019/08/28، تاريخ الإطلاع: 2003/04/28، الموسوعة السياسية http://political-encyclopedia.org/dectionary

فأشكال القوة تغيرت وفقا لتطور التكنولوجيا و المعلومات، فقد أعاد الفضاء الإلكتروني تشكيل مفهوم القوة، ليدشن لنا مفهوم القوة الالكترونية التي ساهمت في إبراز كذلك دور الفاعلون الجدد من غير الدول، مما هدد دور الدول و قلل من سيادتها و حفاظها على أنظمتها السياسية و أمنها القومي. و لم يتوقف الأمر على هذا بل أدى التطور التكنولوجي لظهور أسلحة جديدة صغيرة الحجم قادرة على هدم أنظمة و بناء غيرها. بالإضافة إلى كم الخسائر الإقتصادية و السياسية الناتجة عنها، و لنا في ثورات الربيع العربي نموذج. الذي ساهمت التكنولوجيا في التوعية السياسية للشعوب العربية و تحفزيهم على المشاركة السياسة لمحاربة النظم الديكتاتورية و مواجهة الإرهاب الدولي أحيانا تحت مظلات مخدوعة و واهية.[1]

من بين المنظرين الذي نبه إليها **جوزيف ناي** الذي عرفها بأنها مجموعة الموارد المتعلقة بالتحكم في و السيطرة على أجهزة الحاسبات و المعلومات، و الشبكات الإلكترونية، و البنية التحتية المعلوماتية، و المهارات البشرية المدربة للتعامل مع هذه الوسائل.

من بين مرتكزات هذه القوة وجود نظام متماسك يعظم القوة المتحصلة من التناغم بين القدرات التكنولوجية، السكانية، الإقتصادية، الصناعية، القوة العسكرية، إرادة الدولة، و غيرها بما يسهم في دعم إمكانات الدول على ممارسة الإكراه أو الإقناع أو ممارسة التأثير السياسي في أعمال الدول الأخرى بغرض الوصول للأهداف الوطنية من خلال قدرات التحكم و السيطرة على الفضاء الإلكتروني.

من بين التداعيات أن هذه القوة أعطت دفعا جديدا للدول من جهة لتدعيم القوة الناعمة، حيث بات الفضاء الإلكتروني مسرحا لشن هجمات تخريبية ترتبط بنشر المعلومات المضللة و الحرب النفسية و التأثير في توجهات الرأي العام و النشاط السري و الاستخباراتي، و من جهة

1- فارس قرة، المرجع السابق، ص 23.

ثانية، تبني الدول لزيادة الإنفاق في سياسات الدفاع الإلكتروني و حماية شبكاتها الوطنية من خطر التهديدات، و بناء مؤسسات وطنية للحماية الإلكترونية.[1]

الفرع الأول: ظهور القوة السيبرانية

منذ ظهور الإنترنت، و جعلها في متناول الحكومات و الشعوب و الأفراد، بعدما كانت حكرا للإستخدامات العسكرية فقط، تغيرت المفاهيم و إزداد هذا العالم تناقضا و غموضا، فتخلت الجيوش عن سياسة تجهيز المقاتلين بالعتاد الثقيل، و مختلف المعدات الوقائية و الضرورية اللازمة للمعارك الطويلة الأمد و مجهولة الزمان و المكان، فتغيرت معايير القوة، بتغير ساحات المواجهة من ساحات مكشوفة إلى فضاءات إفتراضية.[2]

أولا :التحولات في مضامين القوة و ظهور القوة السيبرانية:

أصبح الفضاء السيبراني أحد العناصر الأساسية التي تؤثر في النظام الدولي بما يتيحه من أدوات تكنولوجية مهمة لعمليات الحشد و التعبئة في العالم، فضلا عن التأثير في القيم السياسية، فسهولة الإستخدام و رخص التكلفة إزداد من قدرته على التأثير في مختلف مجالات الحياة سواء السياسية أو الإقتصادية أو الإجتماعية و حتى الإيديولوجية و بات جليا من يمتلك آليات توظيف البيئة السيبرانية يصبح أكثر قدرة على تحقيق أهدافه و التأثير في سلوك الفاعلين المستخدمين لهذه البيئة.

- سيسكو شركة أمريكية عملاقة متخصصة بعلم الشبكات بشكل عام.
- وكالة حكومية مكلفة بالدفاع السيبراني الفرنسي تأسست في 07 جويلية 2009.

1- فارس قرة، المرجع نفسه، ص 22.

2- إسماعيل زروقة، " الفضاء السيبراني و التحول في مفاهيم القوة و الصراع "،" مجلة العلوم القانونية و السياسية"، المجلد 10، ع 1، جامعة محمد بوضياف، المسيلة، ، 2019، ص 17-18.

من الأمور المتعارف عنها في العلاقات الدولية أن مصادر قوة الدولة تتغير، فإلى جانب القوة الصلبة المتمثلة في القدرات العسكرية و الإقتصادية، تزايد الإهتمام بالأبعاد الغير المادية للقوة، و من تم بروز القوة الناعمة التي تعتمد على جاذبية النموذج و الإقناع.

لقد تعددت التعاريف حول مفهوم القوة فنجد القوة الصلبة مفهومها مرتبط بالمفهوم التقليدي للقوة و الذي يعرف على أنها القدرة على فرض السيطرة على الآخرين عن طريق الإكراه أو الحوافز المادية، أما القوة الناعمة فهي إستخدام الجاذبية بدلا من الإرغام، أو دفع المال.[1]

مع ثورة المعلومات ظهر شكل جديد من أشكال القوة و هو القوة السيبرانية Cyber power التي لها تأثير كبير على المستوى الدولي و المحلي فمن ناحية أدت إلى توزيع و إنتشار القوة بين عدد كبير من الفاعلين، مما جعل قدرة الدولة على السيطرة موضع شك، و من ناحية أخرى منحت للفاعلين الأصغر قدرة أكبر على ممارسة كل من القوة الصلبة و القوة الناعمة عبر الفضاء السيبراني و هو ما يعني تغيرا في علاقات القوى في السياسة الدولة.

يعد جوزيف س ناي "Joseph s.nye" من أبرز المهتمين بالقوة السيبرانية حيث يعرفها بأنها القدرة على إستخدام الفضاء السيبراني لإيجاد مزايا الدولة و التأثير على الأحداث المتعلقة بالبيئات التشغيلية الأخرى و ذالك عبر أدوات سيبرانية، كما يوضح جوزيف أن مفهوم القوة السيبرانية يشير إلى "مجموعة الموارد المتعلقة بالتحكم و السيطرة على أجهزة الحاسبات و المعلومات و الشبكات الإلكترونية و البنية التحتية المعلوماتية و المهارات البشرية " المدربة للتعامل مع هذه الوسائل[2]، و إن إنتشار القوة ظاهرة صينية إرتبطت بتعاظم دور الفاعلين من

1- فريدة طاجين، مرجع سابق، ص 18 .

2- إسماعيل زروقة، مرجع سابق، ص 19.

غير الدول، ذالك لأن المعلومة لم تعد حكرا على الدول فالقطاع الخاص يساهم بنسبة كبيرة من إمتلاك و إدارة التكنولوجيا الحديثة و وسائل الإتصال و المعلومات.[1]

يتناول مفهوم القوة السيبرانية مجمل القضايا التي تتعلق بالتفاعلات الدولية العسكرية و الإقتصادية و السياسية و الثقافية و الإعلامية و غيرها و حتى تتمكن الدولة من ممارسة النفوذ داخليا أو خارجيا عبر القوة السيبرانية يجب أن تتوفر مجموعة من العناصر أهمها:

- **وجود بنية تحتية سيبرانية:** تشمل أجهزة الكمبيوتر و شبكات الإتصالات، و البرمجيات، و قواعد البيانات لمختلف الأنظمة و القطاعات.
- **بنية مؤسسية:** تتولى مهمة القوة السيبرانية و تحقيق الأمن السيبراني للدولة.
- **بنية تشريعية:** تكون ضامنة و محددة لإستعمال القوة السيبرانية.
- **إستراتيجية بأهداف واضحة:** تحدد طرق العمل و الأهداف المرجوة.

ثانيا: أنماط إستخدام القوة في الفضاء السيبراني:

قد بين جوزيف ناي أنماطا لإستخدام القوة السيرانية و ميز بين الإستخدام الصلب و الإستخدام الناعم، و تفصيلها كالتالي:

1- قدرة الفاعل (أ) على التأثير على سلوكيات الفاعل (ب) و دفعه للقيام بأعمال لم يكن ليقوم بها:

- **و تكون مصدرا للقوة الصلبة:** و ذالك بإستخدامه لمقدراته و أدواته لتدمير أجهزة الدولة عبر قطع كبلات الإتصالات أو تدمير أنظمة الإتصالات أو الأقمار الصناعية أو إستخدام الأسلحة السيبرانية كالفيروسات لتدمير الأنظمة المعلوماتية لمنشأة حيوية، و هذا يهدد أمن الدولة و السكان.

1- تغريد صفاء، " أثر السيبرانية في تطور القوة"، مجلة حمورابي، جامعة النهرين، العدد 33-34، العراق، 2020، ص 153.

– **و تكون مصدرا للقوة الناعمة:** و ذالك من خلال التأثير في سلوك الفاعل الدولي مثل: إستخدام اليوتوب لتخطي التعميم الإعلامي أو فضح الإنتهاكات المرتكبة من طرف الأنظمة المستبدة كما جرى عام2007 بتصوير فجاعة النظام العسكري الحاكم في ميانمار (بورما سابقا) حيث بثت على الإنترنت كما تستخدم أيضا لإدارة العمليات النفسية و التأثير في الرأي العام و تكوين تحالفات دولية و في عمل أجهزت الإستخبارات الدولية، و تمثل أيضا في وضع الدولة لمعايير ملزمة للبرمجيات و إستخدام الجماعات الإرهابية للفضاء السيبراني للتجنيد.

2– قدرة العنصر الدولي على التحكم في أجندة الآخرين من خلال منعه من تنفيذ بعض خططه الإستراتيجية: و بالرجوع إلى ما حدث عام 2010 حيث قامت إيران بإبطاء سرعة الإنترنت لإعاقة بث فيديوهات معرضة و بالتالي أحبطت إستراتيجيتهم.

