RIMAK International Journal of Humanities and Social Sciences
ISSN: 2717-8293
Volume 6, Issue 1, January 2024

Received: 25/11/2023 **Accepted:** 20/12/2023 **Published:** 01/01/2024

THE GROWING THREAT TO THE SECURITY OF INSTITUTIONS AND COUNTRIES AS A RESULT OF ELECTRONIC PIRACY IN CYBERSPACE, "LIBYA IS A MODEL"

Prof.Dr.Ehab A. NAAS [1]

Rimar Academy ,Libya

Abstract:

Terrorism is the obsession experienced by all countries and people fear it to the point that it has become a part of daily life. Hardly a day goes by without a terrorist act beginning somewhere in the world. It has become unique and news of terrorism is shared in the media and receives the attention of people of all cultural levels and inclinations and existence. On the ground, it is due to policies and locations.

However, history has advanced, but at the present time even after another very exciting new one, especially after the amazing spread of modern technology and the emergence of the information network (the Internet), which enables devastating bloody operations to be carried out with minimal effort and many security elements continue to prevent them from scratch. Or catch them later.

Cyber war is one of the most prominent features of political and commercial conflicts between countries. In theory, cyber war means malicious activities through the Internet supported by a country, which target infrastructure, facilities, government institutions, industrial networks, and research, and are capable of disrupting the operation of vital infrastructure.

Key Words: Cyber Terrorism, Cyber War, Cyber Power, Cyber-Crime, Cyber Space.

http://dx.doi.org/10.47832/2717-8293.27.17

[1] alnaass.en@gmail.com

التهديد المتصاعد لأمن المؤسسات والدول نتيجة القرصنة الإلكترونية بالفضاء السيبراني "ليبيا أنموذجًا"

أ. د. إيهاب عبدالرزاق النعاس

أكاديمية ريمار ، ليبيا

الملخص:

الإرهاب هو الهاجس الذي تعيشه جميع الدول ويتخوف منه الأفراد حتى أصبح جزءًا من الحياة اليومية، ولا يكاد يمر يوم دون أن تقع عملية إرهابية في مكان ما من العالم، وأصبحت أنباء وأخبار الإرهاب تحتل الصدارة في وسائل الإعلام، وتحظى بانتباه الناس على اختلاف مستوياتهم الثقافية وميولهم السياسية ومواقع وجودهم على ظهر الأرض.

ورغم أن الإرهاب قديم قدم التاريخ إلا أنه في الوقت الحاضر اتخذ بعدًا جديدًا مثيرًا للقلق، خصوصًا بعد انتشار التقنية الحديثة بصورة مذهلة وظهور شبكة المعلومات (الإنترنت)، مما مكن الإرهابيون من تنفيذ عمليات دموية مدمرة بأقل مجهود ودون تمكن الجهات الأمنية من منعهم ابتداءً أو ضبطهم بعد ذلك.

وتعد الحرب السيبرانية من أبرز معالم الصراعات السياسية والتجارية بين الدول، من الناحية النظرية يقصد بالحرب السيبرانية الأنشطة الخبيثة من خلال شبكة الإنترنت المدعومة من دولة ما، والتي تستهدف البنى التحتية أو المنشأت والمؤسسات الحكومية والشبكات الصناعية والأبحاث، وهي قادرة على تعطيل تشغيل البنية التحتية الحيوية.

الكلمات المفتاحية: الإرهاب السيبراني، الحرب السيبرانية، القوة السيبرانية، الجريمة السيبرانية، الفضاء الإلكتروني.

المقدمة:

تختلف الجرائم السيبرانية كثيرًا عن الجرائم التقليدية من حيث طبيعتها ونطاقها ووسائلها وأدلتها، فقد أدى التطور السريع في مجال تقنية المعلومات والاتصالات وشبكة الإنترنت إلى ظهور أنماط جديدة من الجرائم جاءت عن طريق الاستغلال السيئ للتكنولوجيا، مما ترتب عليه خلق ظاهرة إجرامية جديدة تتم عن طريق هجمات واختراقات وتسلل داخل النظم المعلوماتية إما بغرض تدمير تلك النظم أو الحصول على معلومات سرية سواء عسكرية أو اقتصادية، كما أنه صار من السهل جدًا توظيفُ المجرمين والإرهابيين لهذه التقنيات المتطوِّرة في وضع خُططهم الإجرامية والإرهابية وتنفيذها والترويج لها حتى غدت هذه الوسائلُ العصرية تحدِّيًا جِدِّيًا خطرًا يهدِّد المجتمع الدَّولي بأسره.

ويرى الدكتور ناه ليانغ توانغ "Dr. Nah Liang Tuang" أستاذُ الدراسات الدَّولية في كلية راجاراتنام "Rajaratnam College" في سنغافورة أن هذا التقدُّمَ التقني إنما هو سيفٌ ذو حدَّين؛ فعلى حين يمكن أن يُستخدمَ الحدُّ الأول خطَّ دفاع في وجه الجريمة والإرهاب، فإن الحدَّ الآخر يُستغَل لاقتراف الجريمة وممارسة الإرهاب. إذ إن التقنية المتقدِّمة مثل تشفير الهواتف الذكية، وإنترنت الأشياء، وانتشار شبكات الحواسيب في القطاعات الحيوية الكافة ولا سيَّما الأمنية والعسكرية منها، وفي الخِدْمات العامَّة الحيوية، تُتيح الكثيرَ من المزايا العملية؛ ولكنها في الوقت نفسه تفتح البابَ على مِصراعَيه للتهديدات السيبرانية الخطِرة، وتتسبب بنشوء نِقاط ضعف سيبرانية.

وتتسم الجرائم السيبرانية بطابع سرية الهوية ولا تترك سوى القليل من الأثر، بالإضافة إلى ذلك لا تقف أمام الجرائم السيبرانية أي قيود إقليمية أو زمنية، ويمكن أن تسبب أضرارًا فورية لعدد لا يحصى من الضحايا.[2]

ويهدف "برنامج أمن الفضاء الإلكتروني والتقنيات الحديثة" التابع للجنة الأمم المتحدة لمكافحة الإرهاب على وجه الخصوص إلى تعزيز قدرات الدول الأعضاء على منع الهجمات السيبرانية التي تقوم بها الجهات الفاعلة الإرهابية ضد البنية التحتية الحيوية، كما يسعى أيضًا إلى تخفيف تأثير هذه الهجمات الإلكترونية واستعادة وإصلاح الأنظمة المستهدفة في حالة حدوث تلك الهجمات.[23]

مشكلة البحث:

يعد هذا البحث محاولة لتشخيص إشكاليات الحرب السيبرانية وقد يساعد في الإجابة على الأسئلة المحورية الآتية:

- ما هي الدوافع المولدة للإرهاب السيبراني؟
- ما هي طبيعة الانعكاسات الاجتماعية والسياسية والاقتصادية والأمنية وتأثيرها على الأمن القومي؟

---

[2](3) د. شريف محمد كشك، آلية جديدة للأمن السيبراني في دول الخليج، على الرابط التالي:

http://www.akhbar-alkhaleej.com/news/article/1217656

- ما هي السبل والتدابير لمواجهة الإرهاب السيبراني؟

أهداف البحث:

يهدف هذا البحث إلى تحليل طبيعة الإرهاب السيبراني وبيان نطاقه سعيًا لتحقيق عدة أهداف أهمها:

- إبراز خطورة ظاهرة الإرهاب السيبراني على الأمن القومي الليبي.

- محاولة الوقوف على العوامل المؤدية لانتشار ظاهرة الإرهاب السيبراني.

- إلقاء الضوء على القوانين الدولية والإقليمية والمحلية وآليات الدولة الليبية في التعامل مع الإرهاب السيبراني ومكافحته والحد من انتشاره.

أهمية البحث:

نظرًا لاتساع نطاق استخدام التكنولوجيا الحديثة في العالم، أصبحت ظاهرة الإرهاب السيبراني من أخطر القضايا الدولية في العصر الحاضر، لذا من الأهمية بمكان معرفة أسبابها لمعرفة كيفية مكافحتها في ظل قلة الدراسات والبحوث حولها.

يسعى الباحث إلى رصد جريمة الإرهاب السيبراني في ليبيا والآثار المترتبة عليها والجهود التي تبذلها الدولة لمكافحتها.

منهجية البحث:

يعتمد البحث على المنهج الوصفي التحليلي، وسيتم التركيز على الآلية التي تتبع لكبح هذه الظاهرة وفقًا للتشريعات الوطنية والاتفاقيات والقوانين الدولية.

وللوقوف على هذه الظاهرة بشكل يتناسب مع موضوع البحث؛ فإننا سوف نقوم بتقسيم البحث إلى المحاور التالية:

المحور الأول: ماهية جريمة الإرهاب السيبراني؟ والتمييز بينه وبين المفاهيم المتداخلة معه، ثم بيان خصائصه

المطلب الأول: تعريف الإرهاب السيبراني

المطلب الثاني: أسباب ودوافع الإرهاب السيبراني

المطلب الثالث: خصائص وأهداف الإرهاب السيبراني

المحور الثاني: مظاهر الإرهاب السيبراني وأشكاله

المطلب الأول: تبادل المعلومات الإرهابية ونشرها من خلال الشبكة المعلوماتية

المطلب الثاني: إنشاء المواقع الإرهابية السيبرانية

المطلب الثالث: تدمير المواقع والبيانات السيبرانية والنظم المعلوماتية

المطلب الرابع: التجسس السيبراني

المحور الثالث: الإرهاب السيبراني الخطر القادم

المطلب الأول: تهديدات ومخاطر الإرهاب السيبراني

المطلب الثاني: الاتفاقيات والقوانين الدولية والاقليمية في مكافحة الجرائم السيبرانية

المطلب الثالث: الجهود الدولية والوطنية في مكافحة جريمة الإرهاب السيبراني

المحور الرابع: الخاتمة، النتائج والتوصيات

المحور الأول

ماهية جريمة الإرهاب السيبراني

والتمييز بينه وبين المفاهيم المتداخلة معه

ويشتمل على المطالب الآتية:

المطلب الأول: تعريف الإرهاب السيبراني، والتمييز بينه وبين المفاهيم المتداخلة معه

المطلب الثاني: أسباب ودوافع الإرهاب السيبراني

المطلب الثالث: خصائص وأهداف الإرهاب السيبراني

المطلب الأول

مفهوم الإرهاب السيبراني

لقد تعددت تعاريف الإرهاب واختلفت وتباينت في شأنه الاجتهادات، ولم يصل المجتمع الدولي حتى الآن إلى تعريف جامع مانع متفق عليه للإرهاب، ويرجع ذلك إلى تنوع أشكاله ومظاهره وتعدد أساليبه وأنماطه واختلاف وجهات النظر الدولية والاتجاهات السياسية حوله، وتباين العقائد والإيديولوجيات التي تعتنقها الدول اتجاهه، فما يراه البعض إرهابًا يراه الآخر عملاً مشروعًا.

الإرهاب الإلكتروني:

"يعد من الجرائم المستحدثة التي أثرت عليها العولمة من خلال التكنولوجيا التي جعلت من العالم قرية صغيرة، وسهلت من طرق ارتكاب الإجرام ولعل أخطره هو الإرهاب الذي يحصد أرواح الأبرياء بسبب خسائر فادحة في الأموال والممتلكات، وأمام هذه التحديات يستوجب علينا تحديد مفهوم لظاهرة استعمال التكنولوجيا من قِبل الإرهابي، واستعراض خصائصها المميز لها عن باقي الجرائم."(4)[3]

يُعرف الإرهاب الإلكتروني بأنه "العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول أو الجماعات أو الأفراد على الإنسان، في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق، باستخدام الموارد المعلوماتية والوسائل الإلكترونية، بشتى صنوف العدوان وصور الإفساد".(5)[4]

---

[3] (4) عبدالنور بعجي، نسيمة مالك الإرهاب الإلكتروني: بين الجريمة وضرورة المكافحة، كلية الحقوق الجزائر،2022م، ص67.

