

جامعة عمار ثليجي بالأغواط
كلية الحقوق و العلوم السياسية
قسم الحقوق



مذكرة مقدمة ضمن متطلبات نيل شهادة الماستر في الحقوق بعنوان:

الجرائم السيبرانية في ظل الأزمات
الإقليمية

تخصص قانون جنائي

تحت اشراف الأستاذ :

* د رزق الله العربي

من إعداد الطالب :

• غزال زوهير

لجنة المناقشة :

الأستاذ بوقرين عبدالحليم رئيسا

الأستاذ رزق الله العربي مشرفا

الأستاذ رابحي لخضر عضوا مناقشا

السنة الجامعية: 2021/2022





والصلاة والسلام على أشرف خلق الله سيدنا محمد النبي الكريم وعلى
آله وصحبه أجمعين :

أهدي هذا النجاح الى من غرس في قلبي ثمرة النجاح إلى روح أبي
الزكية الطاهرة رحمة الله عليه

-الى نبع الحنان وجنة تحت الأقدام امي الغالية حفظها الله

- إلى زوجتي العزيزة تركية

قرة عيني وسندي ونور دربي ، شجعتني على مواصلة الدراسة ووقفت
إلى جانبي في السراء والضراء فباركها لي وأحفظها ياالله

- إلى المؤسسات الغاليات

- ابتايا يارا أسيل و أميرة أفنان .

- فبارك يا الله فيما رزقنا وأحفظهما يا الله وأرعاهما

- إلى أخي سليمان وأخواتي الكريمات وأزواجهن وبناتهم وأبنائهم

- إلى والدي زوجتي الحاج لعلی رحمة الله عليه والوالدة حفظها الله

- وإلى عائلتها الصغيرة بوداود و الإخوة أحمد ومسعود و الأخوات و

أزواجهن وبناتهم وأبنائهم

زهير

شكر و عرفان

نحمد الله عز وجل الذي وفقنا في اتمام هذا العمل المتواضع .

أتقدم بجزيل الشكر والتقدير إلى الأستاذ الدكتور المشرف رزق الله العربي ، على كل ما قدمه لي من توجيهات ساهمت في إثراء موضوع الدراسة.

كما اتقدم بجزيل الشكر إلى أعضاء اللجنة المناقشة

كما أتقدم بالشكر والتقدير إلى صهري المؤطر الدكتور بوداود أحمد الذي رافقني وساندني بنصائحه وأمد لي يد العون في إنجاز هذا البحث

كما أتقدم إلى زوجتي تركية ركيزة دربي بالشكر والتقدير والإعتراز على الدعم والتشجيع والصبر في إنجاز هذا العمل .

الفصل التمهيدي

ملخص الدراسة

الجريمة السيبرانية هي إحدى الجرائم المعاصرة التي أصبحت تمثل خطرا على الفرد والمجتمع وعلى أمن الدولة ، إذ أنها تتقدم بوتيرة سريعة باستخدام المجرمون أحدث التقنيات في تنفيذ هجماتهم السيبرانية ، لذا كان علينا مواكبة الفضاء السيبراني و التعرف على طرق التصدي لهذه الجرائم المستحدثة بسن القوانين والأنظمة التي تختص بمكافحة الجرائم السيبرانية وفرض العقوبات على المجرمين ، ولهذا أحببت أن أقدم هذه الدراسة لإعطاء نظرة حول الجرائم السيبرانية في التعدي على انتهاك المعلومات سواء أكانت على الفرد أو على الشركات أو الكيانات المنظمة ، حتى أيضا على الحكومات والدول ، ولوجود هذه الإشكالية تناولنا في هذا البحث مفهوم الجريمة السيبرانية والإطار القانوني للجريمة السيبرانية ودارسة الجوانب الموضوعية من أركان وعقوبات ، وكذلك الجوانب الإجرائية من الاستدلال والتحقيق والمحاكمة في الجريمة السيبرانية ، ووضع النتائج والتوصيات لما توصل إليه الباحث.

Summary:

Cybercrime is one of the contemporary crimes that have become a threat to the individual, society and the security of the state, as it advances at a rapid pace using criminals with the latest technology in carrying out their cyber attacks, so we had to keep up with cyberspace and learn about ways to address these new crimes by enacting laws and regulations to combat Cybercrime and penalties for criminals. That is why I liked to present this research paper to give a look at cybercrime in infringement of information violations, whether it is on the individual or on companies or organized entities, even also on governments and states, and for the existence of this problem we addressed in this research the concept of cyber crime and the legal framework of cyber crime and a study of aspects Objectivity of the pillars and penalties, as well as procedural aspects of reasoning, investigation and trial in cyber crime, and the development of the results and recommendations of what the researcher reached.

المقدمة

من المسلم به، والحقيقة التي لا يمكن إنكارها أننا أصبحنا اليوم نعيش عصر تكنولوجيا المعلومات والاتصالات التي باتت هي الأساس الذي يعتمد عليه في شتى المجالات، ولدى جميع المؤسسات، سواء أكانت مؤسسات عامة تملكها حكومات الدول أم مؤسسات خاصة يملكها الأفراد، فتقنية المعلومات وشبكات الاتصالات هي الأداة الأساسية المستخدمة في إدارة شؤون الدول وتقديم الخدمات وتسهيلها عن طريقها.

لقد ساهم التقدم التكنولوجي والإنترنت في التطور المذهل لوسائل الإعلام و الاتصال في العالم على جميع الأصعدة والمستويات، الأمر الذي أدى إلى إفراز نوع جديد من الجرائم وهي ما اصطلح عليها بالجرائم السيبرانية، وقد بدت النصوص الجزائية التقليدية قاصرة عن ملاحقة هذا النوع من الجرائم، ذلك أن التشريع وُلِدَ الحاجة، بدأ المجتمع الدولي في تنظيم تشريعات لمواجهة هذا النوع الجديد من الجرائم الذي ظهر مصاحباً لاستخدام الحاسب الآلي، و إن ثمة تباين كبير بشأن المصطلحات المستخدمة للدلالة على هذه الظاهرة الإجرامية الناشئة في العالم الافتراضي.

لم تتطرق التشريعات العربية إلى جرائم الحاسب الآلي إلا فيما ندر، ولعل السبب في ذلك أن ثورة الحاسب الآلي في البلدان العربية حديثة النشأة، لأن الاعتماد على تطبيقات الحاسب الآلي فيها بدأ في نهاية العقد الأخير من القرن الماضي، على عكس البلدان الغربية التي اعتمدت الحاسب الآلي منذ عقدين من الزمن أو أكثر، الجرائم على غرار باقي الدول تشهد حركة متسارعة في مجال الإجرام السيبراني الإلكتروني، خاصة أمام الاستعمال الواسع لشبكة الإنترنت وضعف المراقبة والمتابعة الدورية لاستخدامها، مما يزيد من فرص قيام هذه الجرائم.

فالهجوم السيبراني هو هجوم عبر الإنترنت يقوم على التسلل إلى مواقع إلكترونية غير مرخص بالدخول إليها، بهدف تعطيل أو إتلاف البيانات المتوفرة فيها أو الاستحواذ عليها، وهي عبارة عن سلسلة هجمات إلكترونية تقوم بها دولة ضد أخرى، أو أشخاص ضد أشخاص آخرين أو هيئات و مؤسسات حكومية و غير حكومية في أي مكان

من العالم، فالخصائص المميزة لشبكة الإنترنت أنها لا تعرف الحدود الدولية، فالمستخدم لشبكة الإنترنت يمكنه التنقل بين أرجاء العالم وهو في مكانه أمام شاشة الحاسب الآلي أو التليفون المحمول، ويترتب على الطبيعة الدولية لشبكة الإنترنت أن الجرائم التي ترتكب من خلالها تكون لها صفة الجرائم الدولية، أو الجرائم العابرة للحدود، فمن الممكن أن يشترك أكثر من شخص في أكثر من دولة في ارتكاب جريمة واحدة يقع ضحيتها عدة أفراد مقيمون في بلدان متعددة، ومما يزيد الأمر صعوبة هو اختلاف البيئات والعادات والتقاليد والثقافات والديانات بين الدول المرتبطة بالإنترنت بما يترتب عليه من اختلاف التشريعات في مسائل أساسية بين دول المشرق والمغرب والعالم الإسلامي، فقد يثبت على شبكة الإنترنت معلومات أو صور قد تكون مشروعة في بلد نشأتها ولكنها قد تكونت غير مشروعة في بلد آخر، ويضاف إلى ذلك أن اختلاف التشريعات في تأسيس اختصاصها الجنائي بسبب تعدد الأسس التي يقوم عليها هذا الاختصاص، قد يؤدي إلى تنازع الاختصاص بين الدول بالنسبة إلى جرائم الإنترنت العابرة للحدود، فقد يحدث أن ترتكب جريمة في إقليم دولة معينة ويكون مرتكب الجريمة شخص أجنبي، فتخضع هذه الجريمة للاختصاص الجنائي للدولة الأولى استناداً لمبدأ الإقليمية، وتخضع كذلك للاختصاص الدولة الثانية على أساس مبدأ الاختصاص الشخصي في جانبه الإيجابي.

وحرصاً من المشرع الجزائري على التصدي للجريمة السيبرانية، قام باستحداث آليات إجرائية تتناسب وطبيعة هذه الجريمة، نظراً لعجز الإجراءات التقليدية في مواجهة هذا النوع من الجرائم التي تتميز بالتطور المستمر .

إشكالية الدراسة:

كلما زاد تطور ثورة المعلومات والتكنولوجيا زاد معها التطور في هذه الجرائم ، و مثلما توجد عصابات و ميليشيات تلعب دورا في الأزمات و الحروب التقليدية هناك أيضا عصابات و جيوش إلكترونية تنشط في ظل الأزمات ، ولذلك أصبحنا نرى صورا مستحدثة لتلك الجرائم السيبرانية ولوجود هذه الإشكالية قررت أن أدرس الموضوع من حيث الجوانب الموضوعية والإجرائية لأثر الجرائم السيبرانية على الأزمات الإقليمية ، فيكون الإشكال الذي ننطلق منه كالتالي:

ما مدى تأثير الجرائم السيبرانية في الأزمات الإقليمية ؟.

و يتفرع من هذا الإشكال جملة من الإشكالات:

1— ما هو تعريف الجريمة السيبرانية و ما هي خصائصها؟

2— هل هناك إطار قانوني موحد للجريمة السيبرانية ؟

3— على أي أساس يكون الاستدلال و المحاكمة على الجريمة السيبرانية؟.

أسباب اختيار الموضوع:

ترجع أسباب اختيار موضوع " الإجرام السيبراني " إلى الرغبة في التعرف على هذا النوع الجديد من الجرائم، التي تنتشر اليوم بصورة واسعة وتتفاقم داخل المجتمع الجزائري في ظل الظروف الإقليمية التي تعيشها ، و تكالب عدد من الأعداء عليها ، بغية زعزعة أمنها و استقرارها و تشتيت وحدة بنيتها ، ومن جهة أخرى المساهمة لمعرفة الآليات المرصودة لمكافحة مثل هذه الجرائم سواء الدولية منها أو الوطنية ، ثم إن هذا الموضوع في حد ذاته متجدد و متسارع في التطور تسارع التطور التكنولوجي.

أهداف الدراسة:

يهدف هذا البحث إلى محاولة التعريف بالجريمة السيبرانية وتحديد أنواعها، مع الإشارة إلى صورها و المخاطر المترتبة عنها في ظل الأزمات الإقليمية ، و كذا العرف على الآليات الدولية والوطنية المقررة لمكافحة الجرائم السيبرانية، ومدى كفاية القوانين الحالية لمواجهتها.

أسباب اختيار الموضوع:

لعل من الأسباب الموضوعية التي دفعتني للبحث في هذا الموضوع ، هو انتشاره بشكل رهيب في السنوات الأخيرة ، و بخاصة في ظل الظروف التي تعيشها بلادنا الجزائر و اشتداد هذا الشكل من الجرائم تجاه مجتمعنا من قبل أجهزة و دول تسعى لزعزعة أمنها و استقرارها ، كما أن الجريمة الإلكترونية تمس كل القطاعات، إذ أن الدولة تسعى إلى إنشاء إدارة إلكترونية، حكومة إلكترونية، وهذا ما يساعد على انتشار هذا النوع من الجرائم ومن الأسباب الشخصية التي دفعتني للكتابة في هذا الموضوع، هو أن مجرد اسمها يكتسي جانبا من الغموض خصوصا في إطار مكافحتها، فتجعل العقل يفكر في شكل مسرح الجريمة، وطريقة التفتيش وغيرها من الإجراءات، وهذا ما أعطاني دافع للبحث وحب التعرف عليها باعتبارها متعلقة بالعالم الافتراضي، الجريمة الإلكترونية موضوع حديث يمس الواقع المعاش، كما أن الجريمة الإلكترونية تمس كل القطاعات، إذ أن الدولة تسعى إلى إنشاء إدارة إلكترونية، حكومة إلكترونية، وهذا ما يساعد على انتشار هذا النوع من الجرائم، وللإجابة على الإشكالية المطروحة، اعتمدت في ذلك على بعض المناهج الملائمة وطبيعة الموضوع، منها المنهج الاستقرائي وذلك باستقراء وجمع المادة العلمية من مختلف المراجع، ثم المنهج التحليلي الوصفي إذ قمت بوصف الظاهرة وبيان المفاهيم القانونية الخاصة ، وتحليل المفاهيم وشرحها بالتفصيل، ثم المنهج المقارن من خلال مقارنة الجريمة الإلكترونية بالجريمة التقليدية، متبعا في ذلك خطة منهجية ثنائية الفصول، حيث خصصت الفصل الأول للتأصيل النظري لمفاهيم الجريمة السيبرانية و الأزمات الإقليمية ، تطرقت من خلاله لتعريف الجريمة السيبرانية، أسبابها و تمييز صورها ، ثم تعريف الأزمات الإقليمية ، أنواعها و مراحلها و النماذج الاتصالية و الإدارية في إدارة الأزمات ، أما الفصل الثاني فخصصته لتجليات الحرب السيبرانية بين الأنظمة ، و تطرقنا من خلاله لنموذج الكيان الصهيوني المحتل و اعتماده على الحرب السيبرانية ،

ثم صور الحرب الالكترونية للكيان الصهيوني على الأمة العربية و الجزائر، و انتهينا في هذا الفصل بالموقف الداخلي و الدولي و استراتيجيات المواجهة .

الدراسات السابقة:

إن البحث في موضوع الإجرام السيبراني يتميز بوفرة المراجع حول هذا الموضوع حيث تم التطرق إليه ومعالجته في العديد من الرسائل ومذكرات الماجستير فيما يصطلح عليه بالجرائم الإلكترونية أو الجرائم المعلوماتية.

ولقد تم الاعتماد على البعض منها في إعداد هذا البحث، وبالأخص في تحديد مختلف التعاريف الفقهية و الخصائص المميزة للجريمة السيبرانية و المجرم السيبراني، من بين هذه الدراسات نذكر

-كتاب بعنوان جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، لمؤلفه الدكتور علي جعفر ، حيث بين من خلاله الأحكام العامة لجريمة تقنية المعلومات ومختلف تقسيمات الجريمة السيبرانية بالنظر لآراء فقهاء القانون الجنائي.

-كتاب بعنوان الجرائم المعلوماتية للدكتور أحمد خليفة الملط، يتحدث فيه عن مختلف صور الجريمة السيبرانية، كجرائم الاعتداء على المال المعلوماتي، وجرائم الغش المعلوماتي، جريمة إتلاف المعلومات وغيرها .

_____ ورقة بحثية بعنوان الجرائم السيبرانية، للدكتورة روان بنت عطية الله الصحفي، تحدثت فيها عن الجرائم السيبرانية في التعدي على انتهاك المعلومات سواء أكانت على الفرد أو على الشركات أو الكيانات المنظمة ، و أيضا على الحكومات والدول.

— كتاب حرب الفضاء الالكتروني، للدكتور محمود محارب ، تحدث فيه عن اهتمام مراكز الأبحاث والنخب في الكيان المسمى " إسرائيل" بموضوع الحرب في الفضاء الالكتروني و صور ممارستها له من خلال أجهزتها الاستخباراتية.

الفصل الأول: التأسيس النظري لمفاهيم الجريمة
السيبرانية و الأزمات الإقليمية

المبحث الأول : ماهية الجريمة السيبرانية

المطلب الأول: تعريف الجريمة السيبرانية

أطلقت على الجريمة المرتكبة بواسطة الأنترنت عدة تسميات مختلفة تماشياً مع تطورها الزمني، ولقد عرفها الفقه الجنائي عدة تعاريف وفقاً لأسس مختلفة ، كما عرف المشرع الجزائري أيضاً هذا النوع من الجرائم.

الفرع الأول: تعريف الجريمة السيبرانية:

إن مصطلح الجرائم السيبرانية هو إحدى المصطلحات الحديثة والمستخدمه عن جرائم الإنترنت الذي تعددت مصطلحاته وذلك لنشأة وتطور ظاهرة الإجرام المرتبط والمتصل بتقنية المعلومات ، وفي الحقيقة لو تأملنا نجد بأن مصطلح الجرائم السيبرانية (cyber crime) هو مصطلح غير عربي ، لكنه هو المتداول والمستخدم حديثاً في وقتنا الحالي في هيئة الاتصالات وتقنية المعلومات وكذلك في المؤتمرات والندوات (كملتقى الجرائم السيبرانية والأدلة الرقمية) الذي نظمته جامعة الأمير نايف العربية للعلوم الأمنية في مدينة الرياض عام 2112 م ، وكذلك نجد كلمة سيبراني (cyber) قد ارتبط بالأمن الإلكتروني .

أولاً: التعريف اللغوي

أ— تعريف الجريمة: جاءت الجريمة في اللغة لمعنيين هما:

الأول : الذنب ، نقول جرم وأجرم ، واجترم بمعنى واحد .

الثاني : الجنابة ، كقولهم جرم إليهم وعليهم جريمة ، أجرم جني جنابة وجرم إذا عظم جرمه أي أذنب¹.

¹ — خالد حسن أحمد لطفي ، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية ، دار الفكر الجامعي ، الإسكندرية ، الطبعة الأولى ، 2020 م ، ص 13.

ب — تعريف السيبرانية في اللغة: كما تطرقنا سابقا بأن (cyber) هي كلمة انجليزية ، "ولقد عرّف قاموس

أكسفورد كلمة سيبراني ، أو Cyber، بأنها صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي².

ثانيا: التعريف الشرعي للجريمة:

تعرف الجريمة بأنها " إتيان فعل محرم معاقب على فعله ، أو ترك فعل محرم معاقب على تركه ، أو هي فعل أو ترك نصت الشريعة على تحريمه و العقاب عليه³.

ثالثا: التعريف القانوني للجريمة:

عرّفت الجريمة من الناحية القانونية بتعريفات متعددة منها:

هي إتيان فعل أو تركه عن إرادة جنائية إضراراً بمصلحة اجتماعية حماها المشرع بقواعد تجرمه وتعاقب عليه جزائياً⁴ .

من جهتي كباحث أرى أن هذا التعريف و إن كان لأمس الجوانب الموضوعية و الشكلية للجريمة إلا أنه ليس تعريفا شاملا ذلك أنه يحصر الجريمة المرتكبة في نطاقها المحلي.

الفرع الثاني: تعريف الجريمة السيبرانية:

² — وليد أحمد الروضان ، ما لفرق بين أمن المعلومات والأمن السيبراني ، صحيفة الجزيرة الإلكترونية ، مؤسسة الجزيرة للصحافة و الطباعة و النشر، 2018 ، العدد 16631 .

³ — سامي علي حامد عياد ، الجريمة المعلوماتية وإجرام الإنترنت ، دار الفكر الجامعي ، الإسكندرية ، بدون طبعة ، 2007 م ، ص 12.

⁴ — عبد العزيز بن غرم الله آل جار الله، جرائم الإنترنت وعقوباتها وفق نظام مكافحة الجرائم المعلوماتية السعودي دراسة مقارنة (ويليه آثار العولمة على مستخدمي الإنترنت) ، دار الكتاب الجامعي ، الرياض ، الطبعة الأولى ، 2017 م ، ص 79.

إن الجرائم السيبرانية تعد من الجرائم التي تباينت تسمياتها عبر المراحل الزمنية لتطورها ، فكانت بداية من مصطلح إساءة استخدام الكمبيوتر ، مروراً باصطلاح احتيال الكمبيوتر ، والجريمة المعلوماتية ، فاصطلاحات جرائم الكمبيوتر ، والجريمة المرتبطة بالكمبيوتر ، وجرائم التقنية العالية ، إلى جرائم الهاكرز ، فجرائم الإنترنت ، إلى آخر المصطلحات⁵.

ولهذا فإننا نجد في كل مرة مع ظهور مصطلح جديد لجرائم الإنترنت يظهر لنا تعريفاً جديداً ، فقهاء القانون لم يستقروا على تعريف واحد ، فنحن لا نستتكر ذلك أبداً لأنه من الطبيعي جداً أن يكون هذا الاختلاف وهذا التنوع في المفاهيم والآراء ، وذلك يرجع لحدثة الجرائم السيبرانية و لاختلافات الثقافات والقوانين بين الدول ، وأيضاً خشية في أن يحدوا المصطلح في نطاق ضيق أو محدد ، فمنهم من عرف الجرائم السيبرانية : بأنها "هي التي تتم بواسطة الكمبيوتر أو أحد وسائل التقنية الحديثة على كمبيوتر آخر أو أحد وسائل أو أحد وسائل التقنية الحديثة ، مع ضرورة توفر شبكة اتصال فيما بينهما ، والبعض الآخر عرفها : بأنها " نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود.

الفرع الثاني: التعريف القائم على خصائص محل الجريمة

يرتكز أصحاب هذا الاتجاه على وسيلة ارتكاب الجريمة، طالما أن وسيلة ارتكاب الجريمة هي الكمبيوتر أو إحدى وسائل التقنية الحديثة المرتبطة به، فتعتبر الجريمة من ضمن جرائم الإنترنت⁶، حيث يضيق أنصار هذا الاتجاه من نطاق هذه الجريمة، و يحدونها في الحالات التي تمس مكونات الحاسوب غير المادية، كالبرامج والبيانات والمعطيات المخزنة في ذاكرته⁷، ومن ذلك نجد تعريف مكتب تقييم التقنية في

⁵ — عبد العزيز بن غرم الله آل جار الله ، مرجع سابق ، ص 70.

⁶ — يوسف صغير، الجريمة المرتكبة عبر الإنترنت، مذكرة ماجستير، جامعة مولود معمري بتيزوزو، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2012-2013، ص 08.

⁷ — عبد العال الديربي ومحمد صادق إسماعيل، الجريمة الإلكترونية، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2012، ص 42.

الولايات المتحدة الأمريكية حيث يرى بأنها " الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا ."⁸

وعرفها البعض الآخر بصياغة أخرى وهي: تلك الجرائم الناتجة عن استخدام التكنولوجيا والتقنية الحديثة المتمثلة في الكمبيوتر والانترنت، بأعمال وأنشطة إجرامية تهدف إلى تحقيق عوائد ضخمة جراء أعمال غير شرعية، يعاد ضحها في الاقتصاد الدولي عبر شبكة الإنترنت باستخدام النقود الإلكترونية أو بطاقات السحب التي تحمل أرقاما سرية للشراء عبر الإنترنت، أو تداول الأسهم وممارسـة الأنشطة التجـارية عبر هـذه الشبكة⁹.

يرد في هذا الإطار الأستاذ فاندerson . R على واضعي هذا التعريف بقوله: " ليس لمجرد أن الحاسب قد استخدم في الجريمة، أن نعتبرها من جرائم الإنترنت " والحجة التي اعتمدها في نقده، مفادها أنه لا يمكن وضع تعريف لهذا النوع من الجرائم دون الرجوع إلى العامل الأساسي المكون لها، و أن الاعتماد فقط على الوسائل المستخدمة لتحقيقها، لا يكفي لاعتبار مجرد استخدام الحاسب الآلي في الجريمة أنها من جرائم الانترنت"¹⁰.

الفرع الثالث: التعريف القائم على أساس المعرفة والتحكم في التكنولوجيا

يستند أنصار هذا الاتجاه إلى معيار شخصي، إذ يجب أن يكون القائم بهذه الجرائم ملما وعارفا بتقنية المعلومات¹¹ ، ومن قبيل هذه التعاريف نجد التعريف الذي أتى به الأستاذ ديفيد تومبسون (Tompson David) للجريمة المرتكبة عبر الإنترنت بأنها " أي جريمة يكون متطلبا لاقتوافها أن تتوافر لدى فاعلها

⁸ — المرجع نفسه.

⁹ — عبد الله عبد الكريم عبد اهلل، جرائم المعلوماتية والإنترنت، منشورات الحلبي الحقوقية، بيروت، 2007، ص15.

¹⁰ — يوسف صغير، المرجع السابق، ص 10.

¹¹ - رحيمة نميلي، " خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة "، مداخلة مقدمة في أعمال المؤتمر الدولي الرابع عشر، طرابلس، الموسوم بعنوان: الجرائم الإلكترونية طرابلس، يومي 24 و 25 مارس 2017، ص 05.

معرفة بتقنية الحاسب¹² ، كما قدم الفقيه ستين سكيولبيرج (Stein Schiolberg) تعريفه لجرائم الحاسب بقوله: " أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه والتحقيق فيه وملاحقته قضائياً¹³ " ، ولقد أخذت وزارة العدل الأمريكية بهذا التعريف في التقرير الصادر عنها سنة 1989 و المتعلق بجرائم الإنترنت¹⁴ .