3– ترتيب أولويات العناصر و ذالك من خلال أن يقوم الفاعل (أ) بترتيب أولويات الفاعل (ب): و نمط القوة الصلبة هنا في حجب مواقع عن المواطنين و ترك أخرى و هذا ما فعلته العديد من الدول، أما نمط القوة الناعمة فيكون بنشر أو تقديم قيم و ثقافات عبر الإنترنت مثل: تصوير قيم رافضة لنشر الإباحية عبر الإنترنت.[1]

إذن إن الهدف من إستخدام القوة السيبرانية يعد غرضا إستراتيجيا ذا صلة بتحقيق أهداف السياسة إذ يدور الهدف الإستراتيجي للقوة السيبرانية في خلق ميزة لصناع القرار هي فهم البيئة الإستراتيجية في السلم و الحرب و إفتقار العدو لهذه الميزة في الوقت نفسه (فهم التحديات و الفرص في الفضاء السيبراني).[2]

1– فريدة طاجين، مرجع سابق، ص 29.

2– تغريد صفاء، مرجع سابق، ص 154.

الفرع الثاني: الهيئات الفاعلة في المجال السيبراني

جاءت ثورة المعلومات لتتحدي الإفتراض الأساسي للمدرسة الواقعية القائل بأن الدول هي أقوى الجهات الفاعلة، و بالتالي أهمها في السياسة الدولية، فتتحدى المعلوماتية أسبقية الدولة، بسبب زيادة مشاركة الجهات الفاعلة غير الحكومية التي تهدد ديناميكيات السلطة التقليدية، و تزداد أهمية الجهات الفاعلة غير الحكومية في العلاقات الدولية وفقا لجوزيف ناي حول إنتشار السلطة، ففي المجال السيبراني يمكن للمجرمين من الأفراد و المنظمات و الجماعات الإرهابية الإستفادة من إمكانية الوصول للإنترنت لتهديد هيمنة الدولة، كما تلعب الشركات الخاصة دوراً، كمزود للأمن و مصدر للضعف في ذات الوقت و على الرغم من أن الدول لا تزال هي الجهات الفاعلة الأكثر هيمنة عندما يتعلق الأمر بالنزاع السيبراني، تلعب الجهات الفاعلة غير الحكومية و الإرهابيون دوراً، لكن تكتيكاتهم كانت عمومتً غير فعالة أو استخدمت كغطاء للدول القومية التي تسعى لإخفاء أفعالها حيث حدد جوزيف .س ناي ثلاثة أنواع من الفاعلين الذين يمتلكون القوة و هم: الدولة، و الفاعلون من غير الدول، و الأفراد:[1]

أولا: الدولة

تعتبر الدولة فاعل محوري في تسيير الفضاء السيبراني إنطلاقا من إمكانياتها المادية و البنيوية و البشرية و القانونية و يجدر الإشارة هنا إلى الإحتكار القانوني للدولة بواسطة أجهزتها المختلفة و لذالك لابد لها من التحكم في مجال الفضاء السيبراني و هو الفضاء الذي يزاحمها فيه العديد من الفواعل الأخرى التي قد تصل حد تهديد مصالحها.

1- بول ويلكينسون، العلاقات الدولية، مقدمة قصيرة جداً لبني عماد تركي(ترجمة) 2013، مؤسسة هنداوي، متوفر بتاريخ 28 أفريل 2023 https://www.hindawi.org/books/93705863/3.

1- **الفاعلون من غير الدول:** و هنا يأتي دور الأفراد و الجماعات و المنظمات الغير حكومية و الشركات الذين أصبحوا بإمكانهم التحكم في توجهات الدول و إدارتها وفق سياسات معينة من خلال الفضاء السيبراني و أهم هذه الفواعل:

أ- **الشركات متعددة الجنسيات:** لإمتلاكها موارد للقوة تفوق قدرت بعض الدول و لا ينقصها سوى شرعية ممارسة القوة التي هي حكرا على الدولة فمثلا نجد شركات جوجل google Amazon و أمازون appel و آبل ميكروسوفت microsoft المنتشرة في مختلف دول العالم التي تمتلك قواعد بيانات عملاقة.[1]

و تستطيع من خلالها إستكشاف و إستغلال الأسواق و التأثير في إقتصاديات الكثير من الدول و في ثقافة المجتمعات و توجهاتها، و هذا ما حدث في الأزمة بين شركة جوجل و الصين حول المحتوى أو فضيحة تسريب بيانات مستخدمي فايسبوك لصالح شركة **"كامبردج أناليتيكا"** التي تم الإستعانة بها لصالح حملة الرئيس الأمريكي **ترامب**.[2]

ب- المنظمات الغير حكومية: تعتمد هذه المنظمات بشكل كبير على شبكة الإنترنت و وسائل التكنولوجية الحديثة في تعبئة الرأي العام و الضغط على الحكومات من خلال ترتيب الحملات الإجتماعية و تعبئة المجتمع المدني من أجل الضغط على الحكومات للتغيير في سياسات معينة مثلما تقوم به اليوم معظم منظمات البيئة العالمية على إثر قرار الرئيس الأمريكي **ترامب** التخلي على إتفاقيات التغير المناخي.

1- فريدة طاجين، مرجع سابق، ص 20.

2- إسماعيل زروقة، مرجع سابق، ص 19.

ت- حركات التحرر الوطني: تعتبر من أبرز الفواعل الدولية من غير الدول مثل : **حركة حماس** و **حزب الله** و إن كان يشارك هذه الحركات عدد كبير من الأفراد بصفاتهم الشخصية و يقومون بإرسال هجمات سيبرانية ضد أهداف العدو، و على الإنترنت مدافعا عن القضية.[1]

ث- المجموعات الإفتراضية: هم القراصنة الذين ينشطون في الفضاء السيبراني بحرية كل حسب أهدافه و دوافعه و إيديولوجيته بحرية....إلخ.[2]

ج- المنظمات الإجرامية و الجريمة الإلكترونية: هي المؤثرة في التفاعلات الدولية و غالبا ما تحميها الحكومات الضعيفة و الفاسدة و هذه المنظمات الإجرامية تقوم بالقرصنة السيبرانية بهدف سرقة المعلومات أو إختراق الحسابات البنكية و تحويل أرصدة منها، أو من خلال وجود السوق السوداء على الإنترنت لبيع المعلومات المالية المتعلقة بكلمات المرور الشخصية، و الحسابات البنكية و بطاقات إئتمان حيث تكلف الجرائم السيبرانية الشركات أكثر من ترليون دولار سنويا. و من الصعوبة الكشف عن هويتها و ذالك راجع للميزة التي يتمتع بها الفضاء السيبراني من قابلية التخفي و هناك أنواع من الجرائم التي يمكن أن تتم بواسطة الفضاء السيبراني و قد يتعرض لها المستخدم أو يكون طرفا فيها و هو لا يدري.

ح- المنظمات الإرهابية (الإرهاب السيبراني): هم المجموعة الأحدث و الأكثر خطورة، لأن دافعهم ليس المال فقط بل لديهم قضية يدافعون عنها و عادة ما يقومون بإرسال رسائل تهديد أو تدمير البيانات المخزنة في نظم المعلومات الحكومية بمجرد تسجيل وجهة نظرهم كما أن مكان تواجدهم غير محدود فعملهم من أي مكان في العالم و هذا ما يصعب إقتناصهم.

1- فريدة طاجين، مرجع سابق، ص 21.

2- يوسف بوغرارة، مرجع سابق، ص 104.

3- الأفراد: فاعلا مهما في الفضاء السيبراني حيث أن له القدرة على إحداث ثورة في المعلوماتية و تصبح تلك الثورة مجال إستخدام للدولة نفسها و مثال ما قام به **مارك زوكرباغ** عام 2004 بتأسيسه شبكة **الفيس بوك** لتستقطب أكثر من مليار مستخدم عبر العالم، فمواقع التواصل الإجتماعي كان. لها دورها بارزا لتنظيم عدة مظاهرات في مختلف دول العالم.[1]

الفرع الثالث: كيفية الإبلاغ عن الجريمة و التحقيق و التحري

إن جمع الإستدلالات من الإجراءات التي تسبق التحقيق و رفع الدعوى الجنائية و التي يختص بها مأموري الضبط الجنائي و التي يكون النائب العام مشرف و مسؤول عن أعمالهم، و إجراءات جمع الإستدلال ينطوي فيها عملية البحث و التحري حول الجريمة و التمهيد للتحقيق فيها و التي تختص بها النيابة العامة دون غيرها.

فالإستدلال هو: " مجموعة الإجراءات الأولية السابقة على تحريك الدعوى الجنائية و التي تستهدف التحري عن الجرائم و التثبت من وقوعها و جمع معلومات كافية بشأنها، و إثبات الآثار التي تولدت عنها على وجه يتيح لسلطة التحقيق التصرف في التهمة، سواء بتحريك الدعوى الجنائية الناشئة عنها، أو بحفظ أوراقها و صرف النظر عنها، فهو إجمالا بمثابة إعداد العناصر اللازمة للتحقيق في الجريمة.[2]

أولا :كيفية الإبلاغ عن الجريمة

على رجال الضبط الجنائي بحسب المهمات الموكلة إليهم و حسب إختصاصاتهم بأن يستقبلوا جميع البلاغات و الشكاوى التي تردهم في الجرائم، و لقد حدد نظام الإجراءات الجزائية السعودي في المادة 26 رجال الضبط الذين خولهم النظام بالقيام بأعمال الضبط و هم:

- أعضاء هيئة النيابة العامة في مجال إختصاصاتهم.

1- فريدة طاجين، مرجع سابق، ص 20.

2- محمد حميد المزمومي، مرجع سابق، ص 97.

– مدير الشرطة و معاونيهم في المدن و المحافظات و المركز.

– الضباط في جميع القطاعات العسكرية بحسب المهمات الموكلة إليهم في الجرائم التي تقع ضمن إختصاص كل منهم.

– محافظي المحافظات و رؤساء المراكز.

– رؤساء المراكب السعودية البحرية و الجوية في الجرائم التي ترتكب على متنها.

