دراسة لظاهرة الإرهاب الإلكتروني

A study of the phenomenon of electronic terrorism

فايزة نجاري بن حاج علي ♦

جامعة مولود معمري –تيزي وزو- الجزائر

nedjari.fayza15@gmail.com

تاريخ الإرسال: 2021/11/17	تاريخ القبول: 2021/12/14	تاريخ النشر: 2022/06/03

الملخص:

مهما اختلفت النظريات و تعددت الآراء و تباينت الفلسفات الأمنية المطروحة، و مهما اختلفت التوجهات و تعددت الرؤى في تعريف الإرهابوسبل مواجهته، إلا أن الإجماع على خطورة الظاهرة الإرهابية أمر واضح المعالم محسوم الموقف، و بظهور التكنولوجيا الرقمية و الطفرة المعلوماتية الهائلة التي شهدها العالم في أواخر القرن المنصرم، برز نمط جديد من أنواع الإرهاب يعتبر أكثر فتكا ودمارا، يهدد أمن البنا التحتية الحيوية للدول، ألا و هو الإرهاب الإلكتروني.

تعتبر آليات الإرهاب الإلكتروني بعيدة كل البعد عن العنف، فهي آليات مادتها الأساسية التكنولوجيا الرقمية و ساحة البرمجيات، و عليه فإن السياسة العامة للأمن السيبراني قد وضعت أسلحة رقمية و برمجيات دقيقة تعمل على إحباط تلك الهجمات من خلال عمليات التشفير، و برامج محاربة الفيروسات، و الجدران النارية الواقية، غير ان التحول في مفاهيم هذا الأخير-الأمن السيبراني- في العصر الحديث و الأخطار المحدقة به و تعدد الهجمات المبتكرة في تهديده، وضع المجتمع الدولي أمام مسؤوليات جديدة و تحديات صعبة، رغم ان هناك بعض الدول سارعت للوفاء بالتزاماتها القضائية بتحقيق الأمن و دعمه و ردع الساعين في زعزعته، عبر خلق سياسات حديثة في مواجهة هذا النوع من الإرهاب، و وضع خططا استراتيجية وقائية و ردعية متعددة تهدف من خلالها إلى كبح نشاط الإرهاب الإلكتروني على الساحة السيبرانية و الحد من فعاليته، كما قامت بحوكمة الأمن السيبراني و هذا من خلال خلق خلايا لإدارة الأزمات و المخاطر الناجمة عن هجمات هذا النوع الجديد من التهديد-الإرهاب الإلكتروني- وكذا توفير الموارد المادية و التقنية و البشرية الخاصة لذلك.

الكلمات المفتاحية:ارهاب، تجسس، تهديد، ترويع، مكافحة.

♦ المؤلف المرسل

Abstract:

Whatever the differences between the theories, opinions and philosophies of security, and whatever the differences between trends and visions in the definition of terrorism and the means to deal with it, the consensus on the seriousness of the phenomenon terrorist is clearly defined by the situation and with the emergence. digital technology and the huge information boom that the world has witnessed. At the end of the last century, a new type of terrorism appeared, considered more deadly and destructive, threatening the security of the vital infrastructure of countries, namely electronic terrorism.

The mechanisms of electronic terrorism are far removed from violence, as they are the mechanisms of its main substance, digital technology and software arena, and therefore the general policy of cyber security has developed digital weapons and software that thwart these attacks through encryption operations, and anti-virus and firewall protection programs. However, the evolution of the concepts of the latter - cybersecurity - in the modern era and the dangers that surround it and the multiplicity of innovative attacks that threaten it, has placed the international community in front of new responsibilities and difficult challenges, even if some countries have hastened to fulfill their legal obligations to ensure security and support it and deter those who seek to destabilize it By creating modern policies in the face of this type of terrorism, and by developing multiple preventive strategic plans and deterrents aimed at curbing the activity of electronic terrorism in the cyber arena and reducing its effectiveness, as well as the governance of cyber security by creating cells to manage crises and risks resulting from attacks of this new type threat - electronic terrorism - as well as the provision of specific material, technical and human resources for this purpose.

Keywords:.Terror, espionage, threat, intimidation, combat.

مقدمة:

مهما اختلفت النظريات و تعددت الآراء و تباينت الفلسفات الأمنية المطروحة, و مهما اختلفت التوجهات و تعددت الرؤى في تعريف الإرهابوسبل مواجهته، إلا أن الإجماع على خطورة الظاهرة الإرهابية أمر واضح المعالم، محسوم الموقف،فبظهور التكنولوجيا الرقمية و الطفرة المعلوماتية الهائلة التي شهدها العالم في أواخر القرن المنصرم، برز علينا نمط جديد من أنماط الإرهاب، يهدد أمن البنية التحتية الحيوية الحرجة للدول، كما لا يقل فتكا عن غيره من أنماط الإرهاب و أشكاله، ألا و هو الإرهاب الإلكتروني، الذي اعتبر بعض الباحثين آلياته مماثلة لأسلحة الدمار الشامل, ذلك بأنه يستهدف من خلالها أهدافا استراتيجية قد تصل إلى

التحكم عبر القرصنة في منشآت حيوية حرجة، فضلا عن قدرته في التحكم عبر برامجه في المفاعلات النووية، و أجهزة الرقابة الأمنية من شبكات النقل الجوي و البري و البحري، و قدرته اللامحدودة في اختراق بنوك المعلومات و الاطلاع من خلاله على أكثر معاملاتها سرية و حيوية, ناهيك عن كونه آلية بالغة النفاذ في تجنيد الإرهابيين و نشر التطرف بكل أشكاله.

و لقد عرفت وتيرة الإرهاب الإلكتروني تصاعدا مقلقا للمجتمع الدولي في السنوات الأخيرة، و لم يعد نطاقها يقتصر فقط على الجماعات الإرهابية المتطرفة، بل تعدى ذلك كله ليصبح آلية و وسيلة خطيرة في يد بعض الدول، التي تحقق من خلالها مكاسب سياسية مختلفة، و أهدافا سلطوية استبدادية متعددة، و خلق استراتيجيات جديدة في ممارسة النفوذ و رعايته مما يزيد من تعقد تحديات مواجهته و مجابهته من جهة، و تحديد معالمه و تميزه عن الحرب السيبرانية و المقاومة من جهة أخرى.

إن التحول في المفاهيم الأمنية في العصر الحديث بتحول الأخطار المحدقة به و تعدد الهجمات المبتكرة في تهديده قد وضع المجتمع الدولي أمام مسؤوليات جديدة و تحديات صعبة، و قد سارعت الكثير من الدول في محاولة للوفاء بالتزاماتها القضائية بتحقيق الأمن و دعمه و ردع الساعين في زعزعته، عبر خلق سياسات حديثة في مواجهة الإرهاب الإلكتروني،و وضع خططا استراتيجية وقائية و ردعية مختلفة، و كذا خلايا لإدارة الأزمات و المخاطر الناجمة عن هجماته.

و رغم المجهود الدولية التي تسعى من خلاله الدول إلى تحويط الساحة السيبرانية بمجموعة من الآليات الدفاعية ضد الهجمات الإرهابية، إلا أنها قد تخفق في إحباط تلك الهجمات و ردعها، و لكي لا ينفلت الجناة من العقاب، سعت الدول إلى خلق آليات تحقيق جديدة تمكن من خلالها الجهات الأمنية و الضبطية من الكشف عنها و ملاحقة الجناة و تقديمهم أمام العدالة، و قد وضعت لها حجيتها القانونية و قوتها الإثباتية أمام المحاكم المختصة، و من الآليات الحديثة التي لم تحظى بدراسة أكاديمية وافية، نجد الطب الشرعي الرقمي، الذي يجمع بين الطابع التخصصي التقني و بين الطابع القانوني، كما يعتبر آلية غاية في الفعالية في الكشف عن الجرائم الإرهابية السيبرانية، و تحديد الجناة و محاكمتهم بناء على تقاريرها.

الإرهاب الإلكتروني ممدد فعلي للأمن الوطني و الدولي، و مع هذا فإن المجال التشريعي لا يزال يعاني من قصور شديد، مع أن المجتمع الدولي يسعى حثيثا إلى وضع استراتيجية ذات فعالية قصوى في مواجهة هذه الظاهرة المستجدة و تحقيق الأمن الرقمي و السيبراني، و عليه فإننا نطرح الإشكالية التالية: **ما هو الإرهاب الإلكتروني؟ والى أي بعد تمكنت فيه الدول تأمين الساحة الإلكترونية ضد هجماته؟**

للإجابة على اشكاليتنا نتطرق لدراسة هذا الموضوع من حيث دراسة مفهوم الظاهرة التي تعتبر مشكل عويص و خطير اذ لا يوجد ضابط عالمي او حتى اقليمي موحد لتحديد ماهيته، ثم ان الوسائل المخصصة لمجابهته في الشق الثاني من البحث المقدم تثبت لنا مدى خطورة هذا النوع من الإرهاب، لنعمد في الخاتمة الى دراسة

تقييميةوإجابة عن الإشكالية مع توصيات قد تساهم بشكل فعال في تضييق الحصار على سلوكيات هذا الإرهاب ان لم نقل قد تجعل من مكافحته امر ليس بالمستحيل .