[4] (5) يونس عرب، "الإطار القانوني للإرهاب الإلكتروني واستخدام الإنترنيت للأغراض الإرهابية، بحث مقدم لمؤتمر جامعة نايف العربية للعلوم".

ويعتمد الإرهاب الإلكتروني على استخدام الامكانيات العلمية والتقنية واستغلال وسائل الاتصال والشبكات المعلوماتية، من أجل تخويف وترويع الآخرين وإلحاق الضرر بهم أو تهديدهم، مثل ما حصل في العام 2000، حينما أدى انتشار فيروس الحاسوب "I love you" إلى إتلاف معلومات قدرت قيمتها بنحو (10) مليارات دولار أمريكي. وفي العام 2003م أشاع فيروس "بلاستر" الدمار في نصف مليون جهاز من أجهزة الحاسبات الإلكترونية، وقدر مجلس أوروبا في الإتفاقية الدولية لمكافحة الإجرام عبر الإنترنيت كلفة إصلاح الأضرار التي تسببها فيروس المعلوماتية بنحو (12) مليار دولار أمريكي سنويًا.(6[5]

كما عرفت الموسوعة السياسية الإرهاب بأنه: "استخدام العنف غير القانوني، أو التهديد به بأشكاله المختلفة كالاغتيال والتشويه والتعذيب والتخريب والنسف، بغية تحقيق هدف سياسي معين مثل كسر روح المقاومة والالتزام عند الأفراد، وهدم المعنويات عند الهيئات والمؤسسات، أو كوسيلة من وسائل الحصول على المعلومات أو مال، وبشكل عام هو استخدام الإكراه لإخضاع طرف مناوئ لمشيئة الجهة الإرهابية".(7[6]

في ثمانينيات القرن العشرين كان أول ظهور لمفهوم الإرهاب السيبراني "Cyberterrorism"، فقد عرفه باري كولين "Barry Collin" بأنه "هجمة إلكترونية غرضها تهديد الحكومات أو العدوان عليها، سعيًا لتحقيق أهداف سياسية أو دينية أو أيديولوجية، وأن الهجمة يجب أن تكون ذات أثر مدمر وتخريبي مكافئ للأفعال المادية للإرهاب".(8[7]

وفي عام 1998، نشر المشروع العالمي للجريمة المنظمة التابع لمركز الدراسات الإستراتيجية والدَّولية في واشنطن CSIS، تقريرًا بعنوان "جرائم الإنترنت والإرهاب الإلكتروني والحرب الإلكترونية: تجنب حدوث ووترلو إلكترونية "Cybercrime, Cyberterrorism and Cyberwarfare: Averting an Electronic Waterloo"، والذي كان يعتبر أولَ مساهمة رئيسة في هذا المجال.(9[8]

وعرف دورثي دينينغ "Dorothy Denningg" الإرهاب السيبراني على أنه "الهجوم القائم على مهاجمة الحاسوب، وأن التهديد به يهدف إلى الترويع أو إجبار الحكومات أو المجتمعات لتحقيق أهداف سياسية أو دينية أو عقائدية، وينبغي أن يكون الهجوم مدمرًا وتخريبيًّا لتوليد الخوف بحيث يكون مشابهًا للأفعال المادية للإرهاب".(10[9]

يعرفه جيمس لويس "James Lewiss" على أنه "استخدام أدوات شبكات الحاسوب في تدمير أو تعطيل البنى التحتية الوطنية المهمة مثل: الطاقة والنقل، والعمليات الحكومية، أو بهدف ترهيب حكومة ما أو مدنيين".(11[10]

---

[5] (6) علي عدنان الفيل، الإرهاب الإلكتروني، مجلة الجامعة الخليجية، المجلد 2، قسم القانون، العدد 2010/2.

[6](7) عبد الوهاب الكيالي، الموسوعة السياسية، ج7 (بيروت: المؤسسة العربية للدراسات والنشر، 1994)، ص153.

[7](8)عادل عبد الصادق، الإرهاب الإلكتروني: القوة في العلاقات الدولية نمط جديد وتحديات مختلفة (القاهرة: مركز الدراسات السياسية والاستراتيجية،2009)، ص109.

[8](9)عبد الستار عبد الرحمن، الإرهاب السيبراني خطر يهدد العالم، على الرابط التالي:

https://imctc.org/Arabic/ArticleDetail/Index/637180424114481635

[9](10) Denning,Dorothye.,"Cyber terrorism", Global Dialogue, Aug 2000, p10

[10](11) https://smtcenter.net/?p=8215

وتعرفه وزارة الدفاع الأمريكية بأنه "عمل إجرامي يتم الإعداد له باستخدام الحاسبات ووسائل الاتصالات وينتج عنه عنف وتدمير أو بث الخوف تجاه متلقي الخدمات بما يسبب الإرتباك وعدم اليقين".(12[11]

ويعرفه مكتب التحقيقات الفيدرالي الأمريكي على أنه "الهجوم المتعمد ذو الدوافع السياسية ضد أنظمة المعلومات، وبرامج الكمبيوتر، والبيانات المخزنة من قبل مختلف الفاعلين".

ويعرف الإرهاب السيبراني على أنه نقطة التقاء الفضاء الإلكتروني والإرهاب، وهو يشير إلى الهجمات والتهديدات غير القانونية بالهجوم على أجهزة الكمبيوتر والشبكات والمعلومات المخزنة فيها عندما يتم ذلك لتخويف أو إكراه حكومة أو شعبها لتحقيق أهداف سياسية أو اجتماعية.(13[12]

وهو التهديد أو الهجوم غير القانوني بشن هجماتٍ على أجهزة الكمبيوتر، وأنظمة المعلومات، والبرامج، والبيانات، بهدف ترهيب وإكراه الحكومات تحقيقًا لمختلف الأهداف.

والإرهاب السيبراني هو محاولة خبيثة ومتعمدة من قبل فرد أو منظمة لاختراق نظام المعلومات الخاص بفرد أو مؤسسة.(14[13]

يميز البعض من الباحثين نوعين من الإرهاب السيبراني؛ يشير أولهما إلى الإرهاب السيبراني الخالص " Pure Cyber Terrorism"، والذي يتصل بالهجمات المباشرة على البنية التحتية للضحية لتحقيق أهداف مختلفة، بينما يُشير الثاني إلى الإرهاب السيبراني الهجين "Hybrid Cyber Terrorism"، وفيه يستخدم الإرهابيون الفضاء السيبراني في مختلف الأنشطة الدعائية والحرب النفسية، والتخطيط لهجمات إرهابية فعلية، وتجنيد أعضاء جدد، وجمع الأموال، والتبرعات... الخ.(15[14]

أولاً: هناك تداخل بين مفهوم الإرهاب السيبراني وبين عدد من المفاهيم الأخرى، سنستعرضها بإيجاز وهي:

1. القوة السيبرانية:

يعرفها دانيال كوين على أنها "استخدام الفضاء السيبراني لخلق مزايا والتأثير على الأحداث في جميع البيئات العملياتية وعبر أدوات القوة." ويقصد بالعملياتية المجالات الخمسة للقوة وهي البحرية، والبرية،

[11](12) صليحة محمدي، الإرهاب الإلكتروني والامن القومي للدول: نمط جديد وتهديدات مختلفة، المجلة الجزائرية للأمن والتنمية، ص67.

[12](13) R. Ahmad and Z. Yunos, "A Dynamic Cyber Terrorism Framework" Int. J. Comput. Sci. Inf. Secur., vol. 10, no. 2, pp. 149–158, 2012.

[13](14) What Are the Most Common Cyber Attacks?:https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

[14](15) رغدة البهي، الإرهاب السيبراني: المفهوم والسمات والأنماط، المركز المصري للفكر والدراسات الاستراتيجية، على الرابط التالي:

https://www.ecsstudies.com/7141

والجوية، والفضائية والفضاء السيبراني. كما يقصد بأدوات القوة، الأبعاد الأربعة للقوة والمتمثلة في الدبلوماسية، والمعلومات، والاقتصاد والجيش.(16[15]

2. الجريمة السيبرانية:

لا يوجد تعريف محدد للجريمة السيبرانية، فهناك من يعرفها على أنها "كل فعل ضار بالآخرين عبر استعمال الوسائط الإلكترونية مثل: الحواسيب، أجهزة الموبايل، شبكات الاتصالات الهاتفية، شبكات نقل المعلومات، شبكة الإنترنت أو الاستخدامات غير القانونية للبيانات الحاسوبية أو الإلكترونية عموما". (17[16]ويعرفها آخرون بأنها "نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود."(18[17]

3. الحرب السيبرانية:

يقصد بالحرب السيبرانية أساليب الحرب ووسائلها التي تعتمد على تكنولوجيا المعلومات وتستخدم في سياق نزاع مسلح.

أي هي الهجمات والعمليات التي ترتكب ضد أو بواسطة شبكات الحواسيب وأنظمة البيانات بين الدول أو الجماعات المسلحة المنظمة في سياق نزاع مسلح، أو سياسات الردع المتبادل.(19[18]

وتعد الحروب السيبرانية ميدان رابع من ميادين الحروب فهي حروب خفية تقتحم الأنظمة الإلكترونية وتسبق العمل العسكري.

تستهدف الحرب السيبرانية الأنظمة العسكرية والبنية التحتية الحيوية للدولة فضلاً عن الشبكات الذكية وشبكات المراقبة الإشرافية وحيازة البيانات (SCADA) التي تسمح لها بالعمل والدفاع عن نفسها.(20[19]

تصنف الهجمات السيبرانية ضمن أبرز المخاطر التي تحيط بالدول، حيث زادت حجم الهجمات السيبرانية بين الدول في الفترة الحالية، لذلك قامت الدول بتخصيص وحدات إلكترونية خاصة بالأمن السيبراني وزادت من حجم صلاحياته.(21[20]

---

[15](16) فريدة طاجين، سياسات الدفاع الماليزية في ظل التهديدات الأمنية للبيئة الرقمية: الواقع والتحديات، ص342.

[16](17) http://www.ifegypt.org/NewsDetails.aspx?Page_ID=1244&PageDetailID=1324

[17](18) محمود أحمد القرعان، الجرائم الإلكترونية (عمان: دار وائل للنشر والتوزيع، الطبعة الأولى، 2017)، ص11.

[18](19) هالة أحمد الرشيدي، هل من حرب سيبرانية بين الولايات المتحدة وروسيا؟، جريدة الأهرام، 4 يناير 2021.

[19](20) حمدون إ. تورية، البحث عن السلام السيبراني، الإتحاد الدولي للإتصالات والإتحاد العالمي للعلماء، 2011، ص ص 8،9.