– رؤساء مراكز الأمر بالمعروف و النهي عن المنكر في حدود إختصاصاتهم.

1– الواجبات المحددة لرجال الضبط الجنائي:

أ– تلقي البلاغات و الشكاوي و التحري عنها:

عادة تبقى الجريمة مستترة حتى يصل خبرها إلى السلطات المختصة، و أي إخبار أو بلاغ عن الجريمة لابد و أن يتضمن على الأقل معلومات أولية عن الجريمة مثل محل الجريمة و مكان وقوعها و نوعها، و يتم الكشف عن الجرائم السيبرانية بوضع برمجيات حاسوبية معينة خصوصا فيما يخص جرائم القرصنة أو نشر المواد الإباحية.

للحصول على البيانات المتعلقة بإرتكاب الجريمة من نظام الحاسب الآلي لأن هناك و سيلتان تستندان إلى معايير تقنية و قانونية و تتمثل في الآتي:

– يتم الحصول على المعلومات عن طريق إعتراض أو رصد البيانات المنقولة من الموقع أو إليه أو في إطاره.[1]

ب– أدوات الإبلاغ عن الجرائم السيبرانية:

لقد حددت المملكة العربية السعودية أدوات البلاغ عن الجرائم السيبرانية و هي كالآتي:

– عن طريق الشرطة حسب الإختصاص المكاني.

1– خالد حسن أحمد لطفي، مرجع سابق، ص 99.

- الإتصال على الرقم 989
- التطبيق الإلكتروني (كلنا أمن) على الأجهزة الذكية.
- البوابة الإلكترونية لوزارة الداخلية (أبشر)
- هيئة الأمر بالمعروف أو النهي عن المنكر عن طريق الهاتف 1909 أو الموقع الإلكتروني https://www.pv.gov.sa/Pages/PVHome.aspx
- عن طريق إرسال بريد الكتروني لهيئة الإتصالات و تقنية المعلومات Info.cybercrime@moisp.gov.sa
- عن طريق البلاغ عن حادثة سيبرانية في موقع الإلكتروني للهيئة الوطنية لأمن السيبراني https://www.my.gov.sa/wps/portal/snp/main

2- معاينة مسرح الجريمة:

المقصود به هي تلك الآثار التي يتركها مستخدم الشبكة السيبرانية المشتملة على الرسائل المرسلة منه أو التي يستقبلها و كافة الإتصالات التي تمت من خلال الحاسب الآلي و الشبكة، فالمعاينة في الجرائم التقليدية قد تحتوي على آثار مادية فعلية، و لكن في الجرائم السيبرانية قد تطول الفترة الزمنية بين وقوع الجريمة و إكتشافها مما يعرض الآثار الناجمة عنها إلى المحو أو التلف أو العبث بها، كما يستطيع مأمور الضبط الجنائي الإستعانة بأهل الخبرة عند إجراء المعاينة إذا لزم الأمر، و ذلك لإعطاء رأيهم الفني في ذلك، و إذا تمت المعاينة بعد وقوع الجريمة في المجال: السيبراني فيجب مراعاة الآتي:[1]

- تصوير الحاسب و الأجهزة الطرفية المتصلة به على أن يتم تسجيل وقت و تاريخ و مكان التقاط كل صورة.
- العناية بملاحظة الطريقة التي تم بها إعداد النظام.

1- خالد حسن أحمد لطفي، مرجع سابق، ص 102.

- ملاحظة و إثبات حالة التوصيلات و الكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عمليات المقارنة و التحليل حين عرض الأمر فيما بعد على المحكمة.
- التحفظ على مستندات الإدخال و المخرجات الورقية للحاسب ذات الصلة بالجريمة، لرفع و مضاهاة ما قد يوجد عليها من بصمات.
- قصر مباشرة المعاينة على الباحثين و المحققين الذين تتوافر لهم الكفاءة العلمية و الخبرة في مجال الحاسبات.[1]

3- سماع أقوال الشهود و المشتبه بهم:

في الواقع نادرا ما نجد شاهدا على وقائع الجريمة السيبرانية، و ذلك لعدة أسباب أهمها أن الجرائم السيبرانية تتطلب دراية كافية بالجوانب الفنية و التقنية للحاسب الآلي، كما أن الجرائم السيبرانية ترتكب في هدوء أي أن الجاني يرتكبها وحده دون وجود أحد معه، و كما أنها لا تترك أي آثار خارجية يشهد بها أحد كما هو المعتاد في الجرائم التقليدية.

و ليس لمأمور الضبط الجنائي أن يأمر بإحضار متهم أو شاهد، بل له إستدعاء من يشاء لسماع أقواله، و إذا رفض الحضور فليس له إكراه في ذلك، أو إحضاره بمذكرة قبض، لأن هذا من إختصاص النيابة العامة.[2]

4- الإستعانة بالخبراء:

تستعين الشرطة و سلطات التحقيق أو المحاكمة بأصحاب الخبرة الفنية المتميزة في مجال الحاسب الآلي، و ذلك بغرض كشف غموض الجريمة أو تجميع أدلتها و التحفظ عليها، و بناء عليه فإن الإستعانة بخبير فني في المسائل الفنية البحتة أمر واجب على جهة التحقيق و القاضي، فهو أوجب في مجال الجرائم السيبرانية، حيث تتعلق بمسائل فنية آية في التعقيد

1- خالد حسن أحمد لطفي، المرجع السابق، ص 103.

2- المرجع نفسه.

و محل الجريمة فيها غير مادي، و التطور في أساليب ارتكابها سريع و متلاحق، و لا يكشف غموضها إلا متخصص و على درجة كبيرة من التميز في مجال تخصصه.

5-التحفظ على أدوات الجريمة

يقوم رجل الضبط الجنائي بضبط الكيانات المادية السيبرانية في مسرح الجريمة مثل أجهزة الربط بالشبكات و الطابعات و غيرها، و تقوم النيابة العامة من ضبط الكيانات المعنوية السيبرانية بإكتشافها من بعد ضبط الكيان المنطقي للحاسب الآلي مثل البرامج و الفيروسات و البيانات و المعلومات المسروقة و كل المواد المعنوية التي تتعلق بالجريمة و تم إرتباطها بالحاسب الآلي.

6- تحرير محضر الواقعة:

يجب أن تثبت جميع الإجراءات في محاضر موقع عليها منهم، مبينا بها وقت إتخاذ الإجراءات و مكان حصوله، و توقيع الشهود و الخبراء و ترسل المحاضر للنيابة العامة مع الأوراق المضبوطة.

ثانيا: كيفية البحث و التحقيق و التحري في الجريمة السيبرانية:

يعتبر التحقيق هو المرحلة الأولى للدعوى الجنائية التي تسبق المحاكمة، و تقوم به النيابة العامة بعد البلاغ عن القضية و إحالتها لها، إذا توجد بها دوائر متخصصة في التحقيق في الجرائم السيبرانية، تسمى بدوائر المال، تقوم هذه الدوائر بإستجواب المتهم و التحقيق معه في الجريمة المنسوبة إليه.

تتميز بأنها ذات طبيعة قضائية و يمكن مباشرتها بطريقة القهر و الإجبار بخلاف إجراءات الإستدلال التي تتميز بطبيعة إدارية، كما تتميز إجراءات التحقيق أيضا بأن ما ينتج عنها من أدلة يمكن أن يعتمد عليها في إصدار أحكام القضاء الجنائي بعكس إجراءات

الإستدلال التي تكون مكملة لأدلة أخرى، و تكون إجراءات التحقيق بجمع الأدلة من المعاينة و ندب الخبراء و التفتيش و ضبط الأشياء و مراقبة المحادثات و تسجيلها و سماع الشهود و الإستجواب و المواجهة، و لا يلزم المحقق ترتيب معين عند مباشرة هذه الإجراءات.[1]

1- المعاينة:

على المحقق ضبط كل ماله علاقة بالجريمة، و إثبات حالة الأشخاص و الأماكن و الأشياء ذات الصلة بالجريمة، و قد يكون إثبات المعاينة مع الجرائم السيبرانية أمرً أصعبا للفترة الزمنية التي قد تطول ما بين وقوعها و إكتشافها مما يؤدي بها إلى تلف البيانات أو نقلها أو إخفائها.

هنا نلاحظ بأن المعاينة قد تكون إجراء تحقيق أو إستدلال، و لا تتوقف طبيعتها على صفة من يجريها بل على مدى ما يقتضيه إجراؤها من مساس بحقوق الأفراد و حرياتهم، فإذا جرت المعاينة في مكان عام كانت إجراء إستدلال، و إذا إقتضت دخول مسكن أو مكان له حرمة خاصة كانت إجراء تحقيق.[2]

2- ندب الخبير:

للمحقق أن يستعين بالخبراء المختصين لإستكمال إجراءات التحقيق، و هذا بالفعل ما تتطلبه طبيعة الجرائم السيبرانية الذي تقتضي معرفة تامة بنظم الحاسبات و مهارة و تقنية فنية عالية تمكنهم من مباشرة التحقيق في مجال الجرائم السيبرانية. و قد تعددت النصوص المذكورة في اللائحة التنفيذية لنظام الإجراءات الجزائية السعودي في ندب الخبراء ما يلي:

1- محمد حميد المزمومي، مرجع سابق، ص 165.

2- المرجع نفسه، ص 167.

- يكون ندب المحقق للخبير لإبداء رأيه في مسألة متعلقة بالتحقيق وفقا لما ورد في – المادة 76 من النظام مكتوبا، و يحدد في الندب المهمة المطلوبة و المدة – المحددة لإنجازها، و يخضع الخبير أثناء مباشرته مهمته لرقابة التحقيق.
- للمحقق تمكين الخبير من الإطلاع على الأوراق و المستندات المتعلقة بطلب الخبرة.
- يلتزم الخبير المنتدب بالمهمة المكلف بها.