أولا- مفهوم الإرهاب الإلكتروني

1: تعريف الإرهاب الإلكتروني

يجب الإقرار بأن مسألة تعريف الإرهاب الإلكتروني تعتبر من المسائل المعقدة و الصعبة، فلم يرد لحد الآن تعريف واضح و دقيق يعالج هذه المسألة معالجة شافية كافية، و معظم التعاريف المقترحة هذه الظاهرة إنما تستند إلى المفهوم التقليدي للظاهرة الإرهابية، فالإرهاب الإلكتروني يلتقي مع الإرهاب التقليدي في الغرض و الهدف منه كما أشارت إلى ذلك **آين إيمبار**، فالإرهاب السيبراني بذلك لا يعتبر جريمة مستقلة بذاتها، بل هي جريمة تندرج ضمن الظاهرة الإرهابية التي يتم توظيف آليات فريدة في تنفيذها [1].

ذهب **دوروثيدينج** (**Dorothy Denning**) في تعريف الإرهاب السيبراني على أنه: **(هجمات غير قانونية أو تهديدات بالهجوم على أجهزة الكمبيوتر والشبكات والمعلومات المخزنة فيها، عند القيام به لتخويف أو إكراه حكومة أو شعبها على تعزيز أهدافهم السياسية أو الاجتماعية)**، أما **جيمس لويس** (James lewis) فقد ذهب في تعريفه على أنه: **(استخدام أدوات شبكة الكومبيوتر لغلق البني التحتية الوطنية الحرجة مثل الطاقة، النقل، المعاملات الحكومي، أو لإكراه أو تخويف الحكومة أو السكان المدنيين)**[2].

وذهبت الباحثة **بدرة هويمل الزين**، في تعريف على أنه: **(عبارة عن الاعتداء أو التهديد به ماديا أو معنويا، باستخدام وسائل إلكترونية، يصدر من الدول أو الجماعات أو الأفراد على السواء، و يمثل اعتداء على الإنسان في دينه، أو نفسه، أو عرضه، أو عقله، أو ماله، أو يكون إرهابا محله الفضاء الإلكتروني)** [3].

و نلاحظ عدم تجانس واضح في هذه التعريفات الثلاث رغم أننا نرى أنها الأكثر جودة بين كل التعريفات المقترحة، فكل تعريف من التعريفات الثلاث يركز على جانب و يهمل جانبا آخر، فتعريف **دروثيدينج** يهمل الهجمات التي تستهدف البنى التحية التي يتم تسيرها من خلال هذا الفضاء، بينما تعريف **جيمس لويس** نجده يهمل الهجمات التي تستهدف الفضاء الإلكتروني بحد ذاته، فضلا عن إهماله للهجمات المادية على الفضاء الإلكتروني و اقتصر على الأسلحة الإلكترونية فقط، أما **بدرة هويمل الزين**، فهو حاول بشكل جيد استدراك ما أهمل في التعريفين السابقين، غير أن أنه أهمل هو الآخر الهجمات التي تستهدف البنية التحتية الحرجة.

([1])نقلا عن: عبد القادر دندن و آخرون، العلاقات الدولية في عصر التكنولوجيات الرقمية: (تحولات عميقة... مسارات جديدة)، الطبعة الأولى، الأردن، مركز الكتاب العربي، 2021، ص 143.

([2])ZahriYunos, Rabiah Ahmad and Noor AzwaAzreenAbd Aziz, The Concept of Cyber Terrorism, **SEARCCT'S sélection of articles**, volume 01, Southeast Asia Regional Centre for Counter-Terrorism, ministry of foreugn affairs, Malaysia, 2013, PP. 68-79.

([3]) بدرة هويمل الزين، الإرهاب في الفضاء الإلكتروني: (دراسة مقارنة)، أطروحة دكتوراه في فلسفة في القانون العام،غير منشورة، كلية الحقوق، جامعة عمان العربية، 2012، ص 73.

و ترى الباحثة أن يعرّف الإرهاب الإلكتروني على أنه: (الاستغلال غير المشروع للثغرات الأمنية في نظم تشغيل أجهزة الكمبيوتر وآلات الاتصال والشبكات المتصلة المغلقة أو المفتوحة، أو بتنفيذ هجوم مادي، من أجل القيام بأعمال موصوفة بالخطورة والضرر على نفس تلك الأجهزة أو الآلات أو الشبكات وملحقاتها، والبني التحتية الحرجة المتعلقة بها، أو عن طريق توظيفها لدعم الأعمال الموصوفة بالإرهاب بهدف ممارسة الضغط عن طريق إثارة الذعر والرعب بدافع سياسي أو إيديولوجي أو بدافع الانتقام من شخص طبيعي كان أو معنوي).

2: خصائص الإرهاب الإلكتروني

يتميز الإرهاب الإلكتروني بخصائص و سمات تجعله متفردا عن الإرهاب التقليدي و يمكن حصرها في النقاط التالية:

- جريمة الإرهاب الإلكتروني جريمة ناعمة فهي جريمة لا تطلب عنفا و لا قوة مادية إذ يكفي وجود حاسب آلي متصل بشبكة الإنترنت للقيام بتوظيف الأسلحة الإلكترونية لتنفيذ هجمات إرهابية سيبرانية؛
- جريمة الإرهاب الإلكتروني جريمة عابرة للحدود، فهي جريمة عالمية لا تعترف بالحدود الإقليمية والسيادية؛
- تتميز أيضا جريمة الإرهاب الإلكتروني بأنها جريمة يعصب اكتشافها ويقل التبليغ عنها كما أنها جريمة معقدة و صعبة الإثبات كونها لا تترك أثرا ماديا يعول عليه في ذلك، كما أن الأدلة الإلكترونية غالبا ما يقدم الجناة على إتلافهابكل سهولة وبسرعة فائقة؛
- جريمة الإرهاب الإلكتروني جريمة يتعاون فيها في الغالب أكثر من شخص واحد وغالبا ما يكونون هؤلاء الأشخاص أصحاب معرفة مستفيضة بتقنيات المعلومات، أو ممكن لهم القدر الكافي من المعارف و الخبرات في مجال التعاطي مع هذه التقنيات[1].

3: التمييز بين الإرهاب الإلكتروني و غيره من المفاهيم

أ/التمييز بين الإرهاب الإلكتروني والمقاومة الإلكترونية

الإرهاب الإلكتروني هو من بين تجليات الحرب الإلكترونية و صورة من صورها، فهو ينطلق من الأسس و التصورات الإيديولوجية التي تتبناها الجماعة و تؤمن بها، و هدفه واضح و محدد و يتمثل في تجسيد التصورات الإيديولوجية للجماعة الإرهابية و إدراجها في صيغتها المادية، بينها المقاومة الإلكترونية هي تسخير الفضاء الإلكتروني للقيام بالاحتجاج على أوضاع سائدة أو لدفع الظلم و الاستبداد، و هي تقوم على أسس مشروعة معترف بها في القوانين و الأعراف الدولية كالدفاع الشرعي و الحق في تقرير المصير، فالفرق بين

(1)إسراء طارق جواد كاظم الجابري، الإرهاب الإلكتروني: (دارسة مقارنة)، جزء من متطلبات نيل شهادة الماجستير في القانون العام،غير منشورة، كلية الحقوق، جامعة النهروان، جمهورية العراق، 2012، ص: 37-38.

الإرهاب و المقاومة ينكشف بوضوح من خلال القصد الذي تسعى إلى تحقيقه، فالمقاومة تهدف إلى إزاحة اعتداء صدر عن محتل أو عن سلطة مستبدة، وغالبا ما يكون في إطار داخلي و لا يكتسب صفة العالمية، بينما الإرهاب ذو طابع دولي، و مقاصدها مستوحاة من إيديولوجيات متطرفة، و هجماتها ليست ذات أهداف نهائية بل هي وسيلة للتأثير السياسي و قلب موازين القوى [1].

تنبثق ضرورة التمييز بين الإرهاب الإلكتروني و المقاومة الإلكتروني من نفس الضرورة القائمة بين الإرهاب و المقاومة في إطار الفكر التقليدي، و يمكن حصر هذه الأهمية في ثلاث نقاط أساسية؛ تتجلى أولها في رصد الأحكام القانونية التي تتناول موضوع المقاومة كآلية يتم اللجوء إليها في تقرير المصير و مكافحة الاستعمار بكل مشتملاته، أما ثانيها فتتجلى في الإقرار بهذا الحق و جعله كآلية في بناء صلات وثيقة بين مختلف الشعوب قائمة على اعتبارات حقوق الإنسان و مقتضيات العدالة الدولية و حفظ السيادة و الوحدة الوطنية في الدولة، أما ثالثها فتتمحور على فكرة وضع إرهاب الدولة موضعا يمكن من خلاله أن يدان على الصعيد العالمي [2]

ب/التمييز بين الإرهاب الإلكتروني والجريمة الإلكترونية

الفرق بين الإرهاب الإلكتروني والجريمة الإلكترونية يتجلى في الغاية التي تحرك كل منهما، فالإرهاب الإلكتروني له أهداف سياسية يسعى إلى تحقيقها باللجوء إلى الساحة الإلكترونية، بينما الجريمة الإلكترونية لا ترتقي إلى هذا المستوى في قصدها الإجرامي، فمفهوم الإرهاب الإلكتروني و إن كان يتضمن جرائم إلكترونية كالتجسس و الاختراق و القرصنة و التشهير و التحريض عبر المواقع الإلكترونية و انتحال الشخصية و انتهاك الخصوصية و تهديد التجارة الإلكترونية و التعدي على التعاملات المالية و المصرفية و لكن هذا التضمن مقتصر فقط على التوظيف و لا يتعداه إلى الغاية [3]، فكلاالأعمال الإرهابية الإلكترونية هي من ضمن الجرائم الإلكترونية ولكن العكس غير صحيح [4]

ج/التمييز بين الإرهاب الإلكتروني وحرب المعلومات

تعرّف حرب المعلومات على أنها: **(...نشاط اتصالي مخطط له لا يحمل عنفا، يوجه نحو العدو، و يوجه من السلطات نحو شعبها و يوجه نحو الشعوب الصديقة...)**[5]، فحرب المعلومات من خلال هذا التعرف تتميز

([1])عادل عبد الصادق، الإرهاب الإلكتروني: (القوة في العلاقات الدولية، نمط جديد و تحديات مختلفة)، مصر، مركز الأهرام للدراسات السياسية و الاستراتيجية، 2009، ص 145.