[20](21) https://www.europarabct.com

4. الأمن السيبراني:

الأمن السيبراني هو ممارسة حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية، وعادة ما تهدف هذه الهجمات الإلكترونية إلى الوصول إلى المعلومات الحساسة أو تغييرها أو تدميرها وابتزاز المال من المستخدمين أو مقاطعة العمليات التجارية العادية.(22[21]

5. البيئة الرقمية:

تعرف البيئة الرقمية على أنها سياق أو مكان يتم تمكينه بواسطة التكنولوجيا والأجهزة الرقمية، التي غالباً ما تنتقل عبر الإنترنت، أو غيرها من الوسائل الرقمية، مثل شبكة الهاتف المحمول تشكل السجلات والأدلة على تفاعل الفرد مع البيئة الرقمية بصمتها الرقمية.(23[22]

المطلب الثاني

أسباب ودوافع الإرهاب السيبراني

الأسباب العامة للإرهاب السيبراني:

إن أسباب الإرهاب ودوافعه تختلف في درجة أهميتها حسب الاتجاهات السياسية والظروف الاقتصادية والأحوال الاجتماعية وكذلك الاختلاف الديني والعقائدي، ويمكننا إيجاز أسباب ظاهرة الإرهاب فيما يلي:

أولاً: الدوافع الشخصية:

تتعدد الدوافع الشخصية المؤدية للإرهاب، ويمكن بيان أبرزها في الآتي:

1. افتقاد الشخص لأهمية دوره في الأسرة والمجتمع وفشله في الحياة الأسرية، مما يؤدي إلى اكتساب بعض الصفات السيئة ومن ضمنها عدم الشعور بالانتماء والولاء للوطن.

2. الرغبة في الظهور وحب الشهرة بحيث لا يكون الشخص مؤهلا فيبحث عما يؤهله باطلا فيشعر ولو بالعدوان والتخريب والتدمير.

[21](22) What Is Cybersecurity? https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

[22](23) What is Digital Environment, https://www.igi-global.com/dictionary/models-of-competences-for-the-real-and-digital-world/7610

3. نقمة الشخص على المجتمع الذي يعيش فيه نتيجة للظلم وإهدار الحقوق.

ثانيا: الدوافع الفكرية:

تتنوع الدوافع الفكرية المؤدية لظاهرة الإرهاب ويمكن بيان أهمها فيما يلي:

1. الجهل بمقاصد الشريعة الإسلامية المتمثل بالظن لا باليقين والتثبت، والفهم الخاطئ للدين، وتفسيره تفسير خاطئ والجهل بقواعد الدين الحنيف وآدابه وسلوكه.

2. الانقسامات الفكرية المختلفة بين التيارات المتنوعة والمختلفة.

3. التطرف وهو أمر بالغ الخطورة في أي مجال من المجالات وخاصة المجالات الفكرية.

ثالثاً: الدوافع السياسية:

من أبرز الأسباب والدوافع السياسية لظاهرة الإرهاب ما يأتي:

1. غياب العدالة الاجتماعية وعدم المساواة في توزيع الثروة الوطنية والتفاوت في توزيع الخدمات والمرافق العامة والتقصير في أمور الرعية.

2. معاناة بعض المجتمعات والشعوب الدولية من الظلم والاضطهاد والسيطرة الاستعمارية وسلب الأموال وخرق القوانين والمواثيق الدولية مما يدفع الشعوب إلى التشدد والتطرف.

المطلب الثالث

خصائص وأهداف الإرهاب السيبراني

للإرهاب السيبراني العديد من الخصائص التي تميِّزه عن الإرهاب في صورته التقليدية، والتي تسعى في نهاية الأمر لتحقيق أهداف غير مشروعة.(24[23]

أولاً: خصائص الإرهاب السيبراني:

يتميز الإرهاب السيبراني بعدة خصائص وسمات:

1. إن الإرهاب السيبراني إرهاب عابر للقارات والحدود وغير خاضع لنطاق إقليمي محدود.

(24)[23]علي عدنان الفيل، الإجرام الإلكتروني: دراسة مقارنة، ط1(بيروت: منشورات زين القانونية، 2011)، ص74.

2. صعوبة اكتشاف أثر الجاني في مرتكب واقعة الإرهاب السيبراني، حيث يوجد العديد من الصعوبات التي تقف حائلًا دون الوصول لدليل مادي يربط الجاني بالواقعة.

3. الإرهاب السيبراني يعد أحد أخطر أنواع الإرهاب، إذ أنه يؤثر بالسلب على الأمن القومي للدولة المستهدفة، وفي هذا الصدد يقول بيتر غرابوسكي "Peter Grabowski" "إن طريقة توظيف تقنية المعلومات الواسعة تعتبر وسيلة لتسهيل الإرهاب، ومن ذلك قرصنة المعلومات الاستخباراتية، واستخراج البيانات، وجمع الأموال، والتوظيف والتعبئة والتدريب عن بعد، مثل التدريب على استخدام تقنية الهجوم ومهاراته، ومشاركة المعلومات ونشر الأدلة مثل أدلة صنع الأسلحة وغيرها".(25[24]

4. الإرهاب السيبراني لا يحتاج عند ارتكابه إلى العنف والقوة بل يتطلب حاسب آلي متصل بالشبكة المعلوماتية ومزود ببعض البرامج اللازمة لذا يوصف بأنه من قبيل الجرائم الناعمة التي لا تتطلب استخداما للقوة في معناها العنيف أو المسلح.

5. مرتكب الجريمة السيبرانية لديه الخبرة في استخدام تكنولوجيا المعلومات، وبالتالي تكون أهدافه ليست صعبة، وبالتالي صعوبة إثبات قيامه بالجريمة نظرًا لسرعة غياب الدليل الرقمي وسهولة إتلافه وتدميره.

ثانيًا: أهداف الإرهاب السيبراني:

يهدف الإرهاب السيبراني إلى تحقيق جملة من الأهداف غير المشروعة، ويمكننا بيان أبرز تلك الأهداف:

1. نشر الرعب والخوف بين الأشخاص والدول والشعوب المختلفة والإخلال بالأمن العام وزعزعة الطمأنينة.

2. إلحاق الضرر بالبنية التحتية المعلوماتية وتدميرها والإضرار بوسائل الاتصالات وتقنية المعلومات أو بالأموال والمنشآت العامة والخاصة.

3. جمع الأموال اللازمة لتمويل العمليات الإرهابية.

(25)[24]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 أبوظبي، 2006، ط1، ص338.

المحور الثاني

مظاهر الإرهاب السيبراني وأشكاله

ويشتمل على المطالب الآتية:

المطلب الأول: تبادل المعلومات الإرهابية ونشرها من خلال الشبكة المعلوماتية

المطلب الثاني: إنشاء المواقع الإرهابية السيبراني

المطلب الثالث: تدمير المواقع والبيانات السيبراني والنظم المعلوماتية

المطلب الرابع: التجسس السيبراني

المطلب الأول

تبادل المعلومات الإرهابية ونشرها من خلال الشبكة المعلوماتية

إذا كان التقاء الإرهابيين والمجرمين في مكان معين لتعلم طرق الإجرام والإرهاب وتبادل الأفكار والمعلومات صعبًا في الواقع فإنه عن طريق الشبكات المعلوماتية تسهل هذه العملية كثيرًا، إذ يمكن أن يلتقي عدة أشخاص في أماكن متعددة وفي زمن معين ويتبادل بعضهم الحديث والاجتماع عبر الشبكة المعلوماتية، بل يمكن أن يجمعوا لهم أتباعًا، وأيضًا نشر أفكارهم ومبادئهم من خلال المواقع والمنتديات وغرف الحوار الإلكتروني.

وعلى الرغم من أن البريد الإلكتروني (E-mail) أصبح من أكثر الوسائل استخدامًا في مختلف القطاعات، وخاصة قطاع الأعمال لكونه أكثر سهولة وأمنًا وسرعة لإيصال الرسائل، إلا أنه يعد من أعظم الوسائل المستخدمة في الإرهاب الإلكتروني، وذلك من خلال استخدام البريد الالكتروني في التواصل بين الإرهابيين وتبادل المعلومات فيما بينهم، بل إن كثيرًا من العمليات الإرهابية التي وقعت في الآونة الأخيرة كان البريد الإلكتروني فيها وسيلة من وسائل تبادل المعلومات وتناقلها بين القائمين بالعمليات الإرهابية والمخططين لها ويقوم الإرهابيون كذلك باحتلال البريد الإلكتروني والاستفادة منه في نشر أفكارهم والترويج لها والسعي لتكثير الأتباع والمتعاطفين معهم عبر الرسائل الإلكترونية.

فمن خلال الشبكة المعلوماتية تستطيع المنظمات والجماعات الإرهابية نشر أفكارها المتطرفة، والدعوة لمبادئها المنحرفة، والسيطرة على وجدان الأفراد واستغلال معاناتهم من أجل تحقيق أغراضهم غير المشروعة والتي تتعارض مع مصلحة المجتمع.

يستخدم الإرهابيون الشبكة العالمية للمعلومات الانترنت بشكل يومي لنشر أفكارهم الهدامة ولتحقيق أهدافهم السيئة، ومن الممكن إبراز أهم استخداماتهم للشبكة فيما يلي:

أولاً: الاتصال والتخفي

تستخدم الجماعات والمنظمات الإرهابية المختلفة الشبكة العالمية للمعلومات في الاتصال والتنسيق فيما بينهم نظرًا لقلة تكاليف الاتصال والوسائل لاستخدام الشبكة مقارنة بالوسائل الأخرى، كما توفر الشبكة للإرهابيين فرصة ثمينة في الاتصال للتخفي وذلك عن طريق البريد الإلكتروني أو المواقع والمنتديات وغرف الحوار الإلكتروني، حيث يتم وضع رسائل مشفرة تأخذ طابعًا لا يلفت الانتباه فلا يضطر الإرهابي الإفصاح عن هويته كما أنها لا تترك أثرًا واضحًا يمكن أن يدل عليه.(26[25]

ثانيًا: جمع المعلومات الإرهابية

تمتاز الشبكة المعلوماتية بوفرة المعلومات الموجودة فيها، كما أنها تعتبر موسوعة إلكترونية شاملة متعددة الثقافات ومتنوعة المصادر وغنية بالمعلومات الحساسة التي يسعى الإرهابيون للحصول عليها، كمواقع المنشآت النووية، ومصادر توليد الطاقة، وأماكن القيادة والسيطرة والاتصالات ومواعيد الرحلات الجوية والمعلومات المختصة بسبل مكافحة الإرهاب نظرًا لما تحتويه من معلومات تفصيلية مدعمة بالصور الضوئية.

ثالثًا: التخطيط والتنسيق للعمليات الإرهابية

العمليات الإرهابية عمل على جانب كبير من التعقيد والصعوبة فهي تحتاج إلى تخطيط محكم وتنسيق شامل وتعتبر الشبكة العالمية للمعلومات وسيلة اتصال بالغة الأهمية للجماعات الإرهابية، حيث تتيح لهم حرية التخطيط الدقيق والتنسيق الشامل لشن هجمات إرهابية محددة في جو مريح، وبعيدًا عن أعين الناظرين مما يسهل على الإرهابيين ترتيب تحركاتهم وتكثيف هجماتهم. (27[26]

رابعًا: الحصول على التمويل

من خلال الشبكة المعلوماتية العالمية وعن طريق الاستعانة ببيانات إحصائية منتقاة من المعلومات الشخصية التي يُدّخلها المستخدمون على الشبكة المعلوماتية، فمن خلال الاستفسارات والاستطلاعات الموجودة على المواقع الإلكترونية يقوم الإرهابيون بالتعرف على الأشخاص ذوي المشاعر الرقيقة والقلوب الرحيمة ومن ثم استجداؤهم بدفع تبرعات مالية لأشخاص اعتباريين يكونون واجهة لهؤلاء الإرهابيين، ويتم ذلك بواسطة رسائل البريد الإلكتروني أو من خلال مساحات الحوار الإلكترونية بطريقة ذكية وأسلوب مخادع بحيث لا يشك المتبرع بأنه سيساعد إحدى التنظيمات الإرهابية.

خامسًا: التعبئة وتجنيد الإرهابيين

[25](26) حسنين شفيق، الإعلام الجديد والجريمة الإلكترونية التسريبات .. التجسس الإلكتروني .. الإرهاب، دار فكر وفن، مصر2014، ص 292.

[26](27) حسنين شفيق، مصدر سبق ذكره،2014، ص292.