ب- المادة 51:

- يقدم الخبير عند إنجاز مهمته المطلوبة منه وفقا لما ورد في المادة 77 – من النظام تقريرا مؤرخا و موقعا منه يتضمن ملخصا للمهمة و إجراءات الكشف – و الفحص و التحاليل الفنية التي باشرها و مشاهدته و النتائج التي خلص إليها بشكل دقيق ومسبب.
- عند تعداد الخبراء و إختلافهم في الرأي فعليهم أن يقدموا تقريرا واحدا يتضمن رأي كل واحد منهم و أسانيده.
- تضم تقارير الخبرة و جميع مرفقاتها إلى ملف الدعوى.[1]

3- التفتيش:

هو إجراء من إجراءات التحقيق التي تؤدي إلى ضبط أدلة الجريمة بعد إكتشافها، و للتفتيش شروط موضوعية تتعلق بسببه وقوع الجريمة بالفعل و أن يوجه إتهام إلى الشخص المراد تفتيشه و الغاية منه من ضبط أشياء تفيد في كشف الحقيقة، و هناك شروط شكلية و هو أن يكون المر بالتفتيش مسببا و حضور المتهم أو ينيبه أو الغير أو من ينيبه التفتيش، و أن يتم تحرير محضر بالتفتيش، و محل التفتيش في الجرائم السيبرانية هو المكونات المادية

1- محمد حميد المزمومي، مرجع سابق، ص 167.

للحاسب الآلي و كذلك البرامج أو الكيانات المنطقية و هي المكونات الغير مادية و تشمل على:

- البيانات المسجلة في ذاكرة الحاسب أو في مخرجاته.
- السجلات المثبتة لإستخدام نظام المعالجة الآلية للبيانات.
- دفتر يومية التشغيل و سجل المعاملات.
- السجلات الخاصة بعمليات الدخول إلى نظام المعالجة الآلية للبيانات و ما يتعلق بها من سجلات كلمات السر، و مفاتيح الدخول، و مفاتيح فك الشفرة.[1]

4- ضبط الرسائل و مراقبة المحادثات:

جاء في نص نظام الأساسي للحكم في المملكة العربية السعودية بأن المراسلات البرقية و البريدية و المخابرات الهاتفية و غيرها من وسائل الإتصال مصونة و لا يجوز مصادرتها أو تأخيرها أو الإطلاع عليها أو الإستماع إليها إلا في الحالات التي يبينها النظام.

من الأهمية القصوى ضرورة وضع الضوابط القانونية التي تنظم الإجراءات المتبعة من قبل سلطة التحقيق أثناء ممارسة أعمالهم في سبيل الكشف الوصول إلى الأدلة الثبوتية في جريمة إرتكبت، و في هذا الشأن فقد نصت المادة 56 من النظام بأنه للرسائل البريدية و الرقمية و المحادثات و غيرها من وسائل الإتصال حرمة فلا يجوز الإطلاع عليها أو مراقبتها إلا بأمر مسبب و لمدة محدودة وفقا لما ينص عليه هذا النظام، و تقضي المادة 57 بأنه لرئيس هيئة التحقيق و الإدعاء العام أن يأمر بضبط الرسائل و الخطابات و الموضوعات و الطرود، و له أن يأذن بمراقبة المحادثات الهاتفية و تسجليها متى كان لذلك فائدة من ظهور الحقيقة من جريمة وقعت على أن يكون الأمر أو الإذن مسببا أو محددا بمدة لا تزيد عن عشرة أيام قابلة للتجديد وفقا للتحقيق، و في ذات الشأن تقضي المادة 58 بأنه للمحقق وحده الإطلاع

1- خالد حسن أحمد لطفي، مرجع سابق، ص 113.

على الخطابات و الرسائل و الأوراق و الأشياء الأخرى المضبوطة و له أن يستمع إلى التسجيلات و له بحسب مقتضيات التحقيق أن يأمر بضبطها أو نسخ منها إلى ملف القضية، أو أن يأمر بردها إلى من كان حائز لها أو مرسله إليه، و على المحقق أن يحافظ على سرية المعلومات من خلال التفتيش و ألا ينتفع بها بأي طريقة كانت أو يفضي بها إلى غيره إلا في الأحوال التي يقضي النظام بها، فإذا أفضي بها دون مسوغ نظامي أو إنتفع بها بأي طريقة كانت تعينت مساءلته.[1]

8- الشهادة:

الشهادة هي إجراء من إجراءات التحقيق، كما أنها إجراء من إجراءات المحاكمة، فيجل أن تؤدى أمام سلطة التحقيق أو أمام المحكمة، إما أن تسمع أقواله أمام الخبير فلا تعد شهادة و لكنه يستطيع القاضي أن يتخذ قرينة إلى جانب قرائن أخرى في الدعوى، و هناك ما يسمى بالشهادة السماعية: كمن يشهد بأنه سمع من آخر أنه شاهد إرتكاب المتهم للجريمة، و هذه تكون قوتها في الإثبات أقل، و هناك الشاهد بالتسامع و هي كأن تكون ترديد لشائعة متناولة بين الناس قد تكون محل صدق أو قد لا تكون، فهذه شهادة لا ترد على الواقعة بالمعنى النظامي الذي أراده المنظم، بل جزء من عمل الخبير،[2] و قد جاء نظام الإجراءات الجزائية و اللائحة التنفيذية منظما للشهادة أمام سلطة التحقيق و ذلك حيث نصت المادة 66: على المحقق أن يثبت في المحضر البيانات الكاملة عن كل شاهد، و تدون تلك البيانات و شهادة الشهود و إجراءات سماعها في المحضر من غير تعديل أو شطب أو كشط أو إضافة، و لا يعتمد شي من ذلك إلا إذا صدق عليه المحقق و الكاتب و الشاهد.

1- محمد حميد المزمومي، مرجع سابق، ص 182.

2- مرجع نفسه، ص 184.

6- الإستجواب:

هو إحدى الإجراءات المهمة من إجراءات التحقيق بهدف الوقوف على حقيقة التهمة من المتهم و الوصول إما إلى إعتراف منه يؤيدها، أو إلى دفاع منه ينفيها و هناك نوعان من الإستجواب:

أ- **الإستجواب الحقيقي:** و هو توجيه التهمة إلى المتهم و مناقشته تفصيليا عنها و مواجهة بالأدلة القائمة ضده.

ب- **الإستجواب الحكمي:** هو مواجهة المتهم بغيره من الشهود أو المتهمين في حكما لإستجواب، فهذه المواجهة تنطوي على إحراجه و مواجهته بما هو قائم ضده.

ت- ضمانات الإستجواب:

- لا يجوز أن يجري الإستجواب غير السلطة المختصة بالتحقيق.
- دعوة محامي المتهم إلى الحضور أثناء إستجوابه.
- يتعين إحاطة المتهم علما بالتهمة المنسوبة إليه.
- يتعين كفالة حرية كاملة للمتهم أثناء إستجوابه.
- لا يجوز إستجواب المتهم خارج مقر جهة التحقيق إلا لضرورة يقدمها المحقق.[1]

هذه جميعها هي إجراءات التحقيق التي تكون من إختصاص هيئة التحقيق و الإدعاء العام (النيابة العامة) و بعد أن ينتهي المحقق من التحقيق في القضية المعروضة عليه، فإنه إما أن يأمر بتقديم المتهم إلى المحاكمة الجنائية و إما أن يصدر فيها أمراً بألا وجه لإقامة الدعوة الجنائية، و المقصود بها قرار المحقق بعدم إحالة الدعوى إلى المحكمة المختصة.

1- محمد حميد المزمومي، مرجع سابق، ص 233.

المطلب الثاني

الاختراق

تعددت الإعتداءات السيبرانية و تنوعت الأساليب، المنتهجة في كيفية شن الإعتداءات، و مع تطور التقنيات التكنولوجية يوما بعد يوم، و التي نتج عنها بالضرورة، إكتشاف فيروسات ضارة و أسلحة إلكترونية أكثر فتكا، ساهمت بشكل ملحوظ في تسهيل عملية إختراق الأجهزة المستهدفة حيث واجهت المنظمات في السنوات الأخيرة تحديا كبيراً تمثل في الإنتقال من شبكات المعلومات و هياكل النظم ذات الملكية الخاصة إلى شبكات المعلومات المفتوحة و هياكل النظم ذات الخدمات و الزبائن المتنوعة و المتعددة.

على الرغم من أن هذه الشبكات زادت من كفاءاة هذه المنظمات و عززت موقفها التنافسي في السوق إلا أنها بذات الوقت – و بسبب طبيعة البيئات المفتوحة التي تتسم بها زادت من مخاطر أمن المعلومات، إذ يؤكد المتخصصون في المجال نظم المعلومات على حقيقة جوهرية هي أن هذه الشبكات تعد سلاحا ذا حدين، فمن جهة أسهمت في إحداث تغييرات جوهرية متسارعة و مطردة في أساليب و إجراءات العمل في المنظمات المختلفة عندما أصبحت عملية جمع البيانات من مصادرها المختلفة و معالجتها و خزن المعلومات و تحديثها و إسترجاعها و إصالها إلى المستفيدين من خلال نظم المعلومات و شبكات الإتصالات المتطورة إحدى أهم السمات في عصرنا الحاضر"عصر ثورة المعلومات" و من جهة أخرى سهلت هذه النظم و الشبكات مهمة إختراق أمن المعلومات و سرقتها أو تحريفها و تشويهها أو إساءاة إستخدامها أو تسريبها خارج القنوات المخصصة لها أو المرخصة بتداولها و الإستفادة منها.[1]

1- David C. Jones , " Computer Advances Create New Data Theft Expo- sures" National Under Writer 97(june 14,1993).

الفرع الأول: مفهوم الإختراق

قد عرفه بعض الفقهاء بأنه قيام شخص بمحاولة الوصول إلى جهاز شخص ما أو الشبكة الخاصة به عن طريق شبكة الإنترنت بإستخدام برامج متخصصة في فك الرموز و الكلمات السرية و كسر الحواجز الأمنية و إستكشاف مواطن الضعف في الأجهزة أو شبكة المعلومات الخاصة بذالك الشخص و عادة ما تكون المخارج (بوابات العبور للمعلومات) الخاصة بالشبكة المحلية و هذه أسهل الطرق إلى جميع الملفات و البرامج الموجودة في ذالك الجهاز.[1]

الإختراق هو أي حادث ينتج عنه وصول غير مصرح به إلى بيانات الكمبيوتر أو التطبيقات أو الشبكات أو الأجهزة، كما ينتج عنه الوصول إلى المعلومات دون إذن، و يحدث عادةً عندما يتمكن المتسلل من تجاوز آليات الأمان.