حسب منظور أصحاب هذا التعريف، لابد من توفر سمات شخصية لدى مرتكب هذه الجريمة، والمحصورة أساساً في الدراية والمعرفة التقنية.

عناك أيضاً اتجاهات أخرى تقدم تعاريف مختلفة للجريمة السيبرانية ، كالتعريف المرتكز حول موضوع الجريمة و يرى أصحاب هذا الاتجاه أن الجريمة السيبرانية ليست التي يكون الحاسب أداة ارتكابها، بل هي التي تقع عليه أو في نظامه ، ومن نماذج مساهمة هذه الفكرة تعريف الفقيه روزنبلات (Rosenblatt) و بعض الخبراء الآخرين، حيث يعرفون الجريمة السيبرانية بأنها " نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه "، و من نفس المنظور يعرفها البعض بأنها غش معلوماتي ينصرف إلى كل سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها¹⁵.

ومن هنا ينشأ التمييز بين التأثيم القانوني وبين التجريم الذي يمثل أقصى درجات التأثيم، فالجريمة اذا انما تمثل اخلاقاً بالتزام مهم في حياة الناس والمجتمع مما يجعلها مستأهلة للعقاب.

¹² — هشام محمد فريد رستم، " الجرائم المعلوماتية أصول التحقيق الجنائي الفني واقتراح إنشاء آلية حربية موحدة للتدريب التخصصي"، بحوث مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات المتحدة كلية الشريعة والقانون، الطبعة الثالثة (المجلد الثاني)، 2004، ص 407.

¹³ — عبد اللطيف معتوق، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة ماجستير، جامعة العقيد الحاج لخضر بباتنة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2011-2012، ص 07.

¹⁴ — سفيان سوير، جرائم المعلوماتية، مذكرة ماجستير، جامعة أبو بكر بلقايد بتلمسان، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2010-2011، ص 12.

¹⁵ — هشام محمد فريد رستم، المرجع السابق، ص 407.

من جملة ما سبق من تعاريف يمكن تعريف الجريمة الالكترونية بأنها عبارة عن اعتداء يطل معطيات الكمبيوتر المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات وفي مقدمتها الإنترنت، فهي جريمة تقنية تنشأ في الخفاء يقارفها مجرمون أذكاء يمتلكون أدوات المعرفة التقنية ، وتوجه للنيل من الحق في المعلومات.

ولعل أبلغ تعريف للجريمة الالكترونية هو مقولة الدكتور محمد صالح العادلي أستاذ القانون الجنائي بكلية الحقوق بمسقط وجامعة الأزهر بمصر ، محامي بالمحكمة العليا الدستورية بمصر حيث يقول عن الجريمة الالكترونية هي: "الابن غير الشرعي الذي جاء نتيجة للتزاوج بين ثورة تكنولوجيا المعلومات مع العولمة أو هي: المارد الذي خرج من القمقم ولا تستطيع العولمة أن تصرفه بعد أن احضرته الممارسة السيئة لثورة تكنولوجيا المعلومات"¹⁶.

المطلب الثاني: خصائص الجريمة السيبرانية

تتميز الجريمة الإلكترونية بخصائص تميزها عن الجريمة التقليدية تتمثل فيما يلي:

الفرع الأول: الجريمة الالكترونية عابرة للحدود

الجريمة الإلكترونية تتسم بالطابع الدولي ، لأن نظام الإنترنت جعل من معظم دول العالم في حالة اتصال دائم على الخط، فالجريمة الإلكترونية لا تعترف بالحدود بين الدول وبالتالي فهي شكل جديد من أشكال الجرائم العابرة للحدود بين الدول ، إذ يمكن من خلال النظام المعلوماتي ارتكاب العديد من الجرائم مثل جرائم التعدي على البيانات وتزوير وإتلاف المستندات الإلكترونية والاحتيايل المعلوماتي والقرصنة وسرقة الأموال.

¹⁶ — مفتاح بوبكر المطردي - الجريمة الالكترونية ، والتغلب على تحدياتها - ورقة عمل مقدمة إلي المؤتمر الثالث

لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان المنعقد في 23-25/9/2012.

إن قدرة تقنية الإنترنت على اختصار المسافات ، انعكست على طبيعة الأعمال الإجرامية ولم تعد الجريمة محلية بل أصبحت عالمية ، والجريمة الإلكترونية يرتكبها صاحبها عن بعد وهو يعني عدم التواجد المادي للجرم المعلوماتي في مكان الجريمة ، ومن ثم تتباعد المسافات بين الفعل الذي يتم من خلال جهاز الكمبيوتر وبين النتيجة أي المعطيات ، والجريمة الإلكترونية تنتقل من دولة لأخرى¹⁷ .

وتعتبر الجريمة الإلكترونية صورة صادقة عن العولمة ، فيمكن ارتكاب هذه الجريمة عن بعد ، وقد يتعد ارتكابها بين أكثر من دولة ، كما أن المواقيت تختلف بين الدول مما يثير إشكالية حول القانون الواجب التطبيق على هذه الجريمة.

إن أخطر الجرائم الإلكترونية العابرة للحدود هي تلك التي تستهدف الدول فتهدد أمنها القومي وسلامتها المالية، ويشمل ذلك التجسس الإلكتروني، (وأبرز أمثلته ما كشفته تسريبات الأميركي إدوارد سنودن بشأن مخططات الإدارة الأميركية للتجسس على اتصالات الأفراد والدول الأخرى)¹⁸، والسرقة المالية، وغيرها من الجرائم العابرة للحدود ، و من أبرز أنواع هذه الجرائم العابرة للحدود:

أولاً: الإرهاب الإلكتروني :

وتدخل فيه الاختراقات التي تكون جزءاً من جهد منظم لإرهابيين إلكترونيين، أو وكالات مخابرات أجنبية، أو أي جماعات تسعى لاستغلال ثغرات أمنية محتملة في الأنظمة الحيوية.

والإرهابي الإلكتروني (Cyber terrorist) هو الشخص الذي يدفع حكومة أو منظمة لتلبية أهدافه السياسية أو الاجتماعية، من خلال إطلاق هجوم إلكتروني على أجهزة حواسيب وشبكات أو على المعلومات المخزنة عليها.

ثانياً: الحرب الإلكترونية:

¹⁷ - خالد ممدوح إبراهيم ، أمن الجريمة الإلكترونية ، الدار الجامعية - الإسكندرية 2008 ص 44.

¹⁸ - الجرائم الإلكترونية، مقال منشور على موقع الجزيرة، على الرابط:

<https://www.aljazeera.net/encyclopedia/conceptsandterminology/2015/4/28>، تاريخ الاطلاع،

وهي حرب قائمة بالفعل بين العديد من الدول ولكن أدواتها أجهزة الحاسوب وشبكات الإنترنت، وأبرز أمثلتها الهجوم الذي تعرضت له البنية التحتية في إستونيا عام 2007 على يد من يُعتقد أنهم قراصنة روسيون.

ويرى محللون أن مثل هذا النوع من الهجمات قد يصبح هو القاعدة في الحروب المستقبلية بين الدول، حيث ستشكل جيوش إلكترونية هدفها اختراق الدول الأخرى وتدمير بنيتها التحتية، وربما يُكلف القادة العسكريين بقيادة مثل هذه الحروب مستقبلاً.

ومن أبرز أمثلتها حالياً مجموعات القراصنة التي تسمى "الجيش الإلكتروني السوري" و"الجيش الإيراني الإلكتروني" و"وحدة جيش التحرير الشعبي الصيني 61486"¹⁹.

الفرع الثاني: صعوبة إثبات الجريمة الإلكترونية:

تتصف هذه الجريمة بالخفاء أي عدم وجود آثار مادية يمكن متابعتها وهي صعوبة الاكتشاف ، كما أنه من الصعوبة تحديد مكان وقوعها وترجع صعوبة إثبات الجريمة المعلوماتية إلى عدة عوامل منها:

1 — أن الجريمة الإلكترونية لا تترك آثار مادية ، فهي جريمة تقع في بيئة إلكترونية يتم فيها نقل المعلومات وتداولها بالنبضات الإلكترونية ولا توجد مستندات ورقية.

فهذه الجريمة عبارة عن أرقام تتغير في السجلات فالجريمة الإلكترونية لا تترك شهوداً يمكن استجوابهم ولا أدلة يمكن فحصها.

2 — صعوبة الاحتفاظ بدليل الجريمة الإلكترونية ، إذ يستطيع المجرم في أقل من ثانية أن يمحو أو يحرف أو يغير المعلومات الموجودة في الكمبيوتر²⁰ .

¹⁹ — المرجع السابق

²⁰ — هشام محمد فريد رستم ، " القانون والكمبيوتر والانترنت " بحث مقدم بجامعة دولة الإمارات العربية المتحدة - 1 - 3

- ماي 2000.

3 — تحتاج الجريمة الإلكترونية لاكتشافها إلى خبرة فنية ، حيث تتطلب جريمة الكمبيوتر إلمام ومعلومات واسعة سواء لارتكابها أو التحقيق فيها.

كما أن رجال الضبطية القضائية يجدون صعوبة للتعامل مع الدليل الإلكتروني ، فقد يتسبب المحقق بدون قصد في إتلاف الدليل الإلكتروني أو تدميره كما في حالة محو البيانات الموجودة على الأسطوانة الصلبة أو قد لا يقوم بمصادرة جهاز الكمبيوتر المستخدم في ارتكاب الجريمة أو الطابعة أو الماسح الضوئي.

لذلك أصبح من الضروري في وقتنا إجراء دورات تدريبية لرجال الضبطية القضائية ورجال القضاء والخبراء والفنيين للتعاون فيما بينهم وصولاً إلى أحسن الطرق لمكافحة الجريمة الإلكترونية²¹.

4 — تعتمد الجريمة الإلكترونية على الخداع والذكاء في التعرف على مرتكبيها ، إن الذي يساعد على عدم التعرف على مرتكبي الجرائم الإلكترونية إحجام البنوك والشركات ومؤسسات الأعمال عن الإبلاغ عما يرتكب من جرائم تجنباً للإساءة إلى سمعتها وهز ثقة العملاء بها ، وإخفاء أسلوب ارتكاب الجريمة خوفاً من قيام الآخرين بتقليد هذا الأسلوب ، وهو ما يدفع المجني عليه إلى الإحجام عن إبلاغ السلطات المختصة بها.

كما أن الجريمة المعلوماتية تعتمد على الذكاء وهي جريمة فردية تعتمد على مهارات عالية وإلمام بتكنولوجيا النظم المعلوماتية²².

وتقع الجريمة المعلوماتية أثناء معالجة البيانات والمعطيات الخاصة بالكمبيوتر وإذا تخلف هذا الشرط تنتفي الجريمة.

وقد حاول مجلس الشيوخ في فرنسا وضع تعريف محدد لعملية المعالجة الآلية للبيانات أو المعطيات ولكنه عدل عنه باعتبار أن هذه الجريمة عملية فنية تخضع للتطور السريع وبالتالي أي تعريف لها سيكون

²¹ — تقرير الأونكتاد 10 نوفمبر 2005 ملتقى الأمم المتحدة حول التجارة والتنمية ص 2.

²² — أحمد خليفة الملط - الجرائم المعلوماتية ، دار الفكر الجامعي ، دون ذكر الطبعة، دون ذكر دار النشر، 2005 ص

113 وما بعدها.

ناقصاً²³، وكان هذا التعريف ينص على " كل مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تتكون كل منها الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط ، والتي يربط بينها مجموعة من العلاقات والتي يتم عن طريقها تحقيق نتيجة معينة وهي معالجة المعطيات على أن يكون هذا المركب خاضعاً لنظام الحماية الفنية ، والجريمة المعلوماتية تقع أثناء المعالجة الآلية للبيانات في مرحلة إدخال البيانات أو أثناء مرحلة المعالجة أو أثناء مرحلة إخراج المعلومات.

ففي مرحلة إدخال المعلومات ، تترجم المعلومات إلى لغة مفهومة من قبل الآلة يكون من السهل إدخال بيانات لا علاقة لها تماماً بالمعطيات الأساسية ومحو البيانات المطلوب إدخالها.

وفي مرحلة المعالجة حيث يمكن إدخال بيانات غير مصرح بها واستبدالها بالبيانات الأساسية أو تشغيل برامج جديدة تلغي عمل البرامج الأصلية جزئياً أو كلياً.

أما المرحلة الأخيرة فيتم التلاعب بالنتائج التي يخرجها النظام المعلوماتي تتمثل في بيانات غير صحيحة أدخلت فيها معالجة غير صحيحة²⁴.

الفرع الثالث: المجرم الإلكتروني

يتميز المجرم المعلوماتي عن غيره من المجرمين العاديين الذين جنحوا إلى السلوك الإجرامي النمطي بعدة خصائص عددها الأستاذ Parker فيما يلي²⁵:

1 — المجرم المعلوماتي مجرم متخصص ومحترف في تنفيذ جريمته الإلكترونية، حيث ان ارتكابها يتطلب التغلب على تقنيات حماية أنظمة الكمبيوتر.

²³ — علي عبد القادر القهوجي ، الحماية الجنائية للبيانات المعالجة إلكترونياً ، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت - والذي عقد بتاريخ 1 - 3 ماي 2000 كلية الشريعة والقانون - دولة الإمارات العربية ، ص 42 وما بعدها.

²⁴ — نائلة عادل محمد فريد ، جرائم الحاسب الآلي الاقتصادية ، منشورات الحلبي الحقوقية ، 2005 ص 106.

²⁵ — عبد العال الديربي: الجريمة المعلوماتية - تعريفها - أسبابها وخصائصها، 13 يناير 2013، منشور على الموقع

التالي: www.acconline.com/article.detail.aspx?id:7509

2 — خلافاً على المجرم العادي المجرم المعلوماتي لا يلجأ إلى العنف في تنفيذ جرائمه، فهو مجرم ذكي يتمتع بالمهارة والمعرفة وبدرجة عالية من الثقافة.

3 — يوجد عدة أنواع من المجرمين المعلوماتيين، فهناك:

أ — طائفة الأشخاص الذين يرتكبون جرائم المعلوماتية بغرض التسلية والمزاح مع الآخرين دون إحداث أي ضرر ويسمونهم (Pranskers)

ب — طائفة الأشخاص الذين يستهدفون الدخول إلى أنظمة الحاسبات الآلية الغير المصرح لهم بهدف الفضول أو اكتساب الخبرة أو لمجرد القدرة على اختراق هذه الأنظمة ويسمون (Hackers).

ج — طائفة الأشخاص الذين يستهدفون الحاق خسائر بالمجني عليهم، دون ان يكون الحصول على مكاسب مالية ضمن هذه الاهداف، ويندرجون تحت طائفة مختبري فيروسات الحاسبات الآلية وموزعيها ويسمون (Malicieuses hackers)

د — طائفة الأشخاص الذين يهدفون إلى إلحاق الأذى بالمجني عليهم، ويكون الباعث إيجاد حلول لمشاكل مادية تواجه الجاني لا يستطيع حلها بالطرق العادية ويسمون بـ : (Personnel problem solvers)

هـ — طائفة الأشخاص الذين يهدفون إلى تحقيق ربح مادي بطريق غير مشروع ويسمون بـ : (Green criminals).²⁶

المطلب الثالث: أنواع الجريمة السيبرانية:

²⁶ — عبد العال الديربي: المرجع نفسه.

لقد اختلف الفقه والقانون في تصنيف الجرائم الالكترونية باختلاف الزاوية التي ينظر منها إزاء الاعتداء الموجه ضد أحد مكونات النظام المعلوماتي.

وعليه سنقوم في هذا المطلب بتقسيم الجرائم الالكترونية وفقا لما أقره فقهاء القانون الجنائي ثم تقسيمها وفقا لما أقرته التشريعات المقارنة.

الفرع الأول :تقسيمات الفقه للجرائم الالكترونية:

اختلف الفقه الجنائي حول تقسيم الجرائم الالكترونية، حيث قد يكون النظام المعلوماتي هو نفسه موضوع أو محل الجريمة الالكترونية ومن ناحية أخرى، قد يكون النظام المعلوماتي هو أداة الجريمة ووسيلة تنفيذها:²⁷

أولا :الجرائم الواقعة بواسطة النظام المعلوماتي:

يعد الحاسب الآلي في هذا النوع من الجرائم وسيلة لتسهيل النتيجة الإجرامية ومضاعفا لجسامتها ويهدف الجاني من وراءها إلى تحقيق ربح مادي بطريقة غير مشروعة، تستخدم النظام المعلوماتي في حد ذاته أو برامجه كوسيلة لتنفيذ الجريمة²⁸ .

وتنقسم هذه الجرائم بدورها إلى:

1 — الجرائم الواقعة على الأشخاص:

رغم تطور الحياة اليومية للأفراد والمجتمع بفضل استعمالهم للفضاء الافتراضي إلا أنه أصبح سلاحا فتاكا في يد المجرمين للدخول إلى المعلومات الخاصة للأشخاص ,وعليه ظهرت عدة أنواع خاصة من الجرائم الالكترونية الواقعة على الاشخاص كجريمة التهديد والمضايقة والملاحقة، خاصة عن طريق البريد

²⁷ — صالح شنين: الحماية الجزائية لبرامج الحاسب الآلي، دراسة مقارنة رسالة لنيل شهادة الماجستير، جامعة بسكرة - كلية الحقوق والعلوم السياسية، 2007 - 2008، ص: 107.

²⁸ — سوير سفيان: الجرائم المعلوماتية، مرجع سابق ، ص 33.

الالكتروني بإرسال رسالة خاصة للترويع والتهديد أو عن طريق وسائل الحوارات المختلفة على شبكة الانترنت: ك (الفيس بوك، والفايبر والواتساب)²⁹، وكذلك جريمة القذف والسب وتشويه السمعة للمساس بشرف الغير وكرامتهم واعتبارهم عن طريق وسائل الاتصال المباشر أو الكتابة أو عن طريق المطبوعات أو المبادلات الالكترونية (بريد الكتروني) صفحات الويب، غرف المحادثة³⁰.

كما تعتبر من أهم الجرائم الالكترونية الواقعة على الأشخاص صناعة ونشر الإباحة والجنس سواء للبالغين والأطفال خاصة، حيث يتعرض الأطفال للاستغلال الجنسي على الانترنت بأشكال متعددة انطلاقاً من الصور إلى التسجيلات المرئية للجرائم الجنسية العنيفة، حيث تستمر معاناتهم ما بعد ارتكاب الجريمة بسبب إمكانية تناقل الصور عبر الانترنت³¹.

ويضاف إلى الجرائم الالكترونية الشخصية جرائم انتحال الشخصية والتغريب والاستدراج باستخدام شخصية شخص آخر للاستفادة من سمعته مثلاً أو ماله أو صلاحياته أو تتخذ هذه الجريمة وجهان: انتحال شخصية الفرد وانتحال شخصية المواقع³².

2 — الجرائم الواقعة على الأموال:

لقد صاحب تطور شبكة الإنترنت تطور وسائل الدفع والوفاء، وأضحت جزء لا يتجزأ من المعاملات الإلكترونية وفي خضم هذه التداول المالي عبر الإنترنت ظهرت عدة جرائم الكترونية على الأموال مثل: السطو والسرقه، والتحويل الالكتروني غير المشروع للأموال وقرصنة أرقام البطاقات المغنطة، حيث

²⁹ — وسف صغير: المرجع السابق، ص: 50.

³⁰ — عبد الرحمن بن عبد الله السيد: الأحكام الفقهية للمعاملات الالكترونية (الحاسب الآلي وشبكة المعلومات و الانترنت)، دار الوراقين للنشر والتوزيع، بيروت، الطبعة الأولى، 2004، ص: 312.

³¹ — كريستا سكولمان: عن جرائم الانترنت طبعها وخصائصها، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية 19 و 20 يونيو 2007، ص: 40.

³² — عمرو عيسى الفقي: الجرائم المعلوماتية، جرائم الحاسب الآلي والانترنت في مصر والدول العربية، المكتب العربي الحديث، الاسكندرية 2006، ص: 102.

أصبحت إمكانية خلق مفاتيح البطاقات والحسابات البنكية بالطريقة الغير المشروعة ممكنة عبر قنوات شبكة الانترنت³³.

كما ظهرت جريمة القمار وغسيل الأموال عبر الانترنت بظهور الكازينوهات الافتراضية أو أندية القمار الافتراضية التي أصبحت فيما بعد مسرحا كذلك لجريمة غسيل الأموال، حيث ساعدت الشبكة العنكبوتية في انتشارها وتطورها بنقل هذه الجريمة من دولة إلى دولة أخرى لاستثمارها في مجالات مشروعة³⁴.

ومن أهم الجرائم الالكترونية على الأموال ، نذكر جريمة المخدرات على الانترنت حيث تتخذ المواقع الالكترونية للترويج للمخدرات وتسويقها للناشئ لاستخدامها، وتعليمه كيفية صناعتها بكافة أصنافها وأنواعها³⁵.

3 — الجرائم الواقعة على أمن الدولة:

تعد هذه الجرائم من أخطر الجرائم الالكترونية خاصة الارهاب المعلوماتي والجريمة المنظمة المعلوماتية، حيث أتاحت الانترنت للكثير من المنظمات الارهابية الترويج لأفكارها ومعتقداتها ،وأدت إلى ظهور جريمة أخرى أخطر منها وهي جريمة التجسس الالكتروني على الدول بالإطلاع على مختلف الأسرار العسكرية والاقتصادية بين الدول المتصارعة، كما تعطى الشبكة العنكبوتية فرصا للتأثير على المعتقدات الدينية وتقاليد المجتمعات مما سهل خلق الفوضى داخل الدولة والمساس بأمنها الداخلي وبنظامها العام .

ثانيا :الجرائم الواقعة على النظام المعلوماتي:

³³ — خالد ممدوح إبراهيم: أمن الجريمة الالكترونية، مرجع سابق ، ص: 76 وما بعدها.

³⁴ — صالحة العمري: جريمة غسل الأموال وطرق مكافحتها-مجلة الاجتهاد القضائي، العدد الخامس، مخبر اثر الاجتهاد القضائي على حركة التشريع، جامعة محمد خيضر بسكرة، ص: 179..

³⁵ — سامي علي عياد حامد: الجريمة المعلوماتية وإجرام الانترنت، مرجع سابق ، ص: 77.

إضافة إلى الجرائم المعلوماتية التي تقع باستخدام النظام المعلوماتي هناك نوع آخر من الجرائم المعلوماتية يمس النظام المعلوماتي ويستهدف إما المكونات المادية للنظام المعلوماتي أو المكونات المنطقية أو المعلومات المدرجة بالنظام المعلوماتي³⁶.

الفرع الثاني: الجرائم الواقعة على المكونات المادية للنظام المعلوماتي:

يقصد بالمكونات المادية للنظام المعلوماتي بالأجهزة والمعدات الملحقة به والتي تستخدم في تشغيله كالاسطوانات والشرائط والكابلات، ونتيجة للطبيعة المادية لهذه المعدات تكون الجرائم الواقعة عليها تقليدية كأن تكون محل للسرقة وخيانة الأمانة أو الاتلاف العمدي أو الإحراق أو العبث بمفاتيح التشغيل، مما يترتب عليها خسائر كبيرة، ولقد حدث هذا النوع من الجرائم في فرنسا ،وأدى إلى إتلاف معدات مؤسسة كبيرة ومتخصصة في بيع الأنظمة وتوثيق المعلومات الحسابية، وقدرت الخسائر بـ 5 ملايين فرنك فرنسي³⁷.

1— الجرائم الواقعة على البرامج الالكترونية:

وتنقسم هذه الجرائم بدورها إلى الجرائم الواقعة على البرامج التطبيقية، عن طريق تحديد البرنامج أولاً ثم التلاعب به أو تعديله، ومن أمثلتها قيام أحد المبرمجين بالبنوك الأمريكية بتعديل برنامج بإضافة دولار واحد على كل حساب يزيد عن عشرة دولارات وقام بتقييد المصاريف الزائدة في حساب خاص به أطلق عليه اسم (Zzwick)³⁸، وكذلك تضم هذه الجرائم الجرائم الواقعة على برنامج التشغيل وهي البرامج المسؤولة عن عمل النظام المعلوماتي، ومن حيث قيامها بضبط ترتيب العمليات الخاصة بالنظام، وتقوم هذه الجريمة عن طريق تزويد البرنامج بمجموعة تعليمات إضافية للوصول إليها بشيفرة تسمح بالدخول إلى جميع المعطيات التي يتضمنها النظام المعلوماتي ومثالها: جريمة تصميم برنامج وهمي من خلاله تنفذ الجريمة، ومثاله ما قامت به إحدى الشركات التأمين الأمريكية في مدينة لوس انجلوس بواسطة

³⁶— سوير سفيان، المرجع السابق، ص: 39.

³⁷ - Lucas (A) : droit de Informatioque, paris, PUF,1987, p 519 – 521.

³⁸— سوير سفيان، المرجع السابق، ص: 42.

مبرمجها تصميم برنامج يقوم بتصنيع وثائق تأمين لأشخاص وهميين بلغ عددهم 46000 بهدف تقاضي هذه الشركة لعمولات من اتحاد شركات التأمين.

2 — الجرائم الواقعة على المعلومات المدرجة بالنظام المعلوماتي:

لقد عرف القانون الفرنسي الصادر في 29 جويلية 1982 الخاص بالاتصالات السمعية والبصرية المعلومات بأنها³⁹: (sons d'images de documents, de données ou de message de) (toute nature

كما عرفها الفقيه الفرنسي (Catala) على أنها "رسالة معبر عنها في الشكل يجعلها قابلة للنقل أو الإبلاغ للغير". بينما عرفها القضاء الفرنسي بأنها: "وسيلة للمعرفة قابلة لكي تحفظ أو تبلغ بواسطة الاصطلاحات.