تستخدم الجماعات والمنظمات الإرهابية الشبكة المعلوماتية العالمية في نشر ثقافة الإرهاب والترويج لها، وبث الأفكار والفلسفات التي تنادي بهم كما تسعى جاهدة إلى توفير أكبر عدد ممكن من الراغبين في تبني أفكارها ومبادئها، ومن خلال الشبكة المعلوماتية تقوم التنظيمات الإرهابية بتكوين قاعدة فكرية لمن لديهم ميول واستعداد للإنخراط في الأعمال التدميرية والتخريبية مما يوفر لديها قاعدة لمن تجمعهم نفس الأفكار والتوجهات فيسهل تجنيدهم لتنفيذ عمليات إرهابية في المستقبل.

إن استقدام عناصر جديدة داخل التنظيمات الإرهابية يحافظ على بقائها واستمرارها لذا فإن الإرهابيين يقومون باستغلال تعاطف بعض أفراد المجتمع مع قضاياهم، فيجتذبونهم بأسلوب عاطفي وعبارات حماسية براقة وذلك من خلال غرف الحوار والمنتديات والمواقع الإلكترونية.

سادساً: التدريب الإرهابي السيبراني

تحتاج العمليات الإرهابية إلى تدريب خاص ويعد التدريب من أهم هواجس التنظيمات الإرهابية وقد أنشئت معسكرات تدريبية سرية كما ظهر بعضها في وسائل الإعلام، لكن مشكلة معسكرات التدريب الإرهابية أنها دائمًا معرضة للخطر ويمكن اكتشافها ومداهمتها في أي وقت لذا فإن الشبكة المعلوماتية بما تحتويه من خدمات ومميزات أصبحت وسيلة مهمة للتدريب والتخطيط والتنفيذ، كما قامت بعض الجماعات الإرهابية بإنتاج أدلة إرشادية للعمليات الإرهابية، وهذه الأدلة يمكن نشرها عبر الشبكة المعلوماتية لتصل إلى الإرهابيين في مختلف أنحاء العالم وغني عن البيان ما تشتمل عليه الشبكة المعلوماتية من كم هائل من المواقع والمنتديات والصفحات التي تحتوي على كتيبات وإرشادات تبين كيفية تصنيع القنابل والمتفجرات والمواد الحارقة والأسلحة.

سابعًا: إصدار البيانات الإلكترونية

تقوم المنظمات الإرهابية باستخدام الشبكات المعلوماتية في نشر بياناتها الإرهابية المختلفة، وذلك عن طريق المواقع الإلكترونية أو بواسطة رسائل البريد الإلكتروني أو من خلال منتديات الحوار وساحاته، وقد ساعدت القنوات الفضائية التي تسارع في الحصول على مثل هذه البيانات الإرهابية ومن ثم تقوم بنشرها عبر وسائل الإعلام في مضاعفة انتشار تلك البيانات ووصولها إلى مختلف شرائح المجتمع.

وتأخذ البيانات الصادرة من قبل التنظيمات الإرهابية اتجاهات متنوعة فتارة ترسم أهدافًا وخططًا عامة للتنظيم الإرهابي، وأحيانًا تكون للتهديد والوعيد لشن هجمات إرهابية معينة في حين تصدر معلنة عن تبني تنفيذ عمليات إرهابية محددة، كما تصدر تارة أخرى بالنفي أو التعليق على أخبار وتصريحات صادرة من جهات أخرى(28[27].

المطلب الثاني

إنشاء المواقع الإرهابية الإلكترونية

(28)[27]عبد الرحمان السند، وسائل الإرهاب الإلكتروني- حكمها في الإسلام وطرق مكافحتها، اللجنة العلمية للمؤتمر 15 العالمي عن موقف الإسلام من الإرهاب، جامعة الإمام محمد بن سعود الإسلامية، ص5.

يقوم الإرهابيون بإنشاء وتصميم مواقع لهم على الشبكة العالمية للمعلومات الإنترنيت لبث أفكارهم الضالة والدعوة إلى مبادئهم المنحرفة ولإبراز قوة التنظيم الإرهابي، وللتعبئة الفكرية وتجنيد إرهابيين جدد، ولإعطاء التعليمات والتلقين الإلكتروني، وللتدريب الإلكتروني من خلال تعليم الطرق والوسائل التي تساعد على القيام بشن هجمات إرهابية، فقد أنشأت مواقع إرهابية إلكترونية لبيان كيفية صناعة القنابل والمتفجرات والأسلحة الكيماوية الفتاكة ولشرح طرق اختراق البريد الإلكتروني وكيفية اختراق وتدمير المواقع الإلكترونية والدخول إلى المواقع المحجوبة، ولتعليم طرق نشر الفيروسات ونحو ذلك.(29[28]

والموقع عبارة عن معلومات مخزنة بشكل صفحات وكل صفحة تشتمل على معلومات معينة تشكلت بواسطة مصمم الصفحة باستعمال مجموعة من الرموز تسمى لغة تحديد النص الأفضل (hyber text mark up language html) ولأجل رؤية هذه الصفحات يتم طلب استعراض شبكة المعلومات العالمية (www browser) ويقوم بحل رموز ((htmlوإصدار التعليمات لإظهار الصفحات المكتوبة وإذا كان الحصول على مواقع افتراضية أو وسائل إعلامية كالقنوات التلفزيونية والإذاعية صعبًا بالنسبة للإرهابيين فان إنشاء مواقع خاصة بهم على الشبكة العالمية للمعلومات "الانترنت" لخدمة أهدافهم وترويج أفكارهم الضالة أصبح سهلاً وممكنًا، ولذا فإن معظم التنظيمات الإرهابية لها مواقع إلكترونية وهي بمثابة المقر الإفتراضي لها.

إن الوجود الإرهابي النشط على الشبكة المعلوماتية متنوع ومراوغ بصورة كبيرة فإذا ظهر موقع إرهابي اليوم فسرعان ما يغير عنوانه الإلكتروني غدًا ثم يختفي ليظهر مرة أخرى بشكل جديد وتصميم مغاير وعنوان إلكتروني مختلف، بل تجد لبعض المنظمات الإرهابية آلاف المواقع حتى تضمن انتشارًا أوسع، وحتى لو تم منع الدخول على بعض هذه المواقع أو تعرضت بعضها للتدمير تبقى المواقع الأخرى ويمكن الوصول إليها، ومن الأمثلة على بعض المواقع الإلكترونية التي قام بإنشائها وتصميمها بعض التنظيمات الإرهابية ما يأتي:(30[29]

1. موقع النداء: وهو الموقع الرسمي لتنظيم القاعدة بعد أحداث الحادي عشر من سبتمبر عام 2001، ومن خلاله تصدر البيانات الإعلامية للقاعدة.

2. ذروة السنام: وهي صحيفة إلكترونية دورية للقسم الإعلامي لتنظيم القاعدة.

3. صوت الجهاد: وهي مجلة نصف شهرية يصدرها ما يسمى تنظيم القاعدة في جزيرة العرب، وتتضمن مجموعة من البيانات والحوارات مع قادة التنظيم ومنظريه.

4. البتار: وهي مجلة عسكرية إلكترونية متخصصة تصدر عن تنظيم القاعدة، وتختص بالمعلومات العسكرية والميدانية والتجنيد.

(29)[28]مصطفى يوسف كافي، ماهر عودة الشمايلة، محمود عزت اللحام، الإعلام والإرهاب الإلكتروني، الطبعة الأولى، دار الإعصار العلمي، عمان . الأردن، 2015، ص154.

(30)[29] إيهاب شوقي، الإرهاب الإلكتروني وجرائمه، http://www.assakina.com/awareness-net/rebounds/81251.html

وقد وجد الإرهابيون غايتهم في تلك الموارد المعلوماتية والوسائل الإلكترونية التي جلبتها حضارة التقنية في عصر المعلومات فأصبح للمنظمات العديد من المواقع على الشبكة العالمية للمعلومات، وصارت تلك المواقع من أبرز مظاهر وأشكال الإرهاب الإلكتروني.

أما التنظيم الإرهابي "داعش" فله أكثر من 50ألف موقع الكتروني، و90 ألف صفحة باللغة العربية على موقع التواصل الاجتماعي «فيس بوك» و40 ألفًا بلغات أخرى، وهذا ما ساهم في تجنيده حوالي 3400شاب شهريًا عبر حملاته الإلكترونية، وهذا حسب تقرير للخبير الأمني في قضايا الإرهاب الرقمي جيف باردين "Jeff bardin"[30]31)."

المطلب الثالث

تدمير المواقع والبيانات الإلكترونية والنظم المعلوماتية

تقوم التنظيمات الإرهابية بشن الهجمات الإرهابية السيبرانية من خلال الشبكة المعلوماتية؛ بقصد تدمير المواقع والبيانات الإلكترونية والنظم المعلوماتية، وإلحاق الضرر بالبنية المعلوماتية التحتية وتدميرها، وتستهدف الهجمات الإرهابية في عصر المعلومات ثلاثة أهداف أساسية غالبًا، وهي الأهداف العسكرية والسياسية والاقتصادية، وفي عصر ثورة المعلومات تجد الأهداف الثلاثة نفسها وعلى رأسها مراكز القيادة والتحكم العسكرية ثم مؤسسات المنافع كمؤسسات الكهرباء والمياه، ومن ثم تأتي المصارف والأسواق المالية؛_وذلك لإخضاع إرادة الشعوب والمجتمعات الدولية.

إن عملية الاختراق السيبراني تتم عن طريق تسريب البيانات الرئيسة والرموز الخاصة ببرامج شبكة الإنترنت، وهي عملية تتم من أي مكان في العالم دون الحاجة إلى وجود شخص المخترق في الدولة التي يتم اختراق مواقعها، فالبعد الجغرافي لا أهمية له في الحد من الإختراقات المعلوماتية، ولا تزال نسبة كبيرة من الإختراقات لم تكتشف بعد بسبب التعقيد الذي يتصف به نظم تشغيل الحاسب الآلي والشبكات المعلوماتية.

ومن الممكن تصور هجوم سيبراني على أحد المواقع الإلكترونية بقصد تدميرها وشلها عن العمل، حيث يمكن أن يقوم الإرهابيون بشن هجوم مدمر لإغلاق المواقع الحيوية على الشبكات المعلوماتية، وإلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات ومحطات توليد الطاقة والماء، ومواقع الأسواق المالية بحيث يؤدي توقفها عن العمل إلى تحقيق آثار تدميرية تفوق ما تحدثه القنابل والمتفجرات من آثار.

إن من الوسائل المستخدمة حاليًا لتدمير المواقع ضخ مئات الآلاف من الرسائل الإلكترونية (E-mail) من جهاز الحاسوب الخاص بالمدمر إلى الموقع المستهدف للتأثير على السعة التخزينية للموقع، فتشكل هذه الكمية الهائلة من الرسائل المستخدمة الإلكترونية ضغطًا يؤدي في النهاية إلى تفجير الموقع العامل على الشبكة، وتشتيت البيانات والمعلومات المخزنة في الموقع، فتنتقل إلى جهاز المعتدي أو تمكنه من حرية التجول في الموقع المستهدف بسهولة

[30](31) محمود خليل، 50 ألف موقع إلكتروني لداعش.. ولإرهاب يحاصر الإنترنت،
http://www.alittihad.ae/details.php?id=64991&y=2015&article=full

ويسر، والحصول على كل ما يحتاجه من أرقام ومعلومات وبيانات خاصة بالموقع المعتدى عليه، وتعد الفيروسات من أخطر آفات الشبكة المعلوماتية والفيروس عبارة عن برنامج حاسوبي يلحق ضررًا بنظام المعلومات والبيانات ويقدر على التضاعف والانتشار والانتقال من جهاز إلى آخر.(32[31]

السيناريوهات المحتملة للإرهاب السيبراني في عصر المعلومات:

لقد قام خبراء الجرائم السيبراني والأمن المعلوماتي بوضع أكثر من سيناريو محتمل للهجمات الإرهابية وأودعها في البحوث والدراسات والتقارير التي تعالج هذه المسالة، ويمكن تقسيم هذه السيناريوهات إلى ما يأتي:

1. استهداف النظم العسكرية:

تستهدف هذه النوعية من الهجمات عادة الأهداف العسكرية غير المدنية، والمرتبطة بشبكات المعلومات ويعد هذا السيناريو من أخطر السيناريوهات المحتملة التي قد تعصف بمجتمعنا المعاصر، وتبدأ المرحلة الأولى من هذا السيناريو باختراق المنظومات الخاصة بالأسلحة الاستراتيجية، ونظم الدفاع الجوي والصواريخ النووية.