كما يعرف الإختراق بأنه القدرة على الوصول لهدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف.[2]

إستنادا إلى تعريف الإختراق و الموقع الإلكتروني الذي ذكر من قبل، يمكن إستنتاج أن إختراق الموقع الإلكتروني أو الإختراق على موقع الشبكة الدولية هو الوصول غير القانوني إلى الموقع الإلكتروني للشبكات بغرض إساءة الإستخدام أو الحصول على المنافع من خلال تخريب المعلومات أو سرقتها أو التجسس.[3]

الإختراق و هو دخول شخص بطريقة متعمدة إلى حاسب آلي أو موقع إلكتروني أو نظام معلوماتي أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها، و قد جرمت جميع

1- عقبة عباس، تحسين أداء نظم كشف الإختراق في الشبكات المعرفة برمجيا بإستخدام تعلم الأدلة، أطروحة ماجستير، المعهد العالي للعلوم التطبيقية و التكنولوجيا، الجامعة العربية السورية، 2019، ص 15.

2- المرجع نفسه، ص 16.

3- Nudirman Munir, Pengantar Hukum Siber Indonesia, (Depok: Raja Grafindo Persada, 2017) hlm.228.

الدول عمليات الإختراق بكافة صورها و رتبت على ذلك جزاءات متفاوتة حسب الجرم المرتكب و تناول ذلك في أكثر من مادة.[1]

الفرع الثاني: أنواع و آثار الإختراق

مع تطور تكنولوجيا الإعلام و الإتصال، التي تمخض عنها ظهور مصلح الأمن السيبراني، الذي بات مطلب و غاية لمختلف، المؤسسات، و الحكومات و الدول، التي باتت تجابه مختلف الإعتداءات السيبرانية، التي تعتمد على إختراق النظم الإلكترونية، بطرق جد متطور لا تكاد تترك آثارا للجريمة الإلكترونية، و من أهم الآثار التي يمكن من خلالها معرفة ما إذا كان هناك إختراق على النظم الإلكترونية أم لا.

أولا: أنواع الإختراق:

أنواع الإختراقات كثيرة جداَ، و لكننا نستطيع حصرها بعدة مفاهيم رئيسية:

1- الدخول إلى النظام و البقاء غير المشروع فيه:

تقع هذه الجريمة من أي إنسان أيا كانت صفته سواء كان يعمل في مجال الأنظمة أم ليست له علاقة بالحاسب الآلي و شبكاته و سواء كانت لديه المقدرة الفنية على الإستفادة من النظام أم لا، إنما فقط يكفي أن يكون له حق الدخول إلى النظام، و من الممكن التحقق من الدخول متى كان الدخول مخالفا لإرادة صاحب النظام و من له حق السيطرة عليه مثل تلك، الأنظمة التي تتعلق بأسرار الدولة أو دفاعها أو تتضمن بيانات شخصية تتعلق بحرمة الحياة الخاصة للفرد.[2]

1- ناصر محمد البقمي، جرائم المعلوماتية و مكافحتها في المملكة العربية السعودية، مطابع الحميضي، الرياض، 2009، ص 165.

2- فريدة طاجين، مرجع سابق، ص 22.

2- إعاقة أو تخريب تشغيل نظم معالجة البيانات:

السلوك الإجرامي في هذه الجريمة ينصرف إلى كل عمل من شأنه إرباك عمل نظام معالجة البيانات و من شأن نشاط الجاني إعاقة أو إفشال نظام التشغيل في الإرسال كذلك يمكن أن يؤدي إلى توقيف النظام عن العمل بصورة دائمة أو مؤقتة أو أن يستخدم الجاني في إرتكاب الجريمة أي وسيلة من شأنها أن تعيق سير النظام كالإعتداء المادي أو المعنوي على النظام و من أمثلة ذلك إعاقة النظام بطريقة مادية هو أعمال العنف المادي على أجهزة الحاسوب و شبكة الإتصالات عن طريق تخريبه بكسرها أو سكب أي مادة عليها، أما الإعاقة غير المادية تعتمد على إدخال الفيروس في الجهاز أو عمل بعض التغيرات على كلمة المرور.

3- التلاعب في بيانات نظم معالجة البيانات:

النشاط الإجرامي في هذه الصورة من صور الإختراق تتمثل في أفعال الإدخال أو المحو و التعديل، فالجريمة في هذه الحالة تقع على المعطيات أو البيانات المعالجة آليا دون المعلومة ذاتها لكن القاسم المشترك بين هذه الأفعال جميعا هو إنطوائها على التلاعب في المعطيات التي يتظمنها نظام معالجة البيانات بإدخال معطيات جديدة أو غير صحيحة أو محو أو إدخال تعديلات أخرى.[1]

يمكن تقسيم الإختراق من حيث محل الإعتداء إلى ثلاثة أنواع:

- إختراق المزودات أو الأجهزة الرئيسية للشركات و المؤسسات و ذلك بإختراق الجدران النارية و التي توضع عادة لحمايتها.
- إختراق الأجهزة الشخصية و العبث بما تحويه من معلومات و هي طريقة شائعة لسذاجة أصحاب الأجهزة الشخصية.

1- جمال زين العابدين أمين أحمد، جرائم إختراق النظم الإلكترونية بين التشريع المصري و المغربي، مجلة مستقبل العلوم الإجتماعية، جامعة عبد الملك السعدي، المغرب، 2018، ص 119.

- التعرض للبيانات أثناء إنتقالها و التعرف على شفرتها إن كانت مشفرة و هذه الطرقة تستخدم في كشف أرقام بطاقات الإئتمان و كشف السرية للبطاقات البنكية.[1]

ثانيا: أثار الإختراق:

من أهم الآثار التي من خلالها يمكن معرفة إذا كان هناك إختراق أم لا و التي نلخصها في ما يلي:

- تغير الصفحة الرئيسية لموقع الويب كما حدث لموقع قناة الجزيرة الفضائية مؤخرا إثر عرضها لصور الأسرى الأمريكيين على شاشتها و موقعها حيث قامت جهة ما بإختراق موقعها و نظامها و تعطيلهما و غيرت الصفحة الرسمية لها بالعلم الأمريكي.
- السطو بقصد الكسب المادي كتحويل حسابات البنوك أو الحصول على خدمات مادية أو معلوماتية، كأرقام بطاقات الإئتمان و الأرقام السرية الخاصة بالبطاقات البنكية.
- آثار فردية مما يترتب على الفرد من إنتهاك الخصوصية و سرقة بياناته و معلوماته.
- آثار إدارية مثل تدمير النظم الإدارية الإلكترونية للدولة أو المؤسسات الخاصة.
- يؤدي الإختراق إلى تدمير البنية التحتية المعلوماتية للدولة.[2]

من أجل ضمان حماية دائمة للنظم الإلكترونية من الإختراق و عواقبه لابد من القيام بعدة خطوات بشكل دوري و رغم بساطتها في الظاهر إلا أنها جد مهمة، و أهم هذه الخطوات:

- إستخدام كلمات مرور قوية و التي تجمع بين تسلسلات عشوائية من الأحرف الكبيرة و الصغيرة و الأرقام و الرموز، بحيث يكون إختراقها أكثر صعوبة من كلمات المرور البسيطة، مثل عدم إستخدام أسماء العائلة أو تواريخ الميلاد.

1- جمال زين العابدين أمين أحمد، المرجع السابق، ص 118.

2- المرجع نفسه، ص 123.

- الحرص على تغيير كلمات المرور بإنتظام بحيث يعمل التغيير المنتظم لكلمات المرور على التقليل من المخاطر التي تتعرض لها بسبب إختراقات البيانات غير المعلنة.
- النسخ الإحتياطي بحيث تؤدي بعض إختراقات البيانات إلى تشفير الملفات و طلب فدية لإتاحتها مرة أخرى للمستخدم، أما إذا كانت لديك نسخة إحتياطية، فإن بياناتك ستكون آمنة في حالة حدوث إختراق.[1]

1- مني عبد الله السمجان، مرجع سابق، ص 12.

خاتمـــة

خاتمة:

و في الأخير نتوصل إلى أن التطور التكنولوجي و ان كان له الفضل في توفير فضاء تلاقت فيه الشعوب مع بعضها البعض رغم بعد المسافات و الإختلاف في نمط الحياة، إلا أنه لم يستطيع توفير الحماية لهذا المولود الجديد العالم الغريب و المتجدد من عديد الخروقات و التجاوزات التي حولته من فضاء للسلم و الأمن إلى مسرح لعدم الإستقرار و اللأمن، من بين هذه الإختراقات المساس بأمن الأشخاص من خلال سرقة المعطيات الشخصية للأفراد، بحيث كثرت عمليات المساومة و لم يعد يسلم فرد من هذه العمليات، سواء كان مسئولا أو مواطنا مما جعل حياة البشر و خصوصياتهم ملاذ للإبتزاز بشكل لا يصدق، ثم إنتقلت العدوى للمساس بأمن الدول من خلال التجسس و التخريب لنيل من المنشآت الحيوية، الأجهزة الأمنية، المؤسسة العسكرية، المؤسسات الحكومية، الشركات و البنوك. مع العلم أن عمليات الإختراق بلغت مستويات من شأنها المساس بالأمن الوطني، القومي و العالمي.

أمام هذه المخاطر التي لا تعرف حدود أصبحت القابلية للعطب إحدى الهواجس التي تعاني منها الدولة لدرجة أنه أصبح من الصعب جدا على الدول توفير الحماية لأنظمتها المعلوماتية خاصة و ان التدفق الهائل الذي تعرفه عملية الإستعمال المتزايد لأجهزة الإعلام الثورة المعلوماتية، دفع بها إلى إطلاق صفارات الإنذار و الدخول في حالة حرب دائمة مع فواعل ممن يمتلكون المهارة و الوسيلة المعلوماتية و لهم القدرة على توظيفها لإختراق كل الأنظمة الحساسة مهما كانت القدرات و الإحتياطات الأمنية المتوفرة.

