مركز دراسات الخليج والجزيرة العربية
تأسس عام ١٩٩٤م - جامعة الكويت

جامعة الكويت
KUWAIT UNIVERSITY

آليات مواجهة الإرهاب الإلكتروني في دول مجلس التعاون الخليجي على ضوء تطور أداء التنظيمات الإرهابية

شيماء سمير محمد حسين

باحثة في العلاقات الدولية والتنظيم الدولي

التقرير الاستراتيجي

العدد (٣٣)

يوليو ٢٠٢٣م

أُسس **مركز دراسات الخليج والجزيرة العربية بجامعة الكويت** في عام ١٩٩٤م، بوصفه مركزاً بحثياً يهتم بالبحوث والدراسات العلمية ذات الصلة بالقضايا التي تهم دولة الكويت ومنطقة الخليج والجزيرة العربية على وجه التحديد، ومنطقة الشرق الأوسط والقضايا الدولية عموماً.

ومن هذا المنطلق يقوم المركز بشكل دوري بإصدار «**التقرير الاستراتيجي**» الذي يتناول القضايا الاستراتيجية التي تهم دولة الكويت والمنطقة. ويهدف المركز من خلال هذا التقرير إلى تقديم تحليل استراتيجي للقضايا والمستجدات المتعلقة بأمن المنطقة، ما يمكن أن يساهم في خدمة الباحثين والمهتمين في الشؤون الاستراتيجية. كما يسعى المركز من خلال هذا التقرير إلى تقديم الرؤى والتوصيات اللازمة لصناع القرار السياسي بما يخدم تحقيق المصلحة الاستراتيجية لدولة الكويت.

أعضاء مجلس إدارة
مركز دراسات الخليج والجزيرة العربية

أ. د. عثمان حمود الخضر
القائم بأعمال نائب مدير جامعة الكويت للأبحاث (رئيس مجلس الإدارة)

أ. د. يعقوب يوسف الكندري
القائم بأعمال مدير المركز. نائب رئيس مجلس الإدارة

داخل جامعة الكويت

أ. د. عبيد سرور العتيبي
القائم بأعمال رئيس قسم الجغرافيا
كلية العلوم الاجتماعية ـ جامعة الكويت

أ. د. غانم حمد النجار
قسم العلوم السياسية
كلية العلوم الاجتماعية ـ جامعة الكويت

أ. د. فايز منشر الظفيري
قسم المناهج وطرق التدريس
كلية التربية ـ جامعة الكويت

أ. د. يوسف ذياب الصقر
قسم الفقه المقارن والسياسة الشرعية
كلية الشريعة والدراسات الإسلامية
جامعة الكويت

خارج جامعة الكويت

د. بدر عثمان مال الله
المدير العام للمعهد العربي للتخطيط
دولة الكويت

سعادة السفير / سميح عيسى جوهر حيات
مساعد وزير الخارجية لشؤون آسيا
وزارة الخارجية ـ دولة الكويت

سعادة السفير / عبد العزيز الشارخ
المدير العام السابق لمعهد سعود الناصر
الدبلوماسي الكويتي ـ دولة الكويت

د. ناصر جاسم الصانع
الهيئة العامة للتعليم التطبيقي والتدريب
دولة الكويت

الناشر

مركز دراسات الخليج والجزيرة العربية

جامعة الكويت

ص.ب: ٦٤٩٨٦ الشويخ (ب)

الرمز البريدي: ٧٠٤٦٠، الكويت

هاتف : ٢٤٩٨٤٦٣٩ ـ ٢٤٩٨٤٦٥٨ (٩٦٥+)

البريد الإلكتروني **cgaps@ku.edu.kw**
Gulf_center@yahoo.com

الموقع الإلكتروني **www.cgaps.ku.edu.kw**

الآراء الواردة في هذه الدراسة لا تعبّر بالضرورة عن اتجاهات يتبناها مركز دراسات الخليج والجزيرة العربية بجامعة الكويت

الطبعة الأولى . الكويت . ٢٠٢٣م

تمهيد:

ساهمت الثورة التكنولوجية والمعلوماتية التي شهدها العالم خلال السنوات الأخيرة في بروز أنواع جديدة من الجرائم الإرهابية المنظمة، وفي مقدمتها الإرهاب الإلكتروني، الذي بات يمثل ظاهرة بالغة الخطورة ومتسارعة التطور على نحو غير مسبوق.

ويثير الإرهاب الإلكتروني العديد من القضايا ذات الصلة بمواجهته وآليات التصدي الفعال له، وفي مقدمة ذلك الأمن السيبراني.

وتتبدى خطورة الإرهاب الإلكتروني في اتساع نطاق آثاره لتشمل عدة دول، وصعوبة تتبع منفذيه، وغياب منظومة قانونية دولية ـ حتى الآن ـ لمحاسبة ومعاقبة القائمين بهذه الجرائم، وممولیها، وداعميها.

انطلاقاً من ذلك، يتناول هذا العدد من (التقرير الإستراتيجي) آليات دول مجلس التعاون لدول الخليج العربية وتشريعاتها لمواجهة الإرهاب الإلكتروني، ومستقبل هذه الجهود خلال الفترة المقبلة.

مدير المركز

أ. د. يعقوب يوسف الكندري

المحتويات	رقم الصفحة

المحتويات	رقم الصفحة

جامعة الكويت
KUWAIT UNIVERSITY

مركز دراسات الخليج والجزيرة العربية

ملخص:

خلّف التطور الهائل في تكنولوجيا المعلومات تطوراً مضاداً على مستوى أداء التنظيمات الإرهابية، التي عملت على تطوير آلياتها في مواجهة التدابير الأمنية المتبعة تجاهها، حيث عملت على استثمار وجودها في البيئة الإلكترونية في صورة إرهاب إلكتروني لتعويض ما فقدته على أرض الواقع من معسكرات وأفراد وتمويل وعمليات عبر عدة آليات، الأمر الذي تم مواجهته من قِبل الدول وفي مقدمتها دول الخليج العربي، عن طريق اتباع آليات مضادة من شأنها تقليل ومواجهة الخسائر التي نتجت عن ظاهرة الإرهاب الإلكتروني، ومن ثم يسعى التقرير الاستراتيجي إلى تحليل الآليات المختلفة المتبعة من قِبل دول مجلس التعاون الخليجي في مواجهة ظاهرة الإرهاب الإلكتروني ومدى فاعلية هذه الآليات في التقليل من الخسائر الناتجة عن هذه الظاهرة.

الكلمات المفتاحية: الإرهاب الإلكتروني، آليات، دول الخليج العربي، مكافحة الإرهاب، التنظيمات الإرهابية.

مقدمة:

إن الطفرة الكبيرة التي حدثت في تكنولوجيا المعلومات صاحبتها طفرة أخرى في عالم الجريمة الإرهابية؛ لتنتج لنا نوعية من الجرائم المستحدثة التي عُرفت باسم الجرائم الإرهابية الإلكترونية، والتي مارستها التنظيمات الإرهابية لتؤكد سيطرتها على البيئة الإلكترونية عوضاً لها عن الخسائر التي تكبدتها في بيئتها الواقعية جراء الحرب ضد الإرهاب، وذلك من خلال فرض أذرعها بعدة آليات قامت عن طريقها بتحقيق أغراضها بنشر الفكر المتطرف والحصول على الدعم المادي واللوجيستي والتجنيد والتمويل والدعاية لأنشطتها، ناهيك عن الأضرار التي وجهتها تلك التنظيمات للمواقع الاقتصادية والتجارية والأمنية والعسكرية.

ومن هنا بات الأمن السيبراني في حاجة إلى تحديث وتطوير لمواكبة الجرائم الإرهابية في صورتها المتطورة، وهو ما اتجهت له دول العالم خاصة بعد أحداث الحادي عشر من سبتمبر عام ٢٠٠١م، وهو ما تمخض عنه توقيع ٣٠ دولة على الاتفاقية الدولية الأولى لمكافحة الإجرام عبر الإنترنت في بودابست عام ٢٠٠١م.[1]

١- مخاطر الإرهاب الإلكتروني تتزايد، مركز الإمارات للدراسات والبحوث الاستراتيجية، بتاريخ ٢١ مارس ٢٠٠٤م، متاح على:
https://www.ecssrae/reports_analysis/%D%85%9AE%D%8A%D%8A%7D%84%9D%8A%7D%84%9D%8A%5

ومـن ثـم اتجهـت باقي الـدول إلى العمل على اسـتحداث وسـائل وقائية من شـأنها تخفيـف حدة آثـار الإرهاب الإلكتروني، وكان منهـا دول مجلس التعاون لـدول الخليـج العربية، التـي عملت على تطوير جهودهـا في مختلف الاتجاهات لمواجهـة الجرائـم الإلكترونيـة عمومـاً، والجرائـم الإرهابيـة الإلكترونيـة عـلى وجـه الخصـوص، وهـو مـا ظهـر مـن خـلال عـدة آليـات شـملت تطويـر مؤسسـات أمنيـة ومراكـز بحثيـة وتعليمية، واسـتحداث منظومـة قوانين قادرة عـلى التصـدي لمثـل هـذه النوعيـة مـن الجرائـم المسـتحدثة عـلى ضـوء التطـور المـوازي لأداء التنظيـمات الإرهابيـة المعـاصرة.