وتعد المعلومة المعالجة آليا ذات أهمية كبيرة باعتبارها أساس عمل النظام المعلوماتي، لما لها من قيمة اقتصادية، وتنتم الجرائم عليها من خلال التلاعب فيها بصفة مباشرة أو غير مباشرة أو عن طريق اتلافها أو استبدالها أو محوها وهذا ما تسمى بجريمة الغش أو التزوير المعلوماتي ومثالها ما قام به شخص يدعى Vladimir Ioriblit بإسرائيل باستخدام طريقة تدعى bluff وهو موظف بوزارة المالية، حيث قام بإدخال فواتير وهمية لا حصر لها وتحويل ما تم سداده من هذه الفواتير لحساب الشركات الوهمية التي قام بإنشائها⁴⁰.

الفرع الثالث: تقسيمات التشريعات المقارنة للجرائم الالكترونية:

لقد تعددت الجرائم الالكترونية بتعدد وسائلها وأنماطها في مختلف التشريعات المقارنة خاصة في أوروبا، حيث كانت الدول الأوروبية الأكثر نضجا في العالم في التعامل مع هذه الظاهرة الإجرامية، وفي مقدمتها فرنسا وبريطانيا حيث سن المشرع الفرنسي رقم 19 - 88 الصادر في 05 كانون الثاني 1988 الخاص

³⁹ — غنية باطلي: المرجع السابق، ص: 58 - 59.

⁴⁰ — محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري و المقارن ، دار الجامعة الجديدة للنشر

2007، ص 88،

بالولوج في الجرائم المعلوماتية كما تضمن قانون العقوبات الفرنسي في المادة 462 فقرة 4 منه جريمة الولوج إلى نظام المعالجة الآلية أو النفاذ الغير المشروع، وشدت العقوبة في حالة إذا انجر عن هذا الولوج محو أو تعديل المعطيات المعالجة آلياً، كما نص على تحريم إتلاف المعطيات أو تزوير المستندات المعالجة آلياً أو استعمالها وعاقب عليها بعقوبة الحبس أو الغرامة. بينما في بريطانيا صدر قانون إساءة استخدام الحاسوب لسنة 1990 وبدأ سريانه بتاريخ 29 أوت 1990، وقسم الجرائم الالكترونية إلى:

أ- الدخول غير المصرح به لنظام الحاسوب.

ب- نفس الفعل السابق لكن بنية ارتكاب أو تسهيل ارتكاب فعل آخر.

ج التعديل أو التحويل الغير مصرح به لنظام الحاسوب بقصد إضعاف أو تعطيل النظام.

وأهم تصنيف للجرائم الالكترونية جاءت به الاتفاقية الأوروبية بشأن الجرائم الالكترونية لسنة 2001، وهي اتفاقية بودابست لسنة 2001، حيث قسمت هذه الاتفاقية هذه الجرائم إلى:

الطائفة الأولى: الجرائم التي تستهدف سرية وسلامة وتوفر المعطيات، أي الجرائم التي تستهدف معطيات الكمبيوتر سواء بالاطلاع عليها أو إفشائها أو تصويرها، أو إتلافها.

الطائفة الثانية: وهي الجرائم المرتبطة بالكمبيوتر أي الجرائم التي يلعب فيها الكمبيوتر أو الحاسب الآلي دور الوسيلة كجرائم الاحتيال والتزوير الالكتروني.

الطائفة الثالثة: الجرائم المرتبطة بالمحتوى، أي يلعب فيها الكمبيوتر دور البيئة الجرمية كجرائم المواد اللااخلاقية للأطفال، وجرائم القمار وغسيل الأموال والمخدرات.

الطائفة الرابعة: وهي الجرائم المتعلقة بحقوق الملكية الفكرية كحقوق المؤلف وهو نص مكمل لما جاءت به قوانين الملكية الفكرية المقررة وطنياً ودولياً⁴¹.

⁴¹ — يونس عرب، تطور التشريعات في مجال مكافحة الجرائم، الالكترونية، هيئة تنظيم الاتصالات، سلطنة عمان، مسقط،

2 و 4 أبريل 2006، ص ص: 21، 22، 23.

أما في الجزائر، فلقد أحدث المشرع الجزائري قسم في قانون العقوبات في القسم السابع مكرر من الفصل الثالث الخاص بجرائم الجنايات والجنح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات⁴²، حيث نصت المواد 394 مكرر، و399 مكرر 1، 394 مكرر 2، 394 مكرر 3، والمادة 394 مكرر 4، والمادة 394 مكرر 5، والمادة 394 مكرر 6، والمادة 394 مكرر 7، وباستقراءنا لهذه المواد يتضح أن المشرع الجزائري قد قسم الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، أو الجرائم الالكترونية إلى الطوائف التالية:

الطائفة الأولى: طبقا للمادة 390 مكرر من قانون العقوبات وهي جرائم الولوج إلى المعطيات المعالجة آليا عن طريق الغش والتزوير وكذا جريمة الحذف والتغيير والتخريب في هذه المعطيات ويعاقب الجاني بعقوبة 3 أشهر إلى سنة وبغرامة من خمسين ألف إلى مائة ألف دينار وتضاعفت العقوبة إذا ترتب عن الفعل الإجرامي حذف أو تغيير المعطيات، كما يعاقب الجاني بـ 6 أشهر إلى سنتين وغرامة من خمسين ألف إلى مائة وخمسين ألف دينار وفي حالة التخريب النظام المعلوماتي.

الطائفة الثانية: الجرائم الالكترونية بواسطة النظام المعلوماتي وأهمها استعمال أو إفشاء أو نشر معلومات منصوص عليها في قانون العقوبات، وكذا البحث أو التجميع في معطيات مخزنة في نظام معلوماتي، كجرائم التحويل الالكتروني والسطو والنصب والاحتيال والسلب وغيرها، وهذا ما نصت عليه المادة 394 مكرر 2، وعقوبتها من شهرين إلى 3 سنوات وبغرامة 1000.000 دج إلى 5000.000 دج.

الطائفة الثالثة : الجرائم الالكترونية المتعلقة بأمن الدولة و مؤسساتها كجرائم التجسس و الارهاب و عقوبتها تضاعف عقوبة الطائفة الثانية لخطورتها طبقا للمادة 394 مكرر 3

الطائفة الرابعة: الجرائم الالكترونية للشخص المعنوي، حيث نص المشرع الجزائري على خلاف التشريعات المقارنة الأشخاص المعنوية بنص خاص وعقوبتها تعادل خمس مرات الجرائم المرتكبة من طرف الشخص الطبيعي طبقا للمادة 394 مكرر 4 من قانون العقوبات الجزائري.

⁴² — نظر القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات ، الجريدة الرسمية رقم

كما عاقب المشرع الجزائري على الشروع في الجريمة الالكترونية كما هو الحال في الجريمة العادية أو التقليدية بنفس العقوبة للجريمة الكاملة مع تكييفها جنحة وفقا لقانون العقوبات الجزائري، كما نص كذلك على الاشتراك في الجريمة الالكترونية كما هو الحال في الجريمة العادية ويأخذ الشريك في الجريمة الالكترونية نفس العقوبة المقررة للشريك في الجريمة العادية أو التقليدية طبقا لقانون العقوبات الجزائري، كما نص كذلك على جريمة الاتفاق الجنائي الالكتروني للوقاية من ارتكاب الجريمة الالكترونية، طبقا للمادة 394 مكرر 5 من القانون 04 - 15 المعدل والمتمم لقانون العقوبات.

ويلاحظ أن المشرع الجزائري قد توسع في نطاق الجرائم الالكترونية سواء وقعت على النظام المعلوماتي أو بواسطته، وسواء وقعت على الأشخاص أو الأموال أو على أمن الدولة ومؤسساتها، كما أقر جريمة جديدة الكترونية وهي جريمة الاتفاق الجنائي الالكتروني رغم أنها من الأعمال التحضيرية لارتكاب الجريمة وشدد عقوبتها وذلك خشية استعمال النظام المعلوماتي كوسيلة لارتكاب الجريمة وتسهيلها⁴³.

و ما يعاب على المشرع الجزائري عدم افراد معيار واضح وواحد في تقسيم الجرائم الالكترونية و تحديد عقوبتها، وكان من الاحسن اتباع المنهاج المتبع من طرف الفقه و هو تقسيمها الى جرائم واقعة على النظام المعلوماتي و جرائم واقعة بواسطة النظام المعلوماتي، بعد تحديد المصطلحات الخاصة بها لتسهيل فهم ماهيته.

⁴³ - نفس المرجع.

المبحث الثاني: ماهية الأزمات الإقليمية

المطلب الأول: الأزمة و مفهوم الأمن الإقليمي

يشار الى مفهوم الأزمة الدولية بأنها مجموعة من التفاعلات المتعاقبة بين دولتين أو أكثر تعيش في حالة صراع شديد يصل احياناً الى احتمال عالي لنشوء الحرب ووقوعها ، وفيها يواجه صاحب القرار موقفاً يهدد المصالح العليا للوطن ويتطلب وقتاً للتعامل مع هذا الموقف باتخاذ قرارات جوهرية.

تتسم الأزمة الدولية بثلاث مواقف¹:

1 — موقف يتضمن درجة عالية من التهديد للأهداف والقيم والمصالح الجوهرية للدول وبحيث يدرك صناع القرار ذلك التهديد لمصالح دولهم.

2 — موقف يدرك فيه صناع القرار أن الوقت المتاح لصنع القرار واتخاذ هو وقت قصير ، ويستلزم ذلك سرعة فائقة ومعالجة الموقف.

3 — موقف مفاجئ حيث تقع الأحداث الخالقة للأزمة على نحو يفاجئ صانع القرار.

يتداخل مفهوم الأزمة الدولية كثيراً مع مفهوم الصراع الدولي مما يسبب خلط بين التعريفين ، حيث ان الصراع الدولي هو ذلك الموقف الذي ينتج عن الاختلاف في الأهداف والمصالح.

أولاً: أسباب حدوث الأزمة الدولية:

تعددت اسباب الأزمة الدولية وعادة تكون على شكل ظواهر لحالة اساسية واحدة هي مساسها بالأمن القومي والمصالح الحيوية نذكر منها²:

• تحدث من اجل الموارد كالمياه والغذاء والمراعي.

¹ — الأزمة الدولية ، خصائصها و مفاهيمها، نقلا عن الموقع: [الموسوعة السياسية\(political-encyclopedia.org\)](http://political-encyclopedia.org)

² — نفس المرجع.

· الصراع من أجل التوسع السكاني، الصراع الأيديولوجي والاجتماعي، الصراع على الأسواق ومصادر المواد الأولية ، والصراع على النفوذ.

· الاستعمار فهو بحد ذاته يمثل مصدراً أساسياً للأزمات الدولية بما يوفره من فرص كبيرة لنشوب العنف المسلح في البلدان الخاضعة له.

· محاولة الدول لتغيير الوضع الراهن في دولة أخرى يعد سبباً في نشوء الأزمة الدولية للحصول على مكاسب استراتيجية جديدة لصالح الدولة القائمة بالمحاولة.

· الفقر والتخلف والجهل والعوز والفتنة والأمراض والتعليم المحدود وندرة الموارد وتدهور البيئة والكوارث الطبيعية . كل هذه الأمور تشكل ارضاً خصبة لنشوء الأزمات.

· تنامي الاشاعات بين الدول

· وجود بؤرة خلاف لم تحسم رغم مرور الوقت

· خرق الدول للاتفاقيات القائمة بينها

ثانياً: خصائص الأزمة الدولية:

1- هي محطة تحول حاسم غالباً ما تتسم بالمفاجئة في نسق داخلي أو دولي تهدد مصالح دولية معينة وتثير نوعاً من الذهول والهرج لدى القوى المعنية بها³.

2- تتطلب جهداً كبيراً لتلافي تطوراتها السلبية التي قد يمتد خطرها للمستقبل.

3- قد تخلق حالة من التوتر العالمي خلال فترة زمنية قصيرة في ظل العلاقات الدولية المتشابكة حالياً.

4- تضع صانعي القرار في محك حقيقي بحيث تتطلب اتخاذ قرارات واجراءات سريعة وراجحة.

³ - نفس المرجع.

ثالثاً: مراحل الأزمة الدولية

تمر الأزمة الدولية بعدة مراحل هي:

1- مرحلة الإنذار المبكر

2- مرحلة النشوء والتبلور

3- مرحلة النمو والصعود والانتشار

4- مرحلة الانفجار

5- مرحلة تثبيت أو رسوخ الأزمة

6- مرحلة إيجاد الحلول

المطلب الثاني: مفهوم الأمن الإقليمي

مصطلح النظام الإقليمي في معناه العلمي، و كمستوى لتحليل العلاقات الدولية، مفهوم حديث لم تشر إليه الدراسات إلا في الستينات و السبعينات، وان كان يمكن إرجاع جذوره في الفكر السياسي المتعلق بالشؤون الدولية إلى زمن بعيد، أين كان مفهوم الإقليمية (Regionalism) أحد الموضوعات الأساسية في مجال التنظيم الدولي، و دار جدل طويل حول ما سمي بالعالمية في مواجهة الإقليمية (Universalism versus Regionalism) و أي المنهجين ينبغي إتباعه لتنظيم المجتمع الدولي و حفظ السلم الدولي⁴.

و يمكننا في هذا الاتجاه الاعتماد على ما ذهب إليه ناصيف حتى في تعريفه للنظام الإقليمي بأنه يشمل أي كيان ذي خصوصية في عضويته في مقابل الكيانات المفتوحة العضوية لجميع الدول (أي النظام الدولي)، وهنا يمكن ملاحظة أن النظام الإقليمي هو عبرة عن مجال سياسي لتفاعل عدة دول تربطها روابط مميزة عن غيرها. و أحيانا تتقصد تلك الدول جعل ذلك التمايز مقتنا في عمليات سياسية محددة عسكرية، أو

⁴ Barry, buzan. People, states and Fear. The international security problems in international-romatons-london : wheatsh, 1983.P123 .

اقتصادية أو ثقافية، بعضها أو كلها في آن واحد، و بهذا قد يشمل النظام دولا متجاورة، بمعنى أن الإقليمية تساوي منطقة جغرافية محددة. و قد لا يشمل النظام دولا متجاورة، بمعنى أن الإقليمية ترتبط بالتضامن بين الدول لا بالجوار الجغرافي (كالروابط القومية، التاريخية، الاقتصادية، الحضارية...) ⁵ إذا تتأسس الإقليمية على فكرة إقامة تنسيق بين عدة دول بقصد ضمانه مصالحها المشتركة، و استثمار مزايا المنطقة السياسية. فإقامة نظام إقليمي يشترط إمكانات بناء ترتيبات محددة و تأسيس علاقات إقليمية مميزة، علاوة على توفر الإرادة السياسية.

إن النظرة التي قدمها كل من لويس كنتوري (Louis Cantori) و ستيفن شبيغل (Steven Spiegel) في دراستهما "السياسة الدولية للأقاليم"، (The International Politics of Regions) تسمح لنا بعملية تحليل العلاقات الدولية في إطار إقليم ما من وجهة نظر التفاعلات بين دول الإقليم، إلى جانب عملية المقارنة بين الأقاليم الموجودة بعضها مع الآخر، المعاصرة منها و التاريخية، إلى جانب أنها تبرز لنا مختلف أشكال التغلغل الممارس من طرف القوى الكبرى اتجاه هذه الأقاليم و الأساليب والآليات المستخدمة على جانب مدى التغلغل.

إن عملية عرض الفكر المتعلق بتعريف النظم الإقليمية يجعلنا نميز بين ثلاثة اتجاهات حول معيار تعريف النظام الإقليمي:

الأول: يركز على اعتبارات التقارب الجغرافي ⁶، (Geographic Proximity Approach).

الثاني: يركز على وجود عناصر التماثل بين الدول التي تدخل في نطاق إقليم ما من النواحي الثقافية ، الاجتماعية، الاقتصادية (Homogeneity Approach) .

⁵ — عكروم، ليندة. تأثير التهديدات الأمنية الجديدة على العلاقات بين دول شمال وجنوب المتوسط. الأردن: دار ابن بطوطة للنشر و التوزيع، 2011. ص 73.

⁶ — المرجع نفسه.

الثالث: ينتقد الاتجاهين السابقين، على أساس أن الدول المتجاورة، المتشابهة لا يشترط بالضرورة أن تكون على علاقات وثيقة فيما بينها، وأن العامل الحيوي في أي نظام إقليمي هو مدى وجود تفاعلات سياسية و اقتصادية و اجتماعية بين الدول وبعضها البعض (Interaction Approach).

يبدو أنه على الرغم من الاختلافات المسجلة حول تعريف النظام الإقليمي و مكوناته، إلا أن هناك ميلا عاما للاتفاق حول أن أهم عناصر النظام الإقليمي هي⁷:

— أن حجم التفاعلات بين الدول المتقاربة جغرافيا عادة ما يكون أكبر و أكثر بين تلك غير المتجاورة .
— يشتمل على ثلاث دول على الأقل.

— وحدات النظام الإقليمي تدخل في شبكة معقدة من التفاعلات السياسية والاقتصادية و الاجتماعية الخاصة بالنظام، و التي تمتلك ديناميكيتها الذاتية، و قواعد حركتها المنبثقة من هذه التفاعلات باستقلال عن النظام الدولي، أو حتى نفوذ القوى الكبرى، لا يتضمن هذا بالطبع افتراض الاستقلال الكامل للتفاعلات التي تجري في نظام إقليمي ما، فهذا لا يمكن تصوره في ضرورة الاتصالات و المواصلات المعاصرة، واعتبارات الإستراتيجية الدولية.

المطلب الثالث : باري بوزان و مركب الأمن:

من أجل فهم أفضل لنظرية المركب الأمن الإقليمي سوف يتم التركيز وبشكل كبير على إسهامات كل من باري بوزان و أولي وايفر (Buzan & Waever) في دراستهما التي جاءت تحت عنوان " الأقاليم و القوى"⁸، مع الإشارة إلى أنهما لم يحتكرا لوحدهما مسألة تطوير هذه النظرية بصفة كلية و إنما هناك مقاربات أخرى ساهمت في تطويرها و توسيعها بشكل كبير على غرار تأثيرات مرحلة ما بعد الحرب الباردة و العلاقات الدولية إلى جانب نظريات التنمية و تشكيل التكتلات الإقليمية، فكل من باري بوزان و

⁷ — قوجيلي، سيد أحمد. تطور الدراسات الأمنية ومعضلة التطبيق في العامل العربي. أبو ظبي: مركز الإمارات للدراسات والبحوث الاستراتيجية، 2012، ص 28

⁸ Buzan, Barry, and Waever, Ole. region and powers : the structure of international security. Newyourk : combrige university, 2003.P 214.

وايفر طوراً تحليلياً عاماً للأمن الإقليمي داخل نظام عام و في إطار العلاقات الدولية، كما أنها نظرية تم تطويرها بصفة خاصة لتشكّل تحولاً جديداً في الدراسات الأكاديمية، فهي تتبع حاضر المركبات الأمنية الإقليمية في النظام الدولي وتضع في الحسبان مختلف العناصر الأخرى التي من شأنها التأثير على بنية المركب الأمني.

يؤكد بوزان بأن التطور نحو مفهوم "القوى الكبرى" ينطبق أكثر على الغرب أين يتمتع الأفراد بدرجة أمن أكبر، ومن ناحية النظام الدولي لا يرى بوزان بأن "إقصاء الفوضى" هو استجابة لمعضلة الأمن⁹، (Security Dilemma) وحول التمييز الواقعي بين النظام الداخلي (Domestic Order) والفوضى الدولية، يتوقع بوزان بأن النظام الدولي يسير نحو "فوضوية ناضجة" Mature Anarchy "و هو النموذج الأكثر استقراراً للفوضى الدولية. كإطار لتحليل العلاقات الدولية، يبدو مفهوم المركب الأمني هو الآخر معنياً بالصعوبات الموجودة

حول المفاهيم، و لكننا هنا نقبل بوجهة نظر باري بوزان القائلة: "الأمر يتعلق بتحليل خاطئ و أكبر من امتلاك تصور نسقي لديناميكية إقليمية للأمن و ليس الحصول على موضع تساؤل حولها.

خلاصة الفصل:

تتميز الجريمة الالكترونية عن الجريمة التقليدية من حيث تعريفها وخصائصها و أركانها و كذا القانون الواجب التطبيق عليها, حيث اوجد الفقه الجنائي عدة معايير لتحديد ماهيتها منها معيار وسيلة ارتكاب الجريمة و معيار محل الجريمة ومعيار الجمع بين عدة معايير.

و ترتباً على ذلك, اتسمت الجريمة الالكترونية بخصائص عديدة اهمها انها جريمة عابرة للحدود تمارس داخل او بواسطة النظام المعلوماتي ,وترتكب من طرف مجرم معلوماتي يوصف بالسرعة و الذكاء و المهارة , كما انها صعبة الاثبات مقارنة بالجريمة العادية لأنها سريعة التنفيذ ومتطورة بتطور الوسائل التكنولوجية . مما ادى الى ظهور انواع كثيرة منها قسمها الفقه و التشريع الجنائي الى جرائم واقعة على النظام المعلوماتي و جرائم واقعة بواسطة النظام المعلوماتي.

كل هذه الخصائص للجريمة الالكترونية , اوجدت صعوبة في تحديد القانون الواجب التطبيق عليها و القضاء المختص بمنازعاتها مما ادى بالقوانين المقارنة و القانون الجزائري الى تبني التعاون و المساعدة القضائية لمكافحة هذه الجرائم عن طريق ابرام الاتفاقيات الدولية و الاقليمية و عقد المؤتمرات و الندوات لاكتساب الخبرة الكافية لمواجهة هذه الجرائم ذات البعد العالمي.

الفصل الثاني : تجليات الحرب السيبرانية بين الأنظمة

المبحث الأول: الكيان الاسرائيلي المحتل و تجليات الحرب السيبرانية

تشكل أجهزة الحاسوب ولوحة المفاتيح أحدث ساحات المعارك التي يخوضها الكيان الاسرائيلي المحتل ضد أعدائه، وتعد أكثر المعارك تكلفة وخسائر بسبب استهداف مؤسسات حيوية واستراتيجية عليهم.

أضافت الأوساط العسكرية والأمنية للكيان الاسرائيلي المحتل جبهة قتالية جديدة بجانب ساحات البر والبحر والجو، هي جبهة الحرب الإلكترونية "السايبير"، التي تستنزفها استخباراتيا وماليا بشكل باهظ، مما يتطلب تسليط الضوء عليها، وإظهار أهميتها وخطورتها، وحجم الخسائر التي تسببها، والجهات التي تستهدفها عبر الشبكة العنكبوتية، والوسائل المضادة التي ابتكرتها لحماية نفسها من هذه الجبهة التي تضربها في خاصرتها الرخوة، وفي الوقت ذاته سطوتها في عالم السايبير، و منها أيضا استهداف الدول و الحكومات التي ترفض الاعتراف بها كدولة و تقف إلى جانب القضية الفلسطينية و على رأسها بعض الدول العربية.

المطلب الأول: طبيعة و أثر الحرب السيبرانية بين الكيان و المنظومة العربية

الفرع الأول : تاريخ و طبيعة الصراع العربي الإسرائيلي

أولا : طبيعة الصراع:

يعتبر الصراع العربي الإسرائيلي من أكثر الصراعات التاريخية الممتدة -أي التي تزيد عن خمسين عاما متواصلة- التي عرفها العالم المعاصر، وبالطبع تمتد جذور ومصادر الصراع إلى أواخر القرن التاسع عشر وحتى قيام الكيان الصهيوني في فلسطين عام 1948.

يتميز الصراع العربي الإسرائيلي عن غيره من الصراعات بأنه يشمل مختلف الجوانب الإستراتيجية والسياسية والعسكرية والاقتصادية والثقافية وغيرها، هذا فضلا عن الاستخدام المكثف من قبل العقيدة الصهيونية للأساطير والمزاعم الدينية المؤسسة على التفسير المحرف واختلاق وقائع دينية من التوراة والتلمود وغيرهما من التفسيرات الدينية المحرفة التي مزجها قادة المشروع الصهيوني مع العقيدة الأيديولوجية العلمانية لهذا المشروع ومقولاتها الرئيسية.

من جانب آخر تتفرد إسرائيل في إطار هذا الصراع بتبني مفاهيم شاذة ومتفردة عن الأمن القومي ومتطلبات الحفاظ على الوجود وسلامة الكيان الترابي لإسرائيل، إذ يلاحظ أن جميع تصرفات إسرائيل الداخلية والخارجية اقتصاديا وسياسيا تخضع لمقتضيات الأمن حيث تتبع خيارات إسرائيل السياسية وغير السياسية دائما من متطلبات الأمن الإسرائيلي الذي صار يشغل القيمة العليا بين شتى القيم الإسرائيلية الكبرى ويزداد شذوذ هذا التصور خصوصا مع عالم ما بعد الحرب الباردة والقرن الحادي والعشرين الذي احتلت فيه الجغرافيا الاقتصادية محل الجغرافيا السياسية أو الجيوبولتكس، وزادت عمليات وتفاعلات التكامل العالمي والإقليمي على أسس من الاعتماد المتبادل والاندماج الاقتصادي والتقني، في حين أصبح يعرف باسم الوظيفية الجديدة.