([2]) ناصر الهاشمي، الإرهاب: (الجذور، المظاهر، و سبل المكافحة)، الطبعة الأولى،الأردن، دار الحامد للنشر و التوزيع، 2016، ص 163.

([3])عادل عبد الصادق، المرجع نفسه، ص 131.

([4])حكيم غريب، مكافحة الأشكال الجديدة للإرهاب الدولي، الجزء الثاني، أطروحة دكتوراه منشورة،كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر3، السنة الجامعية 2013-2014، الصفحة 793.

([5]) ياسر بكر، حرب المعلومات، الطبعة الثانية، توزيع أخبار اليوم، فبراير 2017، مصر، ص ص: 97-98: النسخة الرقمية على الرابط: = https://www.noor-book.com/

بأنها حرب لينة أو ناعمة، إذا يتم توظيف العنف كآلية أو وسيلة فيها، فضلا على أنها لا تستهدف فقط الأعداء و لا توظفها فقط الأنظمة الاستبدادية، بل تستهدف حتى الجهات الصديقة.

و ثمة علاقة وطيدة بين الإرهاب الإلكتروني وحرب المعلومات، ولا يمكن التمييز بينهما إلا وفق الغاية والهدف، فالإرهاب الإلكتروني يحوم حول مفهوم حرب المعلومات إذ أنه في حربه الإلكترونية يستعين بها لتحقيق أهدافه، والحرب المعلوماتية قد تتحول إلى إرهابي إلكتروني تأخذ تكييفها القانوني وهذا إما لكونها أداة تستعملها و توظفها الجماعات الإرهابية، وإما لكون وسائلها وأهدافها هي نفس تلك الأهداف والوسائل التي تتبناها الجماعات المتطرفة [1].

ثانيا-آليات الإرهاب الإلكتروني

1: آليات تستهدف الأنظمة الحاسوبية

يعتبر تعطيل الأنظمة المعلوماتية من بين أهم الآليات التي يستخدمها الإرهابيون في شن هجماتهم الإلكترونية إذ يقومون بإغراق المواقع أو الأنظمة الحاسوبية بكم هائل من الرسائل الإلكترونية في وقت واحد الأمر الذي يحدث فيها تلفا بليغا لتجاوز تلك الرسائل القدرة الاستيعابية للأنظمة، كما يتم أيضا استغلال الثغرات الأمنية التي يعاني منها أنظمة لاختراقها و العمل بعدها على تخريب نقطة الاتصال الأمر الذي يؤدي إلى التوقف الكلي أو الجزئي للأنظمة الحاسوبية كالهجمة الإلكترونية التي نفذتها منظمة إرهابية عام 2000 في أستراليا حيث تم القيام باختراق أنظمة الحاسوب و تخريب شبكة الصرف الصحي لأحدى مدنها [2].

2: آليات تستهدف المعلومات

تتخذ الهجمات السيبرانية العديد من الصور و الأشكال، و لعل أبرزها ما يلي:

أ/ **إتلاف المعلومات**

هو من أخطر آليات الإرهاب الإلكتروني التي استهدف المعلومات وهي تقع من خلال الحواسب الآلية أو الشبكات العنكبوتية [3]، ويتم فيها إتلاف البيانات المسجلة داخل الحواسيب وبيانات الشبكات المغلقة أو المفتوحة، وإتلاف بيانات البرامج الحساسة وبيانات نظم التحكم والمتابعة عن طريق اللجوء إلى استخدام البرمجيات الخبيثة من فيروسات وديدان قادرة إلى مسح و إتلاف المعلومات [4].

([1])عادل عبد الصادق، المرجع السابق،ص ص: 137-138.

([2]) حسن بن أحمد الشهري، الإرهاب الإلكتروني: (حرب الشبكات)، **المجلة العربية الدولية للمعلوماتية**، المجلد 04، العدد 08، جامعة نايف العربية للعلوم الأمنية، الرياض، يناير 2018، ص 15:

([3]) عبد الله بن حسين آل حجراف القحطاني، تطوير ممارات التحقيق الجنائي في مواجهة الجرائم المعلوماتية، جامعة نايف العربية للعلوم الأمنية، 2014، ص 42.

([4])حكيم غريب، مرجع سابق، ص ص: 820-821

ب/تزوير المعلومات

يتطلب هذا النوع من الصورة الإجرامية نوعا من معرفة تقنية عالية نظرا لارتباطها بالصياغة التقنية لبرامج معالجة المعلومات، وتتم باستعمال تقنيات مختلفة من أجل التغيير والتبديل والتلاعب بالبيانات أو المعلومات المخزنة في ذاكرة الحاسب الآلي [1].

ج/اعتراض المعلومات

يطلق عليه أيضا اسم الإعاقة أو التشويش، و هي آلية من الآليات التي يتم من خلالها التشويش على المعلومات من خلال توظيف إشعاعات أو موجات **كهرومغناطيسية** أو **هيدروصوتية** تعمل على الحيلولة دون قيام الوسائط والعتاد الإلكتروني والهيدروصوتي التي تقوم بتسيير الأسلحة والآليات الحربية والهياكل المعلوماتية الأخرى بدورها وعملها بكفاءة و فاعلية [2].

د/التجسس الإلكتروني

التجسس الإلكتروني هو اختراق يهدف إلى التعرف على المعلومات التي يحتويها الحاسب الآلي دون ممارسة أي شكل من أشكال الهجمات التي قد تؤدي إلى تلفها [3]، و غالبا ما يتم التركيز بصفة خاصة على الحصول وحيازة المعلومات الاقتصادية نظرا لأهميتها التي عبر عنها المرشح الأمريكي لرئاسة وكالات المخابرات الأمريكية في معرض جوابه عن سؤال وجهته إليه لجنة الكونجرس عما ينوي التركيز عليه في حالة قبول ترشحه فأجاب: التجسس الاقتصادي [4]، كما يتم التركيز أيضا على القطاعات الخاصة بالقوات المسلحة نظرا لأهمية المعلومات التي تحويها [5].

3: آليات تستهدف الأفراد

يتم استهداف الأفراد بهجمات الإرهاب الإلكتروني من خلال العديد من الآليات والهجمات السيبرانية، و يعد تجنيد الإرهابيين وحشدهم أحدى تلك الآليات، فضلا عن توظيف الفضاء الإلكتروني لأغراض تدريب الإرهابيين و منحهم ساحة للتلاقي وتبادل الخبرات، ويتم استهداف الأفراد أيضا عبر الفضاء السيبراني من

([1]) فصيل بدري، مكافحة الجريمة المعلوماتية في القانون الدولي و الداخلي، أطروحة لنيل شهادة الدكتوراه في القانون العام، غير منشورة،كلية الحقوق، جامعة الجزائر1 – بن يوسف بن خدة – السنة الجامعية 2017-2017، ص 37.

([2]) أنظر: أ. ي. بالي، ن. ب. مارين، موسوعة الحرب الإلكترونية، ترجمة: (يوسف إبراهيم الجهاني)، الطبعة الأولى، سورية،دار الحوار، 1992، ص 15.

([3]) سامر مؤيد عبد اللطيف، الحرب في الفضاء الرقمي رؤية مستقبلية، **مجلة رسالة الحقوق**، المجلد 07، العدد 02، كلية القانون،العراق، جامعة كربلاء، 2015، ص ص: 74-121: https://www.iasj.net/iasj/article/104012

([4]) نبيل علي, العرب و عصر المعلومات، عالم المعرفة، المجلس الوطني للثقافة و الفنون و الآداب، رقم الكتاب 184, الكويت، ص ص: 218-219.

([5]) نعيم سعيداني، آليات البحث و التحري في الجرائم المعلوماتية في القانون الجزائري, مذكرة لنيل شهادة الماجستير في العلوم القانونية، غير منشورة،كلية الحقوق و العلوم السياسية, جامعي الحاج لخضر، باتنة، السنة الجامعية 2012-2013، ص 64.

خلال انتهاك خصوصياتهم، والتعدي على حرماتهم، ونهب أموالهم، وخلق جو من الرعب من خلال نشر التهديدات و إرهابهم نفسيا.

المطلب الثالث: الخطورة الإجرامية للإرهاب السيبراني

الفرع الأول: الغاية من هجمات الإرهاب السيبراني

لا يختلف الإرهاب الإلكتروني في أهدافه عن الإرهاب التقليدي إلا في بعض الجزئيات البسيطة، فهو عدوان غاشم يسعى إلى تحقيق جملة من الأهداف يمكن اختزالها فيما يلي :

- التخويف والترويع ونشر الرعب بين الأفراد والدول والشعوب؛
- تقويض دعائم الأمن والطمأنينة في المجتمع؛
- الإضرار بالبني التحتية للمعلومات والمساس بسلامة المنشآت العامة والخاصة؛
- تهديد و إحراج سلطات الدول والمنظمات وابتزازها؛
- الرغبة في الثأر والانتقام [1].