2. استهداف محطات توليد الطاقة والماء:

أصبح الاعتماد على شبكات المعلومات وخصوصًا في الدول المتقدمة من الوسائل المهمة لإدارة نظم الطاقة الكهربائية ويمكن للهجمات على مثل هذا النوع من شبكات المعلومات أن تؤدي إلى نتائج خطيرة، وخصوصًا في ظل اعتماد الإنسان المعاصر على الطاقة الكهربائية فإن شبكات المعلومات المرتبطة بشكل مباشر أو غير مباشر بشبكات الطاقة الكهربائية تعتبر من الأهداف الأولى التي قد يستهدفها الإرهاب الالكتروني.

3. استهداف البنية التحتية الاقتصادية

أصبح الاعتماد على الشبكات المعلوماتية شبه مطلق في عالم المال والأعمال، مما يجعل هذه الشبكات نظرا لطبيعتها المترابطة وانفتاحها على العالم هدفًا مغريًا للمجرمين والإرهابيين، ومما يزيد من إغراء الأهداف الاقتصادية والمالية هو أنها تتأثر بشكل ملموس بالانطباعات السائدة والتوقعات والتشكيك في صحة هذه المعلومات، أو تخريبها بشكل بسيط يمكن أن يؤدي إلى نتائج مدمرة وإضعاف الثقة في النظام الاقتصادي.

4- استهداف نظم المواصلات

ويتضمن هذا السيناريو اختراق نظم التحكم بخطوط الملاحة الجوية والبرية والبحرية، وإحداث خلل في برامج هبوط الطائرات وإقلاعها؛ مما قد ينجم عنه حصول تصادم فيما بينها، أو تعطيل نظم الهبوط فلا تستطيع الطائرات الوصول إلى مدرج مطار من المطارات، كما يحتمل تمكن قراصنة المعلومات من السيطرة على نظم التحكم بتسيير القطارات، وتغيير مواعيد الانطلاق بحيث تسود الفوضى أو تتصادم هذه القطارات فيما بينها وكذا بالنسبة للسفن والناقلات والغواصات البحرية.

(32)[31]عبد الرحمان السند، وسائل الإرهاب الالكتروني . حكمها في الإسلام وطرق مكافحتها، اللجنة العلمية للمؤتمر 15 العالمي عن موقف الإسلام من الإرهاب، جامعة الإمام محمد بن سعود الإسلامية، ص11.

5- استهداف نظم الاتصالات

ويشمل هذا السيناريو اختراق الشبكات المعلوماتية والشبكة الهاتفية الوطنية، وإيقاف محطات توزيع الخدمة الهاتفية وقد تمارس سلسلة من الهجمات على خطوط الهواتف المحمولة ومنع الاتصال بين أفراد المجتمع ومؤسساته الحيوية الأمر الذي ينشر حالة من الرعب والفوضى، وعدم القدرة على متابعة تداعيات الهجمات الإرهابية المعلوماتية، ولا يتوقف الأمر عند هذا الحد فقط بل هناك العديد من الأهداف الأخرى التي يمكن للمجرمين والإرهابيين المتمكنين من خلالها أن يشيعوا الفساد وينشروا الفوضى، فهناك على سبيل المثال شبكات المعلومات الطبية والتي يمكن من خلال مهاجمتها واختراقها ومن ثم التلاعب بها مما يؤدي إلى حصول خسائر بشرية، ومن أمثلة ذلك في العالم الغربي ما قام به أحد المجرمين من الدخول إلى سجلات المستشفيات والتلاعب بملفات المرضى بشكل أدى إلى حقن هؤلاء بأدوية وعلاجات كانت مميتة بالنسبة لهم، كما يمكن لها أن تحدث آثارًا مدمرة على الصعيد الاجتماعي.

المطلب الرابع

التجسس الإلكتروني

يقوم الإرهابيون بالتجسس على الأشخاص أو الدول أو المنظمات أو الهيئات أو المؤسسات الدولية أو الوطنية، ويتميز التجسس الالكتروني بالطريقة العصرية المتمثلة في استخدام الموارد المعلوماتية والأنظمة الإلكترونية التي جلبتها حضارة التقنية في عصر المعلومات، وتستهدف عمليات التجسس الإرهابي في عصر المعلومات ثلاثة أهداف رئيسية وهي: التجسس العسكري والتجسس السياسي والتجسس الاقتصادي.

وفي عصر المعلومات ومع وجود وسائل التقنية الحديثة فإن حدود الدولة مستباحة بأقمار التجسس والبث الفضائي، وقد تحولت وسائل التجسس من الطرق التقليدية إلى الطرق الإلكترونية خاصة مع ظهور الشبكات المعلوماتية وانتشارها عالميًا، ومع توسع التجارة الإلكترونية عبر الشبكة العالمية للمعلومات تحولت مصادر المعلومات التجارية إلى أهداف للتجسس الاقتصادي.

إن محاولة اختراق الشبكات والمعلومات والمواقع الإلكترونية من قِبل العابثين من مخترقي الأنظمة المعلوماتية (hackers) لا يعد إرهابًا، فمخاطر هؤلاء محدودة وتقتصر غالبًا على العبث أو إتلاف المحتويات والتي يمكن التغلب عليها باستعادة نسخة أخرى مخزنة في موقع آمن، ويكمن الخطر في عمليات التجسس التي تقوم بها التنظيمات الإرهابية، وأجهزة الاستخبارات المختلفة من أجل الحصول على أسرار ومعلومات الدولة ومن ثم إفشائها لدول أخرى معادية، أو استغلالها بما يضر المصلحة العامة والوحدة الوطنية للدولة.(33[32]

(33)[32]علي عدنان الفيل، الإجرام الإلكتروني- دراسة مقارنة، الطبعة الأولى، منشورات زين الحقوقية، بيروت،2011، ص53.

وتتم عملية إرسال نظم التجسس الإلكتروني بعدة طرق ومن أشهرها البريد الإلكتروني، حيث يقوم الضحية بفتح المرفقات المرسلة ضمن رسالة غير معروفة المصدر، وهناك طرق أخرى لزرع أحصنة طروادة، وكذلك عن طريق إنزال بعض البرامج من أحد المواقع غير الموثوق بها.

وتتجلى الخطورة في ضعف الوسائل الأمنية المستخدمة في حماية الشبكات الخاصة بالمؤسسات والهيئات الحكومية، ولا يمكن حتمًا الاعتماد على وسائل الحماية التي تنتجها الشركات الأجنبية، فهي ليست آمنة، ولا يمكن الاطمئنان لها تمامًا.

وتجدر الإشارة إلى أن الطرق الفنية للتجسس المعلوماتي سوف تكون أكثر الطرق استخدامًا في المستقبل من قبل التنظيمات الإرهابية؛ نظرًا لأهمية المعلومات الخاصة بالمؤسسات والقطاعات الحكومية، وخصوصًا العسكرية والسياحية والاقتصادية وهذه المعلومات إذا تعرضت للتجسس والحصول عليها فسوف يساء استخدامها من أجل الإضرار بمصلحة المجتمع والوطن.

المحور الثالث

الإرهاب السيبراني الخطر القادم

ويشتمل على المطالب الآتية:

المطلب الأول: تهديدات ومخاطر الإرهاب السيبراني

المطلب الثاني: الاتفاقيات الدولية والإقليمية في مكافحة الجرائم السيبرانية

المطلب الثالث: الجهود الدولية والوطنية في مكافحة جريمة الإرهاب السيبراني

المطلب الأول

تهديدات ومخاطر الإرهاب السيبراني

ينطلق الإرهاب بجميع أشكاله وشتى صنوفه من دوافع متعددة، ويستهدف غايات معينة، ويتميز الإرهاب السيبراني عن غيره من أنواع الإرهاب بالطريقة العصرية المتمثلة في استخدام الموارد المعلوماتية والوسائل الإلكترونية التي جلبتها حضارة التقنية في عصر المعلومات، لذا فإن الأنظمة الإلكترونية والبنية التحتية المعلوماتية هي هدف الإرهابين.

لقد زادت الخطورة الإجرامية للجماعات والمنظمات الإرهابية، فقامت بتوظيف طاقتها للاستفاضة من تلك التقنية واستغلالها في إتمام عملياتها الإجرامية وأغراضها غير المشروعة.

إن خطورة الإرهاب السيبراني تزداد في الدول المتقدمة والتي تدار بنيتها التحتية بالحواسيب الآلية والشبكات المعلوماتية، مما يجعلها هدف سهل المنال، فبدلاً من استخدام المتفجرات تستطيع الجماعات الإرهابية من خلال الضغط على لوحة المفاتيح تدمير البنية المعلوماتية، وتحقيق آثار تدميرية تفوق مثيلتها المستخدم فيها المتفجرات، حيث يمكن شن هجوم إرهابي لإغلاق المواقع الحيوية وإلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات، أو قطع

شبكات الاتصال بين الوحدات والقيادات المركزية، أو تعطيل أنظمة الدفاع الجوي، أو إخراج الصواريخ عن مسارها، أو التحكم في خطوط الملاحة الجوية والبحرية أو اختراق النظام المصرفي وإلحاق الضرر بأعمال البنوك وأسواق المال .

وتأسيسًا على ما سبق يمكننا القول بأن الإرهاب الحالي السيبراني هو إرهاب المستقبل وهو الخطر القادم، نظرًا لتعدد أشكاله وتنوع أساليبه، واتساع مجال الأهداف التي يمكن من خلال وسائل الاتصالات وتقنية المعلومات مهاجمتها في جو مريح وهادئ، وبعيد عن الإزعاج والفوضى، مع توفير قدر كبير من السلامة والأمان للإرهابين.

أولا: التهديد والترويع الإلكتروني

تقوم المنظمات والجماعات الإرهابية بالتهديد عبر وسائل الاتصالات ومن خلال الشبكة العالمية للمعلومات وتتعدد أساليب التهديد وتتنوع طرقه؛ وذلك من أجل نشر الخوف والرعب بين الأشخاص والدول والشعوب محاولة الضغط عليهم للرضوخ لأهداف تلك التنظيمات الإرهابية من ناحية، ومن أجل الحصول على التمويل المالي لإبراز قوة التنظيم الإرهابية من ناحية أخرى.

وقد يلجأ إرهابي (الإرهاب السيبراني) إلى التهديد وترويع الآخرين عن طريق الاتصالات والشبكات المعلوماتية؛ بغية تحقيق النتيجة الإجرامية المرجوة، ومن الطرق التي تستخدمها الجماعات الإرهابية للتهديد والترويع الإلكتروني إرسال الرسائل الإلكترونية المتضمنة للتهديد (E-mails) وكذلك التهديد عن طريق المواقع والمنتديات وغرف الحوار والدردشة الإلكترونية.