يضاف إلى ذلك أن إسرائيل تكاد تكون الدولة الوحيدة في العالم التي تصر على إعادة الهيكلة التامة للنظام الإقليمي الرئيسي وللنظم الإقليمية الفرعية المحيطة بها، فهي تزعم أن هناك ضرورة قصوى لتفجير وإزالة النظام الإقليمي العربي بل ولتفتيت الكيان الاجتماعي القومي العربي ليس ذلك فحسب وإنما أيضا تفتيت النسيج الاجتماعي الوطني لكل قطر عربي على حدة.

ثانيا: القضية الفلسطينية محور الصراع

لقد مر النظام الدولي منذ اندلاع الصراع العربي الإسرائيلي وحتى الآن بمراحل تطور متعددة ودخل عليه متغيرات كثيرة طوال تلك الفترة¹، ومع ذلك بقي هذا الصراع متأججا، ولكن الشيء اللافت للنظر هو أن الوضع العربي في معادلة الصراع كان ينتقل دائما من سيء إلى أسوأ، وكانت قدرة الدول العربية على استثمار التحولات التي تطرأ على النظام الدولي محدودة. ويرجع ذلك إلى اختلاف الدوافع والمصالح والأهداف اختلافاً بيناً بين الدول العربية، بالرغم من أن الدول العربية - جميعاً - تعلن دائماً أن صراعها مع إسرائيل هو صراع مصير، إلا أن سلوكها الفعلي لا يعكس هذا النوع من الخطاب السياسي حيث يتباين موقفها حسب قربها أو بعدها عن بؤرة الصراع ووفقاً لاعتبارات أيديولوجية وسياسية أخرى. فالصراع العربي الإسرائيلي هو بالنسبة لدول المواجهة صراع وجود ومصير، أما بالنسبة لغير دول

¹ — محمد السيد سعيد، " تحليل مقارنة لتجارب التسوية الإقليمية"، مجلة السياسة الدولية، القاهرة، الأهرام، العدد 95، يناير 1989م، ص71-87.

الجوار، فهو مجرد قضية دعم وتضامن مع الأشقاء. وفي مقابل هذا التباين والاختلاف في الموقف العربي تشكل إسرائيل طرفاً واحداً ومتجانساً. ولهذا الوضع انعكاساته الخطيرة والمتباينة على علاقة طرفي الصراع بالعالم الخارجي، حيث توظف إسرائيل سياساتها الخارجية على كافة الأصعدة السياسية والاقتصادية والاجتماعية والثقافية وغيرها لخدمة دعم عملية بناء القوة الذاتية الإسرائيلية. أما الدول العربية، وعلى الرغم من وجود - أحياناً - علاقات خاصة بين بعض الدول العربية والولايات المتحدة، لا توظف مثل هذه العلاقات في حالة وجودها دائماً وبالضرورة لصالح دعم الموقف العربي في هذا الصراع².

حالت هذه الخلافات دون تعبئة الطاقات العربية وحشدتها في مواجهة الخطر الإسرائيلي. وما تزال الخلافات العربية - العربية وعجز العالم العربي عن الاتفاق على استراتيجية لإدارة الصراع مع إسرائيل أهم المعطيات التي تفسر العجز العربي في تعامله مع التحولات التي تجرى في العالم، وخلال الفترة 1980 - 1985 كانت صورة الصراع العربي - الإسرائيلي في سياق العلاقة بين القوتين العظميتين تبدو على النحو الآتي³:

-تراجع اهتمام الولايات المتحدة بالبحث عن حل شامل للصراع والاكتفاء بالدور الذي يضمن عدم انهيار معاهدة السلام المصرية - الإسرائيلية.

-التركيز على منطقة الخليج باعتبارها منطقة تتصل اتصالاً مباشراً بالأمن القومي للولايات المتحدة بصفة خاصة والغرب بصفة عامة.

-ممارسة أكبر قدر ممكن من الضغط على النظم الراديكالية في العالم العربي وفي مقدمتها سوريا وليبيا واليمن الجنوبي، كجزء من الحرب الباردة ضد الاتحاد السوفيتي، وذلك لأن الاتحاد السوفيتي كان يعتمد على هذه الدول وبصفة خاصة سوريا.

² - أيمن السيد عبد الوهاب، "حركات الإسلام السياسي ونمط جديد من التفاعلات العربية"، السياسة الدولية، القاهرة، الأهرام، العدد 113، 1993م، ص 89.

³ - James Rosenau, Turbence in World Politics: A Theory of change and continuity (New York: Harvester / Wheatsheab, 1990) p. p. 47 - 66.

وبانتهاء الحرب الباردة تأثر الصراع العربي الإسرائيلي وعملية تسويته حيث فرض هذا التغير قيود على القدرة العربية في الوصول إلى تسوية تلبي الحد الأدنى من الحقوق الشرعية⁴.

وترتبط هذه القيود بالتفكير السوفيتي الجديد بالنسبة للسياسة الخارجية السوفيتية ككل، حيث يعتمد هذا التفكير على منهج براجماتي في تعامله مع معطيات النظام العالمي والمشكلات الإقليمية والدولية المعاصرة. ووفقاً لهذا التفكير أصبحت قضية التوصل إلى أرضية مشتركة للتفاهم مع الولايات المتحدة والانفتاح على الغرب والحد من سباق التسلح وتخفيف حدة التوتر على الصعيدين العالمي والإقليمي هي القضايا الحاكمة لجميع أبعاد السياسة الخارجية للاتحاد السوفيتي.

وقد انعكست هذه التوجهات الجديدة على سياسة الاتحاد السوفيتي تجاه الصراع العربي - الإسرائيلي بشكل مباشر وحاد حيث احتلت العلاقات الإسرائيلية - السوفيتية.

ثالثاً: بيغاسوس نموذج للحرب السيبرانية الاسرائيلية:

يعتبر "بيغاسوس" من أخطر برامج التجسس "وأكثرها تعقيداً"، وهو يستهدف بشكل خاص الأجهزة الذكية التي تعمل بنظام التشغيل "آي أو إس (iOS)" لشركة آبل، لكن توجد منه نسخة لأجهزة أندرويد تختلف بعض الشيء عن "آي أو إس".

— أوضحت شركة "كاسبرسكي- (Kaspersky)" المتخصصة في برامج الحماية من الفيروسات- أن "بيغاسوس" من نوع "البرامج الضارة المعيارية(modular malware)"، أي أنه مؤلف من وحدات، حيث يقوم أولاً بعملية "مسح (Scan)" للجهاز المستهدف، ثم يثبت الوحدة الضرورية لقراءة رسائل المستخدم وبريده الإلكتروني، والاستماع إلى المكالمات، والتقاط صور للشاشة، وتسجيل نقرات المفاتيح، وسحب سجل متصفح الإنترنت، وجهات الاتصال⁵.

⁴ — احمد يوسف، اوسلو كإطار للتسوية، في: احمد الرشيدى (محرر)، القضية الفلسطينية وأفاق التسوية، القاهرة، مركز البحوث والدراسات السياسية، 1998م، ص16-23.

⁵ — يخرق الهوايف المحملة.. حكاية برنامج التجسس الإسرائيلي "بيغاسوس" | أخبار الموسوعة | الجزيرة نت

كما أن بإمكان "بيغاسوس" الاستماع إلى ملفات الصوت المشفرة، وقراءة الرسائل المشفرة بفضل قدرته على تسجيل نقرات المفاتيح وتسجيل الصوت، حيث يسرق الرسائل قبل تشفيرها والرسائل الواردة بعد فك تشفيرها.

تعد شركة "أن أس أو" الإسرائيلية هي الشركة الأم المطورة لبرنامج "بيغاسوس". قام بتأسيس الشركة أشخاص عملوا سابقاً في الوحدة "8200"، إحدى أقوى أذرع الاستخبارات الإسرائيلية، التي يتركز عملها على التجسس على المؤسسات والأفراد حول العالم.

علاقة كبيرة تربط بين أصحاب الشركات الرائدة في مجال التكنولوجيا والوحدة "8200"، مع الإشارة إلى أن معظم المدراء في شركة "أن أس أو" هم من خريجي هذه الوحدة.⁶

المطلب الثاني : الحرب السيبرانية الاسرائيلية على الجزائر

الفرع الأول : التهديد الالكتروني الاسرائيلي على الجزائر

ولأنّ الحروب بعد التطور العلمي والتقني والتكنولوجي قد تطورت كثيراً ودخلنا في عصر الجليل الخامس من الحروب وهي الحروب السيبرانية الالكترونية، فإذا كان الهدف من الحرب العالمية الأولى 1914-1918 هو إسقاط الإمبراطورية الروسية وحكم عائلة رومانوف بالأساس⁷، وكان الهدف الرئيسي من إشعال فتيل الحرب العالمية الثانية 1939-1945 هو تقسيم ألمانيا وانتقال إدارة المعسكر الغربي الاستعماري من فرنسا وبريطانيا إلى أمريكا بينما كان من أهم أهداف الحرب الباردة هو إسقاط الاتحاد السوفياتي 1917-1990 وخلق نظام معولم أحادي القطبية قيادةً وتوجيهاً وسيطرةً، بينما الهدف من الجيل الرابع من الحروب وهي الحروب الناعمة وهي من أخطر أنواع الحروب وتعني احتلال الدّول والشعوب فكرياً وثقافياً ومعرفياً، بالإضافة إلى احتلالها اقتصادياً عن طريق تحكم الشركات الكبرى في

⁶ — ممدوح أنيس فتحي، القوة العسكرية المصرية واثر التحولات الاستراتيجية على الدور المصري الإقليمي، عبد العليم محمد (محرر)، تسوية الصراع العربي الإسرائيلي: دور مصر الإقليمي، القاهرة، مركز الدراسات السياسية والإستراتيجية بالأهرام، 1997م، ص 90-91.

⁷ — التقرير الاستراتيجي العربي 1995م، القاهرة، مركز الدراسات السياسية والاستراتيجية بالأهرام 1996م، ص 13.

الدول وإدارتها من خلف الستار وتحت غطاء نشر الديمقراطية وحقوق الإنسان والتدخل في شؤونها تحت يافطة محاربة الإرهاب العالمي التكفيري العابر للقارات، بينما أحدث أنواع الحروب وأخطرها وأكثرها ضرراً وتأثيراً من الناحية الأمنية والإستراتيجية على الدول فهي الحروب السيبرانية أو الالكترونية والتي تستطيع من خلالها شل الأنظمة التكنولوجية والتقنية والالكترونية والصحية وإحداث أضرار بالغة بالبنية التحتية لدول وإعاقتها اقتصادياً عن طريق التلاعب بالبورصات الوطنية وسرقة البطاقات الائتمانية والحسابات المصرفية وبدأت هذه الحروب وتطورت بشكل مهول منذ سنة 2005 وكان لظهور منظمة أنونيمس القبعات البيضاء دور فعال وبارز في إشعالها ونقلها إلى مختلف دول العالم، وعملت أجهزة الاستخبارات العالمية والغربية على توظيف جيوش من التقنيين وخبراء تكنولوجيا التجسس والاختراق والقرصنة الالكترونية لاعتراضها ومحاولة تفكيكها وفك شفراتها لما كانت تسببه لدول الكبرى من ضرر بالغ انتقاماً لفقراء والقضايا العادلة في العالم ومنها القضية المركزية عربياً وإسلامياً ألا وهي القضية الفلسطينية⁸.

هذه القضية التي بقيت بدون حل رغم مرور أكثر من 65 سنة على احتلال واغتصاب أرض عربية طاهرة رغم كل الجهود التي بذلتها عدة دول عربية وعلى رأسها الجزائر من أجل حلها نهائياً وإعادة كافة الحقوق المسلوقة إلى الشعب الفلسطيني صاحب الحق الشرعي والتاريخي في كل شبر منها، فالمواقف الجزائرية الثابتة اتجاهها جعلتها محل استهداف مركز ودائم من طرف المنظومة الغربية الصهيونية التي حاولت بكل الأساليب والوسائل التأثير على القرار السيادي الجزائري لإدخالها ضمن منظومة التسوية والتطبيع، وكان للحرب السيبرانية الالكترونية دور كبير في تفعيل منظومة الصراع العربي الإسرائيلي، فدولة بني صهيون التي عملت المستحيل من أجل اختراق الجزائر والتجسس عليها جندت خبراء المؤساد وضباط الوحدة 8200 التي تعتبر وحدة النخبة الالكترونية في الجيش الصهيوني والمسئولة عن رسم الإستراتيجية الدفاعية والهجومية في هذا المجال لوزارة الدفاع الإسرائيلية، وتشكيل وحدة متخصصة في الحرب الالكترونية اسمها "وحدة الدفاع الالكتروني" وذلك طبقاً لما قاله أوفري آفي رئيس قسم المواقع الالكترونية التابعة لحكومة الإسرائيلية والتي تتعرض مواقعها لعدة هجمات تصل إلى المئات

⁸ — عميرة أيسر، الحروب السيبرانية بين الجزائر و إسرائيل، نقلا عن الموقع: <https://www.raialyoum.com>

يوميًا لحمايتها،فإسرائيل التي باتت توجّه مجموعة من أقمارها الاصطناعية باتجاه الجزائر والدول العربية وهذه الأقمار الفضائية المرتبطة بأنظمة توجيه واتصال تخضع لقيادة الأركان العامة الصهيونية لتجسّس على المواقع الدّفاعية والجوية الجزائرية ومواقع إطلاق الصواريخ ومحاولة التسلل لأنظمتها من أجل التحكم بها أو إتلافها ومنها منظومة أقمار “أفق” والتي يصل عددها حالياً لتسعة أقمار تجسّسية. إذ تمّ إطلاق أفق 8 بتاريخ 21 كانون الثاني 2008 من قاعدة صواريخ هندية وهو ذو قدرة تجسّسية ودقة عالية تصل إلى القدرة على التّمييز من مسافة 10 سنتم،بالإضافة لقمر أفق 9 والذي تمّ إطلاقه بتاريخ 22 حزيران 2010 من قاعدة بلماشيم الجوية⁹، وهو يحمل مستشعرات التصوير المرئي والحراري،بالإضافة إلى سلسلة أقمار آموس AMOS التي تأخذ طابعاً مدنياً ولكنه تجسّسيّ بحت،وبعض هذه الأقمار تقوم برصد كل حركة صغيرة أو كبيرة في الجزائر وعلى مدار السّاعة،فإسرائيل التي أصبحت تخاف من تنامي القدرات الجزائرية الأمنية وتطور ترسانتها العسكرية باعتبار أنّ الجزائر تمتلك الجيش الثاني عربياً من حيث الجهوزية القتالية وتطور المعدات العسكرية و27 عالمياً وذلك من خلال بحث أجراه الموقع المتخصص “غلوبال فاير باوزر” سنة 2015،والذي يعتبر من أهم المؤسسات البحثية الأمنية المتخصصة في تصنيف الجيوش العالمية ودراسة تطور قدراتها الدّفاعية والهجومية سنوياً،بالإضافة إلى أنّ لإسرائيل قواعد وفرق تجسّسية سيبرانية على الحدود المغربية وهذا ما كشفت عنه الموقع الفرنسي awdnews وذلك في إطار حديثه عن التعاون الصهيوني المغربي في عدّة مجالات ومنها الحروب التجسّسية الالكترونية على الجزائر،وكشف الموقع عن وثيقة موجهة لمسؤولين مغاربة بتاريخ 28 يوليو 2008 فيها تفاصيل دخول مسؤولين صهاينة إلى المغرب منهم نائب رئيس ومدير شركة Nos marketing وذلك لاستكمال زرع معدات الاستماع والرصد الالكتروني مع الجارة الشرقية للمغرب أي الجزائر¹⁰.

-بالمقابل فإنّ الجزائر التي أصبحت تمتلك أنظمة تكنولوجية والكترونية متطورة استطاعت بفضلها صدّ العديد من الهجمات الالكترونية التجسّسية عليها والتي استهدفت مواقع أمنية عالية الحساسية منها مقر وزارة الدّفاع الوطني وهيئة قيادة الأركان ومقر رئاسة الجمهورية ومقر قيادة القوات الجوية وغيرها،بل

⁹ — مجلة المجلة، العدد 1017، 1999م.

¹⁰ — المرجع نفسه.

وانتقلت من الدّفاع إلى وضعية الهجوم عن طريق استعمال الطائرات بدون طيار والتي حلقت فوق القدس وعدّة مناطق في فلسطين المحتلة وأصابت الصهاينة بموجة من الذُّعر والهلع الغير متوقعة ¹¹، ومنها الهجمات التي استهدفت مواقع عبرية سنة 2012 واستطاعت المخابرات الجزائرية بفضلها أن تصل إلى مئات الوثائق والمعلومات السّرية عن وحدات الجيش الصهيوني وأسماء ضباط الموساد وحسابات لرجال أعمال صهاينة ومئات الأسماء لبطاقات ائتمانية صهيونية، ورغم أن أجهزة الأمن الجزائرية لم تعلن عن مسؤوليتها عن تلك العملية، ولكن طبيعة المهام وعدد الجزائريين المشاركين فيها ونوعية التقنيات العالية وتوقيت تلك الهجمات تدلُّ دلالةً قطعية على أنها لم تكن لتتمّ دون تنسيق عالٍ مع أجهزة المخابرات والأمن الوطنية، وكان لتفكيك وحدة الموساد في غرداية المتخصصة في التجسس المعلوماتي والإلكتروني قبل مدّة أثرٌ بالغ في كشف المخططات الصهيونية والحرب الالكترونية على الجزائر أو جزء منها على الأقل، ورغم كل ما ترصده دولة الكيان العبري الغاصب من مليارات الدولارات سنوياً من أجل استهداف الجزائر إلكترونياً وتكوينها لآلاف الشباب الصهيوني عبر مختلف دول العالم لكي يصبحوا خبراء في الحروب السيبرانية لتجسّس على منظومة الدّول التي تعادي إسرائيل ومنها الجزائر ورغم مشاركة بعض السيّانيم في الجزائر وخارجها في هذه الحرب الافتراضية والتي لها أهمية قصوى في عصرنا الحديث. ولكن فشلت رغم كل الإمكانيات الموهلة المخصصة لها في معرفة أدقّ الأسرار عن المنظومة العسكرية الجزائرية وخططها الإستراتيجية في حل نشوب حروب صلبة مادية ضدّها في المستقبل.

الفرع الثاني: الارهاب الالكتروني و التهديدات على الأمن الجزائري

تشهد الساحة الأمنية الجزائرية كغيرها من الدول العديد من المخاطر والتهديدات التي فرضتها الثورة التكنولوجية الحديثة، خاصة بعد انتشار وسائل التواصل الاجتماعي والعديد من المواقع الالكترونية التي تحمل أفكارا هدامة تهدد استقرار الوطن ووحدته، وتدعو الى نشر الفوضى والعنف والتطرف والكراهية والانقسام. ومن أهم المخاطر التي تترتب عن استخدام التكنولوجيا الحديثة على الأمن الجزائري الإرهاب

¹¹ — لمزيد من التفاصيل، ينظر: عزمي عاشور، "موريتانيا وإسرائيل علاقات دبلوماسية"، مجلة السياسة الدولية، القاهرة،

الأهرام، عدد 139، يناير 2000م، ص 145-147. بدر حسن شافعي، "سياسة مصر الخارجية تجاه أفريقيا والأحادية

القطبية"، مجلة السياسة الدولية، القاهرة، الأهرام، عدد 139، يناير 2000م، ص 117

الإلكتروني، ويقصد به " العدوان أو التخويف أو التهديد ماديا أو معنويا باستخدام الوسائل الإلكترونية الصادر من الدول أو الجماعات أو الأفراد على الإنسان في دينه، أو نفسه، أو عرضه¹²، أو عقله، أو ماله، بغير حق بشتى صنوفه وصور الإفساد في الأرض"، ويعتبر أحد أخطر التهديدات التي تستهدف أمن جميع الدول بما في ذلك الدولة الجزائرية، وهذا ما أكده القائد العام للدرك الوطني الجزائري في كلمة له ألقاها بمناسبة افتتاح الندوة الدولية حول "الأمن السيبراني"، حيث قال: "إن الإرهاب الإلكتروني بات من أخطر الجرائم التي تستهدف الجزائر، من خلال تنامي مظاهر الترويج لكل أشكال العنف والإرهاب والتطرف، باستعمال أحدث التقنيات التكنولوجية خاصة شبكات التواصل الاجتماعي والمنديات الإلكترونية". ولذلك دعا إلى إطلاق خلايا أمنية متخصصة هدفها العمل على "تعزيز إجراءات الرقابة لحماية المواطن الجزائري، وخاصة عنصر الشباب، من مثل هذه الجرائم الإلكترونية الخطيرة جداً على استقرار البلاد". وذلك من خلال قيامها بتعقب وملاحقة كل الأنشطة المتعلقة بالتجنيد للإرهاب والإجرام المنظم العابر للحدود، وتكييفها بالوسائل التكنولوجية العصرية". وذلك يتطلب حسب ضرورة "التسلح بكل الوسائل التكنولوجية والفعالة لمحاربة إيديولوجيات العنف والتطرف وكل أشكال الجريمة المنظمة والعابرة للأوطان، 26من خلال اعتماد آليات عملية للتعاون بين كل الشركاء الفاعلين في هذا المجال".

ومن أهم المواقع الإلكترونية التي تدعو إلى التعبئة والتجنيد والدعوة إلى الانضمام إلى التنظيمات الإرهابية مايلي¹³: موقع النداء :وهو الموقع الرسمي لتنظيم القاعدة بعد أحداث الحادي عشر من سبتمبر عام 2001م، ومن خلاله تصدر البيانات الإعلامية للقاعدة. ذروة السنام :وهي صحيفة إلكترونية دورية للقسم الإعلامي لتنظيم القاعدة. صوت الجهاد :وهي مجلة نصف شهرية، يصدرها ما يسمى بتنظيم القاعدة في جزيرة العرب، وتتضمن مجموعة من البيانات والحوارات مع قادة التنظيم ومنظريه. البتار: وهي

¹² — أيسر محمد عطية، دور الآليات الحديثة للحد من الجرائم المستحدثة، الإرهاب الإلكتروني و طرق مواجهته، ورقة

مقدمة في الملتقى العلمي، الجرائم المسحذة في ظل التحولات و المتغيرات الاقليمية و الدولية، خلال الفترة 02-04 سبتمبر ، 2014، ص 09.

¹³ — إيهاب شوقي، الإرهاب الإلكتروني و جرائمه، من الموقع :

(<http://www.anntv.tv/new/showsubject.aspx?id=121062> .ت.ن) تم تصفحه يوم يوم 28-01-2022.على الساعة 18.30.

مجلة عسكرية إلكترونية متخصصة، تصدر عن تنظيم القاعدة، وتختص بالمعلومات العسكرية والميدانية والتجنيد .

أما التنظيم الإرهابي "داعش" فله أزيد من 50 ألف موقع إلكتروني، 90 ألف صفحة باللغة العربية على موقع التواصل الاجتماعي «فيس بوك»، و40 ألفاً بلغات أخرى، وهذا ما ساهم في تجنيده حوالي 3400 شاب شهرياً عبر حملاته الإلكترونية، وهذا حسب تقرير للخبير الأمني في قضايا الإرهاب الرقمي جيف باردين .

ورغم الخطورة الكبيرة التي تخلفها مثل هذه المواقع الإلكترونية على أمن واستقرار المجتمعات، إلا أن تأثيرها على المجتمع الجزائري كان قليلاً. فقد كشف السيد محمد عيسى وزير الشؤون الدينية والأوقاف، أن التجنيد الإلكتروني لداعش في الجزائر عن طريق شبكة الأنترنت ومواقع التواصل الاجتماعي لم يتجاوز 100 ، وهو رقم ضئيل إذا ما قورن بعدد المجندين في دول عربية أخرى. 29 شاب جزائري ويمكن تبرير ذلك بنتائج العشرية السوداء التي عاشها الجزائريون نهاية القرن الماضي، وكذا التحصن الجزائري ضد الفكر التطرفي العابر للحدود، إضافة إلى الفشل الذريع الذي منيت به ما يعرف بثورات الربيع العربي، والذي كان له تأثير كبير على ضرورة البحث عن آليات أخرى للتغيير السلمي في المجتمعات بعيداً عن العنف والتطرف بشتى أشكاله.

ولذلك فالإنترنت يجب أن تبقى فضاء لنشر و مشاطرة العلوم و المعرفة و أداة للإبداع و التقارب و التعاون بين الأفراد و الشعوب و الدول، وليس وسيلة وأداة تهديدية تستغلها الجماعات الارهابية من أجل بلوغ أهدافها الاجرامية ونشر أفكارها التطرفية، كما أشار إلى ذلك السيد وزير الشؤون المغاربية و الاتحاد الإفريقي و جامعة الدول العربية، السيد: عبد القادر مساهل في كلمته خلال أشغال الورشة الدولية حول دور الإنترنت و الشبكات الاجتماعية في مكافحة التطرف و الإرهاب الإلكتروني و الوقاية منهما .

ولعل من أهم الأسباب المؤدية إلى بروز ظاهرة الإرهاب الإلكتروني مايلي¹⁴:

¹⁴ – Gabriel weimann ,cyberterrorism : how real the threat ?united states institute of peace
December 2004.P12.

-ضعف بنية الشبكات المعلوماتية وقابليتها للاختراق: إن شبكات المعلومات مصممة في الأصل بشكل مفتوح دون قيود أو حواجز أمنية عليها، رغبة في تسهيل دخول المستخدمين، وتحتوي الأنظمة الإلكترونية والشبكات المعلوماتية على ثغرات معلوماتية، ويمكن للمنظمات الإرهابية استغلال هذه الثغرات في التسلل إلى البنى المعلوماتية التحتية، وممارسة العمليات التخريبية والإرهابية .