4: أسباب الإرهاب السيبراني

هناك الكثير من الأسباب التي تقف وراء الإرهاب السيبراني، وأغلب تلك الأسباب هي نفسها أسباب الإرهاب التقليدي فيما عدا الجانب التقني والفني منها، و هي تتمحور في ما يلي:

- البطالة أو عدم وجود استقرار مالي لغياب الدخل الفردي المستقر، و غياب الأمن الصحي والثقافي، وسقوط الكثير من الأفراد في بؤرة الغلو العقائدي، و انتشار الفقر و الحرمان [2].

- الأنظمة الاستعمارية التي أحدثت تفاوتا كبيرا بين دول تستحوذ على ثروات العالم وأخرى غارقة في وحل التشتت والفقر الأمر الذي نتج عنه مشاعر الإحباط في الشعوب المستعمرة و ميلها إلى انتهاج النهج العنيف و المتطرف بغية تغيير هذا الواقع المزي الذي تعيشه [3].

- هشاشة أنظمة الكمبيوتر وضعفها والتي غدت مصدر قلق كبير لجميع قطاعات البنى التحتية فقواعد البيانات ووحدات التخزين أصبحت عرضة لأشكال متعددة من التهديدات السيبرانية لوجود ثغرات أمنية

([1]) إسراء طارق جواد كاظم الجابري، مرجع سابق، ص 39.

([2]) عمر أحمد شاهين، من أسباب الإرهاب: المشكلات الاجتماعية- مقدم إلى المؤتمر الإسلامي لمكافحة الإرهاب الذي تنظمه رابطة العالم الإسلامي، مكة المكرمة، المملكة العربية السعودية، 25 فبراير 2015، ص ص: 12-15.

([3])بلقاسم سلطانية و آخرون, علم الاجتماع الإعلامي، دار الفجر للنشر و التوزيع،ص 106.

يمكن أن ينفلت منها القراصنة [1] والتي تتمحور أساسا في ثغرات في أنظمة التشغيل والبرامج الملحقة به، ففي كل مرة يتم الكشف من مظاهر ضعف جديدة، ولا يكاد لو منا أي نظام [2].

- عالمية الفضاء الإلكتروني والذي نتج عنه تغير في مفاهيم المتعلقة بالحدود الجغرافية والإقليمية والأمن القومي وتشكل أنماط جديدة نت التهديدات والتحديات الأمنية [3] التي يشكل الإرهاب السيبراني واحدة منها.

- المجهولية والغفلة وعدم وضوح هوية مرتكبي الجرائم الإلكترونية وعجز الأجهزة الأمنية عن تتبع المجرمين المتورطين فيها، فهي تشكل لهم الخطالحمائي الأمثل ضد الرقابة الأمنية [4]ولعل جريمة الإرهاب السيبراني تعتبر من أهم وأبرز الجرائم السيبرانية التي تستغل هذه المجهولية لتصعيد نشاطاتها وعملياتها التخريبية.

- صعوبة اكتشاف و إثبات الجريمة فالإرهاب الإلكتروني جريمة لا أثر مادي لها، فهي إذا جريمة خفية في سلوكياتها، إذ يمكن للإرهابي أن يخفي بسهولة أي هجوم يقوم به عن طريق التلاعب الرقمي بالبيانات، كما أنها جريمة خفية في أثرها, فهي لا تترك وراءها أي أثر مادي خارجي ملموس, و هذا ما يجعلها التحري عنها أمر صعبا جدا، فطبيعة هذه الجريمة واتسامها بخاصية الخفاء تولد انجذاب الإرهابيين إليها أملا في الأمن من العقاب والمسائلة [5].

5: تداعيات الإرهاب السيبراني

إن الخطورة الإجرامية للإرهاب الإلكتروني تتجلى بكل وضوح من خلال التداعيات والآثار الخطيرة والتي تنجم عن هجماته والتي يمكن أن نختصرها فيما يلي:

- انتهاك خصوصية الأفراد وقمع حرية التعبير والرأي، حيث يتم استغلال هامش الحرية الذي تمنحه منصات الفضاء الإلكتروني للعمل على قهرهم واعتقالهم [6].

- المساس بالأمن الفكري للأفراد عبر خطاب الكراهية والتطرف التي تتميز بنوع من الجاذبية والقدرة على استمالة الشباب وتأجيج مشاعرهم في ساحات الفضاء السيبراني [7].

([1])فريج سعيد العوجي, حروب تقنية المعلومات, دار العلوم العربية للنشر و الإعلام, الطبعة الأولى, 2016, مصر, الصفحة 42

([2])didier**GODART**, sécurité informatique resèques stratégiques et solutions, éditions des Cci de wallonie SA, 2eme Edition Belgique 2005, p 33

([3])عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، جمهورية مصر العربية ،مكتبة الإسكندرية،، 2016، ص ص: 78-80

([4])عبد القادر بن عبد الله الفنتوخ، الجريمة في الأنترنت: (و طرق الحماية منها)، الرياض، مكتبة العبيكان،2012،ص ص: 24-25

([5])ثنيان ناصر آل ثنيان، إثبات الجريمة الإلكترونية، جامعة نايف العربية للعلوم الأمنية، 2012، الصفحة 24 وما بعدها.

([6])عبد الله كريشان، أثر الثورة المعلوماتية الإعلامية في نشر الوعي السياسي لدى الشباب الأردني، دار الجنان للنشر والتوزيع، 2015،ص 100.

([7])فايز بن عبد الله الشهري، الخطاب الفكري على شبكة الإنترنت، جامعة الملك سعود، 1429 هجرية، ص 37.

- تهديد البنية التحتية الحيوية الاقتصادية وتدمير النظم العسكرية ونظم المواصلات والاتصالات ومحاطات توليد الكهرباء وتوزيع المياه [1].

- التأثير على طبيعة العلاقات الدولية، و إشعال فتيل الحرب السيبرانية من خلال تسديد هجمات عالية الخطورة إلى منشآه الدول المستهدفة، وقد أشار الدكتور عادل عبد الصادق إلى عينة مهمة من هجمات بالغة الخطورة والتي قامت بها الولايات المتحدة الأمريكية وإسرائيل ضد المنشآت النووية الإيرانية باستخدام فيروس " ستاكس نات "، بالإضافة إلى قيامها بشن 231 هجوما إلكترونيا ضد روسيا وإيران والصين [2].

ثالثا- تصنيف هجمات الإرهاب السيبراني

1: إرهاب الدولة

لم يتفق الفقهاء والباحثون على الجزم بوجود إرهاب تمارسه الدولة أو تتورط فيه، فأشكال العنف التي تقوم الدولةبممارستها حسب رأي بعض الباحثين داخلة في الإطار العام لمفهوم العدوان المنصوص عليه في القوانين الدولية، غير أن مجمل الآراء تنصب في الإقرار بوجوده واعتباره صورة من صور الإرهاب المجرم دوليا[3]، وينقسم إرهاب الدولة إلى قسمين إثنين:

أ/إرهاب الدولة الداخلي

و هو إرهاب تقوم به السلطة الحاكمة من خلال أجهزتها و مؤسساتها أو عن طريق خلق أو دعم جماعات إرهابية من أجل إثارة الرعب و نشر الخوف والرهبة بين مواطنيها، و ذلك كله أجل بلوغ أهداف عادة ما تكون ضمانا لاستمرارية نظام الحكم القائم و الذي لا يتمتع بتأييد شعبي أو لإبعاد المواطنين عن ممارسة السياسة بقهرهم و التسلط عليهم أو من أجل إضعافإرادتهم في دعم المعارضين للحكومة القائمة، و هذا النوع من الإرهاب تمارسه عادة الأنظمة الديكتاتورية و المستبدة، غير أن الحكومات الديمقراطية يمكن أن تلجأ إلى ممارسة الإرهاب على مواطنيها في حالة استثنائية[4]، و يطلق على هذا النوع من الإرهاب اسم "الإرهاب القهري"، و يتم تعريفه على أنهاك **(الاستخدام المنظم لدرجة كثيفة من العنف بواسطة الأجهزة المركبة للدولة بهدف قمع أو الحد من المعارضة السياسية بين أفراد الشعب)**[5].

([1])حسنين شفيق، الإعلام الجديد والجرائم الإلكترونية، دار فكر وفن للطباعة والنشر والتوزيع، 2015، ص ص: 201-202.

([2])عادل عبد الصادق, أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، أوراق، العدد 23، مكتبة الإسكندرية، 2016،ض 65.

([3])زياد محمد السبعاوي، مجيد خضر السبعاوي، جريمة قتل الحسين و آل بين النبوة، جمهورية مصر العربية، المركز العربي للنشر و التوزيع، الطبعة الأولى، 2018، ص 92.

([4])نجيب نسيب, التعاون القانوني و القضائي في ملاحقة مرتكبي جرائم الإرهاب الدولي، أطروحة الدكتوراه في القانون منشورة، كلية الحقوق و العلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2014، ص ص: 51-52.

([5])حسن عزيز نور الحو، جلال خضير الزبيدي، الإرهاب في القانون الدولي: (دراسة قانونية مقارنة)، الطبعة الأولى،، الأردن، مركز الكتاب الأكاديمي2015، ص 108.

ب/إرهاب الدولة الخارجي

وهو إرهاب تمارسه حكومة دولة ما ضد المدنيين من مواطني دولة أخرى من أجل النيل من إرادتهم وتفكيك معنوياتهم وفضهم عن تأييد الحكومات التابعين لها، ويكون ذلك عن طريق اللجوء إلى استخدام القوة العسكرية أو طريق دعم الجماعات الإرهابية ماديا أو معنويا [1].