ولقد تعددت الأساليب الإرهابية في التهديد فتارة يكون التهديد بالقتل لشخصيات سياسية بارزة في المجتمع وتارة يكون التهديد بالقيام بتفجير منشآت وطنية، ويكون تارة أخرى بنشر فيروسات من أجل إلحاق الضرر والدمار بالشبكات المعلوماتية والأنظمة الإلكترونية في حين يكون التهديد تارة بتدمير البنية التحتية المعلوماتية ونحو ذلك.

ثانيًا: مخاطر الإرهاب السيبراني

في عام 2019أكَّد تقرير المخاطر العالمية الصادر عن المنتدى الاقتصادي العالمي، أن الإرهاب السيبراني أصبح واقعًا لا مفر منه.

ويصف التقرير الهجَماتِ السيبرانيةَ بأنها تلك الهجَماتُ التي تتسبَّب في أضرار اقتصادية كبيرة، أو اضطرابات جيوسياسية، أو مشاهد ومواقف تتصدع فيها الثقة بشبكة الإنترنت على نطاق شاسع.

وتتمثل الهجَمات الإرهابية واسعة النطاق بأفراد أو جماعات غير الحكومية ذات أهداف سياسية أو دينية أو اجتماعية تهدف إلى إلحاق أضرار بشرية أو مادية واسعة النطاق.

وفي هذا الإطار كشف تقرير المنتدى الاقتصادي العالمي عن مخاطرَ عميقة للهجوم الإرهابي السيبراني، حيث أنه له صلة وثيقة بانهيار البِنية التحتية للمعلومات الهامة، وخطر إطلاق أسلحة الدمار الشامل. وقد تتعدد طرائق العمل

من استعمال البرامج التخريبية الخبيثة و(فيروسات) البرامج، إلى حجب الخِدْمات، والأعمال الاستخباراتية التجسُّسية على الشبكة وغيرها.(34[33]

ثالثًا: الآثار الناجمة عن الهجمات السيبرانية:

على الرغم من الإيجابيات الهائلة التي تحققت بفضل تقنية المعلومات، فإن تلك الثورة المعلوماتية المتصاعدة قد صاحبتها في المقابل جملة من الانعكاسات السلبية الخطيرة نتيجة سوء الاستخدام.

1. أثر الهجمات على الوطن العربي**(35[34]**

يمكن أن تكون الجرائم الإلكترونية ضارة على العديد من المستويات، حيث يمكن أن تؤدي إلى فقدان الملكية الفكرية والمعلومات التجارية التنافسية مما يقلل من القدرة التنافسية للشركة.

على الرغم من أن آثار جرائم الإنترنت تختلف، ويمكن أن تهدد الحكومات وحتى أكبر الشركات، إلا أنها تشكل خطرًا خاصًا على الشركات الصغيرة والشركات الناشئة، والتي تميل إلى أن تكون أقل مرونة؛ هذه الشركات لها أهمية حاسمة مع تطور الاقتصاد الرقمي في دول مجلس التعاون الخليجي، حيث تلعب دورًا رئيسيًا في خلق فرص العمل، وضخ المنافسة في السوق وتحفيز الابتكار.(36[35]

وبعبارة أخرى؛ تعد الشركات الصغيرة والمتوسطة اللبنات الأساسية لاقتصاد رقمي مستدام وناجح.

وتتزايد التهديدات السيبرانية في المنطقة، ويعزى ذلك جزئيًا إلى حقيقة أن منطقة الشرق الأوسط ليس لديها هياكل تنظيمية متطورة للغاية لمكافحتها.

أظهر استطلاع حديث أن الخسائر التي تكبدتها الشركات في الشرق الأوسط نتيجة لجرائم الإنترنت أكبر بكثير من خسائر نظيراتها الدولية ففي عام 2015، فقد 56%من الذين شملهم الاستطلاع أكثر من 500.000 دولار أمريكي، مقارنة مع 33%من الشركات على مستوى العالم؛ وفقد 13%ثلاثة أيام عمل على الأقل بسبب آثار الجرائم الإلكترونية، مقارنة بـ 9% من المجيبين العالميين على الدراسة الاستقصائية، وشهد 18% من المجيبين أكثر من 5000هجوم في تلك السنة، وهي نسبة أعلى من أي منطقة أخرى وتقريبا ضعف المعدل العالم.(37[36]

---

[33](34) د. سُني ذو الهدى، تهديد الإرهاب السيبراني . وإمكانية تطبيق اتفاقية الجرائم السيبرانية، على الرابط التالي:

https://imctc.org/arabic/ArticleDetail/Index/637285074665439022 2

[34](35) McAfee and Center for Strategic and International Studies (CSIS) (2013), The Economic Impact of Cybercrime and Cyber Espionage, www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf

[35](36) Iens, J. and Jackson, C. (2015), 'The Importance of Young Firms for Economic Growth', Kauffman Foundation, 13 September 2015, www.kauffman.org/what-we-do/resources/entrepreneurship-policy-digest/the-importance-of-young-firms-for-economic-growt

[36](37) PwC (2016), A false sense of security? Cybersecurity in the Middle East, Global State of Information Security Survey, March 2016, www.pwc.com/m1/en/publications/documents/middle-east-cyber-security-survey.pdf

كما وقعت عدة حوادث في قطر على سبيل المثال، ففي أغسطس 2012، أصيبت شركة قطر للغاز الطبيعي، المعروفة باسمRasgas ، بفيروس أغلق موقع الويب وخوادم البريد الإلكتروني؛ ومع ذلك، لم تؤثر البرامج الضارة على البنية التحتية الرقمية المهمة للشركة والتي تتحكم في إنتاج الغاز الطبيعي وتوصيله؛ وفي عام 2016، استهدف بنك قطر الوطني (QNB) هجومًا أكثر ضررًا، حيث تمكن المتسللون من سرقة كمية هائلة من البيانات بما في ذلك حوالي437،465 من حسابات QNBونشرها على الإنترنت حيث احتوت المعلومات التي تم تسريبها على بيانات شخصية وبيانات اتصال.(38[37]

2. أثر الهجمات على ليبيا

تعرضت شركة ليبيانا لمحاولات اختراق حيث أعلنت مجموعة قرصنة إلكترونية "هكر" تسمى القطط السوداء "black cats" مسؤوليتها عنها.. وأعلنت الشركة القابضة للاتصالات في بيان رسمي عن تعرض شركات "ليبيا للاتصالات والتقنية" و"الجيل الجديد للتقنية" و"المدار الجديد" لهجمات حجب الخدمة، حيث أثرت الهجمات على عدة خدمات وتطبيقات، بما في ذلك تطبيق خدمات المشتركين .MyLTT

وأشارت تقارير دولية لتعرض ليبيا لهجمات بلغت حجمها 114جيجا بايت، مما يعكس تصاعدًا في هذه الأنشطة السيبرانية، وأن إجمالي الهجمات خلال الربع الثالث من عام 2023بلغ قرابة 4400هجمة.

تأتي هذه التطورات في سياق التحديات المتزايدة التي تواجهها البنية التحتية للاتصالات والتقنية في ليبيا، وتؤكد على أهمية تعزيز التعاون والتنسيق بين الجهات المعنية لضمان سلامة البنية التحتية الرقمية وحمايتها من الهجمات السيبرانية.(39[38]

ومن خلال المؤتمر العلمي الدولي الثاني في ليبيا، 22يناير2023م، للأمن السيبراني والتجارب العربية والدولية، الذي ارتكزت محاوره حول مخاطر الإنترنت على المجتمع بين الوقاية والعلاج، والأبعاد التقنية والقانونية لحماية أمن الفضاء السيبراني وتطبيقات الذكاء الاصطناعي بين الفرص والتحديات، تم الإشارة إلى مؤشر الأمن السيبراني العالمي خلال العام 2021-2022الذي جاءت الولايات المتحدة الأمريكية في المرتبة الأولى فيه والهند في أخر القائمة، كما أن الخسائر الإلكترونية المقدرة في الفترة من 2018وإلى 2027سوف تصل 24مليار دولار من أصل 18مليار مما يعني أنها أضرار كارثية فهذه الأرقام جدًا مخيفة.(40[39]

[37](38) Ivanov Anton, Orkhan Mamedov. The Return of Mamba Ransomware Secure list - Information about Viruses, Hackers and Spam. N.p., 09 Aug. 2017. Web. 13 Sept. 2017. https://securelist.com/thereturn-ofmamba-ransomware/79403

[38](39) https://libyaalahrar.tv/tagموقع فالكون فيدز

[39](40) https://www.facebook.com/profile.php?id=100087246084071

المطلب الثاني

الاتفاقيات والقوانين الدولية والإقليمية في مكافحة الجرائم السيبرانية

أولاً: الاتفاقيات الدولية في مكافحة الجرائم السيبرانية

في عام 2016أصدرت لجنةُ اتفاقية الجرائم السيبرانية مذكرة توجيهية تتعلَّق بجوانب الإرهاب السيبراني بموجب اتفاقية بودابست، تعلن فيها أن "الجرائم الموضوعية في الإتفاقية قد تكون أيضًا أعمالاً إرهابية على النحو المحدد في القانون المعمول به". وجاءت هذه المذكرة الإضافية بموجب الإتفاقية في الوقت المناسب، لتسلط المذكرة الضوء على أن هذه الإتفاقية ليست معاهدة مختصة بالإرهاب، إلا أنه يمكن القول: إن الجرائم الموضوعية في الإتفاقية يمكن أن تنفذ على أنها أعمال إرهابية.

تعد هذه الإتفاقية هي أولى الاتفاقيات العالمية المتعلقة بجرائم الإنترنت، وقعت الإتفاقية في العاصمة المجرية بودابست في 23نوفمبر 2001، بهدف التعاون والتضامن الدولي في محاربة الجرائم الإلكترونية، وقعت 26دولة أوروبية على هذه الإتفاقية بالإضافة إلى الولايات المتحدة الأمريكية، وكندا، واليابان وجنوب أفريقيا.(41[40]

وبالرغم من أن هذه الإتفاقية أوروبية المنشأ، إلا أن 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.

ثانيًا: الاتفاقيات والقوانين الإقليمية في مكافحة الجرائم السيبرانية

الإرهاب حسب المادة 147من قانون العقوبات الأردني رقم 16لسنة 1960، والمطبق في الضفة الغربية يعني (جميع الأفعال التي ترمي إلى إيجاد حالة ذعر وترتكب بوسائل كالأدوات المتفجرة، والمواد الملتهبة والمنتجات السامة أو المحرقة، والعوامل الوبائية، أو الجرثومية، التي من شأنها أن تحدث خطرًا عامًا).

أما مفهوم الإرهاب حسب القانون المصري؛ هو كل استخدام للقوة أو العنف أو التهديد أو الترويع يلجأ إليه الجاني تنفيذًا لمشروع إجرامي فردي أو جماعي بهدف الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر إذا كان من شأن ذلك إيذاء الأشخاص أو إلقاء الرعب بينهم أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر أو إلحاق الضرر بالبيئة أو بالاتصالات أو بالمواصلات أو بالأموال أو المباني أو بالأملاك العامة أو احتلالها أو الاستيلاء عليها أو منع أو عرقلة ممارسة السلطات العامة أو دور العبادة أو معاهد العلم أو تعطيل تطبيق الدستور أو القوانين أو اللوائح .

(41)[40]منير محمد الجهيني، ممدوح محمد الجهيني، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها (الإسكندرية: دار الفكر العربي، ط 2004)، ص96.

أما بالنسبة للإتفاقيات العربية لمكافحة الإرهاب فقد عرفت الإرهاب؛ هو كل فعل من أفعال العنف أو التهديد به أيا كانت دوافعه أو أغراضه يقع تنفيذا لمشروع اجرامي فردي أو جماعي من أجل القاء الرعب بين الناس أو ترويعهم بإيذاء أو الحاق الضرر بالبيئة أو بالمرافق العامة أو الخاصة أو تعريض الموارد الوطنية للخطر.