فالجرائم المستحدثة على غرار شبكة **ويكي ليكس** و تسريبات **سنودن** في فضاء إعتبره الإستراتيجيون الأمريكيون المجال الخامس للحرب، من شأنه المساس بالأمن العالمي إن لم تفعل اليقظة المعلوماتية و تستبق وضع الآليات الكفيلة للتأقلم مع التحديات التي تفرزها التطورات التكنولوجية و فرض المراقبة المستمرة لهذا الميدان.

في هذا الإطار توجه صناع القرار على المستوى الدولي إلى الإستعانة بالمجهود العلمي و الأكاديمي لتقديم البدائل العلمية التي شكلت إحدى أهم مضامين السياسات الأمنية وطنيا، إقليميا و دوليا المقترحة و التي تجلت في طرح تصورات و إستراتيجيات الأمن السيبراني ترتكز أساسا على بناء حواجز و جدران تقنية لمنع هذه الهجمات و بالتالي التحكم في أنظمة المراقبة لحماية المنظومة المعلوماتية للمؤسسات و المواطنين.

و في الأخير يمكن القول أنه نظرا لأهمية دراسة موضوع الأمن السيبراني من خلال هذا المشوار العلمي إلى كل الجوانب التي حولت الموقع الجغرافية لكبريات الدول إلى فضاء مفتوح لتلاقي و تقاطع كل أنواع التهديدات التي بدون شك سيكون لها تداعيات على الأمن الوطني و إذا أطفنا إلى ذلك المخاطر السيبرانية، فإن أي دولة مهما كانت قدراتها ستصبح إحدى ضحايا هذه التحديات و تبقى الحماية في حاجة إلى إستثمارات فكرية و مادية هائلة لتصميم و تطوير إستراتيجية أمنية متعددة التخصصات الجوانب التشريعية، التنظيمية، البشرية، المالية، التقنية، و المعلوماتية حتى تستطيع الدولة تأمين الثورة الرقمية للأفراد و المؤسسات و بالتالي التصدي لخطر تشتكي منه اليوم الدول الكبرى.

و ما خلصنا إليه من خلال هذه النتائج بعد كل ما تعرضنا إليه في هذه الدراسة من مختلف الخطوط العريضة حول ما تضمنه الأمن السيبراني من عمليات الدخول و الخروج لمختلف مواقع تداول و تخزين المعلومات و البيانات يستوجب بالضرورة خلق قواعد و آليات تثبيت أصول الأمن لحماية هذه المواقع و أنظمتها المعلوماتية، فلقد حرصنا من خلال هذه الدراسة إلى إستظهار عدد من الإقتراحات و التوصيات التي تبدو لنا محل إنتقاد و دراسة تستدعي الإطلاع و الإنتباه لها وفق الإقتراحات التالية:

– التوقف الفوري من إستيراد أجهزة الحاسوب من دول أخرى مثل أمريكا، لكون أنظمة هذه الأجهزة تحتوى على ثغرات أمنية، مخصصة خصيصا للتجسس على الدول.

– توجيه الإستثمار في العنصر البشري من خلال الرسكلة التي تضمن تجديد المعلومات، و الإطلاع على آخر المستجدات في مجال الأمن السيبراني، و بذالك يسهل مواكبة التطورات الحاصلة في العالم.

– تدعيم الآلية القانونية و المؤسساتية بمزيد من النصوص القانونية و الهياكل المتخصصة من أجل محاولة تحديد هوية الجاني الإلكتروني، و إثبات الجريمة الإلكترونية.

– فتح الباب أما الفاعلين المحلين (الأفراد) من أجل الإستفادة من خبراتهم و تجهيز جيش سيبراني، و هذا راجع لكفئاتهم و تميزهم على المستوى الدولي.

– إنشاء هيئة وطنية مختصة بالجرائم السيبرانية.

– إنشاء مركز إستقبال جميع البلاغات المتعلقة بالجرائم السيبرانية.

– إنشاء كوادر من الفنيين و التقنيين يمتلكون الخبرة و المهارة العالية في المجال السيبراني.

– تكوين خبراء معنيين في مجال الإستدلال و التحقيق السيبراني.

– إعتماد المحاضر و الضبوط و الموثقة من الهيئة الناتجة من التحقيق كأوراق رسمية تقدم لدى المحكمة المختصة.

– إعتماد نظام و لائحة تنفيذية للهيئة.

المراجع

أولا: الكتب

1- أحمد طارق عفيفي صادق، الجرائم الإلكترونية، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2015.

2- إدريس عطية، "مكانة للأمن السيبراني في منظومة الأمن الوطني الجزائري"، جامعة، العربي التبسي، الجزائر، 2019.

3- الهادي كرّو، محاضرات في القانون الجنائي العام، كلية الحقوق و العلوم السياسية، تونس، 1988.

4- إبراهيم إبراهيم، أركان الجريمة و طرق إثباتها في قانون العقوبات الجزائري (أركان الجريمة، أهمية الإثبات الجنائي، طرق الإثبات الجنائية)، دار الخلدونية للنشر و التوزيع، الجزائر، 2007.

5- جوزيف س .ناي الإبن، المنازعات الدولية: مقدمة للنظرية و التاريخ، ترجمة : أحمد أمين الجمل، و مجدي كامل)، الجمعية المصرية لنشر المعرفة و الثقافة العالمية، القاهرة، مصر، 1997.

6- خلفي عبد الرحمان، القانون الجنائي العام(دراسة مقارنة)، دار بلقيس للنشر، الجزائر، 2016.

7- خالد حسن أحمد لطفي، الدليل الرقمي و دوره في إثبات الجريمة المعلوماتية، ط 1، دار الفكر الجامعي، الإسكندرية، مصر، 2020.

8- سلطان عبد القادر الشاوي، المبادئ العامة في قانون العقوبات، المكتبة القانونية، بغداد، العراق، 1991.

9- سمير عالية، أصول قانون العقوبات القسم العام (معالمه، نطاق تطبيقه، الجريمة، المسؤولية، الجزاء)، المؤسسة الجامعية للدراسات و النشر و التوزيع، بيروت، لبنان، 1996.

10- علي راشد، القانون الجنائي، ط 2، دار النهضة العربية، 1974.

11- محمد زكي أبو عامر، قانون العقوبات اللبناني، القسم العام، دار الجامعة، بيروت، لبنان، 1984.

12- علي حسين الخلف، المبادئ العامة في قانون العقوبات، المكتبة القانونية، بغداد، العراق، 1991.

13- عبد الله سليمان، شرح قانون العقوبات الجزائري (الجريمة)، القسم العام، ديوان المطبوعات الجامعية، الجزائر، 2005.

14- علي نعمة جواد الزرفي ، الجريمة المعلوماتية الماسة بالحياة الخاصة دراسة مقارنة، المكتب الجامعي الحديث، الإسكندرية، مصر ،2019.

15- علي عبد القادر القهوجي، شرح قانون العقوبات، القسم العام، منشورات الحلبي الحقوقية، بيروت، لبنان، 2008.

16- محمد الأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، دار حام للنشر و التوزيع، الأردن، 2015.

17- فارس العمارات، إبراهيم محمد الحمامصة، الأمن السيبراني (المفهوم وتحديات العصر)، دار الخليج، للنشر و التوزيع، الأردن، 2022.

18- فخري عبد الرزاق الحديثي، شرح قانون العقوبات، (القسم الخاص)، الجرائم الواقعة على الأشخاص، ط 2، دار الثقافة للنشر و التوزيع، الأردن، 2009.

19- محمود نجيب حسني، شرح قانون العقوبات، القسم العام، المكتبة القانونية، القاهرة، مصر، 1990.

20- محمد حميد المزمومي، الوسيط في شرح نظام الإجراءات الجزائية السعودي، ط 2، مركز النشر العلمي، بجامعة الملك عبد العزيز، جدة، السعودية، 2019.

21- محمود أحمد القرعان: الجرائم الإلكترونية، دار وائل للنشر و التوزيع، الأردن، 2017.

22- يوسف مناصرة: جرائم المساس بأنظمة المعالجة الآلية للمعطيات، دار الخلدونية، الجزائر، 2018.

23- السعيد مصطفى السعيد، الأحكام العامة في قانون العقوبات، ط 1، مؤسسة المعارف للطباعة و النشر، مصر، 1962.

24- يوسف بوغرارة، الإستراتيجية الجزائرية للأمن و الدفاع في الفضاء السيبراني، مجلة الدراسات الإفريقية و حوض النيل، ط 3، المركز الديمقراطي العربي، جامعة مستغانم، الجزائر، 2018.

ثانيا: المذكرات الجامعية:

1- أسامة مهمل، الإجرام السيبراني، رسالة ماجستير، كلية الحقوق و العلوم السياسية، جامعة محمد بوضياف، المسيلة، 2018.

2- حنين جميل أبو حسين، "الإطار القانوني لخدمات الأمن السيبراني"(دراسة مقارنة) رسالة مقدمة لإستكمال متطلبات الحصول على درجة الماجستير، تخصص قانون خاص، كلية الحقوق، جامعة الشرق الأوسط، الأردن، 2021.

3- طباش عز الدين، النظام القانوني للخطأ غير العمدي في جرائم العنف، رسالة لنيل درجة الدكتوراه في العلوم، كلية الحقوق و العلوم السياسية، جامعة مولود معمري، تيزي وزو، 2014.

4- عقبة عباس، تحسين أداء نظم كشف الإختراق في الشبكات المعرفة برمجيا بإستخدام تعلم الآلة، أطروحة ماجستير، المعهد العالي للعلوم التطبيقية و التكنولوجيا، الجامعة العربية السورية، 2019.

5- نبيلة هروال، جرائم الإنترنت دراسة مقارنة، رسالة لنيل الدكتوراه، كلية الحقوق و العلوم السياسية، جامعة بوبكر بلقايد، تلمسان، 2014.

6- نور أمير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، رسالة ماجستير، الجامعة الإفتراضية السورية، 2021.

ثالثا: المطبوعات الجامعية:

1- إيمان محمد الشورة، الأمن السيبراني في البنوك الإسلامية الأردنية، مذكرة بكالوريوس، كلية الشريعة، الجامعة الأردنية، 2018.

2- عنترة بن مرزوق و محي الدين حرشاوي، الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية، قسم الحقوق و العلوم السياسية، جامعة ورقلة، 2017.