و لا ريب أن هاذين النوعين يظهران جليا في ظاهرة الإرهاب الإلكتروني عبر توظيف الفضاء الإلكتروني لقمع المعارضين و التجسس على حياتهم الشخصية و جمع المعلومات عنهم أو لتحديد مكانهم من أجل القبض عليهم أو من خلال قيادة حملة لتشويههم، كما يتم توظيف الإرهاب الإلكتروني ضد مواطني دولة أخرى سواء أكان ذلك بطريق ليّن، كأن يتم التجسس عليهم أو استعمال حرب المعلومات، أو بطريق صلب حينما يتم الحجوم على الأفراد و المواطنين مباشرة، كأن يتم إفراغ حساباتهم البنية، أو اختراق أجهزتهم.

2: إرهاب الجماعات

هو قيام مجموعة من الأفراد في إطار منظم بأعمال إرهابية ضد الدولة أو مؤسساتها ومرافقها أو ضد الشعب للعمل على خلق جو من الرهبة والخوف وانعدام الأمان من أجل إرباك البلاد وإدخالها في دوامة من عدم الاستقرار الداخلي و خلق مستوى عالي من الرعب و الذعر و التهديد تمهيدا للإسقاط نظام الحكم فيها [2]، فإرهاب الجماعات هو إرهاب منظم هيكليا و نشاطيا، فهو إرهاب يملك قيادة تديره و تخطط لنشاطاته بشكل كامل [3].

و إرهاب الجماعات الإلكتروني كثيرا ما تكون نواته جماعات إرهابية قائمة، على الأقل في الفترة الراهنة، فمعظم الإرهاب الإلكتروني لحد الأن إنما تمارسه في الغالب جماعات الإرهاب التقليدي، و لم يتسنى لنا أن نقع على حالة يكون فيها الإرهاب الإلكتروني كتنظيم ينشأ لهذا الغرض.

3: إرهاب الأفراد

إرهاب الأفراد هو قيام أشخاص بصفة منفردة وفردية بالإعدام على ارتكاب أعمال موصوفة بالإرهاب ضد مؤسسات الدولة أو ضد الأفراد من أجل تحقيق أهداف مختلفة ومحددة، و رغم أن إرهاب الأفراد داخل ضمن إرهاب الجماعات إلا أنه بينهما فوارق جوهرية [4]، و يعرف إرهاب الأفراد بأنه: **(جزء من الأعمال التي**

([1])نجيب نسيب، المرجع نفسه، ص ص: 53-54.

([2])يوسف كوران، جريمة الإرهاب والمسؤولية المترتبة عنها في القانون الجنائي الداخلي والدولي، مركز كردستان للدراسات الاستراتيجية، 2007، ص 47.

([3])نسيب نجيب، المرجع السابق، ص 49.

([4])يوسف كوران، المرجع نفسه، ص 47.

يقوم لها فرد أو مجموعة من الأفراد التي تعمل لحسابها الخاص دون أن يكونوا مدعومين من قبل الدولة أو منظمة إرهابية معينة)[1].

و يذهب فريق من الباحثين إلى القول بأن إرهاب الأفراد يعتبر إرهابا نادرا، فالغالب في الإرهاب أنه مرتبط بالجماعات الإرهابية التي تنظّر و تقود و تخطط، و إذا كان هناك حالات فردية للإرهاب فإنما هو إرهاب ذو أهداف قصيرة، فإنما أن تكون مالية أو ظرفية [2].

رابعا- الآليات الفاعلة في تحقيق الامن السيبراني

إن خصوصية الخطورة الإجرامية للإرهاب الإلكتروني تستدعي آليات ذات فعالية كبيرة من أجل ضمان التحقيق الأمثل فيها لردعها وإقامة الدليل الشرعي الذي يكون ذو حجية إثباتية أمام القضاء (المطلب الأول) و العمل على التأمين التقني للفضاء السيبراني (المطلب الثاني) مع هيكلته و حوكمته (المطلب الثالث) و العمل على صياغة الغطاء التشريعي الذي يضمن المكافحة الفعالة لهذه الظاهرة الخطيرة (المطلب الرابع).

1: الطب الشرعي الرقمي في مواجهة الإرهاب السيبراني

أ/تعريف الطب الشرعي الرقمي

إن الطب الشرعي عموما قد أصبح معروفا و كثير التداول في العصر الحديث، و أصبح يمارس على نطاق واسع في العديد من التخصصات، و يمكن تعريفه بأنه المعرفة العلمية و التقنية التي يتم انتهاجها و تطبيقها للتحري و التحقيق في الجرائم و تقدم الأدلة المساعدة للجهات القضائية من أجل حل المسائل الواقعة، فهي إذا نوع خاص من وسائل الإثبات ذات الملائمة لتكون مقبولة كأداة للإقناع و كدليل للإثبات، و إذا أخذنا بمفهوم الطب الشرعي بمعناه الواسع فإنه يضم مجموعة واسعة من الأدلة بما في ذلك الكيانات الرقمية و الهندسية[3]، و بذلك يمكن تعريفه على أنه: **(تحديد و فحص و إعادة بناء الأدلة المستخرجة من أي عنصر من عناصر أنظمة الكومبيوتر و شبكات الحواسيب ووسائطها، و الأجهزة الطرفية للحواسيب التي تسمح لمحللي الطب الشرعي بحل الجرائم المتعلقة بالكومبيوتر)**[4].

ب/مجال تطبيق الطب الشرعي الرقمي

يعمل الطب الشرعي الرقمي على استخلاص الأدلة الرقمية الجنائية من مختلف الوسائط الإلكترونية، و بذلك فإن مجال توظيفه واسع باتساع هذه الوسائط من جهة، و باتساع صيغة الدليل الإلكتروني من جهة

([1])نجيب نسيب، المرجع السابق، ص 48.

([2])هيثم عبد السلام محمد، مفهوم الإرهاب في الشريعة الإسلامية، الطبعة الأولى، لبنان، دار الكتب العلمية، 2005، ص 151.

([3]) MoniphiaOrleaseHewling, Digital forensics: an integrated approach for the investigation of cyber/computer related crimes, thesis degree of Doctor of Philosophy, University of Bedfordshire, September 13, 2013, PP. 19-20

([4]) (Jonathan A. **MATUSITZ**, Cyberterrorism: A postmodern view of networks of terror and how computer security experts and law enforcement officials fight them, thesis Doctor of Philosophy, GRADUATE COLLEGE, Graduate college, University of OKLAHOMA, Norman, Oklahoma, 2006, P.149.

ثانية، فضلا عن اتساع نطاق الإجرام الإلكتروني من جهة ثالثة، فأما عن اتساع الوسائط الإلكترونية، فإن الطب الشرعي الرقمي يمكن أن يكون محله كل جهاز إلكتروني يمكن من خلاله النفاذ إلى الفضاء الإلكتروني بمفهومه الواسع، و يشمل في ذلك الحواسيب، الهواتف الذكية، أجهزة التلفاز الذكية التي يمكن أن ترتيب بالإنترنت، اللوحات الإلكترونية، كاميرات المراقبة، الشبكات العالمية و ما إلى ذلك.

أما من ناحية اتساع الدليل الرقمي، فيمكن أن يكون مجال توظيف الطب الشرعي الرقمي في الحصول على مختلف الأدلة التي يمكن أن تتخذ شكل صور إلكترونية، أو نصوص إلكترونية، أو مشاهد و مقاطع مصورة أو صوتية [1]، كما يمكن أيضا أن يكون الدليل الرقمي عبارة عن أثر إلكتروني آخر كالعنوان الإلكتروني أو تعريف الارتباط [2]أو غير ذلك من الأدلة الأخرى، أما من ناحية الجريمة، فمجال تطبيق الطب الشرعي الرقمي واسع باتساع أنواع الجرائم التي يمكن أن يكون نشاطها على الفضاء الإلكتروني.

ج/تقارير الطب الشرعي الرقمي

يلعب الطبيب الشرعي بصفة عامة دورا توضيحيا مهما للعدالة، و ذلك لكونه خبيرا مختصا و مستشارا في مجال تخصصه، و عمله في ذلك هو تمحيص القضية المعنية من جانبها التقني أو الفني من خلال الإجابة عما طرح عليه من السلطة القضائية من أسئلة بما تمليه مبادئ الأخلاق المهنية من نزاهة و أمانة [3]،و هذا الأمر ينطبق على الطب الشرعي في المجال الرقمي، فالطبيب الشرعي الرقمي مهمته هي تقديم الآراء و الأدلة التي يمكن أن تبصّر الجهات القضائية بملابسات القضية الجنائية التي يكون محلها الفضاء الإلكتروني، و تقاريرهم في ذلك لا بد أن تتمتع بالنزاهة و المصداقية الكافية لقبولها أمام القضاء، و نظرا لكون هذا التخصص من بين التخصصات الحديثة التي تعاني من قصور تشريعي شديد، فإن قواعدها و أصول قبولها أمام الجهات القضائية غير واضحة المعالم، مع أننا نرى أن قواعد قبول هذه النوعية من التقارير لا تختلف كثيرا عن قواعد تقارير الخبراء، إلا في جانبها التقني و الفني.