وبنـاء على المعطيات السـابقة، يسـعى هذا التقرير الاسـتراتيجي إلى تسـليط الضـوء عـلى المسـتجدات المتعلقـة باسـتخدام التنظيـمات الإرهابيـة للفضـاء الإلكـتروني، وتوظيفهـا لتكنولوجيـا المعلومـات بما يخـدم أهدافهـا ومخططاتها، والوقـوف عـلى طبيعـة الآليـات التـي اتخـذت في هـذا الشـأن مـن قبـل دول الخليـج العـربي، سـواء كانـت تلـك الآليـات عـلى صعيـد التشريعـات الوطنيـة أو التعـاون الـدولي والإقليمـي أو التحديثـات في مجـال الأمـن السـيبراني ونشر الوعـي المجتمعـي، ووصـولاً إلى رصد التحديات التي مـا زالت تواجه الجهود الحثيثـة المبذولـة للتصـدي للإرهـاب الإلكـتروني بكافـة صـوره وأشـكاله.

ومن ثم، يسعى هذا التقرير إلى الإجابة عن الأسئلة التالية:

- ✓ مـاذا يُقصـد بمفهـوم الإرهـاب الإلكـتروني والمفاهيـم التـي اشـتقت منه أو تنـدرج تحتـه، ومـا هـي خصائصه؟

- ✓ ما هي آليات عمل الإرهاب الإلكتروني والعوامل التي ساعدت التنظيمات الإرهابية على الاتجاه إليه؟
- ✓ كيف تصدت دول مجلس التعاون الخليجي لظاهرة الإرهاب الإلكتروني؟
- ✓ ما هو مستقبل الجهود الخليجية في مواجهة هذه الظاهرة؟

أولاً ـ مفهوم الإرهاب الإلكتروني وخصائصه:

١- ماهية الإرهاب الإلكتروني:

تعددت المسميات التي أطلقت على الإرهاب الإلكتروني فكان منها: الإرهاب الرقمي، والإرهاب التكنولوجي، والإرهاب المعلوماتي، والإرهاب السيبراني، وكلها تندرج تحت المعنى نفسه وهو ما يقصد به: "الهجمات التي تشنها التنظيمات الإرهابية المعترف بها ضد أنظمة الكمبيوتر بقصد إحداث خلل أو تعطيل مادي لنظام المعلومات"، وهو ما يأخذ عدة أشكال أهمها:

- تمرير الفيروسات إلى شبكات البيانات بغرض تدميرها.
- اختراق الخوادم بغرض تعطيل الاتصال والسطو على المعلومات الحساسة.
- « تهكير» المواقع الإلكترونية الحيوية وجعلها غير متاحة للجمهور، بما ينتج عنه خسائر مادية.
- الهجوم والسيطرة على المؤسسات المالية بدافع تحويل الأموال لخدمة وتمويل العمليات الإرهابية.[٢]

2 -Cyber terrorism, Wegancouncil , Available at : https://www.wigan.gov.uk/resident/crime.emergencies/counter-terrorism/cyber-terrorism/cyber-terrorism.aspx.

أ- مفهوم الإرهاب السيبراني:

كانت أولى بدايات ظهور واستخدام مصطلح الإرهاب السيبراني أو الإلكتروني (Cyberterrorism) في فترة الثمانينيات على يد باري كولين، والذي أقر وقتها بصعوبة الوصول إلى مفهوم شامل للإرهاب التكنولوجي، ولكنه تبنى تعريفاً للإرهاب السيبراني أشار فيه إلى أنه: "أي هجمات إلكترونية غرضها تهديد الحكومات أو العدوان عليها سعياً لتحقيق أهداف سياسية أو دينية أو أيديولوجية، وأن الهجمة يجب أن تكون ذات أثر مدمر وتخريبي مكافئ للأفعال المادية للإرهاب".

وفي تعريف مشابه لجيمس لويس James Lewis أكد 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".

وفي السياق نفسه كان هناك تعريفاً للإرهاب السيبراني لحلف شمال الأطلسي (الناتو) باعتباره "هجوماً إلكترونياً يستخدم أو يستغل شبكات الحاسوب أو الاتصالات لإحداث دمار أو تعطيل كاف لتوليد الخوف أو ترهيب المجتمع وتحويله إلى هدف أيديولوجي".[٣]

ب- مفهوم الجريمة الإلكترونية:

لا يوجد مفهوم محدد تم الاستقرار عليه بشأن الجرائم الإلكترونية، ولكن هناك من عرّفها باعتبارها: "ذلك النوع من الجرائم التي تتطلّب

٣ - محمد كمال، الإرهاب السيبراني.. عندما يستخدم الإرهابي الكيبورد بدلاً من القنبلة (القاهرة: دار كليم للطباعة والنشر والتوزيع، ٢٠٢٢م)، ص١٢.

إلماماً خاصاً بتقنيات الحاسب الآلي ونُظم المعلومات؛ لارتكابها أو التحقيق فيها ومقاضاة فاعلها".[٤]

ولقد عُرفت هذه النوعية من الجرائم عند المشرّع الكويتي باسم (جرائم تقنية المعلومات)، وجاء من خلاله تعريف الجريمة المعلوماتية على أساس أنها: "كل فعل يرتكب من خلال استخدام الحاسب الآلي أو الشبكة المعلوماتية أو غير ذلك من وسائل تقنية المعلومات بالمخالفة مع أحكام القانون".[٥]

في حين عرّف المشرع السعودي هذه الجرائم باسم (الجريمة المعلوماتية) والتي تعد: "كل فعل يرتكب متضمناً الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام".[٦]

في الوقت الذي عرّفها المشرّع القطري بأنها: "أي فعل ينطوي على استخدام وسيلة تقنية المعلومات أو نظام معلوماتي أو الشبكة المعلوماتية بطريقة غير مشروعة، بما يخالف أحكام القانون".[٧]

---

٤ – علي جبار الحسيني ، جرائم الحاسوب والإنترنت (عمان: دار البازوري للنشر والتوزيع ، ٢٠٠٩م) ، ص٣٣.

٥ – قانون رقم ٦٣ لسنة ٢٠١٥م في شأن مكافحة جرائم تقنية المعلومات، ص٣، متاح على:
https://www.moi.gov.kw/main/content/docs/cybercrime/ar/law-establishing-cyber-crime-dept.pdf

٦ – المرسوم الملكي رقم م/ ١٧ لعام ١٤٢٨ ـ المادة الأولى ـ الفقرة الثامنة، هيئة الخبراء بمجلس الوزراء ـ المملكة العربية السعودية، بتاريخ ٢٧ مارس ٢٠٠٧، متاح على:
https://laws.Boe.gov.sa/Boelaws/laws/viewer/ceadb6be81 -e4 -5c919 -91e - 2967202d9643?law1d=25df73d0 -6f4 -49dc -5b010=a9a700f2ec1d

٧ – قانون رقم ١٤ لسنة ٢٠١٤م – قانون مكافحة الجرائم الإلكترونية – البوابة القانونية القطرية، متاح على:
https://almeezan.qa/lawview.aspx?opt&lawid=63668&language=ar#:~:text=%D9%84%A7D9%84%D8%، انظر أيضاً: محمد ابراهيم الزعبي، « فاعلية القوانين والتشريعات العربية في مكافحة الجرائم الإلكترونية. دراسة مقارنة «، المجلة العربية للنشر العلمي، العدد ٣٧/ ٢٠٢١م، عمان، ص٢٧٩، ص٢٨٠.