المطلب الثالث

الجهود الدولية والوطنية في مكافحة جريمة الإرهاب السيبراني

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

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

يبدو أن مجال الأمن السيبراني قد لاقي اهتمامًا كبيرًا من كل الفواعل الدولية في الفترة الأخيرة، وسنتطرق إلى الجهود المبذولة في مجال الأمن السيبراني في الوطن العربي بشكل عام وليبيا بشكل خاص.

أولًا: على الصعيد الدولي

أصدرت الأمم المتحدة مجموعة من القرارات الملزمة عبر جمعيتها العامة، جميعها تحذر من مدى تزايد الاهتمام العالمي لاستخدام تكنولوجيا الاتصال والمعلومات وخشيتها وقلقها من استخدامها على نحو غير سلمي وغير قانوني، ففي 22نوفمبر 2002اتخذت قرارًا بشأن التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وفي ديسمبر من نفس العام اتخذت قرار إرساء ثقافة عالمية لأمن الفضاء الالكتروني واعتبر من القرارات الهامة، التي استهدفت العمل على حماية البنية التحتية الحيوية للمعلومات وحث الدول والمنظمات الدولية والإقليمية على تكثيف التعاون الدولي لمجابهة الإرهاب الإلكتروني.

وفي إطار الجهود الدولية لمكافحة الإرهاب الالكتروني يمكن ذكر إستراتيجية الأمم المتحدة لمكافحة الإرهاب الالكتروني المعتمدة بتاريخ 8سبتمبر 2006، والتي أتت على شكل خطة من شانها تحسين التعاون الدولي لمكافحة هذا النوع من الإرهاب .(42[41]

ثانيًا: على الصعيد العربي

تستثمر الكثير من الدول في الأنظمة والتشريعات والتقنيات والجاهزية للحروب الإلكترونية لما تشكله من خطر عليها، وتضع الكثير من الدول الكبرى الأمن السيبراني ضمن أولوياتها للحد من الحروب الإلكترونية ولتأمين الخدمات والتطبيقات بمختلف القطاعات؛ وتعتبر التجربة العربية جديدة في هذا المجال، وازدادت قدرات كل من عمان وقطر والسعودية، والتي ازدادت قدرتها مؤخرًا في هذا المجال بشكل مطرد حيث أنشأت السعودية الهيئة الوطنية للأمن

[41](42) أثير هلال الدليمي، الإجراءات الدولية لمكافحة جرائم الإرهاب السيبراني، عضو اللجنة القانونية، المنتدى العراقي للنخب والكفاءات.

السيبراني، كما أنشأت أيضًا الاتحاد المحلي للأمن السيبراني، وتأتي هذه القرارات ضمن خطة استراتيجية لبناء ترسانة قوية للأمن السيبراني مما يمكنها من حماية حدودها الإلكترونية بشكل جيد وصارم(43[42] .

وتبذل الدول العربية كل ما في وسعها للحاق بالركب العالمي في مجال تطوير الأمن السيبراني، وفي هذا الصدد عقدت المنظمة العربية للتنمية الإدارية التابعة لجامعة الدول العربية، والمكتب الإقليمي العربي للاتحاد الدولي للاتصالات في شهر نوفمبر2017م، فعالية (الأمن السيبراني في المنطقة العربية)، والتي تتضمن اللقاء الثاني للتجارب الإدارية الناجحة في مجال أمن المعلومات، والمنتدي الإقليمي حول الأمن السيبراني في عصر التكنولوجيا الناشئة، وهدفت هذه الفعالية إلي التعريف بالتجارب الإدارية الناجحة في مجال أمن المعلومات من أجل تعميمها ونشرها والاستفادة منها في الدول العربية مع إقامة حوار مفتوح في الدول العربية لمناقشة تحديات الأمن السيبراني المتعلقة بالتكنولوجيات الناشئة وتطوير آليات دفاعية مبتكرة وفعّالة من منطلق المنظور الوطني، وقد شاركت في الفعالية دول مصر والسعودية وسلطنة عمان والأردن ولبنان وفلسطين والمغرب وسوريا واليمن وجزر القمر وموريتانيا بحضور ممثل عن الأمم المتحد(44[43].

ثالثًا: على الصعيد الوطني

تضمنت آلية مكافحة الإرهاب في ليبيا جملة من القوانين والقرارات لمكافحة الإرهاب والجريمة الإلكترونية، تمثلت في الآتي:

تشريعات وقوانين مكافحة الإرهاب في ليبيا:

- أصدر مجلس النواب قانون رقم (3) لسنة 2014م، بشأن مكافحة الإرهاب، بتاريخ: 19/11/1435هـ الموافق: 19/09/2014م . مدينة طبرق، وقد اشتمل على الأبواب التالية:(45[44]

- الباب الأول: العمل الإرهابي.

- الباب الثاني: الجرائم الإرهابية وعقوبتها والتدابير الاحترازية.

- الباب الثالث: الأحكام الإجرائية.

- الباب الرابع: التعاون القضائي.

- إصدار قرار المجلس الرئاسي رقم (823) لسنة 2020م، بشأن اعتماد الاستراتيجية الليبية لمكافحة الإرهاب التي تضمنت الركائز التالية.(46[45]

(43)[42]حسن بن علي العجمي، الثورة الصناعية الرابعة وتغييرات الحياة الإنسانية، المجلة العربية العدد 498، إبريل 2018، ص15.

(44)[43]عبد المجيد سباطة، دبابات الحروب السيبرانية، المجلة العربية العدد498، ص51.

(45)[44]أصدر مجلس النواب قانون رقم (3) لسنة 2014م، بشأن مكافحة الإرهاب، بتاريخ: 1435/11/19هـ الموافق: 2014/09/19م . مدينة طبرق.

- بناء القدرات المحلية: مواجهة الهجمات الإرهابية والإنقاذ والتقليل من المخاطر.

- رصد النشاطات الإرهابية: رصد المخططات وإحباط الهجمات الإرهابية قبل حدوثها.

- العدالة وحقوق الانسان: حماية أفراد المجتمع من الاستقطاب من قِبل الجماعات المتطرفة.

- حماية المجتمع: تحصين المجتمع ضد التطرف والسلوك الإرهابي.

- وأصدر المشرع الليبي قانون رقم 5 لسنة 2022م، بشأن مكافحة الجرائم الإلكترونية حيث عرف فيه التالي:(47[46]

- الجريمة الإلكترونية: كل فعل يرتكب من خلال استخدام أنظمة الحاسب الآلي أو شبكة المعلومات الدولية أو غير ذلك من وسائل تقنية المعلومات بالمخالفة لأحكام هذا القانون.

- الاختراق: هو القدرة على الوصول إلى أي وسيلة تقنية المعلومات بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاصة.

- القرصنة الإلكترونية: الاستخدام أو النسخ غير المشروع لنظم التشغيل أو البرامج الحاسوبية المختلفة في نظام الحماية الخاصة.

- الفيروسات الحاسوبية: هي نوع من البرامج الحاسوبية ذات طبيعة هجومية تخريبية تلحق ضرر بنظام المعلومات أو البيانات.

- التشفير: عملية تحويل البيانات الإلكترونية إلى رموز غير معروفة أو غير مفهومة يستحيل قراءتها أو معرفتها دون إعادتها إلى هيأتها الأصلية.

- إعاقة الوصول إلى الخدمة أو التشويش عليها: هو إرباك الخدمة وتشمل السيطرة على العمل وحركته بشكل صحيح.

- الدليل الجنائي الرقمي: هو نتائج تحليل البيانات من أنظمة الحاسوب أو شبكات الاتصال أو أجهزة التخزين الرقمية بمختلف أنواعها.

- الهوية الرقمية: هي تمثيل رقمي لمعلومات الفرد داخل المجتمع على المعلومات الدولية بالصبغة التي اعتمدها هذا الفرد والمتوقعة من قبل الآخرين، وقد يكون للفرد أو للجهة هويات رقمية متعددة في المجتمعات الإلكترونية المتعددة.

- أدوات التعريف والهوية: أي آلية أو نظام رقمي أو أداة رقمية تستخدم لتمثيل الهوية الرقمية للأفراد التي تمكنهم من العمل بطريقة آمنة مع واجهات استخدام متناسقة على الأنظمة المختلفة على المعلومات الدولية.

- النقود الإلكترونية: هي قيمة نقدية مخزنة على وسيلة إلكترونية مدفوعة مقدماً وغير مرتبطة بحساب مصرفي، وتحظى بقبول واسع من غير من قام بإصدارها وتستعمل كأداة للدفع لتحقيق أغراض مختلفة.

- البطاقة المصرفية الإلكترونية: أداة صادرة عن مصرف أو مؤسسة مالية تتيح لصاحبها سحب الأموال وتحويلها.

---

(46)[45]قرار رئيس المجلس الرئاسي، رقم (823)، لسنة 2020م، بشأن اعتماد الاستراتيجية الليبية لمكافحة، ليبيا، طرابلس.

[46](47) مجلس النواب، صدر بتاريخ:2202.09.27م، يعمل بأحكام هذا القانون من تاريخ صدوره، ينشر في الجريدة الرسمية ووسائل الإعلام.

- الالتقاط أو الاعتراض: مشاهدة البيانات أو المعلومات أو الحصول عليها.

- الهيئة: الهيئة الوطنية لأمن وسلامة المعلومات المنشأة بموجب قرار مجلس الوزراء رقم 28لسنة 2013م.

يهدف القانون إلى حماية التعاملات الإلكترونية، والحد من وقوع الجرائم الإلكترونية، وذلك بتحديد هذه الجرائم وإقرار العقوبات الرادعة لها، وبما يؤدي إلى تحقيق ما يلي:

- المساعدة على تحقيق العدالة والأمن المعلوماتي.

- حماية النظام العام والآداب العامة.

- حماية الاقتصاد الوطني.

- حفظ الحقوق المترتبة على الاستخدام المشروع لوسائل التقنية الحديثة.

- تعزيز الثقة العامة في صحة وسلامة المعاملات الإلكترونية.

رابعًا: أهم الاستراتيجيات والسياسات التي تَبَنَّتْها ليبيا لمكافحة الإرهاب السيبراني

اتجهت الدول إلى تبني العديد من المبادرات على المستوى الوطني أو الثنائي وذلك من أجل حماية البنية التحتية الكونية للمعلومات من خطر التعرض لمثل تلك الأخطار، فلقد اتخذت ليبيا حزمة من الإجراءات الاحترازية من خلال الآتي:

الهيئة الوطنية الليبية لأمن وسلامة المعلومات:**(48[47])**

قامت الهيئة الوطنية بوضع السياسات الوطنية لأمن وسلامة المعلومات منها:

1. سياسة حماية البيانات.
2. سياسة الإستخدام المقبول.
3. سياسة المستخدم.
4. سياسة مضاد الفيروسات.
5. سياسة حماية الشبكات.
6. سياسة الأطراف الثالثة.
7. سياسة النسخ الاحتياطي.
8. سياسة الأمان المادي.

[47](48) قرار مجلس الوزراء رقم 28 لسنة 2013 بأنشاء الهيئة الوطنية لأمن وسلامة المعلومات ليبيا- طرابلس.