([1]) بصائر علي محمد و مروى عبد الواحد حسن، الدليل الإلكتروني في مجال الإثبات الجنائي، **مجلة لارك للفلسفة و اللسانيات و العلوم الاجتماعية**، المجلد 03، العدد 27، جامعة واسط، 2017، ص ص: 271-285:

([2]) مصطفى عبد الباقي، التحقيق في الجريمة الإلكترونية و إثباتها في فلسطين: (دراسة مقارنة)، **دراسات، علوم الشريعة و القانون**، المجلد 45، العدد 04، ملحق 02، عمادة البحث العلمي و ضمان الجودة، الجامعة الأردنية، 2018، ص ص: 284-299:

([3]) سميرة بيطام، حجية الدليل البيولوجي أمام القاضي الجنائي، الأردن،أمواج للنشر و التوزيع، 2015، ص 81.

2: الحماية التقنية للفضاء الإلكتروني

أ/ آلية التشفير:

يعرّف نظام التشفير على أنه: **(إخفاء المعلومات الموثوقة بطريقة معينة، بحيث يكون معناها غير مفهوم للشخص غير المخول...)**[1]، و نظام التشفير ينقسم إلى عدة أقسام، يمكن أن تدرك على ثلاث فئات رئيسية، أولها التشفير المتناظر الذي يكون فيه المفتاح واحد في تشفير الملف و فك تشفيره، و ثانيها هو التشفير غير المتناظر، أين يكون هناك مفتاحين، عام و خاص، احدهما يشفر و الآخر يفك الشفرة، و ثالث الأنظمة هو نظام يخلط بين النظامين السابقين، فيشفر النص أو الملف بالتشفير المتماثل، ثم يشفر مفتاحه بالمفتاح العام، و يفك تشفيره بالمفتاح الخاص الذي يرسل إلى متلقي النص أو الملف [2].

ومن الواجب لضمان الحماية الكاملة للمعلومات الإلكترونية اعتماد تقنيات تشفير عالية الدقة و الكفاءة بحيث تستطيع تمويه و إبهام المعلومات التي يتم تناقلها عن طريق مختلف الشبكات، و من أبرز تقنيات التشفير التي يتم استخدمها على نطاق واسع هي تقنية (SSL) التي تتوفر في معظم البرامج و الأنظمة الإلكترونية، كما على الأجهزة القيام بالإجراءات اللازمة أيضا لحماية المعلومات الحساسة التي يتم حفظها و تخزينها بحيث يتم حفظها على هيئتها المشفرة ضمانا لعدم التصنت عليها [3].

ب/ برامج مكافحة الفيروسات

برنامج مكافحة الفيروسات هو: (برنامج يتم استخدامه لاكتشاف البرمجيات الضارة كفيروسات الحاسب، دودة الحاسب وأحصنة طروادة، وذلك لمنعها من إلحاق الضرر بالحاسوب أو سرقة البيانات الشخصية عن طريق إزالتها أو إصلاحها) [4]. ويوجد الكثير من البرامج المتعلقة بمكافحة الفيروسات و تتشابه إلى حد كبير ميما بينها في طريقة الاستخدام، إذ تبدأ في إجراء مسح عام للجهاز أو للملفات المختارة للبحث عن برمجيات ضارة داخل الملفات و في حالة وجودها يقوم بمسحها و إتلافها و تعقيم الملفات المصابة بها[5].

([1]) عبد الصبور عبد القوي علي المصري، التنظيم القانوني للتجارة الإلكترونية، الطبعة الأولى، لمملكة العربية السعودية، مكتبة القانون و الاقتصاد، 2012، ص 341.

([2]) سراح حليتيم، خصوصية التوقيع الرقمي في توثيق العقود الإلكترونية، **مجلة الباحث للدراسات الأكاديمية**، المجلد 05، العدد 02، جامعة باتنة 01، الحاج لخضر، باتنة، جويلية 2018، ص ص: 737-752: https://www.asjp.cerist.dz/en/article/59702

([3]) سمية بو مروان، الحكومة الإلكترونية ودورها في تحسين أداء الإدارات الحكومية: دراسة مقارنة، الطبعة الأولى، المملكة العربية السعودية، 2014 مكتبة القانون و الاقتصاد، ص 94.

([4]) مضاد فيروسات (برمجة)، ويكيبيديا، الموسوعة الحرة:
https://ar.wikipedia.org/wiki/%D9%85%D8%B6%D8%A7%D8%AF_%D9%81%D9%8A%D8%B1%D9%88%D8%B3%D8%A7%D8%AA_(%D8%A8%D8%B1%D9%85%D8%AC%D8%A9)

([5]) إيهاب أبو العزم، استخدام الحاسب الآلي وإدارة الملفات، الطبعة الأولى،ليبيا، دار الحكمة للطباعة والنشر والتوزيع، 2012، ص 124.

ج/ الجدران النارية

لقد ظهر استخدام الجدران النارية لتحقيق الأمن في أوائل التسعينات بحيث كانت تقوم بتصفية حركة البيانات اعتمادا على قوانين ومعاملات بسيطة، ثم تطورت حديثا لتكون لها مزايا أرخى مع احتفاظها باستخدام أسلوب فلترة وتصفية البيانات الواردة، من أهم ميزاتها الحديثة قدرتها على إنشاء الشبكات الافتراضية الخاصة، ومراقبة محتوى البيانات والوقاية ومكافحة الفيروسات، وقد تصل مزاياها إلى إدارة نوعية الخدمة [1].

3: حوكمة الأمن السيبراني

أ/ قاعدة البيانات المتعلقة بالأمن السيبراني

هناك الكثير من التجارب الفردية على مستوى الدول لإنشاء قاعدة بيانات معلوماتية عن الإرهاب حيث نجد إقرار مجلس الوزراء الألماني بإنشاء قاعدة بيانات لمكافحة الإرهاب تحتوى على أسماء ثم ثبت تورطهم في عمليات إرهابية حيث يتم صنع بروفايل للمشتبه بهم قائم على التلفون و البريد الإلكتروني و الديانة و السفر و والمعلومات البنكية والعلاقات التي تربطهم بالجماعات الإرهابية، كما ساهمت أستراليا أيضا في إنشاء قاعدة بيانات على نفس النمط و حملتها على شبكة الإنترنت، لكن لحد الآن لا يوجد قاعدة بيانات عالمية في مكافحة الأعمال الإرهابية [2]، فضلا من أن يكون هناك قاعدة بيانات متعلقة بالإرهاب السيبراني و طرق مكافحته وتحقيق الأمن و السلامة السيبرانية.

ب/ هيكلة الأمن السيبراني

تعتبر عملية تحول العمل الفردي للمؤسسات إلى عمل مشترك ومتكامل تتحدد فيه مجموعات عمل مشتركة بين الوكالات باعتماد التسلسل الهرمي لإدارة المخاطر السيبرانية من شأنه أن يحقق عدة مميزات وأهداف أهمها توفير الرقابة ومنهجيات التقييم وطرق تصنيف المخاطر، فتحديد الهياكل بحيث تعمل فيه المؤسسات والاستراتيجية بطريقة متكاملة و مشتركة من شأنه أن يضع استراتيجيات أكبر لضمان الأمن السيبراني في الداخل و الخارج، بحيث يعمل المسؤولون عن الاستراتيجية المختلفة معا و بطريقة تكاملية على التخطيط و التنفيذ و الاستخدام الأكثر فاعلية لموارد المؤسسات، والتحالف أيضا بين مختلف التخصصات الأخرى وبين تخصص الأمن السيبراني و التنسيق بين الخبراء الاستراتيجيين في كل المجالات بحيث يكون التكامل ضامنا لفهم مشترك للتهديدات و العواقب [3]، ليس هذا فحسب، بل إن هيكلة الأمن السيبراني من

([1]) حسن أيمن عبد الله فكري، الجرائم المعلوماتية: دراسة مقارنة، المملكة العربية السعودية، الطبعة الأولى، مكتبة القانون والاقتصاد، 2014، ص 180.

([2]) حسن بن أحمد الشهري، بناء قاعدة بيانات دولية لمكافحة الإرهاب، المجلة العربية للدراسات الأمنية والتدريب، المجلد 26، العدد 51، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، ص 227-251

([3]) (Deb**BODEAU**, Steve **BOYLE**, JennFabius-Greene, Rich **GRAUBART**, Cyber Security Governance, the MITRE corporation, 2010, pt 13-15

شأنه أيضا أن يحدد الأدوار و المسؤوليات الأمنية و التنسيق بين القطاع العام و الخاص في مواجهة الإرهاب السيبراني و تحقيق الأمن على الساحة الإلكترونية.

ج/التوعية في مجال الأمن السيبراني

يجب على المؤسسات والجهات المهنية التأكد من اكتساب العاملين بها التوعية الأمنية الكافية واللازمة والدراية الكاملة بمسؤولياتهم في مجال الأمن السيبراني، والعمل على تزويدهم بالمهارات والكفاءات اللازمة بتنظيم دورات تدريبية في مجال الأمن السيبراني بحيث تمكنهم من ممارسة المهام الأمنية المخولة إليهم من حماية للأصول المعلوماتية والتقنية و تحمل أعباء المسؤولية المنوطة بهم في إطار الأمن السيبراني، و على برامج التوعية أن تكون على قدر كبير من الشمول بحيث تتعرض لأهم المخاطر السيبرانية و ما يستجد فيها، و أساليب الحماية والتعامل معها و لاسيما التعامل مع البريد الإلكتروني و الأجهزة المحمولة ووسائط التخزين و خدمات تصفح الإنترنت و التعامل مع وسائل التواصل الاجتماعي، بالإضافة إلى توعية المستخدمين بالأمن بمقتضيات الأمن السيبراني [1].