وهـذا يقودنـا إلى التسـاؤل التـالي: متى تصبـح الواقعة جريمـة إلكترونية أو إرهابـاً إلكترونياً أو حربـاً إلكترونية؟

ولمعرفة الإجابة عن هذا التسـاؤل يجب علينا التركيز عند طرح المسـميات، حيـث إن كلاًّ منهـم لـه مضمونـه، فالجريمـة الإلكترونيـة هـي: "سـلوك غـير قانـوني يتم باسـتخدام الأجهـزة الإلكترونيـة، وينتج عنها حصـول المجرم على فوائـد ماديـة ومعنويـة مـع تحميـل الضحيـة خسـارة مقابلـة، وغالبـاً مـا يكـون هـدف هـذه الجرائـم هـو القرصنـة من أجـل سرقة أو إتـلاف معلومـات، إذ إن الجريمـة الإلكترونيـة هـي مخالفة ترتكـب ضد أفراد أو جماعـات بدافع جرمي، أو بنيّـة الإسـاءة لسـمعة الضحيـة بطريقة مبـاشرة أو غير مبـاشرة" [٨]

أمـا الإرهـاب الإلكـتروني فعملياتـه أكثـر شـدّة، كذلـك لابـد أن تتوافر فيه أركان الجريمـة الإرهابيـة، حتـى يتم تصنيفهـا باعتبارها سـلوكًا إرهابيًّا، وهذا يكـون عـلى أسـاس هيـكل ومبـدأ الـضرر والهـدف، وكذلـك الجهـة الفاعلـة والغـرض مـن الجريمة.

أمـا مفهـوم الحـرب الإلكترونيـة فهـو يعـرف باعتبـاره "هجومـاً إلكترونيـاً أو سلسـلة مـن الهجـمات التـي تسـتهدف بلـداً مـا، ويكـون لديهـا القـدرة عـلى إحـداث الخـراب في البنيـة التحتيـة الحكوميـة والمدنيـة وتعطيـل الأنظمـة الحيويـة؛ ممـا يـؤدي إلى إلحـاق الـضرر بالدولـة وحتـى الخسـائر في الأرواح،

٨ – الجرائـم الإلكترونيـة والإرهـاب الإلكـتروني، موقـع جهـاز المخابـرات العامـة الفلسـطينية، نـشر بتاريـخ ٣٠ يوليـو ٢٠١٩م، متـاح عـلى:
http://www.pgis.ps/ar/category/%d%8ad%dg%88%dg-84%id%8a%7dg%84%d%85%9d%8ae%d%8a%7d%8a%8ae%d%8a%7d%8a%8d%8b%1d%8a%7d%8aq

حيث تتضمن الحرب الإلكترونية عادة قيام دولة بهجمات إلكترونية على دول أخرى، وذلك من خلال عدة أشكال منها التجسس أو التخريب".

وعلى الرغم من التشابه بين مفهوم الحرب الإلكترونية والإرهاب الإلكتروني، إلا أن الأولى تعد مجموعة فرعية من حرب المعلومات، كما أن لها أهدافًا محددة في الحرب.

٢- خصائص الإرهاب الإلكتروني:

تتمثّل دوافع التنظيمات الإرهابية أو الذئاب المنفردة في اللجوء إلى الإرهاب الإلكتروني في التالي:

أ- لا يحتاج تنفيذها إلى استخدام العنف ولا إلى شراء ونقل للسلاح ولا اللجوء للقوة، فقط كل ما يلزمها حاسب آلي متصل بالشبكة المعلوماتية، وبعض البرامج التي تلزم الغرض نفسه.

ب- إن أبرز ما يميّز الإرهاب الإلكتروني أنه يصنف باعتباره جريمة إرهابية عابرة لحدود الدول والقارات، بالتالي فهو غير خاضع لأحكام نطاق إقليمي محدد.

ج- صعوبة اكتشاف وتتبع الإرهاب الإلكتروني، علاوة على نقص الخبرات اللازمة للتعامل مع مثل هذه الجرائم لدى بعض أجهزة الأمن.

د- صعوبة الإثبات في الإرهاب الإلكتروني، وذلك نظراً لسرعة غياب الدليل الرقمي وسهولة تدميره وإتلافه.[٩]

٩ - المرجع السابق، ص١٣.

هـ- صعوبة تتبع المصدر، مما يجعل مرتكب العمل الإرهابي مجهولاً وغير قابل للتتبع في كثير من الأحيان، علاوة على إمكانية تزييف وسائل الإثبات الرقمية بشكل عمدي.

و- انخفاض تكلفة أعمال الإرهاب الإلكتروني مقارنة بأعمال الإرهاب التقليدي.

ثانياً ـ آلية عمل الإرهاب الإلكتروني:

للإرهاب الإلكتروني آليات متعددة للعمل في الفضاء الإلكتروني، فقد حاولت التنظيمات الإرهابية بعد تدمير أغلب معاقلها جراء التدابير الأمنية والعسكرية لمكافحة الإرهاب تعويض ما فقدته على أرض الواقع من معسكرات وأفراد وتمويل، عن طريق اتباعها عدة آليات، وأهمها:

١- استخدام شبكة المعلومات في الاتصال ونشر المعلومات:

وفرت شبكة المعلومات الدولية وسيلة مهمة لنقل وتبادل المعلومات بين العناصر الإرهابية بشكل آمن إلى حد ما عن الطرق التقليدية التي كانت تتبع في السابق، كتبادل المعلومات والأوامر والتعليمات عن طريق الرسل أو النقاط الميتة، فأصبح البريد الإلكتروني وسيلة تأمين مهمة لسهولة وسرعة الاتصال والمراسلة، والملاحظ أن كثيراً من العمليات الإرهابية التي تمت أخيراً كان البريد الإلكتروني فيها وسيلة لتبادل المعلومات بين مخططي العمليات والعناصر المنفذة، ولم يستقر الأمر إلى هذا الحد، بل استخدمت الرسائل الإلكترونية في عملية نشر الفكر المتطرف والترويج له من قِبل التنظيمات الإرهابية.

كما استطاعت التنظيمات الإرهابية أن توجد لنفسها موطئ قدم على مواقع التواصل الاجتماعي، تلك المنصات التي تشكّل أكبر تجمع من

الفئات العمرية المختلفة خاصة من الشباب والمراهقين، حيث تم توظيف مواقع التواصل المختلفة مثل (الفيسبوك وتويتر واليوتيوب والواتس آب، والانستجرام) وغيرها من التطبيقات في خدمة العمل الإرهابي.

فعلى سبيل المثال قام تنظيم (داعش) بتجنيد ما يقرب من ٨٠٪ من أعضائه عبر شبكات التواصل الاجتماعي، في حين أن ٢٠٪ فقط من عمليات التجنيد كانت تتم داخل السجون أو المساجد، وهذا ما يعكس الفائدة الكبرى التي تنبّه لها التنظيم لأهمية هذه الوسائل الإلكترونية، ففي عام ٢٠١٥م قام التنظيم بإنشاء قناة أطلق عليها (قناة الخلافة)، إلا أنه سرعان ما تم إغلاقها.[١٠]

٢- استهداف وتدمير البنية التحتية لشبكة معلومات المؤسسات الحكومية:

إن تطور وسائل الاتصال وشبكات المعلومات ساعد التنظيمات الإرهابية على تنفيذ عمليات إرهابية أكثر دقة وسهولة وخطورة، مكنتها من استهداف وتدمير الأهداف والمؤسسات الحكومية بفضل السهولة التي خلفها الفضاء الإلكتروني للتوجيه والتحكم في وسائل نقل المتفجرات، ناهيك عن الأمان الذي توفره لاتصال العناصر الإرهابية بعضها البعض، مما خلف خسائر فادحة فاقت في بعض الأحيان خسائر الإرهاب التقليدي.[١١]

١٠ - نورا بنداري، دور وسائل التواصل الاجتماعي في تجنيد أعضاء التنظيمات الإرهابية. دراسة حالة داعش، المركز الديمقراطي العربي، بتاريخ ١٩ يوليو ٢٠١٦م، متاح على:
https://democratica.de/?p=34268

١١- أحمد عبد الله الناهي، صدام عبد الستار رشيد، «السياسة الإعلامية لتنظيم داعش الإرهابي. الأهداف وسبل المواجهة"، المجلة السياسية والدولية – كلية العلوم السياسية – الجامعة المستنصرية، بغداد، عدد ٣٠/ ٢٠١٦م، ص٢٩.