_____ عدم وضوح الهوية الرقمية للمستخدم يجعل الفرصة سانحة للإرهابيين، حيث يستطيع محترف الحاسوب أن يتخفى تحت شخصية وهمية، ويشن بالتالي هجومه الإلكتروني بعيدا عن مراقبة السلطات العامة - .سهولة استخدام شبكة المعلومات وقلة التكلفة: مما هيا للإرهابيين فرصة ثمينة للوصول إلى أهدافهم غير المشروعة دون الحاجة إلى مصادر تمويل ، فشن هجوم إرهابي إلكتروني لا يتطلب أكثر من جهاز حاسب آلي متصل بالشبكة المعلوماتية ومزود بالبرامج اللازمة، فصعوبة الإثبات تعتبر من أقوى الدوافع المساعدة على ارتكاب جرائم الإرهاب الإلكتروني؛ لأنها تساعد المجرم على الإفلات من العقوبة¹⁵.

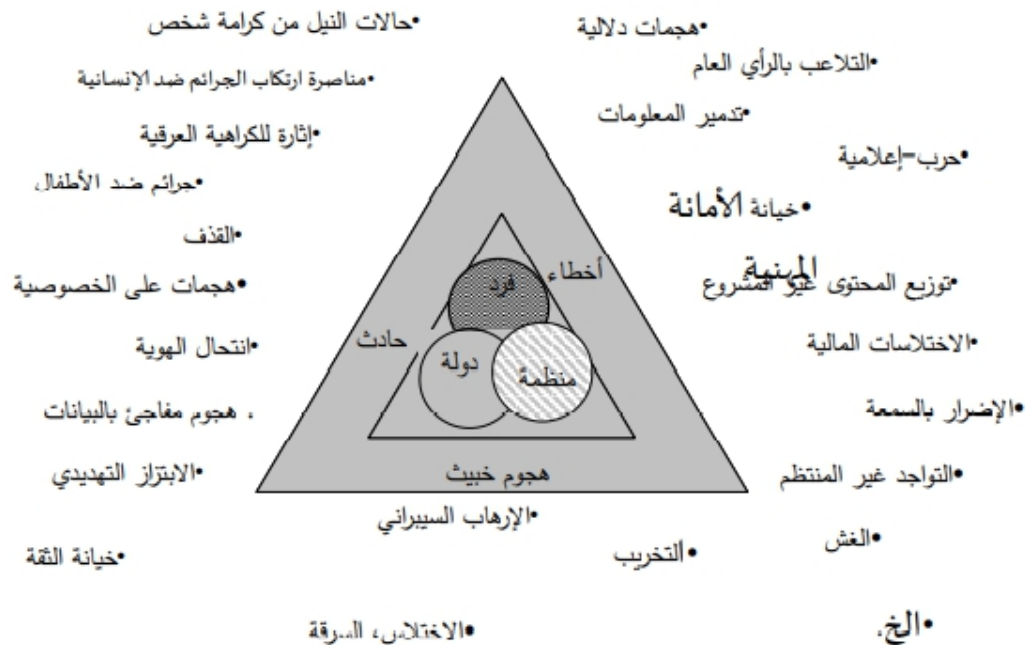
-صعوبة اكتشاف وإثبات الجريمة الإرهابية: خاصة في مجال جرائم الاختراق، مما يساعد الإرهابي على الحركة بحرية داخل المواقع التي يستهدفها قبل أن ينفذ جريمته

_____ الفراغ التنظيمي والقانوني وغياب السيطرة والرقابة على الشبكات المعلوماتية، ولجوء المجرم الإرهابي إلى دول معادية لشن هجومه على الدول الأخرى .كل هذه الأسباب شجعت على انتشار ظاهرة الإرهاب الإلكتروني التي أصبحت الوسيلة المثلى في العمل الإجرامي للتنظيمات الإرهابية المختلفة .

ولا تقتصر التهديدات السيبرانية على قضية الإرهاب الإلكتروني فقط، وإنما تشمل العديد من المخاطر والتهديدات الأخرى التي لا ترتبط بأمن الدول فقط، بل تشمل المجتمع 32كل، فهي متعلقة بأمن الأفراد والمنظمات أيضا، والشكل التالي يوضح ذلك:

¹⁵ _ .عبدالله بن عبدالعزيز بن فهد العجلان، "الإرهاب الإلكتروني في عصر المعلومات" بحث مقدم إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت"، والمنعقد بالقاهرة في 2-4 جوان 2008.

الشكل 1: يوضح مستويات الأمن السيبراني



المصدر: المصدر: الاتحاد الدولي للاتصالات، دليل الأمن السيبراني للبلدان النامية. جنيف: مكتب تنمية الاتصالات، 2009، ص 08

أمام التهديدات والمخاطر المتزايدة التي تخلفها استخدام التكنولوجيا الحديثة في الجزائر فقد بات لزاما اعتماد سياسة أمنية وطنية تضع مسألة توفير الأمن السيبراني على رأس أولوياتها واستراتيجياتها، وذلك من خلال البحث عن آليات وميكانيزمات فعالة يمكن من خلالها إدارة مختلف الحروب السيبرانية سواء باعتماد سياسات وقائية أحيانا أو سياسات علاجية في أحيان أخرى. وقبل التطرق إلى مختلف الجهود الجزائرية في مجال تحقيق الأمن السيبراني لابد بداية من توضيح الترتيب العالمي للجزائر حسب الرقم القياسي العالمي للأمن السيبراني، حيث احتلت الجزائر المرتبة 23 عالميا من أصل 29 مرتبة في مستوى التأهب في مجال الأمن 33 السيبراني، كما هو موضح في الجدول التالي:

الفصل الثاني: تجليات الحرب السيبرانية المبحث الأول : الكيان المحتل و تجليات الحرب السيبرانية

الجدول رقم 1: جدول يوضح الترتيب العالمي للدول حسب الرقم القياسي العالمي للأمن السيبراني.

الترتيب العالمي	الرقم القياسي	البلد
1	0.824	الولايات المتحدة الأمريكية
2	0.794	كندا
3	0.765	استراليا
3	0.765	ماليزيا
3	0.765	عمان
4	0.735	نيوزيلندا
4	0.735	النرويج
6	0.676	اسرائيل
7	0.647	تركيا
8	0.618	قطر
9	0.588	مصر
9	0.588	فرنسا
10	0.559	المغرب
11	0.529	تونس
14	0.441	السودان
17	0.353	الإمارات العربية المتحدة
19	0.294	البحرين
19	0.294	إيران
19	0.294	ليبيا
19	0.294	المملكة العربية السعودية
22	0.206	الأردن
23	0.176	الجزائر
23	0.176	بربادوس
23	0.176	بيلاروس
23	0.176	بليز
23	0.176	بنين
23	0.176	البوسنة والهرسك
23	0.176	بوتسوانا
23	0.176	ملاوي
23	0.176	سوريا
24	0.147	البهاما
24	0.147	موريتانيا
24	0.147	دولة فلسطين
25	0.118	بوروندي
25	0.118	كمبوديا
26	0.088	لبنان
27	0.059	هايتي
28	0.029	العراق
28	0.029	الصومال
29	0.000	هندوراس
29	0.000	ليسوتو

المصدر: المصدر: الاتحاد الدولي للاتصالات، تقرير حول الرقم القياسي العالمي للأمن السيبراني وسمات السلامة السيبرانية. جنيف: الاتحاد الدولي للاتصالات، مكتب تنمية الاتصالات، أبريل 01-06 ص ص، 2015.

أما على المستوى العربي فقد احتلت الجزائر المرتبة العاشرة حسب التزامها بتلك التدابير التي يحددها الرقم القياسي العالمي للأمن السيبراني، والشكل التالي يوضح ترتيب مختلف بلدان منطقة الدول العربية.

الفصل الثاني: تجليات الحرب السيبرانية المبحث الأول : الكيان المحتل و تجليات الحرب السيبرانية

الجدول رقم2: يوضح ترتيب بلدان منطقة الدول العربية حسب الرقم القياسي العالمي للأمن السيبراني.

الدول العربية	قانونية	تقنية	تنظيمية	بناء القدرات	التعاون	الرقم القياسي	الترتيب الإقليمي
عُمان	0.7500	0.6667	1.0000	0.7500	0.6250	0.7647	1
قطر	0.7500	0.8333	0.5000	0.6250	0.5000	0.6176	2
مصر	0.5000	0.5000	0.3750	1.0000	0.5000	0.5882	3
المغرب	0.5000	0.6667	0.7500	0.5000	0.3750	0.5588	4
تونس	1.0000	0.5000	0.6250	0.2500	0.5000	0.5294	5
السودان	0.7500	0.5000	0.5000	0.2500	0.3750	0.4412	6
الإمارات العربية المتحدة	0.7500	0.3333	0.2500	0.5000	12.50	0.3529	7
البحرين	0.7500	0.1667	0.1250	0.3750	0.2500	0.2941	8
ليبيا	0.2500	0.3333	0.3750	0.1250	0.3750	0.2941	8
المملكة العربية السعودية	0.7500	0.3333	0.1250	0.3750	0.1250	0.2941	8
الأردن	0.5000	0.0000	0.5000	0.0000	0.1250	0.2059	9
الجزائر	0.7500	0.0000	0.0000	0.1250	0.2500	0.1765	10
سوريا	0.2500	0.3333	0.1250	0.1250	0.1250	0.1765	10
موريتانيا	0.2500	0.1667	0.2500	0.0000	0.1250	0.1471	11
دولة فلسطين	0.2500	0.0000	0.3750	0.1250	0.0000	0.1471	11
لبنان	0.0000	0.0000	0.0000	0.2500	0.1250	0.0882	12
جيبوتي	0.2500	0.0000	0.0000	0.0000	0.1250	0.0588	13
الكويت	0.0000	0.0000	0.0000	0.1250	0.1250	0.0588	13
اليمن	0.2500	0.0000	0.0000	0.0000	0.1250	0.0588	13
جزر القمر	0.0000	0.0000	0.0000	0.0000	0.1250	0.0294	14
العراق	0.0000	0.0000	0.0000	0.0000	0.1250	0.0294	14
الصومال	0.0000	0.0000	0.0000	0.1250	0.0000	0.0294	14

المصدر: الاتحاد الدولي للاتصالات، تقرير حول الرقم القياسي العالمي للأمن السيبراني وسمات السلامة السيبرانية. المرجع السابق الذكر، ص 11.

من خلال هذا الجدول يمكن القول أن الجهود الجزائرية في مجال تحقيق الأمن السيبراني تبقى ضئيلة، حيث تركزت أساسا في مجال اتخاذ التدابير القانونية دون غيرها من التدابير الأخرى، ويتضح ذلك من خلال صدور القانون رقم 04-09 المؤرخ في 05 أوت 2009 ، الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والتي تم فيه تحديد الحالات التي تسمح باللجوء إلى مراقبة الاتصالات الإلكترونية³⁵ بناء على ما ورد في المادة 4 التي نصت على مايلي¹⁶:

¹⁶ — وفاق العياشي، مكافحة الإرهاب بين السياسة و القانون، الجزائر :دار الخلدونية للنشر و التوزيع، 2006، ص 31.

- _____ للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة
- _____ في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني
- _____ لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية
- _____ في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة. كما نصت المادة 13 على إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وهذا ما تم من خلال صدور المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر سنة 2015، والذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. ومن المهام التي تمارسها الهيئة ما ورد في المادة 4 من المرسوم والتي نصت على مايلي¹⁷:
- _____ اقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها
- _____ تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- _____ -مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بما في ذلك من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية
- _____ ضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة تحت سلطة القاضي المختص وباستثناء أي هيئات وطنية أخرى

¹⁷ - المرجع نفسه.

_____ تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية

_____ السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها

_____ تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال . _____ المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيات الإعلام والاتصال

_____ المساهمة في تحديث المعايير القانونية في مجال اختصاصها.

وإضافة إلى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، فقد أنشأت الجزائر هيئات أخرى تضطلع بأدوار جد هامة في مواجهة مختلف 37 الجرائم الالكترونية.

المطلب الثالث: مظاهر تهديد الارهاب الالكتروني لأمن الدول:

تفاقمت ظاهرة الإرهاب الالكتروني في الآونة الأخيرة وأثرت سلبا على أمن الدول في مختلف الميادين، حيث تستطيع الجماعات والمنظمات الإرهابية من خلال الضغط على لوحة المفاتيح تدمير البنية المعلوماتية، وتحقيق آثار تدميرية تفوق الآثار التي استخدمت فيها المتفجرات، مما يلحق أضرارا بالمؤسسات المالية، وأجهزة الاتصال والبنى التحتية والمؤسسات الحكومية وغيرها من الكيانات التي تعتمد بشكل كبير على شبكة الانترنت، والذي يؤدي بدوره إلى تعطيل المحركات الرئيسية للدولة والإضرار بمواطنيها وأمنها القومي. ومن تداعيات الإرهاب الالكتروني على أمن الدول ما يلي¹⁸:

¹⁸ _____ 1 الإرهاب الالكتروني ... هل يتحول إلى مصدر التهديد الأول في العالم، من الموقع <http://alkhaleejonline.net/articles/1430728333185670700/> الإرهاب-الالكتروني-هل-يتحول-لمصدر-التهديد-

الفرع الأول :تهديد أمني سياسي :

تعمل المنظمات الإرهابية على إلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات، أو قطع شبكات الاتصال بين الوحدات والقيادات المركزية ، أو تعطيل أنظمة الدفاع الجوي، أو إخراج الصواريخ عن مسارها. مما يهدد أمن الدول ، كما تهدد شخصيات سياسية بارزة¹⁹.

في المجتمع بالقتل ، أو بالقيام بتفجير منشآت وطنية، أو بنشر فيروسات من أجل إلحاق الضرر والدمار بالشبكات المعلوماتية والأنظمة الإلكترونية ، إضافة لاختراق البريد الإلكتروني لرؤساء الدول وكبار الشخصيات السياسية وهناك أسرارهم والإطلاع على معلوماتهم وبياناتهم والتجسس عليها لمعرفة مراسلاتهم ومخاطباتهم والاستفادة منها في عملياتهم الإرهابية، أو تهديدهم لحملهم على إتيان أفعال معينة يخططون لاقتوافها.

مثلا في إيطاليا عام 1998م تعرضت عدة وزارات وجهات حكومية ومؤسسات مالية لهجوم من جماعات الألوية الحمراء عن طريق تدمير مراكز المعلومات الخاصة بها²⁰، وفي عام 2010 ظهر ما عُرف باسم "إعصار ويكيليكس" إذ تم استغلال شبكة الإنترنت العالمية في تسريب وثائق تحوي معلومات سرية للغاية مُتداولة بين الإدارة الأمريكية وقنصلياتها الخارجية بدول العالم، وفي مارس 2014 هاجمت مجموعة "ساير بيركوت" الأوكرانية المواقع الإلكترونية لحلف الناتو، ما أدى إلى تعطيل مواقع الحلف لعدة ساعات". كما أعلن الكرملن أن قراصنة حاسوب شنوا هجوماً "عنيفاً" على موقع الرئاسة الروسية، وعطلوا العمل بموقع البنك المركزي الروسي. وأقر مفتش وحدة الجرائم الإلكترونية الأمريكي في أوت 2014، بأن قراصنة أجنبية تمكنوا من اختراق حاسبات تابعة للهيئة الأمريكية لتنظيم الأنشطة النووية مرتين على الأقل خلال السنوات الثلاث الماضية ومؤخراً أكدت صحيفة نيويورك تايمز في تقرير لها في 26 إبريل 2015 أن قراصنة روسيين اطلعوا على رسائل إلكترونية للرئيس الأمريكي باراك أوباما العام الماضي، بعدما تمكنوا من اختراق الشبكة الإلكترونية غير السرية للبيت الأبيض، واطلعوا على أرشيف

¹⁹ عبدالله بن عبدالعزيز بن فهد العجلان، مرجع سبق ذكره ،ص22.

²⁰ — المرجع نفسه

الرسائل الإلكترونية لموظفين في البيت الأبيض يتواصلون يومياً مع أوباما، ومن خلال هذا الأرشيف تمكن القراصنة من قراءة رسائل تلقاها أوباما وهذا ما يهدد الأمن القومي الأمريكي²¹.

أما أمنياً تعمل الجماعات الإرهابية على التسلل الإلكتروني إلى الأنظمة الأمنية في دولة ما وشلها لصالحها ، وفك الشفرات السرية للتحكم بتشغيل منصات إطلاق الصواريخ الإستراتيجية، والأسلحة الفتاكة، وتعطيل مراكز القيادة والسيطرة العسكرية ووسائل الاتصال للجيش بهدف عزلها عن قواتها، والنفوذ إلى النظم العسكرية واستخدامها لتوجيه الجنود إلى نقطة غير آمنة قبل قصفها أو تفجيرها.

· الفرع الثاني: تهديد اقتصادي:

اختراق النظام المصرفي وإلحاق الضرر بأعمال البنوك وأسواق المال العالمية، وتعطيل عمليات التحويل المالي، مما يلحق الأذى بالاستثمار الأجنبي وبالثقة بالاستثمار عامة، وإلحاق الأذى بالاقتصاد الوطني، وتعديل ضغط الغاز عن بُعد في أنابيب الغاز لتفجيرها، ونظم السلامة في المصانع الكيماوية لإحداث أضرار بالناس، ومن أمثلتها قيام بعض الإرهابيين بتحويل ملايين الدولارات من بعض الحسابات الشخصية لكبار العملاء بعد اختراق نظام التحويلات الدولي بين البنوك، وقيام بعض الهاكرز المحترفين بسرقة بيانات بطاقات الائتمان من بعض أكبر مراكز التسوق الإلكتروني الدولية وخصم ملايين الدولارات من أصحاب تلك البطاقات، وكذلك قيام بعض المنظمات الإرهابية بالعمل على تدمير اقتصاد إحدى دول الشرق الأوسط بشراء سندات دولية لتلك الدولة من داخلها عبر البورصات العالمية وبيعها بالخارج بأسعار أقل من قيمتها مما أدى لإنهيار عملتها ... ولتوفير تمويل لأعمالها الإرهابية في الدول التي تم بيع السندات فيها كما منيت عدد من الشركات والمصارف العملاقة بخسائر اقتصادية فادحة نتيجة القرصنة الإلكترونية التي واجهتها. فحسبما أشارت أحدث دراسة أجرتها مؤسسة²² (B2B International) وشركة كاسبرسكي لاب، والتي أعلنت عنها في الخامس عشر من أبريل 5201 فإن 25 % من الشركات في منطقة الخليج تعتبر هجمات (DDoS) أحد أكبر ثلاثة تهديدات تواجه الشركات في المنطقة.

²¹ — رائد العدوان ،"المعالجة الدولية لقضايا الإرهاب الإلكتروني"، محاضرة أقيمت في دورة تدريبية بعنوان توظيف شبكات التواصل الاجتماعي في مكافحة الإرهاب ،الرياض، فيفري 2016، ص ص 09-10.

²² — نوران شفيق، أثر التهديدات الإلكترونية على العلاقات الدولية، (القاهرة: المكتب العربي للمعارف

،2015)، ص.108.

وباعتبارها أحد أهم التقنيات الشائعة التي يستخدمها مجرمو الإنترنت لكسب الأموال، فإن عدد وتأثير هذه الهجمات يتزايد من عام لآخر وهو ما جعل قضية حماية المستخدمين أمراً أولوياً لدى الشركات. وقبل السادس من فبراير 2015، أكدت شركة "كاسيرسكي" الرائدة في مجال الأمن المعلوماتي أن مجموعة من "الهاكرز" تمكنوا من السيطرة على حسابات في مصارف عالمية، وسرقة نحو مليار دولار، إذ استخدموا تقنيات معقدة من أجل الوصول للحسابات، واستغل "الهاكرز" ثغرة بأنظمة أجهزة الحاسوب في المصارف تمكنوا خلالها من نسخ بيانات الحسابات في مدة لا تتجاوز 20 ثانية واستغلوها من أجل تحويل الأموال بسرعة فائقة²³.

الفرع الثالث: تهديد اجتماعي

يؤثر الإرهاب الإلكتروني على حياة المدنيين ورفاهيتهم وحتى ثقافتهم كالتالي: - توجه المنظمات الإرهابية رسائلها للإعلام والجمهور الخاص بالمجتمعات التي تقوم بترويعها وإرهابها، وذلك بهدف شن حملات نفسية ضد الدول العدو ، فهي تعرض أفلاماً مرعبة للرهائن والأسرى أثناء إعدامهم ، مما يؤثر على المدنيين²⁴.

- اختراق صفحة إلكترونية لمستشفى وتهديد حياة المرضى فيه عن طريق التلاعب بأنظمة العلاج عن بُعد بهدف قتل المرضى، وأيضاً في مصانع غذاء الأطفال لتغيير مستويات نسب المواد الغذائية بهدف قتل الأطفال.

- شن عمليات إرهابية على المواقع الحيوية، أو التحكم في خطوط الملاحة الجوية والبرية والبحرية، فمثلاً في يناير 2008 تم قطع الكابل البحري الذي يربط أوروبا بالشرق الأوسط والكابل القريب من ساحل دبي وخليج عمان، مما أدى إلى خسائر بقطاع الاتصالات والتعاملات الإلكترونية أو شل محطات إمداد الطاقة والماء، حيث تشير مصادر كلية الحرب الأميركية إلى أن ضرب مولدات الطاقة الكهربائية

²³ - رائد العدوان ، مرجع سابق.

²⁴ - مصطفى محمد موسى ، الإرهاب الإلكتروني دراسة قانونية - أمنية - نفسية - اجتماعية .(الأردن : دار الكتب والوثائق القومية ، ط.01 ، 2009) ص. 298.

العراقية أدى بشكل غير مباشر إلى موت ما بين 70 إلى 90 ألف مواطن عراقي كنتيجة مباشرة لعدم توفر الطاقة الكهربائية²⁵.

²⁵ — عبد الرحمن بن عبد الله السند، مرجع سبق ذكره. ص. 25.

المبحث الثاني: الموقف الداخلي و الدولي و استراتيجيات المواجهة

المطلب الأول: الجهود الدولية لمكافحة الإرهاب الإلكتروني

عملت وحدات المجتمع الدولي على اتخاذ عدة استراتيجيات لمكافحة الإرهاب الإلكتروني وتحقيق الأمن و الاستقرار.

الفرع الأول: الاستراتيجيات الدولية و الإقليمية

أصدرت الأمم المتحدة مجموعة من القرارات عبر جمعيتها العامة التي توضح مدى تصاعد الاهتمام العالمي باستخدام تكنولوجيا الاتصال والمعلومات استخداما غير سلمي ، ففي 22 نوفمبر 2002 اتخذت قرار بشأن التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي ، وفي ديسمبر من نفس السنة اتخذت قرار إرساء ثقافة عالمية لأمن الفضاء الإلكتروني واعتبر من القرارات الهامة التي استهدفت العمل على حماية البنية التحتية الحيوية للمعلومات وحث الدول والمنظمات الدولية والإقليمية على تكثيف التعاون الدولي لمجابهة الإرهاب الإلكتروني¹.

وفي 2004 تم إنشاء مجموعة الخبراء الحكومية GCE بهدف مناقشة الأخطار القائمة والمحتملة في مجال أمن المعلومات الدولي والإجراءات الممكنة لوضع الأسس الدولية التي تهدف إلى تقوية أمن نظم الاتصالات والمعلومات العالمية، كما شكل الأمين العام للأمم المتحدة كوفي عنان في 2004 فريقا دوليا لدراسة قضية إدارة الانترنت.

كما ساهمت مجموعة الدول الصناعية هي الأخرى في مجابهة الإرهاب الإلكتروني بإنشاء مجموعة فرعية للجريمة عالية التقنية وتبنت ما عرف بالمبادئ العشرة حول مكافحة جرائم الكمبيوتر ، وفي عام

¹ — حمدون تورية، البحث عن السلام السيبراني ، الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء، 2011، ص ص

2000 صدرت مسودة اتفاق عالمي حول مكافحة الإرهاب الإلكتروني من جامعة ستانفورد بهدف الوصول إلى تعاون دولي لمواجهة هجمات الفضاء الإلكتروني².

الفرع الثاني: الاستراتيجيات الدولية:

أنشأت الولايات المتحدة الأمريكية مؤسسة مركز حماية البنية الأساسية القومي ومقرها الدور 11 من مقر مكتب التحقيقات الفيدرالية ، بلغت ميزانية المركز 1.5 مليار دولار للإعداد والمنع والاكتشافات والاستجابة، أي ربط جميع شبكات الأمن الإلكتروني للمراقبة والإشراف، وأن تصبح

المخابرات الأمريكية ومجلس الأمن القومي متحدين في هدف مشترك مع مكتب التحقيقات الفيدرالية¹.

ولقد أصدرت المملكة العربية السعودية بعض الأنظمة واللوائح والتعليمات والقرارات لمواجهة الاعتداءات الإلكترونية والإرهاب الإلكتروني، ونصت تلك الأنظمة على عقوبات في حال المخالفة لهذه الأنظمة والتعليمات واللوائح، كقرار مجلس الوزراء رقم (163) في 24 10 1417هـ الذي ينص على إصدار الضوابط المنظمة لاستخدام شبكة الإنترنت والاشتراك فيها، ومن ذلك³:

1- الامتناع عن الوصول أو محاولة الوصول إلى أي من أنظمة الحاسبات الآلية الموصولة بشبكة الإنترنت، أو إلى أي معلومات خاصة، أو مصادر معلومات دون الحصول على موافقة المالكين، أو من يتمتعون بحقوق الملكية لتلك الأنظمة والمعلومات أو المصادر.

2- الامتناع عن إرسال أو استقبال معلومات مشفرة إلا بعد الحصول على التراخيص اللازمة من إدارة الشبكة المعنية.