3- فريد روابح، محاضرات في القانون الجنائي العام، موجهة لسنة الثانية لسانس، قسم الحقوق، كلية الحقوق و العلوم السياسية، ، جامعة محمد لمين دباغين، سطيف، 2019.

4- محمد إسماعيل المعموري، محاضرات في قسم القانون – الجرائم الإيجابية و السلبية، كلية القانون، جامعة بابل، العراق، 2010.

رابعا: المقالات

1- طلال ياسين العيسى، و عدي محمد عناب: المسئولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء للبحوث و الدراسات الإنسانية، المجلد 19 – العدد 1، الأردن، 2019، ص 86.

2- منى عبد الله السمحان، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية، مجلة كلية التربية، جامعة المنصورة، المملكة العربية السعودية، 2020، ص ص 11-12.

3- بارة سميرة، الأمن السيبراني في الجزائر، المجلة الجزائرية للأمن الإنساني، العدد 4، جامعة قاصدي مرباح، ورقلة، 2017. ص 256.

4- محمود علي عبد الرحمن، أسامة فاروق مخيمر: الفضاء الإلكتروني و أثره على مفاهيم القوة و الأمن و الصراع في العلاقات الدولية، مجلة كلية السياسة و الإقتصاد، جامعة محمد البشير الإبراهيمي، برج بوعريريج، المجلد 16، العدد 15، الجزائر، 2022، ص 438.

7- نسيب نجيب: الحرب السيبرانية من منظور القانون الدولي الإنساني، المجلة النقدية للقانون و العلوم السياسية كلية الحقوق و العلوم السياسية، جامعة تيزي وزو، المجلد 19، العدد 4، الجزائر، 2021، ص 222.

رابعا: النصوص القانونية:

1- القانون رقم 09-04، المؤرخّ في 14 شعبان 1431 الموافق لـ 5 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالتكنلوجيات الإعلام و الإتصال و مكافحتها، الصادر عن الجريدة الرسمية للجمهورية الجزائرية، العدد 47، الصادر بتاريخ 16 أوت 2009.

2- القانون رقم 18-04، المؤرخ في 10 مايو 2018، الذي يحدد القواعد العامة المتعلقة بالبريد و الإتصالات الإلكترونية، ج. ر، عدد 27 ، الصادر بتاريخ 13 مايو 2018.

3- القانون رقم 18-07، المؤرخ في 10 يونيو2018، المتعلق بحماية الأشخاص الطبيعين في مجال معالجة المعطيات ذات طابع شخصي، ج .ر-ج.ج، عدد 34 ، الصادر بتاريخ 10 يونيو 2018.

4- الأمر رقم 66-156، مؤرخ في 8 يونيو 1966، يتضمن قانون العقوبات ،ج. ر - ج.ج، عدد 49، صادر بتاريخ 11 يونيو 1966، المعدل و المتمم بالقانون رقم 16-02، مؤرخ في 19 يونيو2016، ج. ر-ج.ج، عدد 37، صادر بتاريخ 22 يونيو2016.

5- مرسوم رئاسي رقم 20-183، المؤرخ في 13 يوليو2020، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها، ج .ر-ج.ج، عدد 40، الصادر بتاريخ 18 يوليو 2020.

6- الإتفاقية الأوروبية المتعلقة بالجريمة الإلكترونية، بودابست 2001/11/23، مجلس أوروبا، مجموعة المعاهدات الأوروبية، رقم 185، حرر في 23 نوفمبر 2001.

7- الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، المصادق عليها من طرف الجزائر بموجب مرسوم رئاسي رقم 14-252، الموافق لـ 8 سبتمبر 2014، جريدة رسمية، عدد 57، الصادر بتاريخ 28 سبتمبر 2014.

خامسا: المواقع الإلكترونية:

1- فيصل محمد عسيري، الأمن السيبراني و حماية أمن المعلومات، تاريخ الإضافة 02-Application pdf http://www.kutub.info/librairy/book.

2- الحروب السيبرانية، ويكيبديا، تاريخ الإطلاع، 2023/04/11 2- سا 51:31 http://ar.m.wikipedia.org/wiki/d8

3- مها دحام، متاح على الموقع ، تاريخ الاطلاع www.sotsr.com2023/04/09
للمزيد حول فيروسات الحاسب الآلي، https://mawdoo3.com
4- جريمة إتلاف و تدمير المعطيات و البيانات بواسطة الإنترنت، أبريل 5112، متاح على الرابط التالي :https://www.startimes.com

المراجع باللغة الأجنبية:

1- Johnson, D, R. and Post, D. G. (May 1996). Law and borders: the rise of law in cyberspace. Stanford Law Review (48), 1367–1402.

2- Schelling, T. (1994). The threat that leaves something to chance. in : Freedman, L. War. Oxford : Oxford University Press,

3- Ido Kilovaty, Cyber Conflict and The Thresholds Of War, (June 22, 2021). Forthcoming, Is the International Legal Order Unraveling? (David. Available 9Sloss, ed.) Oxford University Press (2022).

4- Jeffrey T. G. Kelsey, Note, Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare.

5- Newly Nasty: Defences Against Cyberwarfare Are Still Rudimentary. That's Scary, ECONOMIST (May 24, 2007), available at: http://www.economist.com/node/9228757?story_id=9228757

6- Officials anonymously leaked qualified reports of U.S. suspicions that the attack emerged in North Korea. U.S. Eyes N. Korea for "Massive" Cyber Attacks, MSNBC.COM (July 9, 2009, 3:31 AM) Available at: http://www.msnbc.msn.com/id/31789294/ns/technology_and_sciencesecurity

7- Ellen Nakashima, Russian Hackers Suspected in Attack That Blacked Out Parts of Ukraine, WASH. POST, Jan. 5, 2016. Available : https://www.washingtonpost.com/world/nationalsecurity/russian-hackerssuspected-in-attack-that-blacked-outparts-ofukraine/2016/01/05/4056a4dc-b3de-11e5-a842-0feb51d1d124_story.html

8- Robert Knake, A Cyberattack on the U.S. Power Grid, COUNCIL ON FOR. REL. (Apr. 3, 2017), available at: https://www.cfr.org/report/cyberattack-us-power-grid

الفهـــرس

الفهـــرس

الملخص

عنوان المذكرة

الأمن السيبراني:

إن الأمن السيبراني قضية ناشئة في حقل العلاقات الدولية من خلال حداثة هذا المجال فهناك تاريخ طويل من التخمينات حول دور التكنولوجيا الرقمية في الدراسات الأمنية، و قد كان هناك تاريخ واسع من الإختبارات النظرية و الأخلاقية بشأن المخاوف المتعلقة بالأمن السيبراني.

تهدف هذه الدراسة إلى التعرف على الأمن السيبراني كونه أصبح مطلبا ضروريا لكل الدول دون إستثناء، لأنه يتعلق بالحماية من المخاطر المحتملة عن طريق مصادر خارجية من خلال الإنترنت، فهو يتعلق بحماية الحواسب المكتبية أو المحمولة من أي نوع من الهجمات و الإختراقات و التهديدات التي تحدث عن طريق الحواسب الأخرى و شبكة الإنترنت بشكل عام، و منه برزت لنا ملامح مشكلة الدراسة الحالية ممثلة في السؤال العام الذي مفاده:

ماذا يقصد بالأمن السيبراني و مدى حاجة العالم له؟

إنبثقت منه جملة من التساؤلات الفرعية:

- ما هي المعايير التي يقوم عليها الأمن السيبراني؟
- ما هي الأهداف التي يسعى الأمن السيبراني إلى تحقيقها؟
- ما هي التحديات و المشاكل التي تعيق الأمن السيبراني؟

وصولا للإجابة عن هذه الإشكالية و عن هذه التساؤلات المتفرعة عنها فإنه إعتمادا على المنهج التحليلي بإعتباره يعمل على الجمع بين القانون و بين فهم الواقع، و ذلك من خلال شرح و تحليل نصوص القانون هذا من جهة و نظرا لمستلزمات موضوع الدراسة فقد إعتمدنا من جهة أخرى على المنهج الوصفي على إعتباره يعد أسلوب من أساليب المنهج التحليلي من

خلال وصف الحالة المراد دراستها و تفسريها بموضوعية تنسجم و معطيات الدراسة و رغبة منا في الوصول إلى إنجاز عمل شامل و متكامل لهذا الموضوع.

أهمية الدراسة:

- الأمن السيبراني من أهم الموضوعات التي تستدعي الغوص في عناصرها و يستحق البحث و بالدراسة في إجراءاتها و ذلك كونها تندرج ضمن الدراسات الأمنية و الإستراتيجية و التعرف على الأمن السيبراني و أشكاله و تهديدات التي تخل بالأمن القومي للدول، و كذلك يعتبر الأمن السيبراني من المواضيع التي تعين بأهمية كبرية لدى الدول، معرفة عناصر الأمن السيبراني و المعايير و المشاكل التي تواجه الأمن السيبراني.

أهداف الدراسة :

هدف من خلال الدراسة الحالية محاولة التعرف على التعرف على الأمن السيبراني من الناحية النظرية، و من خلال ضبط ماهية الأمن السيبراني، و حتديد عناصره، و كشف عن معاييره، و المشاكل التي تواجه المساهمة في خلق و تطوير الوعي الجماعي بشأن الظاهرة و معاجلة الموضوع بأسلوب علمي و ذلك بالإستعانة بمناهج البحث العلمي، و مختلف النظريات التي اهتمت بالموضوع.

أسباب اختيار الموضوع:

إن إختيار موضوع الأمن السيبراني، جاء مدفوعا بجملة من الأسباب منها ما هو موضوعي و منها ما هو ذاتي، و التي يمكن حصرها في الآتي:

أ- الأسباب الموضوعية :

- كون موضوع الدراسة يحوز على إهتمام بالغ الإهتمام لدى صناع القرار.
- الإهتمام بمعرفة و إستكشاف الأمن السيبراني كونه موضوع حديث.

ب- الأسباب الذاتية:

إن الميول الشخصي لمختلف القضايا التي تمس الأمن دفعنا لاختيار هذا الموضوع ضمن قائمة المواضيع المقترحة من قبل الأستاذ المشرف و هذا بهدف الإطالع المعمق عليه خاصة أنه موضوع حديث يعكس الوجه الآخر لتكنولوجيا و أخطارها إذا ما استعملت بطريقة غير مشروعة، و كذا من أجل إثراء الرصيد العلمي و المعرفي باللغة العربية في هذا الموضوع.