ويدل على ذلك مقطع فيديو لتنظيم (القاعدة) يرجع لعام ٢٠١١م، دعا فيه التنظيم السيبرانيين المهرة إلى الهجوم على أنظمة المعلومات الحيوية، من خلال شن غارة معلوماتية على غرار ١١ سبتمبر، شمل الفيديو مقابلات مترجمة مع الخبراء السيبرانيين في الولايات المتحدة يشرحون فيها كيف يمكن لمثل هذه الهجمات أن تتسبب في أضرار كبيرة للبنية الحيوية الداعمة للحياة.[١٢]

٣- الاستفادة من الشبكة المعلوماتية في عمليات التنقيب عن المعلومات:

وفرت شبكة الإنترنت مخزونًا مهماً من المعلومات الاستراتيجية والحيوية للتنظيمات الإرهابية بكل أسف، حيث وجدت العناصر الإرهابية سهولة في الحصول على معلومات حول المنشآت الحيوية والمطارات وبعض الأماكن العسكرية أو الكمائن الأمنية دون الاضطرار إلى اختراق قوانين الشبكة، حيث مثّل ما يقرب من ٨٠٪ من مخزون المعلومات التي اعتمدت التنظيمات الإرهابية من مواقع إلكترونية متاحة للجميع، ناهيك عن استخدام صور القمر الصناعي لبرنامج google Earth وهواتف الجوال التي توفر تحديثات حية للمتعاملين معها حول موقع الرهائن خصوصاً الأجانب، وتوظيفه في العمليات الإرهابية.[١٣]

١٢ - مروة نظير، «جماعات التطرف العنيف ومنصات التواصل الاجتماعي. قراءة في الاستخدامات والعوامل"، المجلة الاجتماعية القومية– المركز القومي للبحوث الاجتماعية والجنائية، القاهرة، عدد ١ يناير/ ٢٠٢٠م، ص١١٧.

١٣ - أسعد طارش عبد الرضا، علي إبراهيم، «الأمن السيبراني ودوره في انتشار ظاهرة الإرهاب في العراق بعد عام ٢٠٠٣م»، مجلة دراسات دولية، عدد ٨٠، ص١٦٣، متاح على:
https://www.iasj.net/iasj/pdf/5e08943c7ae82efb

٤- إنشاء معسكرات افتراضية بديلة للمعسكرات الواقعية:

استطاعت التنظيمات الإرهابية كتنظيمي القاعدة وداعش، استغلال تكنولوجيا المعلومات والاتصالات في عملية التعلم، وذلك تعويضاً عن أماكن التدريب الفعلية التي فقدتها.

فلقد قام تنظيم القاعدة بنشر أكثر من ١٠ آلاف صفحة مكتوبة كمواد تدريبية، والكثير منها قد استلهم من التدريب العسكري البريطاني والأمريكي، إضافة إلى أشرطة فيديو التدريب ومحركات البحث التي نظمها الزرقاوي قبل وفاته، لا سيما استغلال مقاطع اليوتيوب، كذلك منشورات الفيسبوك لتعليم استخدام السلاح وتصنيع المتفجرات، بالإضافة إلى مواقع الويب التي تحتوي على مواد تعليمية وتقنيات للقرصنة وبرامج التشفير؛ مما جعل من تلك المنصات الإلكترونية معسكرات افتراضية على الإنترنت باستخدام مجموعة غنية من مواقع التواصل الاجتماعي.(١٤)

٥- دعم الاستقلال التكتيكي للفروع والعمليات باستخدام شبكة الإنترنت:

مثّل انتقال التنظيمات الإرهابية للفضاء الإلكتروني نوعاً من الاستقلال التكتيكي، فمنه ظهرت العمليات الإرهابية المستقلة والعمليات الانتحارية التي نسبت نفسها لفروع التنظيمات الإرهابية في الكثير من البلدان؛ الأمر الذي نتج عنه صعوبات أمنية واستخباراتية في التعامل مع هذه النوعية من الخلايا.

14 - Weiman,Gabiel."New Terrorism and New Media" . Wilson international center for scholars,Washington D.C ,2014,p4 .

٦- تجنيد جيش جديد من الإرهابيين و"الذئاب المنفردة":

كان من أهم مكاسب التنظيمات الإرهابية عبر الفضاء الإلكتروني حشد واستجماع جيل جديد من الإرهابيين من كل الدول، فقد أشار تقرير لمجلة "فورين بوليسي" الأمريكية في عددها الصادر بتاريخ يناير ٢٠١٠م إلى كيفية استفادة تنظيم القاعدة من الشبكة العنكبوتية، حيث كشفت المجلة عن تزايد أعداد الإرهابيين الذين يعملون على الإنترنت ويتحولون إلى إرهابيين فعليين على أرض الواقع.

وعلى سبيل المثال استطاع تنظيم "داعش" تجنيد أكثر من ٤٠ ألف مقاتل من حوالي ١٠٠ دولة عن طريق شبكة الإنترنت[١٥]، ولم يقتصر التجنيد والحشد من قِبل التنظيمات الإرهابية على فئة الذكور فقط، بل وجد تحول نحو الاتجاه إلى تجنيد المرأة، فوجدت مواقع خُصصت للمرأة (كموقع الخنساء)، والذي عمل على دمج المرأة في مشروع التنظيم الارهابي في العالم الواقعي، ومنه إلى صناعة كتائب نسائية من اللواتي نفذن عمليات انتحارية في أماكن مختلفة بعد ذلك.[١٦]

وفي تقرير نُسب إلى مجموعة العمل المالي الدولية FATF لعام ٢٠١٥م فإن شبكة المعلومات الدولية أصبحت الأكثر دعماً للتنظيمات الإرهابية سواء على مستوى التجنيد أو التمويل.[١٧]

١٥ – الإرهاب الإلكتروني، مرصد الأزهر، بتاريخ ١٩ أكتوبر ٢٠٢٢م، متاح على:
https:/www.azhar.eg/observer%D %8AA%D %8T %9D %8A %7B %5D8 %9A%D -84 %9 %D %8A %7D8 %9A

١٦ ـ بشير البكير، القاعدة في اليمن والسعودية (بيروت: دار الساقي للنشر، ٢٠١٠م)، ص١٣، ص١٤.

١٧ –عبد الستار عبد الرحمن، الإرهاب السيبراني – خطر يهدد العالم، التحالف الإسلامي العسكري لمحاربة الإرهاب، ص٣، متاح على:
articles/pages/articles2322020https://www.imctc.org/ar/elibrary

٧- استعراض القدرات القتالية والتقنية باستخدام شبكة المعلومات:

جرت العادة أن يتم استعراض التنظيمات الإرهابية المعاصرة لقدراتها ومهاراتها القتالية عبر الفضاء الإلكتروني، ناهيك عن استغلال المنصات الإلكترونية لنشر عمليات التنظيم على أرض الواقع لإثبات وجوده من تفجيرات واغتيالات وقطع رؤوس، كنوع من الدعاية للتنظيم وجذب الانتباه لنشاطاته من أجل مزيد من الحشد والتمويل، علاوة على استغلال الأدوات التي يتم التحكم من خلالها في الفئة والعمر والبلد على منصات التواصل الاجتماعي في طلب إعلانات الوظائف التي تغلفها بالمغريات المادية، ليس هذا كل ما في الأمر، بل استطاعت مجموعة من التابعين لتنظيم "داعش" في عام ٢٠١٥م اختراق بعض المواقع الحيوية لنشر محتوياتها المتطرفة أمثلة: موقع وزارة الصحة البريطانية، وموقع الشرطة الماليزية الملكية، وموقع الخطوط الجوية الماليزية، وموقع شبكة التليفزيون الفرنسي TV5 ، وموقع القيادة العسكرية الأمريكية.[١٨]

٨- نشر بيانات التنظيمات الإرهابية وفتاوى المنظّرين المتطرفة:

تقوم التنظيمات الإرهابية باستغلال تواجد شريحة كبيرة على الإنترنت لتعمل على نشر بياناتها المختلفة إما عبر منصاتها ومنتدياتها وإما عبر البريد الإلكتروني، بخلاف كم الفتاوى المتطرفة التي تدعو إلى القتل ونبذ وتكفير الآخر، والتي تقوم تلك التنظيمات بتدشينها في صور كتيبات أو دروس

١٨ - عبد الستار عبد الرحمن، موقع سبق ذكره.

مسموعة أو فيديوهات، فنجد هناك العديد من المواقع التي تعد مكتبات تحوي في طياتها موسوعات وفتاوى لكبار المنظّرين أمثلة: منبر التوحيد والجهاد الذي يضم أغلب ما تم إنتاجه من قِبل كبار قادة التنظيمات الإرهابية أمثلة: أبو قتادة الفلسطيني، وأبو محمد المقدسي، وأيمن الظواهري، وأنور العولقي.[١٩]

كما عمل تنظيم "داعش" على تدعيم قدراته الإلكترونية من خلال عدة أذرع.