3- الامتناع عن الدخول إلى حسابات الآخرين، أو محاولة استخدامها بدون تصريح.

² - بيتر غرابوسكي، جرائم الحاسب الآلي.. الأبعاد العالمية في: القيادة العامة لشرطة أبو ظبي.. شبكات الانترنت وتأثيراتها الاجتماعية والأمنية، مركز البحوث والدراسات الأمنية، القيادة العامة لشرطة أبو ظبي، 2006، ط ١، ص 338.

³ - منير محمد الجهيني، ممدوح محمد الجهيني، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها) الإسكندرية: دار الفكر العربي، ط (2004)، ص 96.

- 4- الامتناع عن إشراك الآخرين في حسابات الاستخدام، أو إطلاعهم على الرقم السري للمستخدم.
 - 5- الالتزام باحترام الأنظمة الداخلية للشبكات المحلية والدولية عند النفاذ إليها.
 - 6- الامتناع عن تعريض الشبكة الداخلية للخطر، وذلك عن طريق فتح ثغرات أمنية عليها.
 - 7- الامتناع عن الاستخدام المكثف للشبكة بما يشغلها دومًا، ويمنع الآخرين من الاستفادة من خدماتها.
 - 8- الالتزام بما تصدره وحدة خدمات (الإنترنت) بمدينة الملك عبد العزيز للعلوم والتقنية من ضوابط وسياسات لاستخدام الشبكة.
 - 9- نص القرار على تكوين لجنة دائمة برئاسة وزارة الداخلية وعضوية وزارات: الدفاع، والمالية، والثقافة والإعلام، والاتصالات وتقنية المعلومات، والتجارة، والشؤون الإسلامية، والتخطيط، والتعليم العالي، والتربية والتعليم، ورئاسة الاستخبارات، ومدينة الملك عبد العزيز للعلوم والتقنية، وذلك لمناقشة ما يتعلق بمجال ضبط واستخدام (الإنترنت) والتنسيق فيما يخص الجهات التي يراد حجبها، ولها على الأخص ما يأتي⁴:
 - أ - الضبط الأمني فيما يتعلق بالمعلومات الواردة أو الصادرة عبر الخط الخارجي للإنترنت والتي تتنافى مع الدين الحنيف والأنظمة.
 - ب- التنسيق مع الجهات المستفيدة من الخدمة فيما يتعلق بإدارة وأمن الشبكة الوطنية.
- وهذا القرار يبين مبادرة المملكة العربية السعودية وسعيها لتنظيم التعاملات الإلكترونية وضبطها.
- وفي مصر يجري العمل في وزارة الاتصالات والمعلومات لإصدار نظام عن الجريمة الإلكترونية، يتضمن عقوبات رادعة لمن يقوم من الأفراد أو المؤسسات بتزوير أو إفساد مستند إلكتروني على الشبكة، أو الكشف عن بيانات ومعلومات بدون وجه حق، وغيرها من صور الجريمة الإلكترونية. ففي 2002

⁴ - Lee Kam Hing and Tan Chee-Beng (editors), The Chinese in Malaysia (New York: oxford university Press, 2000). p150

صدر القرار الوزاري رقم 13507 بإنشاء إدارة لمكافحة جرائم الحاسوب وشبكات المعلومات ويساهم في مكافحة الإرهاب الإلكتروني⁵.

أما في الأردن فيجري العمل لإعداد تنظيم يتعلق بخصوصية المعلومات وسريتها، للمحافظة عليها في ظل التعاملات الإلكترونية عبر الشبكات العالمية للمعلومات، كما تساهم الأردن في إعداد مشروع حول قانون مكافحة جرائم تقنية المعلومات وما في حكمها، والمقدم إلى الإدارة العامة للشؤون القانونية في جامعة الدول العربية.

الفرع الثالث: معاهدة بودابست لمكافحة جريمة الانترنت و النموذج الماليزي

أولا : معاهدة بودابست:

تعد هذه الإتفاقية هي أولى الإتفاقيات العالمية المتعلقة بجرائم الانترنت، وقعت الإتفاقية في العاصمة المجرية بودابست في 23 نوفمبر 2001، بهدف التعاون والتضامن الدولي في محاربة الجرائم الإلكترونية⁶.

وقعت 26 دولة أوروبية على هذه الإتفاقية بالإضافة إلى الولايات المتحدة الأمريكية، كندا واليابان، جنوب أفريقيا.

وبالرغم من ان هذه الاتفاقية أوروبية المنشأ، إلا ان عضويتها مفتوحة لجميع الدول التي تريد الانضمام إليها لتعم الفائدة.

وعلى الرغم من أن هذه الإتفاقية لا تعالج الإرهاب السيبراني على وجه الخصوص، إلا أنها صيغت بطريقة قادرة على تتبع نطاق تهديدات الإرهابيين، لتشمل جريمة الإرهاب السيبراني.

⁵ Z. Yunos, R. Ahmad, S. M. Ali, and S. Shamsuddin, "Illicit Activities and Terrorism in -
Cyberspace : An Exploratory Study in the Southeast Asian Region," in Pacific Asia Workshop
on Intelligence and Security Informatics (PAISI 2012), Malaysia, 29 May, Springer Lecture
5. Notes in Computer Science, Volume 7299/2012, 2012, pp. 27-3

⁶ — أمن الفضاء الإلكتروني، الأمم المتحدة، مكتب مكافحة الإرهاب، على الرابط التالي:

<https://www.un.org/counterterrorism/ar/cybersecurity>

في عام 2016 أصدرت لجنة اتفاقية الجرائم السيبرانية مذكرةً توجيهية تتعلّق بجوانب الإرهاب السيبراني بموجب اتفاقية بودابست، تعلن فيها أن "الجرائم الموضوعية في الاتفاقية قد تكون أيضاً أعمالاً إرهابية على النحو المحدد في القانون المعمول به". وجاءت هذه المذكرة الإضافية بموجب الاتفاقية في الوقت المناسب، لتسلط المذكرة الضوء على أن هذه الاتفاقية ليست معاهدة مختصة بالإرهاب، إلا أنه يمكن القول: إن الجرائم الموضوعية في الاتفاقية يمكن أن تنفذ على أنها أعمال إرهابية، لتسهيل الإرهاب ولدعم الإرهاب، ومن ذلك الجانب التمويلي، أو الأعمال التحضير.

ثانياً: النموذج الماليزي في مكافحة الجريمة الالكترونية

تتعدد الجهود التي تبذلها الدول في مجتمع المعلومات العالمي من أجل العمل على تنظيم عملية وضع السياسات المثلى للتعامل مع الارهاب السيبراني من قبل الحكومات⁷.

قد اتجهت الدول إلى تبني العديد من المبادرات على المستوى الوطني أو الثنائي أو الاقليمي وذلك من أجل حماية البنية التحتية الكونية للمعلومات من خطر التعرض لمثل تلك الاخطار⁸.

ففي ظل التحولات الرقمية التي يعيشها العالم بوجه عام وماليزيا بوجه خاص ظهر نوع جديد من التهديدات الأمنية التي تعتبر البيئة الرقمية عاملاً هاماً في انتشارها، وقد أصبحت هذه التهديدات تمس ليس فقط أمن المؤسسات وإنما أمن الأفراد وبذلك تكون شكلت تحدياً للدولة في سعيها لتحقيق أمنها القومي.

وقد استمرت الدولة الماليزية في تطوير سياسات وبرامج تساعد في تعزيز أمنها السيبراني في إطار رؤية 2020.

ويجدر بالذكر أن الهدف من إطلاق رؤية ماليزيا 2020 هو أن تصبح دولة متقدمة واعتناق الاقتصاد القائم على المعرفة كوسيلة لتحقيق ذلك.

⁷ - Mohd Shamir b Hashim, Malaysia's National Cyber Security Policy: The country's cyber defence initiatives:
<https://ieeexplore.ieee.org/document/5978782>

⁸ - Neville, Spykerman, Malaysia second in world broadband penetration ranking, Monday, 28 Oct 2013
<https://www.thestar.com.my/news/nation/2013/10/28/broadband-penetration-muhyiddin-yassin>

ومن خلال الاختيار الواعي لاستخدام تكنولوجيا المعلومات والاتصالات كأداة للتنمية، فقد أدى ذلك إلى زيادة استخدام أنظمة المعلومات الرقمية في جميع أنحاء الصناعة والمنظمات الخاصة والعامة والمجتمع ككل.

ومما شك فيه إن الاعتماد على أنظمة المعلومات الرقمية يجلب معه نقاط الضعف والمخاطر المتزايدة، لا سيما للبنية التحتية للمعلومات الوطنية الحرجة (CNII) والتي تشمل من بين أمور أخرى الجرائم الإلكترونية مثل القرصنة والتطفل والاحتيايل والمضايقة والرموز الضارة وهجمات الحرمان من الخدمة، كل ذلك يزيد التهديدات السيبرانية التي تهدد السيادة الإلكترونية للدولة⁹.

تم إنشاء العديد من مواقع الانترنت لمكافحة الإرهاب السيبراني والأمن الرقمي، حيث أصبحت بمثابة مؤسسات فكرية وفنية لدعم الأمن الرقمي، وكانت تلك المواقع إما بمبادرة حكومية او من القطاع الخاص او من المجتمع المدني ، فضلا عن مواقع الشركات العاملة في تكنولوجيا الاتصال والمعلومات.

تعد ماليزيا إحدى الدول التي كثفت جهودها في هذا المجال منذ وقت مبكر، كونها دخلت المجتمع المعلوماتي في وقت متزامن مع العديد من دول العالم المتقدم، فقد تم تصنيفها من قبل الخبراء والمتخصصين في مرتبة متقدمة نظرا للإنجازات التي حققتها حتى الآن للإندماج في مجتمع المعلومات¹⁰.

منذ عام 1987 دخلت خدمة الانترنت إلى ماليزيا من قبل المعهد الماليزي للأنظمة الإلكترونية الدقيقة، وذلك من خلال مشروع رنجكوم Rangkom، الذي قام بربط عدة جامعات ماليزية في شبكة واحدة¹¹.

في عام 1991 تحول مشروع رنجكوم Rangkom إلى مزود خدمة يعرض خدماته لعدد محدود من العامة.

⁹ — عادل عبد الصادق، الفضاء الإلكتروني والعلاقات الدولية: دراسة في النظرية والتطبيق (القاهرة: الهيئة العامة للكتاب، 2018)، ص 485.

¹⁰ — المرجع نفسه.

¹¹ — ماليزيا تكثف جهودها لمكافحة الجرائم الإلكترونية، على الرابط التالي:

<https://aswaqpress.com/electronic-attacked-in-malaysia>

وفي عام 1992 تم إطلاق أول مزود ماليزي لخدمات الانترنت RARING، أطلقه المعهد الماليزي للأنظمة الإلكترونية الدقيقة¹².

حيث تفوقت ماليزيا على دول الاسيان بما في ذلك تايلاند التي جاءت في المرتبة الـ 13 وفيتنام التي جاءت في المرتبة الـ 14 والفلبين التي جاءت في المرتبة الـ 18 واندونيسيا جاءت في المرتبة العشرين¹³.

وقد ازداد ظهور أنشطة الإرهاب السيبراني بوضوح في ماليزيا في العقد الماضي، ورفعت دعاوى قضائية بموجب قانون العقوبات في البلاد وتصنف الأحكام تحت الرقم (ج-031) والرقم (ي-031) مختلف الأعمال المرتكبة في سياق الأعمال الإرهابية.

سعت الدولة الماليزية الى تكثيف جهودها الرامية إلى مكافحة الجرائم الإلكترونية أو استخدام الإنترنت لأغراض إرهابية، بما في ذلك تعزيز المرافق الأمنية للإنترنت وتشديد الرقابة على أنظمة التواصل الإلكتروني.

تضع ماليزيا الأمن السيبراني نصب أعينها وتحاول أن تكون نموذجاً لمنطقة آسيا والمحيط الهادي، حيث أنها تقدم ما يقرب من اثنتي عشرة خدمة تلبي احتياجات القطاع العام والقطاع الخاص ومستخدمي الانترنت.

تشريعات وقوانين مكافحة الارهاب السيبراني في ماليزيا

تعد ماليزيا واحدة من أولى الدول في جنوب شرق آسيا التي سنت قوانين وتشريعات الفضاء السيبراني، فهناك عدة قوانين وتنظيمات تبنتها الدولة الماليزية للتعامل مع الارهاب السيبراني والتي كان من أهمها¹⁴:

¹² نفس المرجع.

¹³ -Cybersecurity 2020:Chew Kherk Ying-

<https://practiceguides.chambers.com/practice-guides/cybersecurity-2020/malaysia>

W.Media, Malaysia wages war on cybercrime, Published 10 April¹⁴

2020: <https://w.media/malaysia-wages-war-on-cybercrime>

1. قانون جرائم الكمبيوتر عام 1997¹⁵ :

هو أول تشريع محدد على الإطلاق يتم في ماليزيا لمكافحة الجرائم الإلكترونية. يجرم عمل القرصنة ونشر الفيروسات على أجهزة الكمبيوتر والاتصال غير المشروع للوصول إلى أجهزة الكمبيوتر وارتكاب الجرائم الإلكترونية.

1. قانون التوقيع الرقمي عام 1997.

التوقيع الرقمي هو توقيع إلكتروني يستخدم للتحقق من هوية المرسل / الموقع للرسالة وأيضاً لضمان صحة المعلومات في المعاملات الإلكترونية، ويمكن أن يفي استخدام التوقيع الرقمي المعترف به بمتطلبات السرية ، ومصادقة الهوية، وعدم التنصل، وسلامة المعلومات.

دخل قانون التوقيع الرقمي لعام (DSA) حيز التنفيذ في 1 أكتوبر 1998، بهدف تنظيم استخدام التوقيع الرقمي في ماليزيا، ويضمن أمن القضايا القانونية المتعلقة بالمعاملات الإلكترونية ويتحقق من استخدام التوقيعات الرقمية من خلال الشهادات الصادرة عن المرجع المصدق المرخص (CA)¹⁶.

تعتبر هيئة الاتصالات والوسائط المتعددة الماليزية (MCMC) مسؤولة عن إدارة وتنفيذ أحكام DSA 1997 لغرض المراقبة والإشراف على أنشطة CAs.

1. قانون الاتصالات والوسائط المتعددة عام 1998¹⁷:

تم سنّ القانون في عام 1 نوفمبر 1998 - كان بمثابة تشريع في عام 1997- وقد أجريت تعديلات المره الاولى في عام 2002 والمره الثانية في 1 يناير 2006.

ونص على إنشاء لجنة الاتصالات والوسائط المتعددة الماليزية مع صلاحيات الإشراف على الاتصالات والأنشطة المتعددة الوسائط في وتنظيمها، وتطبيق قوانين الاتصالات والوسائط المتعددة.

1. قانون حماية البيانات الشخصية عام 2010:

¹⁵ I bid.

¹⁶ I bid.-

¹⁷ I bid.-

يهدف قانون حماية البيانات الشخصية الصادر في عام 2010 إلى ضمان عدم إساءة استخدام أي بيانات شخصية يتم جمعها كما يفرض على الشركات الحصول على موافقة من الأفراد قبل جمع بياناتهم الشخصية أو مشاركة بياناتهم مع أطراف أخرى، فضلاً القانون وضع شروط تسجيل لمستخدمي البيانات في صناعات معينة وإلا فإن ذلك قد يعرضهم لعقوبة جنائية بحد أقصى 500000 رينغيت ماليزي أو ما يصل إلى ثلاث سنوات في السجن، أو كليهما¹⁸.

الفرع الثالث : تحديات الأمن السيبراني في ماليزيا والتهديدات الدولية المتزايدة عبر الإنترنت

وفقاً لدراسة أجراها الاتحاد الدولي للاتصالات (ITU) تعد ماليزيا واحدة من أكبر عشر دول مستهدفة بهجمات البرامج الضارة على مستوى العالم¹⁹.

شهدت ماليزيا خرقاً هائلاً للبيانات التي نشأت بسبب البرامج الخبيثة، وكان التأثير المالي ضخماً بسبب اختراق البيانات. كما أن الوعي بالأمن السيبراني في ماليزيا لم يتم توصيله بشكل جيد لجميع المواطنين.

وفقاً لإحصائية قدمها فريق الاستجابة لحالات طوارئ الكمبيوتر، والذي يعمل في إطار Cyber Security Malaysia أن هناك من 2.7 مليون من هجمات الروبوتات الآلية وهجمات عدوى البرامج الضارة بواسطة بروتوكولات الانترنت الفريدة IPS.

كما كشفت إحصائيه أخرى أنه تم الإبلاغ عن أكثر من 9000 قضية تتعلق بالأمن السيبراني في ماليزيا، مثل المضايقات الإلكترونية والاحتيال والتطفل والرموز الخبيثة ورفض الخدمة والمحتوى المرتبط بالبريد العشوائي.

¹⁸ - سُني ذو الهدى، تهديد الأرهاب السيبراني - وإمكانية تطبيق اتفاقية الجرائم السيبرانية، على الرابط التالي:

<https://imctc.org/arabic/ArticleDetail/Index/63728507466543902>

¹⁹ - عادل عبد الصادق، الإرهاب الإلكتروني، مرجع سابق.

تزايدت حوادث الجرائم الإلكترونية بمعدل ينذر بالخطر في ماليزيا ومنطقة جنوب شرق آسيا حيث شهدت المنظمات المزيد من الهجمات الإلكترونية، حيث يستغل مجرمو الإنترنت في ماليزيا الخوف وعدم اليقين المحيطين بنفشي فيروس كورونا.

تم اكتشاف 20 برنامجًا ضارًا مختلفًا مرتبطًا بفيروس كورونا من قبل متخصصي الأمن السيبراني (Kaspersky)، وذكرت مجلة (Forbes) أن ماليزيا هي واحدة من أكثر خمس دول في العالم مستهدفة من قبل مجرمي الإنترنت أثناء تفشي المرض وأصبح معدل الهجمات الإلكترونية في تزايد عن ذي قبل.

وكشفت شركة (Microsoft) في دراسة أجريت عام 2018 أن ماليزيا قد عانت من خسائر اقتصادية بلغت 12.2 مليار دولار أمريكي بسبب الجرائم السيبرانية:²⁰

واكتشفت شركة (Technisanct) الناشئة للأمن السيبراني أن أكثر من 35000 بطاقة ائتمان من عدد من البنوك قد تم اختراقها في ماليزيا وتم بيعها على شبكة الإنترنت.

وقد أطلقت إحدى الشركات التكنولوجية حلاً أطلق (Linkdood) منصة اتصالات صممها خبراء الأمن السيبراني لتمكين الموظفين من تخزين الملفات والتعاون بأمان باستخدام تقنية السحابة الخاصة.

أطلقت (LGMS)، وهي شركة محلية للأمن السيبراني، مختبراً للأمن السيبراني مع مزود الخدمة النمساوي (TÜV Austria).

قال سفير النمسا في ماليزيا الدكتور مايكل بوستل:²¹ "هذه الشراكة لديها القدرة على ترسيخ ماليزيا كمركز لاختبار واعتماد الأمن السيبراني لمنطقة آسيا والمحيط الهادئ."

وقد حققت شركة البيانات الماليزية Strateq أيضاً نجاحاً مؤخراً عندما أعلنت شركة الاتصالات السنغافورية StarHub أنها ستدفع ما يصل إلى 82 مليون دولار سنغافوري مقابل حصة تبلغ 88% في الشركة.²²

R. Ahmad and Z. Yunos, "A Dynamic Cyber Terrorism Framework," *Int. J. Comput. Sci.* -²⁰
Inf. Secur., vol. 10, no. 2, pp. 149–158, 2012.
Ibid.-²¹

وتعمل ماليزيا على إنشاء نظام دفاع إلكتروني متطور اكتمل الآن بنسبة 90% بعد ثلاث سنوات من العمل، وإذا سار العمل وفقاً للخطة ، فستكون ماليزيا في طريقها لتصبح واحدة من أفضل القدرات في المنطقة.

وقد وقعت منظمة Cyber Security Malaysia المرتبطة بالحكومة أيضاً اتفاقية مع Blackberry لحماية بعض البيانات الأكثر أهمية وحساسية في ماليزيا من مجرمي الإنترنت.

تظهر ماليزيا بوادر تحسن في الحرب ضد مجرمي الإنترنت وجدت دراسة حديثة أجرتها شركة Cisco أن الشركات في ماليزيا تلقت تنبيهات إلكترونية أقل بنسبة 3% في عام 2019 مقارنة بعام 2018 ، وهو أفضل من المتوسط في منطقة آسيا والمحيط الهادئ. وذكرت الدراسة أيضاً أن الانتهاكات التي تكلف الشركات مليون دولار أمريكي أو أكثر انخفضت من 50% في 2018 إلى 23% فقط في 2019.

لكن المعركة لم تنته بعد، ما زال أمام ماليزيا ومنطقة آسيا والمحيط الهادئ طريق طويل لتقطعه، ولا تزال المنطقة تتلقى المزيد من التنبيهات على أساس يومي أكثر من المناطق الأخرى التي شملتها الدراسة التي أجرتها شركة Cisco²³.

بينما شهد عدد التنبيهات التي تم التحقيق فيها أيضاً انخفاضاً في جميع أنحاء المنطقة منذ عام 2018.

وضعت الدولة للمستهلكين والعملاء ومستخدمي الإنترنت عدد من الطرق التي يمكن من خلالها المساعدة في منع الجرائم الإلكترونية منها:

لابد من استخدام كلمة مرور مختلفة لكل حساب، تجنب الوصول إلى المعلومات الحساسة وحفظ التفاصيل الخاصة بك عند استخدام شبكة WiFi العامة، قراءة رسائل البريد الإلكتروني بعناية لتجنب هجمات التصيد الاحتيالي، لابد من مراجعة عناوين مواقع الويب والتحقق مما إذا كانت آمنة.

²² — صليحة محمدي، الارهاب الإلكتروني والامن القومي للدول: نمط جديد وتهديدات مختلفة، المجلة الجزائرية للامن والتنمية، ص67.

²³ — تقرير الامم المتحدة، مكافحة استخدام تكنولوجيا المعلومات والانصالات للاغراض الاجرامية، ص48.

المطلب الثاني: جهود الجزائر في مكافحة الجريمة الالكترونية:

الفرع الأول: الجريمة الالكترونية في التشريع الجزائري

عزز المشرع الجزائري بموجب القانون 06-22 نشاط الضبطية القضائية بإجراءات خاصة لمواجهة بعض الجرائم، عرفها الفقه على أنها الإجراءات و التقنيات التي تتخذها الشرطة القضائية بغية البحث و التحري عن الجرائم الخطيرة المقررة في قانون العقوبات و جمع الأدلة و الكشف عن مرتكبيها وذلك دون علم ورضا الأشخاص المعنيين.

و أمام خطورة هذا الإجراء و انقسام الفقه حول مشروعيته من عدمها قسم المشرع الجزائري هذه الأساليب وحصرها بالصور التالية: المراقبة و اعتراض المراسلات و الأصوات و التقاط الصور ثم التسرب، و أضاف القانون 06-01 المتضمن قانون الفساد بمقتضى المادة 56 منه الصور التالية اذا تعلق الأمر بجرائم الفساد و هب ذي التسليم المراقب و التردد الالكتروني و الاختراق.²⁴

أولاً: الجريمة الالكترونية الواقعة على الأسرار

تقوم هذه الجريمة باستعمال النظام المعلوماتي لإفشاء الأسرار، سواء كانت أسرار عامة أو أسرار خاصة تتعلق بالأفراد أو المؤسسات المختلفة. ويتخذ هذا النوع من الجرائم صورتين، الأولى تتعلق بالجرائم الواقعة على أسرار الدولة ، حيث أتاح الأنترنت للكثير من الدول ممارسة التجسس على دول أخرى، وذلك بالاطلاع على الأسرار العسكرية والاقتصادية لهذه الأخيرة خاصة في الدول التي يكون فيها نزاعات ، والثانية تتعلق بالجرائم الواقعة على الأسرار المهنية²⁵، والهدف من ارتكاب هذه الجريمة هو سرقة معلومات قصد التشهير بشخص أو بجماعة معينة أو بيع هذه المعلومات لتحقيق مصالح مختلفة، كالحصول على عائد مادي ممن يهيمه الأمر أو يستخدمها للضغط على أصحابها من أجل القيام بعمل أو الامتناع عن القيام بعمل.

²⁴ - كور طارق، آليات مكافحة جريمة الصرف، دار هومة، الجزائر، الطبعة الثانية 2014، ص131-132.

²⁵ - سوير سفيان ، مرجع سابق.

وقد حرص المشرع الجزائري على حماية هذه الأسرار من خلال الباب الأول المتعلق بالجنايات والجنح ضد الشيء العمومي من المادة 61 إلى المادة 96 مكرر 03، من قانون العقوبات، بالإضافة إلى المادة 394 مكرر التي تنص على²⁶: "تضاعف العقوبات المنصوص عليها في هذا القسم إذا استهدفت الدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام، دون إخلال بتطبيق عقوبات أشد.

ثانيا: الجريمة الالكترونية الواقعة على النظام المعلوماتي

من أجل سد الفراغ الذي عرفه التشريع الجزائري في هذا المجال، جاء القانون رقم 15 04 -الصادر في 10 نوفمبر 2004، المتضمن قانون العقوبات بتجريم كل أنواع الإعتداءات التي تستهدف أنظمة المعالجة الآلية للمعطيات، وقد ورد النص على هذه الجرائم في القسم السابع مكرر من قانون العقوبات، تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، وذلك في المواد 394 مكرر إلى 394 مكرر 07، وتأخذ صور الإعتداء صورتين وهما: الدخول والبقاء في منظومة معلوماتية، المساس بمنظومة معلوماتية، كما تضمن صور أخرى للغش، تمثل في البنود التالية:

البند الأول: تنص المادة 394 مكرر من قانون العقوبات السابق الذكر على معاقبة كل شخص يدخل أو يبقى بواسطة استعمال الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، وإذا نتج عن هذا الدخول أو البقاء تخريب في النظام المعلوماتي فإن العقوبة تضاعف، فالصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء، بينما الصورة المشددة تتحقق في الحالة التي ينتج فيها عن هذا الدخول أو البقاء غير المشروع إما محو أو تغيير في المعطيات الموجودة²⁷.