ختامًا؛

يمكن القول أن مسألة تحقيق الأمن السيبراني في ليبيا يعد أحد أهم التحديات الجديدة للسياسة الأمنية الليبية التي فرضتها التطورات التكنولوجية المتسارعة، ورغم الجهود المبذولة في سبيل تحقيق ذلك إلا أن المراتب التي تحتلها ليبيا عربيًا ودوليًا تشير إلى أنها بحاجة إلى المزيد من الجهود، وهذا حتى يمكن لها أن تنجح في مجال مكافحة مختلف المخاطر التي يفرزها الفضاء السيبراني، والتي يأتي على رأسها الإرهاب السيبراني وغيره من التهديدات التي يمثل الانتصار عليها انتصارًا جديدًا للسياسة الأمنية الليبية التي أثبتت نجاعتها في المكافحة خارج الفضاء السيبراني ولن تدخر أي جهد في إثبات مكانتها في هذا الفضاء الذي لا يعترف بالحدود ولا بالقيود.

الدول العربية لاتزال في حاجة للمزيد من الاستثمار في مجال الأمن السيبراني لاسيما ليبيا، وينقسم الاستثمار لجانبين؛ الأول توطين التكنولوجيا والبني التحتية السيبرانية، والثاني تطوير المهارات والخبرات في سبيل امتلاك قدرات وطنية قادرة على بناء وإدارة وتحليل الأنظمة السيبرانية وتطويرها.

ومن أهم النتائج والتوصيات التي يمكن استخلاصها من هذا البحث:

أولاً: النتائج:

1. رغم الجهود المبذولة في مجال تحقيق الأمن ومواجهة جريمة الإرهاب السيبراني سواء في شقيها القانوني أو المؤسساتي إلا أنها تبقى بحاجة إلى مزيد من الجهود.

2. تحقيق الأمن السيبراني يتطلب ضرورة نشر الوعي المجتمعي بخطورة جريمة الإرهاب السيبراني وتشجيع التكوين العلمي والجامعي المتخصص في دراستها.

3. تؤدي وسائل الإعلام دورًا محوريًا في معالجة أهم القضايا والمشكلات التي تواجه المجتمع، ولذلك وجب العمل على تشجيع تناولها لمواضيع متعلقة بهذه الجريمة الخطيرة وتوضيح آليات الوقاية منها.

4. يتطلب نجاح سياسة تحقيق الأمن ومكافحة جريمة الإرهاب السيبراني ضرورة الإستفادة من التجارب الرائدة في هذا المجال.

5. تؤدي التنشئة الإجتماعية دورًا هامًا في مكافحة مختلف الجرائم سواء التقليدية أو السيبرانية، وهنا وجب الإهتمام بالأسرة، والمدرسة، والمسجد والجامعة، وحتى تنظيمات المجتمع المدني من أجل المشاركة معًا في بناء مجتمع خالٍ من التطرف والإرهاب.

ثانيًا: التوصيات:

1. الإرهاب السيبراني أصبح خطرًا عالميًا يتطلب استجابة دولية وتعاونًا أمميًا، وأصبحت الحاجة ملحة إلى سياسة مشتركة وإطار تشريعي مشترك.

2. إيجاد إطار دولي منسق وقوي لمكافحة الإرهاب السيبراني تتوافق عليه الحكومات والهيئات التنظيمية؛ لتكون قادرةً على تبادل المعلومات الاستخباراتية وغيرها من أشكال التعاون.

3. يجب معرفة القواعد الجديدة للتقنيات واللاعبين الجدد، فبخلاف الإرهابيين التقليديين، إذا خسر الإرهابي السيبراني اليوم، فهو لا يموت بل يتعلم ويزداد خبرة مما لم ينجح فيه، وسيستخدم ما تعلمه في محاولة جديدة ناجحة مستقبلا.

4. التوعية ونشر مفهوم الفضاء السيبراني والتعريف بالأمن السيبراني لكافة عناصر المؤسسات الأمنية والعسكرية والعمل على وضع سياسة خاصة بالأمن السيبراني.

5. 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 تواجهه كل دول العالم بوجه عام وليبيا بوجه خاص.

6. تطوير تقنية آمنة تكون قادرةً على تحديد الأنشطة المشبوهة بواسطة تحليل البيانات العامة والخاصة، وجعل الحواسيب وأنظمتها أقلَّ عرضة للخطر.

7. إدراج مادة الأمن السيبراني ضمن مناهج المؤسسات الأمنية والعسكرية كل حسب المستوى التعليمي.

المراجع:

أولاً: باللغة العربية:

1. أمن الفضاء الإلكتروني، الأمم المتحدة، مكتب مكافحة الإرهاب، على الرابط التالي:

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

2. د. شريف محمد كشك، آلية جديدة للأمن السيبراني في دول الخليج، على الرابط التالي:

http://www.akhbar-alkhaleej.com/news/article/1217656

3. عبدالنور بعجي، نسيمة مالك الإرهاب الالكتروني: بين الجريمة وضرورة المكافحة، كلية الحقوق الجزائر،2022م، ص67.

4. يونس عرب، "الإطار القانوني للإرهاب الإلكتروني واستخدام الإنترنيت للأغراض الإرهابية"، بحث مقدم لمؤتمر جامعة نايف العربية للعلوم.

5. علي عدنان الفيل، الإرهاب الإلكتروني، مجلة الجامعة الخليجية، المجلد 2، قسم القانون، العدد 2010/2.

6. عبد الوهاب الكيالي، الموسوعة السياسية، ج7 (بيروت: المؤسسة العربية للدراسات والنشر، 1994)، ص153.

7. عادل عبد الصادق، الإرهاب الإليكتروني: القوة في العلاقات الدولية نمط جديد وتحديات مختلفة (القاهرة: مركز الدراسات السياسية والاستراتيجية،2009)، ص109.

8. عبد الستار عبد الرحمن، الإرهاب السيبراني خطر يهدد العالم، على الرابط التالي:

https://imctc.org/Arabic/ArticleDetail/Index/637180424114481635

9. صليحة محمدي، الإرهاب الإلكتروني والامن القومي للدول: نمط جديد وتهديدات مختلفة، المجلة الجزائرية للأمن والتنمية، ص67

10. رغدة البهي، الإرهاب السيبراني: المفهوم والسمات والانماط، المركز المصري للفكر والدراسات الاستراتيجية، على الرابط التالي:

https://www.ecsstudies.com/7141

11. فريدة طاجين، سياسات الدفاع الماليزية في ظل التهديدات الأمنية للبيئة الرقمية: الوقع والتحديات، ص342.

12. محمود أحمد القرعان، الجرائم الإلكترونية (عمان: دار وائل للنشر والتوزيع، الطبعة الأولى، 2017)، ص11.

13. هالة أحمد الرشيدي، هل من حرب سيبرانية بين الولايات المتحدة وروسيا؟، جريدة الأهرام، 4 يناير 2021.

14. حمدون إ. تورية، البحث عن السلام السيبراني، الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء، 2011، ص ص 8،9.

15. علي عدنان الفيل، الإجرام الإلكتروني: دراسة مقارنة، ط1(بيروت: منشورات زين القانونية، 2011)، ص74.

16. 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 أبوظبي، 2006، ط1، ص338.

17. حسنين شفيق، الاعلام الجديد والجريمة الالكترونية التسريبات النجس الالكتروني - الإرهاب، دار فكر وفن ، مصر2014، ص 292.

18. حسنين شفيق، مصدر سبق ذكره2014، ص292.

19. عبد الرحمان السند، وسائل الإرهاب الإلكتروني- حكمها في الإسلام وطرق مكافحتها، اللجنة العلمية للمؤتمر 15 العالمي عن موقف الإسلام من الإرهاب، جامعة الإمام محمد بن سعود الإسلامية، ص5.

20. مصطفى يوسف كافي، ماهر عودة الشمايلة، محمود عزت اللحام، الإعلام والإرهاب الإلكتروني، الطبعة الأولى، دار الإعصار العلمي، عمان . الأردن، ،2015 ص154

21. إيهاب شوقي الإرهاب الإلكتروني وجرائمه، على الرابط التالي:

http://www.assakina.com/awareness-net/rebounds/81251.html

22. محمود خليل،50 ألف موقع إلكتروني لداعش الإرهاب يحاصر الإنترنت، على الرابط التالي:

http://www.alittihad.ae/details.php?id=64991&y=2015&article=full

23. عبد الرحمان السند، وسائل الإرهاب الالكتروني- حكمها في الاسلام وطرق مكافحتا، اللجنة العلمية للمؤتمر 15 العالمي عن موقف الإسلام من الإرهاب ، جامعة الإمام محمد بن سعود الإسلامية، ص11.

24. علي عدنان الفيل، الإجرام الإلكتروني- دراسة مقارنة، الطبعة الأولى، منشورات زين الحقوقية، بيروت،2011، ص53.

25. د. سُني ذو الهدى، تهديد الإرهاب السيبراني . وإمكانية تطبيق اتفاقية الجرائم السيبرانية، على الرابط التالي:

https://imctc.org/arabic/ArticleDetail/Index/6372850746654390222

26. منير محمد الجهيني، ممدوح محمد الجهيني، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها (الإسكندرية: دار الفكر العربي، ط 2004)، ص96.

27. أثير هلال الدليمي، الإجراءات الدولية لمكافحة جرائم الإرهاب السيبراني، عضو اللجنة القانونية، المنتدى العراقي للنخب والكفاءات.

28. حسن بن علي العجمي، الثورة الصناعية الرابعة وتغييرات الحياة الإنسانية، المجلة العربية العدد 498، إبريل 2018، ص15.

29. عبد المجيد سباطة، دبابات الحروب السيبرانية، المجلة العربية العدد498، ص51.

30. أصدر مجلس النواب قانون رقم (3) لسنة 2014م، بشأن مكافحة الإرهاب، بتاريخ: 1435/11/19هـ الموافق: 2014/09/19م . مدينة طبرق.

31. قرار رئيس المجلس الرئاسي، رقم (823)، لسنة 2020م، بشأن اعتماد الاستراتيجية الليبية لمكافحة، ليبيا، طرابلس.

32. مجلس النواب، صدر بتاريخ:2202.09.27م، يعمل بأحكام هذا القانون من تاريخ صدوره، ينشر في الجريدة الرسمية ووسائل الإعلام.

33. قرار مجلس الوزراء رقم 28 لسنة 2013، بإنشاء الهيئة الوطنية لأمن وسلامة المعلومات، ليبيا- طرابلس

ثانيًا: باللغة الإنجليزية:

1. Denning,Dorothye.,"Cyber terrorism", Global Dialogue, Aug 2000, p10

2. https://smtcenter.net/?p=8215

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

4. What Are the Most Common Cyber Attacks?:https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

5. http://www.ifegypt.org/NewsDetails.aspx?Page_ID=1244&PageDetailID=1324

6. https://www.europarabct.com

7. What Is Cybersecurity? https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

8. What is Digital Environment, https://www.igi-global.com/dictionary/models-of-competences-for-the-real-and-digital-world/7610

9. McAfee and Center for Strategic and International Studies (CSIS) (2013), The Economic Impact of Cybercrime and Cyber Espionage, www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf

10. iens, J. and Jackson, C. (2015), 'The Importance of Young Firms for Economic Growth', Kauffman Foundation, 13 September 2015, www.kauffman.org/what-we-do/resources/entrepreneurship-policy-digest/the-importance-of-young-firms-for-economic-growt

11. PwC (2016), A false sense of security? Cybersecurity in the Middle East, Global State of Information Security Survey, March 2016, www.pwc.com/m1/en/publications/documents/middle-east-cyber-security-survey.pdf

12. Ivanov Anton, Orkhan Mamedov. The Return of Mamba Ransomware Secure list - Information about Viruses, Hackers and Spam. N.p., 09 Aug. 2017. Web. 13 Sept. 2017. https://securelist.com/thereturn-ofmamba-ransomware/79403

13. https://libyaalahrar.tv/tagموقع فالكون فيدز

14. https://www.facebook.com/profile.php?id=100087246084071