٩- تمويل العمليات الإرهابية باستخدام العملات المشفّرة:

تمكّنت التنظيمات الإرهابية بعد تجفيف منابع تمويلاتها وتصفية المؤسسات الخيرية التي كانت تعتمد عليها في التمويل على أرض الواقع من تعويض خسائرها الاقتصادية إلكترونياً، فاتجهت إلى التمويل عبر العالم الافتراضي وشبكة الإنترنت باستخدام الإرهاب الإلكتروني لجمع الأموال وتمويل أنشطتها الإرهابية، وذلك من خلال الاحتيال الإلكتروني والابتزاز والتعدين غير الشرعي للعملات المشفّرة، وكان من أهم طرق التمويل:

- التبرعات الإلكترونية: وفيها يتم جمع التبرعات عن طريق المواقع الإلكترونية والتطبيقات الخاصة بالجمعيات الخيرية والمنظمات غير الحكومية، علاوة على استخدام العملات الرقمية، الأمر الذي يزيد من صعوبة تتبع المتبرعين.

١٩ - راجع نموذج للمواقع التي تنشر الفكر الجهادي التكفيري لكبار المنظرين – منبر التوحيد والجهاد، متاح على: jahied.eba.com

- التجارة الإلكترونية: ويتم من خلالها بيع المنتجات المزيفة أو المسروقة أو المحظورة عن طريق المواقع الإلكترونية.
- الابتزاز والاحتيال الإلكتروني: ومن خلاله يتم ابتزاز الضحايا للحصول على الأموال، أو استخدام التقنيات الحديثة للتحايل على الأنظمة المالية والمصرفية.

ثالثاً- آليات دول الخليج العربي لمواجهة ظاهرة الإرهاب الإلكتروني:

أولت دول مجلس التعاون الخليجي اهتماماً واسعاً بمجالات مكافحة الإرهاب الإلكتروني في الآونة الأخيرة، فعملت على تطوير استراتيجيات جديدة لتحسين الأمن السيبراني، كان منها: إنشاء فرق خاصة لمكافحة الجرائم الإلكترونية، مع العمل على تحديث التقنيات الأمنية لحماية الأنظمة والبيانات الحساسة، علاوة على إتاحة التدريب والتوعية للمستخدمين والمؤسسات المعنية بمكافحة الجرائم الإلكترونية، مع تشجيع الابتكار والتطوير في مجال الأمن الإلكتروني ودعم الشركات الناشئة والمبتكرة التي تعمل في هذا المجال، مع العمل على إدخال التحسينات على التشريعات الخاصة بالجرائم الإلكترونية لتشمل الإرهاب الإلكتروني. بالإضافة إلى تعزيز سبل التعاون في مجال مكافحة الجريمة الإلكترونية على الصعيد الدولي. ونستطيع إيجاز الإجراءات التي اتخذت لمواجهة الإرهاب الإلكتروني من قبل دول الخليج العربي في النقاط التالية:

١- إدخال التحسينات على التشريعات الوطنية الخاصة بالجرائم الإلكترونية لتشمل الإرهاب الإلكتروني:

- بالنظر إلى دولة الكويت نجدها اتبعت عدة إجراءات في هذا السياق، فقد عملت على تنظيم استخدام وسائل التقنية الحديثة مع تشديد الإجراءات

الصارمة التي تحدث لانتهاكها، فكان هناك حزمة من التشريعات لعل أهمها:

القانون رقم ٩ لسنة ٢٠٠١م بشأن إساءة استعمال أجهزة الاتصالات الهاتفية وأجهزة التنصت والقوانين المعدّلة له، كذلك القانون رقم ٣ لسنة ٢٠٠٦م الخاص بالمطبوعات والنشر، علاوة على القانون رقم ٦١ لسنة ٢٠٠٧م الخاص بالإعلام المرئي والمسموع، والقانون رقم ٢٠ لسنة ٢٠١٤م الذي ينظم المعاملات الإلكترونية، والقانون رقم٣٧ لسنة ٢٠١٤م الخاص بإنشاء هيئة تنظيم الاتصالات وتقنية المعلومات.[٢٠]

كذلك قانون رقم ٦٣ لسنة ٢٠١٥م بشأن مكافحة جرائم تقنية المعلومات، والذي كانت أبرز مواده (المادة ٣) التي نصت على تشديد العقوبة في حالة كون البيانات محل الجريمة حكومية أو متعلّقة بحسابات العملاء في المنشآت المصرفية، وتناولت نفس المادة تجريم أفعال التزوير أو إتلاف المستندات الإلكترونية عُرفية أو حكومية أو بنكية، وكذلك استخدام أي وسيلة من وسائل تقنية المعلومات في تهديد الأشخاص أو ابتزازهم.

في حين نصت المادة (٤) على عقاب من أعاق أو عطّل عمداً الوصول إلى مواقع إلكترونية، وكل من تنصّت على ما هو مرسل عن طريق الشبكة المعلوماتية، كما قضت المادة (٥) على عقاب كل من توصل عن طريق إحدى وسائل تقنية المعلومات إلى بيانات بطاقة إئتمانية واستخدامها في الحصول

٢٠ - حاتم أحمد محمد بطيخ، تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات. دراسة تحليلية مقارنة، ص٢٣، متاح على:
https://jdl.journals.ekb.eg/article_191190_a30e59/boeod/47f4926c2b98b33217.pdf

على أموال الغير، أما المادتان السادسة والسابعة فقد قضت بمعاقبة كل من ارتكب إحدى المحظورات المنصوص عليها في قانون المطبوعات والنشر باستخدام الوسائل الإلكترونية، كما أوجبت المواد ٨، ٩، ١٠ على عقاب كل من استخدم أيًّا من هذه الوسائل في الترويج للاتجار بالبشر أو المواد المخدّرة أو تسهيل الاتصال بالمنظمات الإرهابية وترويج أفكارها أو غسل الأموال.[٢١]

- وفي المملكة العربية السعودية صدر نظام مكافحة جرائم المعلومات بموجب المرسوم الملكي رقم م/ ١٧ بتاريخ ٣/ ٧/ ٨ لعام ٢٠٠٧م، والذي جاء في المادة الثالثة منه على المعاقبة بالسجن بمدة لا تزيد على سنة، وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين لكل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:
- التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي.
- الدخول غير المشروع لتهديد شخص أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً.
- الدخول غير المشروع إلى موقع إلكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه.
- المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرات أو ما في حكمها.

٢١ - قانون رقم ٦٣ لسنة ٢٠١٥م في شأن مكافحة جرائم تقنية المعلومات، موقع سبق ذكره.

- التشهير بالآخرين وإلحاق الضرر بهم عبر وسائل تقنيات المعلومات المختلفة، كما جاء في المادة الرابعة، يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين لكل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

- الاستيلاء لنفسه أو لغيره على مال منقول أو على سند أو توقيع هذا السند، وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب أو انتحال صفة غير صحيحة.

- بينما جاءت المادة السابعة منه لتؤكد على المعاقبة بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين لكل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

- إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره؛ لتسهيل الاتصال بقيادات تلك المنظمات، أو أي من أعضائها، أو ترويج أفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات، أو أي أداة تستخدم في الأعمال الإرهابية.
- الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي مباشر، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب للحصول على بيانات تمس الأمن الداخلي والخارجي للدول أو اقتصادها الوطني.[٢٢]

٢٢ - نظام مكافحة الجرائم المعلوماتية، هيئة الخبراء بمجلس الوزراء، المملكة العربية السعودية، بتاريخ ٣ أبريل ٢٠٢٣م، متاح على:
https://laws.boe.gov.sa/boelaws/lawdetails/25df73d0-6f

علاوة على صدور الأمر الملكي رقم ٦٨٠١ في ١١/ ٢/ ٢٠١٧م بإنشاء هيئة باسم الهيئة الوطنية للأمن السيبراني، بغرض تعزيز الأمن السيبراني وحمايته في المملكة.[٢٣]

– وفي دولة الإمارات العربية المتحدة ظهر اهتمام الدولة بالتصدي للجرائم المعلوماتية في العديد من التشريعات، كان أبرزها: القانون رقم ٢ لسنة ٢٠٠٦م الخاص بمكافحة جرائم تقنية المعلومات، كذلك أصدرت القانون رقم (٣) لسنة ٢٠١٢م الخاص بإنشاء الهيئة الوطنية للأمن الإلكتروني.[٢٤]