البند الثاني: جريمة المساس بمنظومة معلوماتية: صت المادة 394 مكرر 01 من قانون العقوبات رقم 15/04 بمعاقبة كل شخص قام بإدخال معطيات في نظام المعالجة الآلية، أو أزال أو عدل هذه المعطيات وذلك عن طريق استعمال الغش. هذا السلوك الإجرامي يتجسد في ثلاث صور هي الإدخال، المحو،

²⁶ - الأمر رقم 15-04، القانون رقم 04-09، الصادر في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج 2 العدد 47.

²⁷ - حمزة بن عقون، رسالة الماجستير السابقة الذكر، ص 182 -1

التعديل، كما أن المشرع لم يشترط اجتماع هذه الصور بل يكفي أن يصدر عن الجاني إحداها فقط لكي يتوافر الركن المادي، و أفعال الإدخال و الإزالة و التعديل تنطوي على التلاعب في المعطيات التي يحتويها نظام المعالجة الآلية للمعطيات، سواء بإضافة معطيات جديدة غير صحيحة، أو محو أو تعديل معطيات موجودة من قبل، كما أن هذا السلوك يجسد فعل التخريب و إفساد المعطيات التي يتضمنها نظام المعالجة الآلية، مثال ذلك إدخال فيروس المعلوماتية في البرامج من أجل إتلافها.

البند الثالث: أفعال إجرامية أخرى، جرمت المادة 394 مكرر 02 من قانون العقوبات السابق الذكر الأعمال الآتية: تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية، يمكن أن ترتكب بها إحدى جرائم الغش المعلوماتي السابقة الذكر²⁸ ، ويقصد بتصميم المعطيات هنا الفيروسات المعلوماتية، برامج القرصنة التي يمكن أن تستعمل في ارتكاب جرائم معلوماتية إما ضد الأنظمة المعلوماتية، أو المعطيات المعلوماتية في حد ذاتها ، كما جرم المشرع كذلك أفعال الحيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصلة من إحدى جرائم الغش المعلوماتي لأي غرض.

الفرع الثاني : التحقيق الإلكتروني و خصائصه

للتحقيق الإلكتروني مميزات خاصة عن التحقيق الجنائي التقليدي وكذا المحقق الإلكتروني، لمسايرة متطلبات الجريمة الإلكترونية بما فيها العالم الافتراضي الذي ترتكب فيه.

أولاً: منهج التحقيق الابتدائي:

وذلك وفق المعلومات المتوفرة لدى المحقق، وتحديد الفريق الفني اللازم للقيام بمساعدته في أعمال التحقيق وذلك بوضع خطة مناسبة، ولا تبدأ إلا بعد معاينة مسرح الجريمة والتعرف على أنظمة الحماية وتحديد مصدر الخطر ووضع التصورات الكفيلة للتصدي للجريمة، ثم التخطيط الفني للتحقيق من أجل الوصول إلى أفضل الطرق للتعامل مع هذه الجريمة بالتفصيل والوضوح، وبعدها عمل دراسة وافية

²⁸ — در دور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة لنيل شهادة الماجستير، شعبة القانون الجنائي، جامعة منثوري، قسنطينة، 2012 - 2013، بدون صفحة.

وجادة لكافة إجراءات التحقيق ضمن الخطة المسبقة التي تم وضعها وناقشها العاملون في فريق التحقيق، تنسيق جهود الفريق القائم بالتحقيق لتسهيل مهمتهم وعملهم وتقليل الآثار السلبية والإسراع في إنجاز العمل، وهو ما يؤدي إلى ضمان مستوى جيد من الأداء، تحديد الإجراءات المسبقة التي من شأنها التقليل من الأخطاء الفردية التي قد تنتج عن قلة الخبراء أو نقص المعرفة، وبالتالي تساعد على إيجاد درجة جيدة من التقيد بالمستوى المطلوب مع ضمان أن الخطوات التي يقوم بها المحقق خلال جميع مراحل التحقيق تسير ضمن الضوابط التشريعية وتقلل من الأخطاء التي قد تضر بالقضية في مرحلة المحاكمة. ويجب أن تركز خطة العمل على مجموعة من البنود الأساسية، يتم الإرتكاز عليها أثناء تنفيذ الخطة وهي أن يتم تعيين الأشخاص الذين سيتم التحقيق معهم وتحديد النقاط التي يجب إيضاحها معهم وتقدير مدى الحاجة للاستعانة ببعض الفنيين اللازم توافرهم لاستكمال التحقيق، بالإضافة إلى مراعاة الظروف المحيطة بالواقعة، إذ أن هذه الظروف قد تشمل عوامل مهمة يجب مراعاتها عند وضع خطة العمل ومنها: مدى أهمية الأجهزة والشبكات المتضررة لعمل المنظمة- مدى حساسية البيانات التي يحتمل سرقتها أو إتلافها- مدى الإختراق الأمني الذي تسبب فيه الجاني. ثم بعد ذلك وضع الأسلوب الأمثل لعملية التفتيش، وذلك بتحديد نوع الأدلة التي يريد فريق التحقيق البحث فيها²⁹.

ثانياً: خصائص المحقق الإلكتروني

تتمثل في الخصائص الفنية للمحقق الإلكتروني، وتأهيل وتدريب المحقق الإلكتروني³⁰.

أ — الخصائص الفنية :

معرفة الجوانب الفنية والتقنية لأجهزة الحاسوب والانترنت، لأن افتقار ضابط الشرطة القضائية إلى التأهيل الكافي في الميدان التقني قد يؤدي إلى إتلاف وتدمير الدليل- إتباع الإجراءات الصحيحة والمشروعة من أجل سرعة المحافظة على الأدلة الإلكترونية التي تدل على وقوع الجريمة وتخزينها في الأقراص المعدة لذلك، ومنع حذفها والحرص على عدم تعريض وسائط التخزين كالأقراص المرنة لأي

²⁹ — سعيداني نعيم، رسالة الماجستير السابقة الذكر، ص 110-111.

³⁰ — نفس المرجع.

مؤثرات خارجية، كالقوة الكهرومغناطيسية حتى لا تتلف محتوياتها - معرفة آلية عمل تشكيلات الحاسوب والانترنت - معرفة المحقق بالأنظمة المختلفة، لكي يشارك في متابعة فحص وتفتيش مسرح الجريمة - معرفة معطيات الحاسوب لمعرفة صيغ الملفات وما تحتويه - معرفة وإدراك أساليب ارتكاب الجريمة الإلكترونية، وتقنيات الأمن المعلوماتي.

ب — تأهيل وتدريب المحقق الإلكتروني:

لابد من وضع سياسة جنائية رشيدة، تستند على تدريب أجهزة العدالة الجنائية لمكافحة هذه الجريمة، ويمتد هذا التدريب إلى العاملين بأجهزة الضبطية القضائية. ويرى الفقه الجنائي أنه في حالة التدريب على التحقيق يتعين مراعاة شخص المتدرب، ومنهج الدورة التدريبية، وصفة وأسلوب التدريب، كما يجب أن يشمل منهج التدريب تدريس الأساليب الفنية المستخدمة في ارتكاب الجريمة، والمتعلقة بالكشف عنها وكيفية اتباعها ومعاينتها وفحصها فنيا، ومن العقوبات التي تعيق عمل الأجهزة حتى على فرض أنه تم إعدادها الإعداد المناسب، ضخامة حجم البيانات محل الفحص، ما يتعذر على المحقق الكفو الوصول إلى الدليل المناسب³¹.

الفرع الثالث: -العقوبات المطبقة³²:

أولاً: العقوبات المطبقة على الشخص الطبيعي:

³¹ — سعيداني نعيم، مرجع سابق.

³² — النصوص التشريعية:

1- الأمر رقم 10/97 المؤرخ في 1997/03/06 المتعلق بحق المؤلف و الحقوق المجاورة.

2- الأمر رقم 07/03 المؤرخ في 2003/07/19 يتعلق ببراءات الاختراع.

3- القانون 15/04 المؤرخ في 2004/11/10 المعدل و المتمم للأمر 156/66 المؤرخ في

08/06/1966 المتضمن قانون العقوبات.

من خلال استقراء النصوص المتعلقة بالجرائم الماسة بالأنظمة المعلوماتية يتبين لنا وجود تدرج داخل النظام العقابي. هذا التدرج في العقوبات يحدد الخطورة الإجرامية التي قدرها المشرع لهذه التصرفات، إذ نجد سلم خطورة يتضمن ثلاث درجات، جريمة الدخول أو البقاء بالغش في الدرجة الأولى وبعدها في الدرجة الثانية جريمة الدخول والبقاء المشددة، أما الدرجة الثالثة فتحتلها الجريمة الخاصة بالمساس العمدي بالمعطيات.

أ/ الدخول والبقاء بالغش (الجريمة البسيطة): العقوبة المقررة هي 3 أشهر إلى سنة حبس و 50000 دج إلى 100000 دج غرامة (المادة 394 مكرر).

ب/ الدخول والبقاء بالغش (الجريمة المشددة): تضاعف العقوبة إذا ترتب عن هذه الأفعال حذف أو تغيير لمعطيات المنظومة، وتكون العقوبة الحبس من ستة أشهر إلى سنتين وغرامة من 50000 دج إلى 150000 دج إذا ترتب عن الدخول أو البقاء غير المشروع تخريب لنظام اشتغال المنظومة (المادة 394 مكرر/02-03).

نصت المادة 394 مكرر 3 قانون العقوبات على العقوبات التكميلية إلى جانب العقوبات الأصلية و المتمثلة في:

أ/ المصادرة: وهي عقوبة تكميلية تشمل الأجهزة والبرامج و الوسائل المستخدمة في ارتكاب جريمة من الجرائم الماسة بالأنظمة المعلوماتية، مع مراعاة حقوق الغير حسن النية.

ب/ إغلاق المواقع: والأمر يتعلق بالمواقع (les sites) التي تكون محلا لجريمة من الجرائم الماسة بالأنظمة المعلوماتية.

ج/ إغلاق المحل أو مكان الاستغلال: إذا كانت الجريمة قد ارتكبت بعلم مالكيها ومثال ذلك إغلاق المقهى الإلكتروني الذي ترتكب منه مثل هذه الجرائم شرط توافر عناصر العلم لدى مالكيها.

— الظروف المشددة:

أ/ نصت المادة 394 مكرر 2-3 على ظرف تشدد به عقوبة جريمة الدخول والبقاء غير المشروع داخل النظام، ويتحقق هذا الظرف عندما ينتج عن الدخول و البقاء إما حذف أو تغيير المعطيات التي يحتويها النظام وإما تخريب نظام اشتغال المنظومة.

في الحالة الأولى تضاعف العقوبات المقررة في الفقرة الأولى من المادة 394 مكرر ،و في الحالة الثانية تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000 دج إلى 150000 دج.

هذه الظرف المشدد هو ظرف مادي يكفي أن تقوم بينه وبين الجريمة الأساسية وهي جريمة الدخول والبقاء غير المشروع علاقة سببية للقول بتوافره.

ب/ نصت المادة 394 مكرر 3 على أن تضاعف العقوبات المقررة للجرائم الماسة بالأنظمة المعلوماتية وذلك إذا استهدفت الجريمة الدفاع الوطني والهيئات والمؤسسات الخاضعة للقانون العام.

ثانيا: العقوبات المطبقة على الشخص المعنوي:

مبدأ مساءلة الشخص المعنوي وارد في المادة 12 من الاتفاقية الدولية للإجرام المعلوماتي ، بحيث يسأل الشخص المعنوي عن هذه الجرائم سواء بصفته فاعلا أصليا أو شريكا أو مت دخلا كما يسأل عن الجريمة التامة أو الشروع فيها ،كل ذلك بشرط أن تكون الجريمة قد ارتكبت لحساب الشخص المعنوي بواسطة أحد أعضائه أو ممثليه.

هذا مع ملاحظة أن المسؤولية الجزائية للشخص المعنوي لا تستبعد المسؤولية الجزائية للأشخاص الطبيعيين بصفقتهم فاعلين أو شركاء أو متدخلين في نفس الجريمة.

ج/ الاعتداء العمدى على المعطيات : طبقا لنص المادة 394 مكرر 2 فالعقوبة المقررة للاعتداء العمدى على المعطيات الموجودة داخل النظام هي الحبس من ستة أشهر إلى ثلاث سنوات وغرامة من 500000 دج إلى 2000000 دج أما العقوبة المقررة لاستخدام المعطيات في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية وكذا حيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصل عليها من إحدى الجرائم الماسة

بالأنظمة المعلوماتية، العقوبة المقررة هي الحبس من شهرين إلى ثلاث سنوات وغرامة من 1000000 دج إلى 5000000 دج.

كما تجدر الإشارة إلى أن المشرع الجزائري قد أقر في التعديل الأخير لقانون العقوبات المسؤولية الجزائية للشخص المعنوي وذلك في نص المادة 18 مكرر من القانون 15/04 المتضمن قانون العقوبات الذي ينص على أن: " العقوبات المطبقة على الشخص المعنوي في مواد الجنايات و الجنح هي:

أ/ الغرامة التي تساوي من مرة إلى خمس مرات الحد الأقصى للغرامة المقدرة للشخص الطبيعي في القانون الذي يعاقب على الجريمة.

ب/ واحدة أو أكثر من العقوبات الآتية:

- حل الشخص المعنوي

- غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز 5 سنوات

- الإقصاء من الصفقات العمومية لمدة لا تتجاوز 5 سنوات

- المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر نهائيا أو لمدة لا تتجاوز 5 سنوات.

- مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها.

- نشر أو تعليق حكم الإدانة.

- الوضع تحت الحراسة القضائية لمدة لا تتجاوز 5 سنوات ،وتتصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبةه.

بالنسبة لعقوبات الغرامة المطبقة على الشخص المعنوي عند ارتكابه أحد الجرائم الماسة بالأنظمة المعلوماتية فهي تعادل طبقا للمادة 394 مكرر 4 قانون العقوبات 5 مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

ثالثا: عقوبة الاتفاق الجنائي

نصت عليه المادة 11 من الاتفاقية الدولية للإجرام المعلوماتي وقد تبني المشرع الجزائري مبدأ معاقبة الاتفاق الجنائي بنص المادة 394 مكرر 5 ، بغرض التحضير للجرائم الماسة بالأنظمة المعلوماتية ولم يخضعها لأحكام المادة 176 من قانون العقوبات المتعلقة بجمعية الأشرار ،حيث تنص المادة 394 مكرر 5 من قانون العقوبات : " كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل او بعدة أفعال مادية ،يعاقب بالعقوبات المقررة بالجريمة ذاتها."

إن الحكمة التي ارتآها المشرع من تجريم الاشتراك في مجموعة أو في اتفاق بغرض الإعداد لجريمة من الجرائم الماسة بالأنظمة المعلوماتية هو أن مثل هذه الجرائم تتم عادة في إطار مجموعات، كما أن المشرع ورغبته في توسيع نطاق العقوبة أخضع الأعمال التحضيرية التي تسبق البدء في التنفيذ للعقوبة إذا تمت في إطار اتفاق جنائي، بمعنى أن الأعمال التحضيرية المرتكبة من طرف شخص منفرد غير مشمولة بالنص.

ويعاقب المشرع الجزائري على الاشتراك في الاتفاق الجنائي بعقوبة الجريمة التي تم التحضير لها فإذا تعددت الجرائم التي يتم التحضير لها تكون العقوبة هي عقوبة الجريمة الأشد.

وشروط المعاقبة على الاتفاق الجنائي بمن استخلصها من نص المادة 394 مكرر 5 م قانون العقوبات، والتي هي:

-مجموعة أو اتفاق.

-بهدف تحضير جريمة من الجرائم الماسة بالأنظمة المعلوماتية.

-تجسيد هذا التحضير بفعل مادي.

-فعل المشاركة في هذا الاتفاق.

-القصد الجنائي.

فبالنسبة لمجموعة أو الاتفاق يستوي أعضاء الاتفاق في صورة شركة أو مؤسسة أو شخص معنوي، أن يعرف أشخاص الاتفاق بعضهم بعضا كما في العصابة أم تكون مجرد مجموعة من الأشخاص، لا يعرف أحدهم الآخر من قبل و لكن اتفقوا فيما بينهم على القيام بالنشاط الإجرامي ، المهم أن يتم الاتفاق بين شخصين على الأقل ، فإذا ارتكب الشخص العمل التحضيري المادي شخص واحد بمفرده أو بمعزل عن غيره فلا يعاقب في هذه الحالة، فالعقاب لا يتقرر إلا في حالة اجتماع شخصين أو أكثر.

وتكاثف الجهود لا يكفي بل يجب أن يكون بهذه تحضير جريمة من جرائم الماسة بالأنظمة المعلوماتية بمعنى أن الاتفاق يجب أن يكون له هدف إجرامي منذ البداية فعليه إنشاء نادي للمعلوماتية بهدف التكوين أو التسلية العلمية يحول نشاطه لأهداف إجرامية لا يقع تحت طائلة المادة 394 مكرر 5 من قانون العقوبات.

الجنح التي يشكل تحضيرها هدف الاتفاق المنصوص عليه بالمادة 394 مكرر 5 قانون العقوبات هي الجنح الماسة بالأنظمة المعلوماتية وعليه لا يعاقب استنادا لهذا النص الاتفاق بهدف ارتكاب جنحة تقليد البرامج المعاقب عليها بنصوص حق المؤلف وحقوق المجاورة.

التحضير لا يكفي بل يتم تجسيده بفعل مادي، الأمر يتعلق بأعمال تحضيرية مثل تبادل المعلومات الهامة لارتكاب الجريمة كالإعلان على كلمة مرور mots de passe أو رمز الدخول code d'accès الخ.

فعل المشاركة في الاتفاق إذ أن المجرم بنص المادة 394 مكرر 5 ليس الاتفاق وإنما المشاركة من طرف شخص طبيعي أو معنوي فبمجرد الانضمام إلى الاتفاق غير كافي بل يجب توافر فعل إيجابي للمشاركة.

توافر القصد الجنائي لدى أعضاء الجماعة والمتمثل في توافر العلم لدى كل منهم بأنه عضو في الجماعة الإجرامية وأن تتجه إرادة كل عضو أي تحقيق نشاط إجرامي معين وهو العمل التحضيري.

رابعا: عقوبة الشروع في الجريمة

نصت عليه المادة 11 من الاتفاقية الدولية للإجرام المعلوماتي وتبناه المشرع الجزائري في المادة 394 مكرر 7 من قانون العقوبات، فالجرائم الماسة بالأنظمة المعلوماتية لها وصف جنحي ولا عقاب على الشروع في الجنح إلا بنص.

نصت المادة 394 مكرر 7 قانون العقوبات: "يعاقب على الشروع في ارتكاب جنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها."

يبدو من خلال هذا النص رغبة المشرع في توسيع نطاق العقوبة لتشمل أكبر قدر من الأفعال الماسة بالأنظمة المعلوماتية، إذ جعل الشروع في إحدى الجرائم الماسة بالأنظمة المعلوماتية معاقب بنفس عقوبة الجريمة التامة، ومن خلال استقراء نص المادة نستنتج أن الجنحة الواردة بنص المادة 394 مكرر 5 من قانون العقوبات مشمولة بهذا النص، أي أن المشرع الجزائري بهذا المنطق يكون قد تبني فكرة الشروع في الاتفاق الجنائي.

بعض التشريعات المقارنة بما فيها التشريع الفرنسي أخرجت جنحة الاتفاق الجنائي لتحضير جرائم ماسة بالأنظمة المعلوماتية من نطاق الشروع لأنها تعتبر أن في ذلك مساس بالنظرية العامة في القانون الجنائي، لأن التحضير للجرائم الذي يتم في إطار اتفاق أو مجموعة تشكل في حد ذاتها محاولة أو عمل تحضيرية مما يؤدي إلى تبني فكرة الشروع في الشروع.

المطلب الثالث: الويب المظلم (الديب ويب)

الفرع الأول مفاهيم الديب المظلم

يقسم الأنترنت "Web" إلى ثلاثة أنواع في الحقيقة وما تصل إليه محركات البحث المعروفة (Firefox, Google Chrome) جزء منها فقط ويسمى النوع الذي تصله محركات البحث "الأنترنت المرئي"³³.

هناك جزء من الويب (Web) لا تصل إليه محركات البحث يسمى الأنترنت العميق أو الخفي (الديب ويب)، وجزء أكثر خصوصية، وهو موضوع مقالنا "Dark Web" علماً إن Dark Web يشكل جزء من

³³ — هكذا قد تستفيد من «الإنترنت المظلم» - ساسة بوست (sasapost.com)

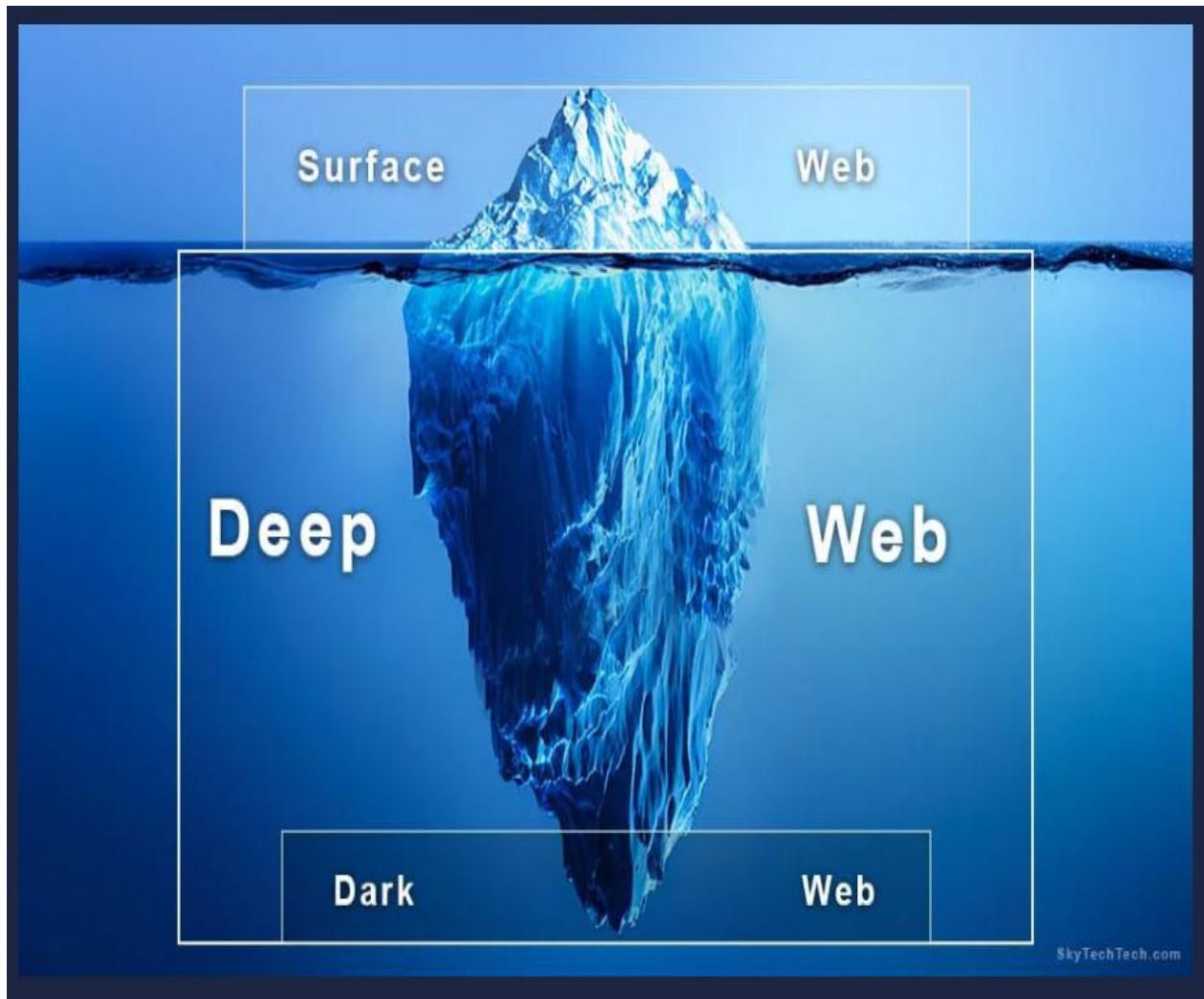
“الأنترنت العميق” أذ يخلط الكثيرين بين الأنترنت المظلم -Dark Web- والأنترنت العميق -Deep Web- وأسفله شرح مفصل لكل واحد من هذه الأنواع³⁴.

الشكل رقم 02: يوضح مساحة توزيع استعمال الانترنت بين الظاهر و المظلم

³⁴ – رغبة البهي، الارهاب السيبراني: المفهوم والسمات والانماط، المركز المصري للفكر والدراسات الاستراتيجية،

على الرابط التالي:

<https://www.ecsstudies.com/714>



المصدر : <https://www.skytechttech.com/dark-web>

الأنترنت العميق أو الخفي أو الديب ويب كلها مسميات إلى الجزء الذي لا تقوم محركات البحث العادية بأرشفته ومثال على ذلك رسائل البريد الإلكتروني الخاصة، والحسابات البنكية، وقواعد البيانات الخاصة بالمؤسسات الأكاديمية، وغيرها من المعلومات (data) التي تتطلب طرق خاصة لدخولها - بريد إلكتروني وكلمة سر - تقع ضمن الديب ويب.