4: الآليات التشريعية لمكافحة الإرهاب السيبراني

أ/ تحقيق الأمن السيبراني في التشريعات الداخلية

عمدت الكثير من الدول على تشريع قوانين تضمن الأمن والسلامة على الفضاء الإلكتروني وتضع الإطار القانوني للجرائم التي يتم ارتكابها على الفضاء الإلكتروني محددتها العقوبات الردعية لها. ففي فرسا مثلا نجد أن المشرع الفرنسي قد سن جملة من القوانين الردعية لحماية البيئة الإلكترونية وعلى رأسها القانون 19-99 المؤرخ بتاريخ 5 كانون ثاني 1988 الخاص ببعض جرائم المعلوماتية و ضمنه قانون العقوبات الفرنسي وجرم فيه الدخول إلى نظم المعالجة الآلية أو البقاء فيها بطريق غير مشروع و شدد العقوبة في أوضاع خاصة متعلقة بالتصرف في تلك المعطيات بالمحو أو التعديل أو التزوير أو الإتلاف[2]،و هناك أيضا تشريعات فرنسا أخرى كالقانون رقم 90/1170 المؤرخ بتاريخ 29 ديسمبر 1990 المتعلق بتنظيم الاتصالات.

أما في الجزائر فهناك العديد من التشريعات المتعلقة بمكافحة الجريمة السيبرانية و الإرهاب السيبراني و تامين الفضاء الإلكتروني و من بينها القانون رقم 15-04 المؤرخ 01 فبراير 2015 والمتعلق بالتوقيع و التصديقي الإلكترونيين و لاسيما في قسمه الجزائي، و القانون رقم 18-04 المؤرخ في 10 مايو 2018 والمتعلق بتحديد القواعد العامة المتعلقة بالبريد و الاتصالات الإلكترونية و لاسيما المواد 165، 171، 177 والقانون رقم 18-05 المؤرخ في 10 مايو 2018 و المتعلق بالتجارة الإلكترونية و لاسيما المادة 05 منه، و القانون رقم 20-05 المؤرخ في 28 افريل 2020 و المتضمن قانون الوقاية من التمييز و خطاب الكراهية و مكافحتها.

([1]) الضوابط الأساسية للأمن السيبراني، الهيئة الوطنية للأمن السيبراني، المملكة العربية السعودية، 2018، ص ص18 -20.

([2]) مركزهردو لدعم التعبير الرقمي، التنظيم القانوني و الجرائم الإلكترونية ما بين أمن المعلومات و تقييد الحريات، القاهرة، 2018، ص 21.

ب/ مكافحة الإرهاب الإلكتروني في إطار هيئة الأمم المتحدة

يعتبر الإرهاب الإلكتروني إرهابا خاصا و فريدا من نوعه، و خاصيته الأساسية أنه إرهاب عابر للحدود، و واسع باتساع رقعة الفضاء الإلكتروني، و لذلك فإن مكافحته و التصدي له لا بد أن تتخذ بعدا عالميا و دوليا، و ليس هناك هيئة دولة أكثر إجماعا عليها من هيئة الأمم المتحدة، لذلك فإنها أخذ في الفترة الأخيرة تصدر من القرارات التي من شأنها أن تشكل الوعي الدولي بخطورة هذا النوع من الإجرام السيبراني، و من بين أهم القرارات الصادرة في هذا الباب القرار 45-121 لسنة 1990، و القرار 53-70 الصادر في 04 ديسمبر 1997، و غيرها كثير [1].

ج/دور المنظمات الإقليمية في تحقيق الأمن السيبراني

لقد صدرت العديد من الاتفاقيات الإقليمية المعنية بمكافحة الجرائم و الإرهاب السيبرانيين، و أهم هذه الاتفاقيات، اتفاقية بودابيست التي تناولت العديد من المحاور الهامة، و من بين أبرزها و أهمها الجانب الموضوعي للجرائم السيبرانية، حيث خصصت فصولا لتحديد أنواع الجرائم و الانتهاكات التي تقع على الفضاء الإلكتروني، كما تعرضت الاتفاقية أيضا إلى الجوانب الإجرائية، و أساليب التعاون بين الدول الأطراف في مكافحة كافة الجرائم التي يتم على أو عبر الفضاء الإلكتروني [2]، كما و صدرت أيضا اتفاقية بنفس المضمون تقريبا عن الدول العربية التي وافق عليها مجلسا وزراء الداخلية و العدل العرب بالقاهرة في 21 ديسمبر 2010، أما إفريقيا فقد صدرت اتفاقية بشان أمن الفضاء الإلكتروني و حماية البيانات ذات الطابع الشخصي- و التي تناولت العديد من المحاور، و التي يبزر من بينها محور تعزيز الأمن الإلكتروني و مكافحة الجريمة الإلكترونية[3].

خاتمة:

تعتبر ظاهرة الإرهاب الإلكتروني من أخطر المظاهر الإجرامية في العصر- الحديث و التي اكتسبت صبغة عابرة للحدود الإقليمية مما يجعلها أكثر تهديدا للأمن و السلم العالميين، فضلا عن خطورتها على الأمن القومي للدول، و ما يزيد من حدة خطورتها عدم وجود آليات تقنية تضمن الدفاع و الردع الإلكتروني لها بصفة نهائية، و عدم وضوح استراتيجية فعالة لمواجهتها خاصة مع وجود فراغ تشريعي و تنظيمي كبير يسمح بالإفلات من المسائلة القانونية و العقاب بما يتناسب مع طبيعة الجرم، إذ أن معظم التشريعات الموجودة لم تتطلق إلى تنظيم قانوني خاص بجريمة الإرهاب السيبراني، رغم أنه يمكن توظيف النصوص التشريعية المتعلقة بالجرائم الإلكترونية عليها، و يمكن أيضا الاعتماد على نصوص مكافحة الإرهاب التقليدي عليها و ذلك باعتبارها جزءً من الظاهرة الإرهابية بصفة عامة.

([1])راجع في ذلك: مركز هردو لدعم التعبير الرقمي، المرجع السابق، ص 27.

([2])راجع في ذلك: الاتفاقية المتعلقة بالجريمة الإلكترونية، مجلس أوربا، بودابست 23 نوفمبر 2001.

([3])راجع في ذلك: اتفاقية الاتحاد الأفريقي بشأن أمن الفضاء الإلكتروني و حماية البيانات ذات الطابع الشخصي، الدور العادية الثالثة و العشرون، قمة رؤساء دول و حكومات الاتحاد الإفريقي، ملاية، عينيا الاستوائية، 17 يونيو 2014.

وعليه مما تقدم ذكره تقترح ما يلي

- الإجماع على تعريف موحد للإرهاب الإلكتروني.

- القيام بتحديث المعاهدات الدولية، و القوانين الداخلية بما يتلاءم و مكافحة الإرهاب الإلكتروني.

- توجيه الجهود نحو بناء أنظمة و برامج لإحباط الهجمات الإرهابية السيبرانية على الصعيد الوطني من جهة، و على الصعيدين الدولي و الإقليمي من جهة أخرى، و هذا من خلال تشجيع البحث التقني و البرمجي و توفير الوسائل و الموارد اللازمة لذلك.

- بناء الوعي و تثقيف أصحاب المصلحة و المستخدمين الأفراد بخطورة هجمات الإرهاب الإلكتروني.

- تعزيز التعاون القضائي الدولي دون المساس بالسلطة و السيادة الداخلية للدول.

قائمة المراجع

1. عبد القادر دندن و آخرون، العلاقات الدولية في عصر التكنولوجيات الرقمية: (تحولات عميقة... مسارات جديدة)، الطبعة الأولى، الأردن، مركز الكتاب العربي، 2021.

.02)ZahriYunos, Rabiah Ahmad and Noor AzwaAzreenAbd Aziz, The Concept of Cyber Terrorism, **SEARCCT'S sélection of articles**, volume 01, Southeast Asia Regional Centre for Counter-Terrorism, ministry of foreugn affairs, Malaysia, 2013.

03. بدرة هويمل الزين، الإرهاب في الفضاء الإلكتروني: (دراسة مقارنة)، أطروحة دكتوراه في فلسفة في القانون العام،غير منشورة، كلية الحقوق، جامعة عمان العربية، 2012.

04. إسراء طارق جواد كاظم الجابري، الإرهاب الإلكتروني: (دارسة مقارنة)، جزء من متطلبات نيل شهادة الماجستير في القانون العام، غير منشورة، كلية الحقوق، جامعة النهروان، جمهورية العراق، 2012.

05. عادل عبد الصادق، الإرهاب الإلكتروني: (القوة في العلاقات الدولية، نمط جديد و تحديات مختلفة)، مصر، مركز الأهرام للدراسات السياسية و الاستراتيجية، 2009.

06. ناصر الهاشمي، الإرهاب: (الجذور، المظاهر، و سبل المكافحة)، الطبعة الأولى، الأردن، دار الحامد للنشر و التوزيع، 2016.

07. عادل عبد الصادق، المرجع نفسه.

08. حكيم غريب، مكافحة الأشكال الجديدة للإرهاب الدولي، الجزء الثاني، أطروحة دكتوراه منشورة، كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر3، السنة الجامعية 2013-2014.

09. ياسر بكر، حرب المعلومات، الطبعة الثانية، توزيع أخبار اليوم، فبراير 2017، مصر، ص ص: 97-98: النسخة الرقمية على الرابط: =

https://www.noor-book.com/%D9%83%D8%AA%D8%A7%D8%A8-%D8%AD%D8%B1%D8%A8-%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA-%D9%8A%D8%A7%D8%B3%D8%B1-%D8%A8%D9%83%D8%B1-pdf

10. عادل عبد الصادق، المرجع السابق.