إضافة إلى القانون الاتحادى رقم ١٢ لسنة ٢٠١٦م بتعديل المرسوم بقانون اتحادي رقم (٥) لسنة ٢٠١٢م بشأن مكافحة جرائم تقنية المعلومات، والذي جاء في المادة الأولى منه المعاقبة بالسجن المؤقت والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تتجاوز مليوني درهم، أو بإحدى هاتين العقوبتين لكل من تحايل على العنوان البروتوكولي للشبكة المعلوماتية باستخدام عنوان وهمي أو عنوان عائد للغير أو بأي وسيلة أخرى، وذلك بقصد ارتكاب جريمة أو الحيلولة دون اكتشافها.[٢٥]

وفي عام ٢٠١٨م قامت بإصدار المرسوم الاتحادي رقم ٤ الخاص بتعديل المرسوم الاتحادي رقم ٥ لسنة ٢٠١٢م، ولذلك تعتبر الإمارات

٢٣ – إبراهيم سليمان، الإرهاب المعلوماتي وتمويله في ضوء النظام السعودي، بنك المعرفة المصري، ٢٠١٩م، ص٢٩٠، متاح على: https://espes/article_journaals.ekb.eg٢١٤٤٩٧

٢٤ – حاتم أحمد محمد بطيخ، مرجع سبق ذكره، ص٢٢.

٢٥ – قانون اتحادي رقم ١٢ لسنة ٢٠١٦م بتعديل المرسوم بقانون اتحادي رقم (٥) لسنة ٢٠١٢م في شأن مكافحة جرائم تقنية المعلومات، بتاريخ ٢٣ مايو ٢٠١٦م، ص٢٠، متاح على:
https://www.moj.gov.ae/ar/laws-andlegislation/latest-legislations-and-laws.aspx=page=1

أول دولة عربية تقوم بإصدار تشريع قانوني مستقل يتعلق بمكافحة الجرائم المعلوماتية، وهو القانون رقم (٢) لسنة ٢٠٠٦م.[٢٦]

كذلك إصدار مرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١م في شأن مكافحة الشائعات والجرائم الإلكترونية، والذي جاء بمجموعة عقوبات وغرامات في مواده لمن يتعرض للأنظمة المعلوماتية لمؤسسات الدولة من خلال:

* اختراق الأنظمة المعلوماتية الخاصة بمؤسسات الدولة.
* الإضرار بأنظمة المعلومات في الجهات المصرفية أو الإعلامية أو الصحية أو العلمية.
* الاعتداء على بيانات المنشآت المالية والتجارية أو الاقتصادية.
* التحايل على الشبكة المعلوماتية بقصد ارتكاب جريمة.
* اصطناع البريد والمواقع والحسابات الإلكترونية الزائفة.
* الاعتراض غير المشروع وإفشاء المعلومات.
* الاعتداء على وسائل الدفع الإلكترونية.
* التجنيد والترويج للجماعات الإرهابية.
* الاتجار والترويج للأسلحة النارية أو الذخائر أو المتفجرات.
* تحويل أو حيازة أو استخدام أو اكتساب أموال غير مشروعة.
* كشف معلومات سرية خاصة بالعمل.

٢٦ - حاتم أحمد محمد بطيخ، مرجع سبق ذكره، ص٢٢.

* إنشاء أو تعديل روبوتات إلكترونية لنقل بيانات زائفة في الدولة.[٢٧]

- أما في مملكة البحرين فقد جاء القانون رقم ٦٠ لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات، والذي احتوى على (٢٤) مادة كان أبرزها المادة الثانية من الفرع الأول منه والتي نصت على أنه: يعاقب بالحبس مدة لا تزيد على سنة، وبالغرامة التي لا تتجاوز ثلاثين ألف دينار، أو بإحدى العقوبتين لمن قام دون مسوّغ قانوني بالدخول إلى نظام تقنية المعلومات أو جزء منه، وإذا نتج عن الدخول إفشاء للبيانات المخزنة في وسيلة أو نظام تقنية المعلومات أو جزء منه عُد ذلك ظرفاً مشدداً.

كما جاء في المادة الثالثة منه بالعقاب بالحبس والغرامة التي لا تتجاوز خمسين ألف دينار أو بإحدى هاتين العقوبتين لمن أحدث تلفاً في بيانات وسيلة تقنية المعلومات، وتضاعف العقوبة إذا ترتب على ارتكاب الجريمة أيًّا مما يلي:

- إعاقة لسير أي من المرافق العامة أو الأعمال ذات المنفعة العامة.
- تهديد لحياة الناس أو أمنهم أو صحتهم.(٢٨)

- بالنسبة لدولة قطر: جاء قانون الاتصالات والذي صدر بموجب مرسوم رقم ٣٤ لسنة ٢٠٠٦م، حيث احتوى على العديد من إجراءات مكافحة الإرهاب

٢٧ - مرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١م في شأن مكافحة الشائعات والجرائم الإلكترونية، وزارة العدل لدولة الإمارات العربية المتحدة، متاح على:
https://www.moj.gov.ae/ar/laws-andlegislation/latest-legislations-and-laws.aspx=page=1

٢٨ - قانون رقم ٦٠ لسنة ٢٠١٤م بشأن جرائم تقنية المعلومات، البوابة الوطنية للحكومة الإلكترونية – مملكة البحرين، بتاريخ ٣٠ سبتمبر ٢٠١٤م ، متاح على:
https://www.lloc.gov.bh/HTM/k6014.htm

الإلكتروني، مثل تحديد هوية المستخدمين وتسجيل الاتصالات والمراسلات الإلكترونية (٢٩)، كذلك جاء قانون مكافحة الجرائم الإلكترونية رقم ١٤ لسنة ٢٠١٤م، والذي تضمن (٥٤) مادة موزعة على خمسة فصول، حيث تناولت عقوبات بالحبس والغرامة لمن يقوم بالجرائم الآتية:

- الحصول على بيانات أو معلومات تمسّ الأمن الداخلي للبلاد أو الخارجي للدولة، أو إلغاء البيانات والمعلومات الإلكترونية أو إتلافها.
- تدمير أو تعطيل النظام المعلوماتي أو الشبكة المعلوماتية.
- التنصت على أي بيانات مرسلة عبر الشبكة المعلوماتية.
- إنشاء موقع لجماعة أو تنظيم إرهابي على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، أو تسهيل الاتصال بقيادات تلك الجماعات أو أي من أعضائها، أو الترويج لأفكارها أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرات أو أي أداة تستخدم في الأعمال الإرهابية.[٣٠]

كذلك جاء قانون حماية البيانات الشخصية القانون رقم (١٣) لعام ٢٠١٦م، والذي يهدف إلى حماية البيانات الشخصية وتنظيم جمع ومعالجة واستخدام المعلومات الشخصية.[٣١]

٢٩ – قانون الاتصالات لدولة قطر – وزارة الاتصالات وتكنولوجيا المعلومات ـ متاح على:
https://www.mcit.gov.qa/ar/documments/document/telecommunications-law-qater

٣٠ – قانون رقم ١٤ لسنة ٢٠١٤م – قانون مكافحة الجرائم الإلكترونية، موقع سبق ذكره.

٣١- قانون رقم ١٣ لسنة ٢٠١٦م بشأن حماية خصوصية البيانات الشخصية، وزارة العدل – دولة قطر، متاح على:
https://www.almeezan.qa/lawviw.aspx?opt&lawid=7121&language=ar

٢- الاتفاقيات الخليجية لمواجهة الإرهاب الإلكتروني:

عملت دول الخليج العربي على محاولة الاستجابة لتحديات الإرهاب الإلكتروني، من خلال مواجهته بمجموعة اتفاقيات كان أهمها: اتفاقية مكافحة تمويل الإرهاب، والتي وقعت في عام ٢٠١٤م، وهي بمثابة اتفاقية إقليمية غرضها مكافحة تمويل الإرهاب وتجفيف منابعه في دول مجلس التعاون لدول الخليج العربي، والتي هدفت إلى: تعزيز التعاون بين الدول الأعضاء فيما يخص إجراءات التحري والمراقبة لمنع تمويل الإرهاب، علاوة على العمل على زيادة الوعي بين الجمهور والمؤسسات المالية والتجارية بشأن خطورة تمويل الإرهاب، مع تعزيز التعاون بين الدول الأعضاء والمنظمات الدولية والإقليمية فيما يخص أمور تبادل المعلومات والخبرات في مجال مكافحة تمويل الإرهاب.