الفرع الثاني: الدارك ويب

ليس بشيء منفصل عن الديب ويب "الأنترنت الخفي" كما ذكر سابقاً، فأى صفحة أنترنت لا تصلها محركات البحث العادية تعتبر جزء من الأنترنت الخفي. يوفر Dark Web بيئة مناسبة لأولئك الذين يبحثون عن مكان يعبرون عن آراءهم بحرية من دون التعرض للملاحقة، ولكنه في نفس الوقت أصبح بيئة حاضنه لجماعات عديدة خطيرة مثل تجار السلاح، والمخدرات³⁵.

لا يمكن الوصول إلى الدارك ويب إلا عن طريق متصفح خاصة يسمى "Tor" ويمكن استخدام محرك البحث تور للولوج إلى الصفحات التي تحمل نطاق ".onion" في نهاية الرابط، ويعتبر نطاق ".onion" هو النطاق المستخدم لأي موقع دارك ويب عكس الصفحات العادية التي تحمل نطاق ".net" أو ".com" في العادة، وأسفله سأقوم بإرفاق إحصائية توضح أبرز الخدمات المخفية التي تقدم على الدارك ويب، وتاريخ الإحصائية يعود إلى عام 2015.

الشكل رقم 03: يوضح أبرز الخدمات المخفية التي تقدم على الدارك ويب

³⁵ - تقرير الأمم المتحدة، مكافحة استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية، ص 48.



المصدر: <https://www.skytechtech.com/dark-web>

بإمكان المتصفح أن يجد كافة أنواع المخدرات الموجودة وغير الموجودة في بلده، حيث يوجد مواقع مخصصة لهذه العمليات مثل: موقع Silk Road الذي تمت السيطرة عليه وإغلاقه من قبل الشرطة عدة مرات، لكن سرعان ما افتتح موقع جديد تحت نفس الاسم، وتتم عمليات البيع والشراء بعملة بتكوين الإلكترونية.

إنّ امتلاكك السلاح بترخيص مسموح قانونياً، لكن أن تملك سلاحاً مخصصاً للاستخدام العسكري وغير مصرح به للمدنيين فهو جناية. وهذا ما ستجده على الديب ويب. كافة أنواع الأسلحة والقنابل بالإضافة إلى إمكانك الحصول على هوية مزورة وجواز سفر مزور، وأيضاً الدفع بعملة بتكوين.

بالإضافة إلى الكثير من الجرائم التي عجزت كل الحكومات على مواجهتها في هذا الفضاء المظلم ، و التي تبث متحدية كل الأجهزة و التشريعات على المباشر فضائع كما يحدث في ما يسمى بالغرفة الحمراء ، هذه حرفياً غرفة مصممة للتعذيب الجسدي للبشر من كافة الأجناس و"الأعمار"، حيث يقام مزاد علني يقرر فيه كيفية تعذيب الشخص واختيار طريقة موته، وتشاهد هذه الجلسات من قبل المرضى نفسياً وعقلياً³⁶.

في الواقع، كانت فكرة الابتعاد عن الرقابة الحكومية أحد الأسباب الرئيسة وراء ظهور الإنترنت المظلم. نحتاج هنا إلى العودة بالتاريخ قليلاً إلى الوراء. في عام 1999، لفت إيان كلارك عالم الكمبيوتر بجامعة إدنبرة بالمملكة المتحدة، الانتباه إلى عيبين في تصميم شبكة الإنترنت التي كان عمرها يبلغ آنذاك 10 سنوات فقط. أوضح كلارك أنه باستخدام نظام العنوان العامة وبرامج التوجيه التي يمكن تتبعها، كان من السهل للغاية مراقبة «الويب» والرقابة عليه.

إذا كانت عادات القراءة ومنشوراتنا مرتبطة دائماً بنا، فإن كلارك يرى أنه يمكن للكيانات القوية مثل الحكومات أو الشركات استخدام هذه المعلومات للسيطرة علينا. علاوة على ذلك، إذا كانت شبكة الويب تعتمد على بنى تحتية مركزية، (مثل «DNS» الذي يترجم الأسماء إلى عناوين الإنترنت)، فإن حظر الوصول إلى مواقع معينة – مثل تلك المواقع التي تعارض وتنتقد الأحزاب الحاكمة والقادة – أصبح أمراً في متناول يد الدولة بمنتهى السهولة.

كان كلارك على حق. نقوم ما يمكن تسميتها «رأسمالية المراقبة» (كما نعرفها الآن) بتتبع كل ما نقوم به على الإنترنت، ونقوم العديد من المواقع والشركات باستغلالنا بالفعل من أجل الربح، ولنا في «فيسبوك»

³⁶ - انظر Lim M. Sweeping the Unclean: **Social Media and the Bersih Electoral Reform**

Movement in Malaysia. Global Media Journal. 2016,

14:27. <https://www.globalmediajournal.com/open-access/sweeping-the-unclean-social-media-and-the-bersih-electoral-reformmovement-in-malaysia.php?aid=8324>

و«جوجل» أكبر وأوضح دليل يتعلق بانتهاك خصوصيتنا بشكل صارخ من أجل مزيد من توجيه الإعلانات لنا. أيضاً، في العديد من أنحاء العالم، تقوم الحكومات بحظر المواقع الإلكترونية التي تعمل ضد توجهاتها.

من أجل ذلك قام كلارك بتطوير شبكة «Freenet» لتكون بديلاً لامركزياً ومجهولاً للإنترنت. وسرعان ما تبعتها شبكات أخرى مع «Tor» و «I2P» مشروع الإنترنت الخفي، هذه الشبكات الثلاث معاً تشكل شبكة الإنترنت المظلم.

بدلاً عن أن تكون غير أخلاقية أو مخفية، يجب أن نفكر أنها الشبكة التي تعمل في «الظلام»، والتي تمثل تعتيماً للاتصالات لا أكثر، العامل الوحيد الذي يميزها عن بقية الإنترنت هو أنها تعمل على برنامج يحجب الطرق التي تتبعها حركة مرور الإنترنت العادية، بحيث لا يمكن تتبع المستخدمين. من الناحية النظرية، لا أحد يعرف من الذي يدير مواقعها على الإنترنت أو من يزورها.

خاتمة

حاولت الدراسة أن تجيب على التساؤلات التي تم طرحها في بداية الدراسة، وتمثلت الإجابات في النقاط الآتية:

1. الإرهاب السيبراني أصبح خطراً عالمياً يتطلب استجابة دولية وتعاوناً أممياً، وأصبحت الحاجة ملحة إلى سياسة مشتركة وإطار تشريعي مشترك في غياب إطار قانوني موحد للجريمة الالكترونية.

2. نستنتج من العرض السابق أن أمن المعلومات التحدي الأكبر الذي يتطلب صياغة الخطط والاستراتيجيات للتعامل مع مخاطره، وفي الوقت ذاته تدريب المزيد من الكوادر البشرية التي يكون بمقدورها ليس فقط مواجهة تلك المخاطر بل إجهاض محاولات اختراق الأجهزة والمؤسسات المختلفة وخاصة الأمنية والدفاعية منها، وهذا هو التحدي الحقيقي الذي يهدد الأمن الإقليمي في ظل الأزمات .

3. تم إنشاء العديد من مواقع الإنترنت لمكافحة الإرهاب الالكتروني والأمن الرقمي، حيث أصبحت بمثابة مؤسسات فكرية وفنية لدعم الأمن الرقمي، وكانت تلك المواقع إما بمبادرة حكومية أو من القطاع الخاص أو من المجتمع المدني، فضلاً عن مواقع الشركات العاملة في تكنولوجيا الاتصال والمعلومات و بناء عليه وضعت الجزائر آليات قانونية للتعامل مع الجريمة الالكترونية.

لقد باتت لقد باتت لزاماً على دول العالم مواكبة التطور التكنولوجي الحاصل في العالم الافتراضي الجديد، الذي صارت المعلومة فيه سيدة دون منازع ومصدراً للقوة و المعرفة و السلطة والمال، بل وأكثر من هذا أصبحت معياراً لتطور الشعوب.

إزاء هذا التطور العلمي، فإن مزايا الأنترنت جلبت معها مخاطر جمة طورها المجرم السيبراني وصارت سلاحاً لا يستهان به لممارسة نشاطاته الإجرامية، إضافة إلى إمكانية ارتكاب الجرائم التقليدية بطرق حديثة، وبهذا ظهرت طائفة جديدة من الجرائم المستحدثة، وباتت القوانين الجزائية الموضوعية

منها والإجرائية، تسعى لمواجهة الجرائم المرتكبة بواسطة الحاسب الآلي. من خلال هذا البحث لوحظت الصعوبات القانونية التي قد تواجه رجال القانون، و خاصة القضاة في تطبيق النصوص الجزائية التقليدية.

إن قواعد الإجراءات الجزائية تبدو قاصرة عن مواجهة الإجرام السيبراني، كفشلها في مجال الضبط والتحري و التحقيق و ثبات الجريمة و استنباط الأدلة النظام المعلوماتي و السيبرانية وصعوبة إثبات الجرائم الإلكترونية بالنظر إلى طبيعة الدليل الذي يتحصل منها، إذ قد يكون هذا الدليل غير مرئي وقد يسهل إخفاؤه أو تدميره، وقد يكون متصلا بدول أخرى فتكون هناك صعوبة للحصول عليه نظرا لتمسك كل دولة بسيادتها، كما وأن هذا الإثبات قد يحتاج إلى معرفة علمية وفنية قد لا تتوافر لدى ضباط الشرطة القضائية والقضاة.

في الأخير وانطلاقا من كل ما سبق يمكن القول أن مسألة تحقيق الأمن السيبراني في الجزائر يعد أحد أهم التحديات الجديدة للسياسة الأمنية الجزائرية، التي فرضتها التطورات التكنولوجية المتسارعة، ورغم الجهود المبذولة في سبيل تحقيق ذلك إلا أن المراتب التي تحتلها الجزائر عربيا ودوليا تشير إلى أنها بحاجة إلى المزيد من الجهود، وهذا حتى يمكن لها أن تنجح في مجال مكافحة مختلف المخاطر التي يفرزها الفضاء الإلكتروني، والتي يأتي على رأسها الإرهاب الإلكتروني وغيره من التهديدات التي يمثل الانتصار عليها انتصارا جديدا للسياسة الأمنية الجزائرية التي أثبتت نجاعتها في مكافحة خارج الفضاء الإلكتروني ولن تدخر أي جهد في إثبات مكانتها في هذا الفضاء الذي لا يعترف بالحدود ولا بالقيود.

قائمة المصادر و المراجع

قائمة المراجع باللغة العربية

- 1- أحمد خليفة الملط - الجرائم المعلوماتية ، دار الفكر الجامعي ، دون ذكر الطبعة، دون ذكر دار النشر، 2005.
- 2- احمد يوسف، اوسلو كإطار للتسوية، في: احمد الرشيدى (محرر)، القضية الفلسطينية وأفاق التسوية، القاهرة، مركز البحوث والدراسات السياسية، 1998م
- 3- بيتر غرابوسكي، جرائم الحاسب الالى..الابعاد العالمية في: القيادة العامة لشرطة أبو ظبي.. شبكات الانترنت وتأثيراتها الاجتماعية والامنية، مركز البحوث والدراسات الامنية، القيادة العامة لشرطة أبو ظبي، ط1، 2006.
- 4- هشام محمد فريد رستم، " الجرائم المعلوماتية أصول التحقيق الجنائي الفني واقتراح إنشاء آلية حربية موحدة للتدريب التخصصي"، بحوث مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات المتحدة كلية الشريعة والقانون، الطبعة الثالثة (المجلد الثاني)، 2004.
- 5- وفاق العياشي، مكافحة الإرهاب بين السياسة و القانون ،الجزائر :دار الخلدونية للنشر و التوزيع ، 2006،
- 6- حمدون تورية، البحث عن السلام السبيراني ، الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء، 2011.
- 7- يونس عرب، تطور التشريعات في مجال مكافحة الجرائم، الالكترونية، هيئة تنظيم الاتصالات، سلطنة عمان، مسقط، 2 و 4 أبريل 2006.
- 8- كور طارق، آليات مكافحة جريمة الصرف، دار هومة، الجزائر، الطبعة الثانية 2014.
- 9- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الالى في القانون الجزائري و المقارن ، دار الجامعة الجديدة للنشر 2007.

قائمة المصادر و المراجع

- 10- ممدوح أنيس فتحي، القوة العسكرية المصرية واثر التحولات الاستراتيجية على الدور المصري الإقليمي، عبد العليم محمد (محرر)، تسوية الصراع العربي الإسرائيلي: دور مصر الإقليمي، القاهرة، مركز الدراسات السياسية والإستراتيجية بالأهرام، 1997م، ص90-91.
- 11- منير محمد الجهيني، ممدوح محمد الجهيني، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها) الإسكندرية: دار الفكر العربي، ط 2004
- 12- مصطفى محمد موسى، الإرهاب الإلكتروني دراسة قانونية -أمنية - نفسية -اجتماعية .(الأردن : دار الكتب والوثائق القومية ،ط.01، 2009.
- 13- نائلة عادل محمد فريد ، جرائم الحاسب الآلي الاقتصادية ، منشورات الحلبي الحقوقية ، 2005.
- 14-نوران شفيق ،أثر التهديدات الإلكترونية على العلاقات الدولية ،(القاهرة :المكتب العربي للمعارف ،2015،
- 15- سامي علي حامد عياد ، الجريمة المعلوماتية وإجرام الإنترنت ، دار الفكر الجامعي ، الإسكندرية ، بدون طبعة ، 2007 م
- 16- عادل عبد الصادق، الفضاء الإلكتروني والعلاقات الدولية: دراسة في النظرية والتطبيق(القاهرة: الهيئة العامة للكتاب، 2018.
- 17- عبد الله عبد الكريم عبد اهلل، جرائم المعلوماتية والإنترنت، منشورات الحلبي الحقوقية، بيروت، 2007.
- 18- عكروم، ليندة. تأثيري التهديدات الأمنية الجديدة على العلاقات بين دول شمال وجنوب المتوسط . الأردن: دار ابن بطوطة للنشر و التوزيع، 2011.
- 19-عبد المنعم المشاط، "الإطار النظري للأمن القومي العربي" في د. عبد المنعم المشاط (محرر)، الأمن القومي العربي: أبعاده ومتطلباته (القاهرة: معهد البحوث والدراسات العربية، 1993)، ص ص 14-17.

قائمة المصادر و المراجع

- 20- عبد العال الديربي ومحمد صادق إسماعيل، الجريمة الإلكترونية، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2012.
- 21- عبد العزيز بن غرم الله آل جار الله، جرائم الإنترنت وعقوباتها وفق نظام مكافحة الجرائم المعلوماتية السعودي دراسة مقارنة (ويليه آثار العولمة على مستخدمي الإنترنت) ، دار الكتاب الجامعي ، الرياض ، الطبعة الأولى ، 2017 م.
- 22- عبد الرحمن بن عبد الله السيد: الأحكام الفقهية للتعاملات الإلكترونية (الحاسب الآلي وشبكة المعلومات و الانترنت)، دار الوراقين للنشر والتوزيع، بيروت، الطبعة الأولى، 2004.
- 23- علي عبد القادر القهوجي ، الحماية الجنائية للبيانات المعالجة إلكترونيا ، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت - والذي عقد بتاريخ 1 - 3 ماي 2000 كلية الشريعة والقانون - دولة الإمارات العربية.
- 24- عمرو عيسى الفقي: الجرائم المعلوماتية، جرائم الحاسب الآلي والانترنت في مصر والدول العربية، المكتب العربي الحديث، الاسكندرية 2006.
- 25- قوجيلي، سيد أمحد. تطور الدراسات الأمنية ومعضلة التطبيق في العامل العربي. أبو ظبي: مركز الإمارات للدراسات والبحوث الاستراتيجية، 2012
- 26- رائد العدوان ،"المعالجة الدولية لقضايا الإرهاب الإلكتروني"، محاضرة أُلقيت في دورة تدريبية بعنوان توظيف شبكات التواصل الاجتماعي في مكافحة الإرهاب ،الرياض، فيفري 2016
- 27- خالد حسن أحمد لطفي ، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية ، دار الفكر الجامعي ، الإسكندرية ، الطبعة الأولى ، 2020 م.
- 28- خالد ممدوح إبراهيم ، أمن الجريمة الإلكترونية ، الدار الجامعية - الإسكندرية 2008.

- 1- Barry,buzan.People,states and Fear.The international security problems in international 'romatons-london : wheatsh, 1983
- 2- Buzan,barry,and waereer , ole'region and powers : the structure of international security. Newyourk : combrige university, 2003
- 3- Gabriel weimann ,cyberterrorism : how real the threat ?united states institute of peace December 2004.
- 4- James Rosenau, Turbuence in World Politics: A Theory of change and continuity (New York: Harvester / Wheatsheab, 1990
- 5- Lee Kam Hing and Tan Chee-Beng (editors), **The Chinese in Malaysia** (New York: oxford university Press,2000
- 6- Lucas (A) : droit de Informatioque, paris, PUF,1987.
- 7- R. Ahmad and Z. Yunos, "A Dynamic Cyber Terrorism Framework," Int. J. Comput. Sci. Inf. Secur., vol. 10, no. 2, 2012.
- 8- Z. Yunos, R. Ahmad, S. M. Ali, and S. Shamsuddin, "Illicit Activities and Terrorism in Cyberspace : An Exploratory Study in the Southeast Asian Region," in Pacific Asia Workshop on Intelligence and Security Informatics (PAISI 2012), Malaysia, 29 May, Springer Lecture Notes in Computer Science, Volume 7299/2012, 2012 **النشريات**
- 1- وليد أحمد الروضان ، ما لفرق بين أمن المعلومات والأمن السيبراني ، صحيفة الجزيرة الإلكترونية ، مؤسسة الجزيرة للصحافة و الطباعة و النشر، 2018 ، العدد 16631 .
- 2- مفتاح بوبكر المطردي - الجريمة الالكترونية , والتغلب على تحدياتها - ورقة عمل مقدمة إلي المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان المنعقد في 23-25/9/2012.
- 3- تقرير الأونكتاد 10 نوفمبر 2005 ملتقى الأمم المتحدة حول التجارة والتنمية ص 2.
- 4- صالحة العمري: جريمة غسل الأموال وطرق مكافحتها-مجلة الاجتهاد القضائي، العدد الخامس، مخبر اثر الاجتهاد القضائي على حركة التشريع، جامعة محمد خيضر بسكرة.
- 5- التقرير الاستراتيجي العربي 1995م، القاهرة، مركز الدراسات السياسية والاستراتيجية بالأهرام 1996م.

قائمة المصادر و المراجع

6- تقرير الامم المتحدة، مكافحة استخدام تكنولوجيا المعلومات والانصالات للاغراض الاجرامية.

المجلات

- 1— ايمن السيد عبد الوهاب، "حركات الإسلام السياسي ونمط جديد من التفاعلات العربية"، السياسة الدولية، القاهرة، الأهرام، العدد 113، 1993م
- 2— محمد السيد سعيد، " تحليل مقارنة لتجارب التسوية الإقليمية"، مجلة السياسة الدولية، القاهرة، الأهرام، العدد 95، يناير 1989م،
- 3— صليحة محمدي، الارهاب الالكتروني والامن القومي للدول: نمط جديد وتهديدات مختلفة، المجلة الجزائرية للامن والتنمية.

المقالات

- 1— أيسر محمد عطية، دور الآليات الحديثة للحد من الجرائم المستحدثة، الإرهاب الالكتروني و طرق مواجهته، ورقة مقدمة في الملتقى العلمي، الجرائم المسحدثة في ظل التحولات و المتغيرات الاقليمية و الدولية، خلال الفترة 02-04 سبتمبر ، 2014،
- 2— هشام محمد فريد رستم، " القانون والكمبيوتر والانترنت" بحث مقدم بجامعة دولة الإمارات العربية المتحدة - 1 - 3 - ماي 2000.
- 3— كريستا سكولمان: عن جرائم الانترنت طبعتها وخصائصها، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية 19 و20 يونيو 2007.
- 4— عبدالله بن عبدالعزيز بن فهد العجلان، "الإرهاب الإلكتروني في عصر المعلومات" بحث مقدم إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت"، والمنعقد بالقاهرة في 2-4 جوان 2008.
- 5— رحيمة نميلي، " خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة "، مداخلة مقدمة في أعمال المؤتمر الدولي الرابع عشر، طرابلس، الموسوم بعنوان: الجرائم الإلكترونية طرابلس، يومي 24 و25 مارس 2017.

الرسائل العلمية

- 1— دردور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة لنيل شهادة الماجستير، شعبة القانون الجنائي، جامعة منثوري، قسنطينة، 2012- 2013
- 2— يوسف صغير، الجريمة المرتكبة عبر الإنترنت، مذكرة ماجستير، جامعة مولود معمري بتيزيوزو، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2012-2013.

قائمة المصادر و المراجع

- 3— سفيان سوير، جرائم المعلوماتية، مذكرة ماجستير، جامعة أبو بكر بلقايد بتلمسان، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2010-2011.
- 4— عبد اللطيف معتوق، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة ماجستير، جامعة العقيد الحاج لخضر بباتنة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2011-2012.
- 5— صالح شنين: الحماية الجزائرية لبرامج الحاسب الآلي، دراسة مقارنة رسالة لنيل شهادة الماجستير، جامعة بسكرة -كلية الحقوق والعلوم السياسية، 2007 – 2008.

المواقع الالكترونية

- 1— الجرائم الالكترونية، مقال منشور على موقع الجزيرة، على الرابط:
<https://www.aljazeera.net/encyclopedia/conceptsandterminology/2015/4/28>
- 2— عبد العال الديربي: الجريمة المعلوماتية – تعريفها – أسبابها وخصائصها، 13 يناير 2013، منشور على الموقع التالي: www.acconline.com/article.detail.aspx?id:7509
- 3— الأزمة الدولية ، خصائصها و مفاهيمها، نقلا عن الموقع: www.encyclopedia.org الموسوعة السياسية-political)
- 4— عميرة أيسر، الحروب السيبرانية بين الجزائر و إسرائيل، نقلا عن الموقع:
<https://www.raialyoum.com>
- 5— إيهاب شوقي، الإرهاب الالكتروني و جرائمه، من الموقع :
(<http://www.anntv.tv/new/showsubject.aspx?id=121062> د.ت.ن) تم تصفحه يوم يوم 28-2022-01 على الساعة 18.30.
- 6— أمن الفضاء الالكتروني، الامم المتحدة، مكتب مكافحة الارهاب، على الرابط التالي:
<https://www.un.org/counterterrorism/ar/cybersecurity>
- 7— [Mohd Shamir b Hashim](https://www.mohdshamirbhashim.com) , Malaysia's National Cyber Security Policy: The country's cyber defence initiatives:
<https://ieeexplore.ieee.org/document/5978782>
- 8— Neville, Spykerman, **Malaysia second in world broadband penetration - ranking**, Monday, 28 Oct 2013

<https://www.thestar.com.my/news/nation/2013/10/28/broadband-penetration-muhyiddin-yassin>

9-ماليزيا تكثف جهودها لمكافحة الجرائم الإلكترونية، على الرابط التالي:
<https://aswaqpress.com/electronic-attacked-in-malaysia>

10- [Chew Kherk Ying](#): Cybersecurity 2020 ,

<https://practiceguides.chambers.com/practice-guides/cybersecurity-2020/malaysia>

W.Media, Malaysia wages war on cybercrime, Published 10 April -11
2020: <https://w.media/malaysia-wages-war-on-cybercrime>

فهرس المحتويات	
	الإهداء
	الشكر
أ-ح	الفصل التمهيدي
ب	ملخص
د	المقدمة
الفصل الأول : التأسيس النظري لمفاهيم الجريمة السيبرانية والأزمات الإقليمية	
19-01	المبحث الأول : ماهية الجريمة السيبرانية
01	المطلب الأول: تعريف الجريمة السيبرانية
06	المطلب الثاني: خصائص الجريمة السيبرانية
11	المطلب الثالث: أنواع الجريمة السيبرانية:
25-19	المبحث الثاني: ماهية الأزمات الإقليمية
19	المطلب الأول: الأزمة و مفهوم الأمن الإقليمي
21	المطلب الثاني: مفهوم الأمن الإقليمي
23	المطلب الثالث : باري بوزان و مركب الأمن
25	خلاصة الفصل:
الفصل الثاني: تجليات الحرب السيبرانية بين الأنظمة	
45-26	المبحث الأول: الكيان الاسرائيلي المحتل و تجليات الحرب السيبرانية
26	المطلب الأول: طبيعة و أثر الحرب السيبرانية بين الكيان و المنظومة العربية
30	المطلب الثاني : الحرب السيبرانية الاسرائيلية على الجزائر
41	المطلب الثالث: مظاهر تهديد الارهاب الالكتروني لأمن الدول
73-46	المبحث الثاني: الموقف الداخلي و الدولي و استراتيجية المواجهة
46	المطلب الأول: الجهود الدولية لمكافحة الارهاب الالكتروني
57	المطلب الثاني: جهود الجزائر في مكافحة الجريمة الالكترونية
67	المطلب الثالث: الويب المظلم (الديب ويب)
74-73	الخاتمة :
81-75	قائمة المراجع والمصادر
83-82	فهرس المحتويات