11. حسن بن أحمد الشهري، الإرهاب الإلكتروني: (حرب الشبكات)، **المجلة العربية الدولية للمعلوماتية**، المجلد 04، العدد 08، جامعة نايف العربية للعلوم الأمنية، الرياض، يناير 2018:

https://repository.nauss.edu.sa/handle/123456789/65241?show=full

12. عبد الله بن حسين آل جحراف القحطاني، تطوير مهارات التحقيق الجنائي في مواجهة الجرائم المعلوماتية، جامعة نايف العربية للعلوم الأمنية، 2014.

13. حكيم غريب، مرجع سابق.

14. فصيل بدري، مكافحة الجريمة المعلوماتية في القانون الدولي و الداخلي، أطروحة لنيل شهادة الدكتوراه في القانون العام، غير منشورة،كلية الحقوق، جامعة الجزائر1 – بن يوسف بن خدة – السنة الجامعية 2017-2017.

15. أنظر: أ. ي. بالي، ن. ب. مارين، موسوعة الحرب الإلكترونية، ترجمة: (يوسف إبراهيم الجهاني)، الطبعة الأولى، سورية، دار الحوار،1992.

16. سامر مؤيد عبد اللطيف، الحرب في الفضاء الرقمي رؤية مستقبلية، **مجلة رسالة الحقوق**، المجلد 07، العدد 02، كلية القانون، العراق، جامعة كربلاء، 2015، https://www.iasj.net/iasj/article/104012

17. نبيل علي, العرب و عصر المعلومات، عالم المعرفة، المجلس الوطني للثقافة و الفنون و الآداب، رقم الكتاب 184, الكويت.

18. نعيم سعيداني، آليات البحث و التحري في الجرائم المعلوماتية في القانون الجزائري, مذكرة لنيل شهادة الماجستير في العلوم القانونية، غير منشورة، كلية الحقوق و العلوم السياسية, جامعي الحاج لخضر، باتنة، السنة الجامعية 2012-2013.

19. إسراء طارق جواد كاظم الجابري، مرجع سابق،.

20. عمر أحمد شاهين، من أسباب الإرهاب: المشكلات الاجتماعية- مقدم إلى المؤتمر الإسلامي لمكافحة الإرهاب الذي تنظمه رابطة العالم الإسلامي، مكة المكرمة، المملكة العربية السعودية، 25 فبراير 2015

21.بلقاسم سلطانية و آخرون, علم الاجتماع الإعلامي، دار الفجر للنشر و التوزيع.

22.فريج سعيد العوجي, حروب تقنية المعلومات, دار العلوم العربية للنشر و الإعلام, الطبعة الأولى, 2016, مصر.

23didier**GODART**, sécurité informatique resèques stratégiques et solutions, éditions des Cci de wallonie SA, 2eme Edition Belgique 2005.

24.عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، جمهورية مصر العربية،مكتبة الإسكندرية،، 2016.

25.عبد القادر بن عبد الله الفنتوخ، الجريمة في الأنترنت: (و طرق الحماية منها)، الرياض، مكتبة العبيكان،2012،ص ص: 25-24

26.ثنيان ناصر آل ثنيان، إثبات الجريمة الإلكترونية، جامعة نايف العربية للعلوم الأمنية، 2012، الصفحة 24 وما بعدها.

27.عبد الله كريشان، أثر الثورة المعلوماتية الإعلامية في نشر الوعي السياسي لدى الشباب الأردني، دار الجنان للنشر والتوزيع،.

28.فايز بن عبد الله الشهري، الخطاب الفكري على شبكة الإنترنت، جامعة الملك سعود، 1429 هجرية، ص 37.

29.حسنين شفيق، الإعلام الجديد والجرائم الإلكترونية، دار فكر وفن للطباعة والنشر والتوزيع، 2015،

30. عادل عبد الصادق, أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، أوراق، العدد 23، مكتبة الإسكندرية.

31.زياد محمد السبعاوي، مجيد خضر السبعاوي، جريمة قتل الحسين و آل بين النبوة، جمهورية مصر العربية، المركز العربي للنشر و التوزيع، الطبعة الأولى، 2018،.

32.نجيب نسيب, التعاون القانوني و القضائي في ملاحقة مرتكبي جرائم الإرهاب الدولي، أطروحة الدكتوراه في القانون منشورة، كلية الحقوق و العلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2014.

33.حسن عزيز نور الحو، جلال خضير الزبيدي، الإرهاب في القانون الدولي: (دراسة قانونية مقارنة)، الطبعة الأولى،، الأردن، مركز الكتاب.

34.نجيب نسيب، المرجع نفسه.

35.يوسف كوران، جريمة الإرهاب والمسؤولية المترتبة عنها في القانون الجنائي الداخلي والدولي، مركز كردستان للدراسات الاستراتيجية، 2007.

36.نسيب نجيب، المرجع السابق.

37. يوسف كوران، المرجع نفسه،.

38. نجيب نسيب، المرجع السابق.

39.هيثم عبد السلام محمد، مفهوم الإرهاب في الشريعة الإسلامية، الطبعة الأولى، لبنان، دار الكتب العلمية، 2005،.

.40MoniphiaOrleaseHewling, Digital forensics: an integrated approach for the investigation of cyber/computer related crimes, thesis degree of Doctor of Philosophy, University of Bedfordshire, September 13, 2013.

.41Jonathan A. **MATUSITZ**, Cyberterrorism: A postmodern view of networks of terror and how computer security experts and law enforcement officials fight them, thesis Doctor of Philosophy, GRADUATE COLLEGE, Graduate college, University of OKLAHOMA, Norman, Oklahoma, 2006.

42. بصائر علي محمد و مروى عبد الواحد حسن، الدليل الإلكتروني في مجال الإثبات الجنائي، **مجلة لارك للفلسفة و اللسانيات و العلوم الاجتماعية**، المجلد 03، العدد 27، جامعة واسط، 2017:

https://lark.uowasit.edu.iq/index.php/lark/article/view/374

43. مصطفى عبد الباقي، التحقيق في الجريمة الإلكترونية و إثباتها في فلسطين: (دراسة مقارنة)، **دراسات، علوم الشريعة و القانون**، المجلد 45، العدد 04، ملحق 02، عمادة البحث العلمي و ضمان الجودة، الجامعة الأردنية، 2018:

https://fada.birzeit.edu/handle/20.500.11889/5731

44. سميرة بيطام، حجية الدليل البيولوجي أمام القاضي الجنائي، الأردن، أمواج للنشر و التوزيع، 2015، ص 81.

([1]) عبد الصبور عبد القوي علي المصري، التنظيم القانوني للتجارة الإلكترونية، الطبعة الأولى، لمملكة العربية السعودية، مكتبة القانون و الاقتصاد، 2012ا.

45. سراح حليتيم، خصوصية التوقيع الرقمي في توثيق العقود الإلكترونية، **مجلة الباحث للدراسات الأكاديمية**، المجلد 05، العدد 02، جامعة باتنة 01، الحاج لخضر، باتنة، جويلية 2018، ص ص: 737-752:

https://www.asjp.cerist.dz/en/article/59702

46. سمية بو مروان، الحكومة الإلكترونية ودورها في تحسين أداء الإدارات الحكومية: دراسة مقارنة، الطبعة الأولى، المملكة العربية السعودية، 2014 مكتبة القانون و الاقتصاد،.

47. مضاد فيروسات (برمجة)، ويكيبيديا، الموسوعة الحرة:

https://ar.wikipedia.org/wiki/%D9%85%D8%B6%D8%A7%D8%AF_%D9%81%D9%8A%D8%B1%D9%88%D8%B3%D8%A7%D8%AA_(%D8%A8%D8%B1%D9%85%D8%AC%D8%A9)

48. إيهاب أبو العزم، استخدام الحاسب الآلي وإدارة الملفات، الطبعة الأولى،ليبيا، دار الحكمة للطباعة والنشر- والتوزيع .124.

49. حسن أيمن عبد الله فكري، الجرائم المعلوماتية: دراسة مقارنة، المملكة العربية السعودية، الطبعة الأولى، مكتبة القانون والاقتصاد، 2014.

50. حسن بن أحمد الشهري، بناء قاعدة بيانات دولية لمكافحة الإرهاب، المجلة العربية للدراسات الأمنية والتدريب، المجلد 26، العدد 51، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، ص 227-251

.51Deb**BODEAU**, Steve **BOYLE**, JennFabius-Greene, Rich **GRAUBART**, Cyber Security Governance, the MITRE corporation, 2010.

52. الضوابط الأساسية للأمن السيبراني، الهيئة الوطنية للأمن السيبراني، المملكة العربية السعودية، 2018، ص.

53. مركزهردو لدعم التعبير الرقمي، التنظيم القانوني و الجرائم الإلكترونية ما بين أمن المعلومات و تقييد الحريات، القاهرة، 2018.

54.راجع في ذلك: مركز هردو لدعم التعبير الرقمي، المرجع السابق،.

55.راجع في ذلك: الاتفاقية المتعلقة بالجريمة الإلكترونية، مجلس أوربا، بودابست 23 نوفمبر 2001.

56.راجع في ذلك: اتفاقية الاتحاد الأفريقي بشأن أمن الفضاء الإلكتروني و حماية البيانات ذات الطابع الشخصي، الدور العادية الثالثة و العشرون، قمة رؤساء دول و حكومات الاتحاد الإفريقي، ملابة، غينيا الاستوائية، 17 يونيو 2014