كما كانت هناك الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠م، وتلك الاتفاقية قد احتوت على بعض المواد التي تعد الأولى في تشريعات الجرائم الإلكترونية في المنطقة، وبالتحديد في الإمارات والمملكة العربية السعودية، وتعد المادة الخامسة عشرة من أبرز المواد بها، حيث عددت الجرائم المتعلقة بالإرهاب المرتكبة بواسطة تقنية المعلومات على النحو التالي: جرائم نشر أفكار ومبادئ جماعات إرهابية والدعوة لها، وتمويل العمليات الإرهابية والتدريب عليها، وتسهيل الاتصالات بين التنظيمات الإرهابية، ونشر طرق صناعة المتفجرات المستخدمة في العمليات الإرهابية، ونشر النعرات والفتن والاعتداء على الأديان والمعتقدات.[٣٢]

٣٢ - انظر نص الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، موقع الجامعة العربية، متاح على:
/https://www.courts.gov.ps/4serfiles/file

٣- إنشاء مراكز متخصصة لمكافحة الإرهاب الإلكتروني:

سعت دول الخليج العربي إلى إنشاء مراكز متخصصة لمكافحة ظاهرة الإرهاب الإلكتروني، فكان منها: إنشاء دولة الإمارات لمركز أطلق عليه (صواب)، حيث عمل على توظيف وسائل التواصل الاجتماعي على شبكة الإنترنت لتصحيح الأفكار المتطرفة من خلال التواصل مع جمهور الإنترنت، مع العمل على تصحيح التفسيرات الدينية الخاطئة التي تبثها التنظيمات الإرهابية.[٣٣]

كذلك يوجد المركز الوطني الإرشادي للأمن السيبراني، والذي أنشأته المملكة العربية السعودية، بهدف تعزيز جهود المملكة في رفع مستوى الوعي بالأمن السيبراني، لتجنب الأخطار التي تشكلها البيئة الإلكترونية، وذلك عبر عدة وسائل منها: التوعية بأخطر الثغرات وكيفية التعامل معها، وإطلاق الحملات والبرامج التوعوية، علاوة على التعاون مع باقي المراكز ذات الصلة.[٣٤]

وفي دولة قطر تم إنشاء الوكالة الوطنية للأمن السيبراني، والتي تهدف إلى ضمان الحماية الإلكترونية للبنية التحتية للدولة، مع تعزيز الوعي السيبراني، ومراقبة الأنشطة المشبوهة في المجال الإلكتروني.[٣٥]

٣٣ – مراكز محاربة التطرف، البوابة الرسمية لحكومة الإمارات العربية، متاح على:
https://u.ae/ar-ae/about-the-uae/culture/tolerance/centers-for-countering-extremism

٣٤ – المركز الوطني الإرشادي للأمن السيبراني، متاح على: https://cert.gov.sa/ar/

٣٥ – الوكالة الوطنية للأمن السيبراني – دولة قطر، متاح على: https://www.ncsa.gov.qa/ar

وفي مملكة البحرين تم إنشاء عدة مراكز، كان أهمها المركز الوطني للأمن السيبراني، وهو المركز الرئيس المعني بشؤون مكافحة الإرهاب الإلكتروني وتطوير استراتيجيات المكافحة والحماية السيبرانية للدولة.[٣٦]

وفي دولة الكويت تعددت المراكز البحثية المعنية بالمكافحة، وكان أهمها المركز الوطني للأمن السيبراني الذي تأسس في ٥ فبراير ٢٠٢٢م، والذي يهدف إلى تبادل البيانات وتعزيز الأمن السيبراني بين المؤسسات الحكومية، وذلك من أجل اتخاذ الحذر قبل وقوع أي هجوم سيبراني.

٣٦ - المركز الوطني للأمن السيبراني – مملكة البحرين، متاح على: https://www.ncsl.gov.bh/

رابعاً- دول مجلس التعاون الخليجي ومستقبل مواجهة الإرهاب الإلكتروني:

لا شك أن المجهودات الوطنية والإقليمية والدولية التي قامت بها دول الخليج العربي ساهمت إلى حد كبير في التصدي لجرائم الإرهاب عمومًا، والإرهاب الإلكتروني خصوصاً، ولكن نحن الآن أمام تطور مرعب لتكنولوجيا المعلومات يصاحبه تطور وتكيف على الصعيد الآخر من التنظيمات الإرهابية، فالإرهاب الإلكتروني نشأ وتطور في بيئة متغيرة، لذلك يلزم مواكبة هذا التطور من جانب الجهات المعنية، ومن ثم يراعى في المستقبل القيام ببعض الإجراءات التي تدعم الجهود المبذولة للحد من ظاهرة الإرهاب الإلكتروني، ومنها:

١- تطوير القدرات التقنية:

تصنف الجرائم الإلكترونية باعتبارها جرائم ذكية نتاج أشخاص مهرة يمتلكون أدوات معرفة تقنية ونسبة ذكاء عالٍ، لذلك لا بد من استمرار العمل على تطوير القدرات التقنية، من أجل التمكن من سرعة الكشف عن هوية مرتكب الجريمة في أقل وقت، مع تفعيل استخدام الذكاء الاصطناعى والتحليل الضوئي لرصد وتحليل الأنشطة الإرهابية على الإنترنت، والعمل

على التحديث المستمر لبرامج الحماية الخاصة بأنظمة الحواسب ومحاولة استخدام برمجيات آمنة ونظم تشغيل خالية من الثغرات.[٣٧]

٢- توفير برامج التدريب المتخصصة للعاملين في مجال الأمن السيبراني:

نتيجة لتضاعف هجمات التنظيمات الإرهابية في البيئة الإلكترونية أصبح من الضروري أن يكون لكل مؤسسة فريق داخلي متخصص في مجال الأمن السيبراني، قادر على مواكبة التطور وسرعة الاستجابة لأي هجمات إلكترونية أو إرهابية، والقيام بدورات تدريبية مستمرة يخضع لها هذا الفريق للتوعية، خاصة في المنشآت الحكومية، وذلك لفهم التهديدات المختلفة لنظم المعلومات وكيفية التعامل معها وقت الأزمة والقواعد الدولية المنظمة لحماية الأمن السيبراني.

٣- العمل على توعية الجمهور بأخطار الإرهاب الإلكتروني:

بما أن هناك شريحة كبيرة من مستخدمي شبكة الإنترنت من جميع الأعمار، فإنه لا بد من العمل على توعيتهم بأخطار الجرائم الإلكترونية والتهديدات التي قد يتعرضون لها من قِبل التنظيمات الإرهابية، خاصة فيما يتعلّق بأساليب التجنيد المحترفة وجمع التبرعات والاستعطاف، وبث الفتاوى والمواد المتطرفة، كذلك ضرورة حث الآباء على متابعة الأبناء حتى لا يقعوا فريسة أنشطة إرهابية، وذلك من خلال مراقبة التغيرات التي تحدث في السلوك، علاوة على التوعية بأساليب الاحتيال الإلكتروني التي

٣٧ - إسراء جبريل رشاد، الجرائم الإلكترونية. الأهداف. الأسباب – طرق الجريمة ومعالجتها، المركز الديمقراطي العربي، ٢٠١٦م، متاح على: https://democratica.de/?p=35426

قد يتعرض لها الأفراد من خلال رسائل التوعية ووسائل الإعلام المختلفة، أو المدارس والجامعات، مع تشجيع الجمهور على الإبلاغ عن أي نشاط مشبوه يتعرضون له.

٤- مواصلة تعزيز التعاون الدولي في مجال مكافحة الإرهاب الإلكتروني:

بما أن الفضاء السيبراني يلغي الحدود ويجعل العالم كله كأنه قرية واحدة؛ لذلك لا بد من تعزيز التعاون من خلال تبادل المعلومات والخبرات الأمنية بين دول المنطقة، بما فيها المعلومات الخاصة بالمواقع المتطرفة والتابعة للتنظيمات الإرهابية التي تتغير باستمرار، مع إجراء التدريبات المشتركة بين الأجهزة الأمنية في دول المنطقة، إضافة إلى تشجيع الاستثمارات في مجال تقنية المعلومات، والعمل على تعزيز التعاون بين المؤسسات الحكومية والقطاع الخاص الذي يعمل في هذا المجال.