ينقسم بحثنا إلى فصلين و هي كالتالي:

تناولنا في الفصل الأول الإطار المفاهيمي للأمن السيبراني من خلال تقسيم هذا الفصل إلى مبحثين حيث خصصنا المبحث الأول ماهية الأمن السيبراني و الذي تطرقنا فيه إلى مفهوم الأمن السيبراني الذي يعرف بأنه أمن الشبكات و المنظمة المعلوماتية، و البيانات و المعلومات و الأجهزة المتصلة بالإنترنت، فهو المجال الذي يتعلق، بأمن بإجراءات و مقاييس، و معايير الحماية المفروض إتخاذها، أو الإلتزام بها، و يرتبط هذا الأمن، ارتباطا وثيقا المعلومات،

فالوصول إلى هذه الأخيرة، أو بثها أو الإطلاع عليها و المتاجرة بها، أو تشويهها و إستغالالها، هو ما يقف غالب الأحيان، وراء عمليات الإعتداء على الشبكات و على الإنترنت بشكل أكثر.

يمكن القول عن الأمن السيبراني هو مجموعة الآليات و الإجراءات و الوسائل و الأطر التي تهدف إلى حماية البرمجيات و أجهزة الكمبيوتر" الفضاء السيبراني بصفة عامة" من مختلف الإعتداءات و الإختراقات و التهديدات السيبرانية التي قد تهدد الأمن القومي للدول.

إذا قمنا بذكر الأمن السيبراني فإن الجريمة السيبرانية ترتبط به و التي تعرف بأنها كل عمل أو إمتناع عن عمل يأتيه الإنسان إضرار بمكونات الحاسب المادية و المعنوية و شبكات الإتصال الخاصة به، بإعتبارها من المصالح و القيم المتطورة التي يحميها القانون و إن طبيعة الجرائم السيبرانية و تميزها عن الجرائم التقليدية يرجع إلى الوسط الذي ترتكب فيه الجريمة و هي الآداة أو الوسيلة التي إستخدمها الجاني في إرتكاب فعله غير المشروع، و تنقسم إلى:

- جرائم تمس خصوصية و سلامة و توافر بيانات و نظم الكمبيوتر.
- جرائم متصلة بالكومبيوتر كالتزوير و الإحتيال عبر الكمبيوتر.
- جرائم إساءة إستخدام وسائل تقنية المعلومات.

لا بد من الإشارة إلى آليات و قوانين الحد من الجرائم السيبرانية خلال وضع قواعد إتفاقية تعير عن تصور دولي موحد من شأنه تدارك النقائص و الثغرات التي تعيير منظومة القوانين الداخلية للدول و ذلك بهدف التقليل من حدة آثار هذه الجريمة، تضافرت الجهود من أجل وضع إطار قانوني إتفاقي يسمح بمتابعة مرتكبي جرائم المعلوماتية و معاقبتهم.

في حين خصصنا المبحث الثاني لأركان الجريمة السيبرانية و القاعدة العامة أن الجريمة تقوم على ركنين أساسيين، فالأول هو الركن المادي الذي يقر أنه "الجريمة دون سلوك مادي "فالعقاب لدينا في القانون الجنائي على النوايا، و لا يتدخل إلاّ إذا تجسدت هذه الأفكار في

العامل الخارجي في شكل مادي ملموس، يلُحق الضرر بالفرد أو يتخد المجتمع " اما الثاني هو الركن المعنوي يتمثل في القصد الجنائي و هو اتجاه إرادة الجاني إلى تحقيق النتيجة الإجرامية مع علمه بأن ما هو مقدم عليه يوقعه في الإثم الجنائي، و لالاتثير مسألة الوقوف على الركن المادي أي صعوباتُ بالنظر إلى خصائصه المادية المدركة بالحواس، غير أن ما يثير الكثير من المشاكل العملية هو كيفية الوقوف على الركن المعنوي، لاسيما أن مسألة الوقوف على توافر الركنين ترتبط بارتباط وجود أو عدم وجود الجريمة و العلاقة السببية تعد من أعقد المسائل و أدقها في التشريع الجنائي فالرابطة السببية في تحديد المسؤولية الجنائية للفاعل هلا أهمية بالغة تظهر على وجه الخصوص في الجرائم السيبرانية بإعتبارها أكبر الجرائم إثارة لمشاكل السببية، إن جرائم الحاسبات بإعتبارها من الجرائم ذات النتيجة التي تقوم مسؤولية الفاعل عنها لمجرد إسناد الفعل المادي للجاني و إنما يتوجب فوق ذلك إسناد النتيجة إلى الفعل للمساءلة عن الجريمة.

أما الفصل الثاني فتناولنا فيه لمجال السيبراني إذ جعلنا من المبحث الأول خاص بأبعاد الأمن السيبراني " البعد العسكري، الإقتصادي، الإجتماعي، السياسي، القانوني " أما مخاطر الأمن السيبراني فتمثلت في الدخول على الأنظمة و ما تحتويه من بيانات و معلومات دون إذن و التجسس على الإتصالات و الحد من سلامة المعلومات، نتيجة التلاعب، و التعديل عليها، و إتلافها، و هذا ما يعد إعتداء بحد ذاته على الحريات و الحقوق الشخصية و الجرائم العادية التي يتم إستخدام الإنترنت في تنفيذها كالسرقة و الغش، و الترويج لنشاطات مخالفة للقانون، و بعد ذكر المخاطر فكان لا بد من التطرق إلى كيفية الردع و الإستراتيجيات السيبرانية في التصدي إلى هذه الإعتداءات و التهديدات و التي تتمثل في البرمجيات، هجمات منصات الخوادم، و كذلك تطرقنا إلى استراتيجيات الجزائرية في الدفاع السيبراني على المستوى الوطني و من الناحية القانونية و العملية و الإدارية و التقنية و كذلك على المستوى الخارجي من خلال

تفعيل المبادئ العامة المتعارف عليها عالميا في مجال مكافحة الجريمة "تبادل المعلومات، تبادل الخبرات و المساعدة الفنية".

أما المبحث الثاني تطرقنا إلى القوة السيبرانية و الإختراق حيث أصبح الفضاء السيبراني أحد العناصر الأساسية التي تؤثر في النظام الدولي بما يتيحه من أدوات تكنولوجية مهمة لعمليات الحشد و التعبئة في العالم، فضلا عن التأثير في القيم السياسية، فسهولة الإستخدام و رخص التكلفة زاد من قدرته على التأثير في مختلف مجالات الحياة سواء السياسية أو اللإقتصادية أو الإجتماعية و حتى الإيديولوجية و بات جليا من يمتلك آليات توظيف البيئة السيبرانية يصبح أكثر قدرة على تحقيق أهدافه و التأثير في سلوك الفاعلين المستخدمين لهذه البيئة ، و من الأمور المتعارف عنها في العلاقات الدولية أن مصادر قوة الدولة تتغير، فإلى جانب القوة الصلبة المتمثلة في القدرات العسكرية و الإقتصادية، تزايد الإهتمام بالأبعاد الغير المادية للقوة، حيث كانت هناك هيئات فاعلة في المجال السيبراني مثل " الدولة، الشركات متعددة الجنسيات، المنظمات الغير حكومية، حركات التحرر الوطني، المجموعات الإفتراضية، الفراد " و كان البد من التطرق كذلك إلى كيفية الإبلاغ عن الجريمة و التحقيق و التحري و ذلك بإدراج واجبات المحددة لرجال الضبط الجنائي، تلقي البلاغات و الشكاوي و التحري عنها، للحصول على المعلومات عن طريق إعتراض أو رصد البيانات المنقولة من الموقع، معاينة مسرح الجريمة، أما كيفية البحث و التحقيق و التحري في الجريمة السيبرانية من خلال " المعاينة، التفتيش، ضبط الرسائل و مراقبة المحادثات، الشهادة، الإستجواب" أما المبحث الثاني تطرقنا إلى الإختراق و لأنه تعددت الإعتداءات السيبرانية و تنوعت الأساليب ، المنتهجة في كيفية شن الهجمات، و مع تطور التقنيات التكنولوجية يوما بعد يوم، و التي نتج عنها بالضرورة، إكتشاف فيروسات ضارة و أسلحة إلكترونية أكثر فتكا، ساهمت بشكل ملحوظ في تسهيل عملية الإختراق و تعرف هذه الأخيرة بأنه أي حادث ينتج عنه وصول غير مصرح به

إلى بيانات الكمبيوتر أو التطبيقات أو الشبكات أو الأجهزة. كماً عندما يتمكن المتسلل من تجاوز آليات الأمان ينتج عنه الوصول إلى المعلومات دون إذن. و يحدث عادة ويوجد العديد من الأنواع منها " الدخول إلى النظام و البقاء غير المشروع فيه، إعاقة أو تخريب تشغيل نظم معاجلة البيانات، التلاعب في بيانات نظم معاجلة البيانات "و في أخر المطاف قمنا بوضع خاتمة جمعت كل ما تحصلنا عليه من نتائج و ملاحظات و توصيات في دراستنا لهذا الموضوع و يمكن القول أنه نظرا لأهمية دراسة موضوع الأمن السيبراني من خلال هذا المشوار العلمي إلى كل الجوانب التي حولت الموقع الجغرافية إلى فضاء مفتوح لتلاقي و تقاطع كل أنواع التهديدات التي بدون شك سيكون لها تداعيات على الأمن الوطني و اذا أطفنا إلى ذلك المخاطر السيبرانية، فإن أي دولة مهما كانت قدراتها ستصبح إحدى ضحايا هذه التحديات و تبقى الحماية في حاجة إلى إستثمارات فكرية و مادية هائلة لتصميم و تطوير إستراتيجية أمنية متعددة التخصصات (الجوانب التشريعية، التنظيمية، البشرية، المالية، التقنية، و المعلوماتية)، حتى تستطيع الدولة تأمين الثورة الرقمية للأفراد و المؤسسات و بالتالي التصدي لخطر تشتكي منه اليوم الدول الكبرى.