الخاتمة:

اتضح مما تقدّم، أنه على الرغم من اختلاف المسميات التي أُطلقت على مفهوم الإرهاب الإلكتروني، إلا أنه لا خلاف على الأضرار التي باتت أمراً حتمياً يستوجب المواجهة المستمرة والمُحدثة، سواء على الجانب النظري أو التطبيقي، وعلى المستوى الفردي أو الجماعي، فكلما طورت الدول آليات المواجهة للإرهاب الإلكتروني، طوّرت التنظيمات الإرهابية هي الأخرى آلياتها بشكل مضاد، فلقد أثبتت هذه النوعية من التنظيمات استطاعتها التكيف مع كافة ما يستجد من تطورات، ولذلك، حتى تؤتي ثمار المكافحة نتائجها، لا بد ألا تتوقف عجلة التطور والمتابعة لكافة المستجدات والآليات الحديثة التي تتبعها التنظيمات الإرهابية، سواء في صورة إجراءات وقائية قبل وقوع التهديد، أو في صورة مكافحة متطورة في حال وقوع التهديد.

وبناء عليه نستطيع الخروج ببعض التوصيات:

١ ـ العمل على المزيد من توحيد جهود المكافحة بين الجهات المختلفة سواء التشريعية أو القضائية أو العسكرية أو الفنية، لتحصينها من اختراق المجرمين الإلكترونيين.

٢ ـ إحكام السيطرة على الأسواق الإلكترونية التي يُحمل من خلالها الألعاب الإلكترونية للأطفال والمراهقين، وذلك للحد من استغلال التنظيمات الإرهابية لها في تنمية السلوك العنيف ومحاولات اختراق العقول، وكنموذج لذلك لعبة (صليل الصوارم) التي أنتجها تنظيم (داعش).

٣ ـ زيادة إنشاء المدارس المتخصصة والكليات التي تعنى بدراسة الأمن السيبراني.

٤ ـ توظيف البرامج الإعلامية والإعلانية للوصول لشريحة عريضة من الجمهور، كذلك التركيز على عمل برامج ولقاءات مع الخبراء والمتخصصين لشرح مثل هذه الأمور وكيفية التغلب عليها.

٥ ـ تدشين المزيد من الصفحات التوعوية سواء الحكومية أو المستقلة عبر وسائل التواصل الاجتماعي، وذلك بغرض بث التوعية المباشرة والمستمرة بين الجمهور بأخطار استخدام الفضاء الإلكتروني وكيفية الحد منها، والإبلاغ عن الأنشطة الضارة.

قائمة المراجع العربية والأجنبية

أولاً . المراجع العربية:

١ . الكتب:

- البكير، بشير، القاعدة في اليمن والسعودية (بيروت: دار الساقي للنشر، ٢٠١٠م).
- الحسيني، علي جبار، جرائم الحاسوب والإنترنت (عمان: دار البازوري للنشر والتوزيع، ٢٠٠٩م).
- كمال، محمد، الإرهاب السيبراني .. عندما يستخدم الإرهابي الكيبورد بدلاً من القنبلة (القاهرة: دار كليم للطباعة والنشر والتوزيع، ٢٠٢٢م).

ب . الدوريات:

- الزعبي، محمد إبراهيم، فاعلية القوانين والتشريعات العربية في مكافحة الجرائم الإلكترونية. دراسة مقارنة، **المجلة العربية للنشر العلمي**، عمان، العدد ٣٧/ ٢٠٢١م.
- الناهي، أحمد عبد الله، رشيد، صدام عبد الستار، « السياسة الإعلامية لتنظيم داعش الإرهابي. الأهداف وسبل المواجهة»، **المجلة السياسية والدولية** - كلية العلوم السياسية - الجامعة المستنصرية، بغداد، عدد ٣٠/ ٢٠١٦م.

- نظير، مروة، «جماعات التطرف العنيف ومنصات التواصل الاجتماعي. قراءة في الاستخدامات والعوامل "، **المجلة الاجتماعية القومية** - المركز القومي للبحوث الاجتماعية والجنائية، القاهرة، عدد ١ يناير/ ٢٠٢٠م.

ج- المواقع الإلكترونية:

- الإرهاب الإلكتروني، مرصد الأزهر، بتاريخ ١٩ أكتوبر ٢٠٢٢م، متاح على:
https:/www.azhar.eg/observer%D8%AA%D9%81%D8%A7%B5%D9%8A%D9%84-%D8%A7%D9%8A

- الجرائم الإلكترونية والإرهاب الإلكتروني، موقع جهاز المخابرات العامة الفلسطينية، نشر بتاريخ ٣٠ يوليو ٢٠١٩م، متاح على:
http://www.pgis.ps/ar/category/%d8%ad%dg%88%dg%84-id8%a7%dg%84%d9%85%d8%ae%d8%a7%d8%a8%ae%d8%a7%d8%a8%d8%b1%d8%a7%d8%aq

- المرسوم الملكي رقم م/ ١٧ لعام ١٤٢٨ - المادة الأولى - الفقرة الثامنة، هيئة الخبراء بمجلس الوزراء - المملكة العربية السعودية، بتاريخ ٢٧ مارس ٢٠٠٧م، متاح على:
https://laws.Boe.gov.sa/Boelaws/laws/viewer/ceadb6be-81e5-4c91-919e-2967202d9643?lawld=25df73d6-0f49-4dc5-b010=a9a700f2ec1d

- المركز الوطني الإرشادي للأمن السيبراني، متاح على:
https://cert.gov.sa/ar/

- المركز الوطني للأمن السيبراني - مملكة البحرين، متاح على:
https://www.ncsl.gov.bh/

- الوكالة الوطنية للأمن السيبراني - دولة قطر، متاح على:
https://www.ncsa.gov.qa/ar

-إبراهيم، علي، طارش، أسعد، « الأمن السيبراني ودوره في انتشار ظاهرة الإرهاب في العراق بعد عام ٢٠٠٣م»، مجلة دراسات دولية، عدد ٨٠، متاح على:
https://www.iasj.net/iasj/pdf/5e08943c7ae82efb

- بطيخ، حاتم أحمد محمد، تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات. دراسة تحليلية مقارنة، متاح على:
https://jdl.journals.ekb.eg/article_191190_a30e59/boeod/47f-4926c2b98b33217.pdf

- بنداري، نورا، دور وسائل التواصل الاجتماعي في تجنيد أعضاء التنظيمات الإرهابية. دراسة حالة داعش، المركز الديمقراطي العربي، بتاريخ ١٩ يوليو ٢٠١٦م، متاح على:
https://democratica.de/?p=34268

- رشاد، إسراء جبريل، الجرائم الإلكترونية. الأهداف. الأسباب - طرق الجريمة ومعالجتها، المركز الديمقراطي العربي، ٢٠١٦م، متاح على:
https://democratica.de/?p=35426

- سليمان، ابراهيم، الإرهاب المعلوماتي وتمويله في ضوء النظام السعودي، بنك المعرفة المصري، ٢٠١٩م ، متاح على :
https://espes/article_journaals.ekb.eg214497

- عبد الرحمن، عبد الستار، الإرهاب السيبراني - خطر يهدد العالم ، التحالف الإسلامي العسكري لمحاربة الإرهاب ، متاح على : /articles/pages/articles2322020https://www.imctc.org/ar/elibrary

- قانون اتحادي رقم ١٢ لسنة ٢٠١٦م بتعديل المرسوم بقانون اتحادي رقم (٥) لسنة ٢٠١٢م في شأن مكافحة جرائم تقنية المعلومات، ٢٣ مايو ٢٠١٦م، متاح على:
https://www.moj.gov.ae/ar/laws-andlegislation/latest-legislations-and-laws.aspx=page=1

- قانون رقم ١٣ لسنة ٢٠١٦م بشأن حماية خصوصية البيانات الشخصية، وزارة العدل - دولة قطر، متاح على:
https://www.almeezan.qa/lawviw.aspx?opt&lawid=7121&language=ar

- قانون رقم ١٤ لسنة ٢٠١٤م - قانون مكافحة الجرائم الإلكترونية - البوابة القانونية القطرية، متاح على:
https://almeezan.qa/lawview.aspx?opt&lawid=63668language=ar:~:text=%d8%A7D9%84%D9%

- قانون الاتصالات لدولة قطر - وزارة الاتصالات وتكنولوجيا المعلومات - متاح على:
https://www.mcit.gov.qa/ar/documments/document/telecommunications-law-qater

- قانون رقم ٦٠ لسنة ٢٠١٤م بشأن جرائم تقنية المعلومات، البوابة الوطنية للحكومة الإلكترونية - مملكة البحرين، بتاريخ ٣٠ سبتمبر ٢٠١٤م، متاح على:

https://www.lloc.gov.bh/HTM/k6014.htm

- قانون رقم ٦٣ لسنة ٢٠١٥م في شأن مكافحة جرائم تقنية المعلومات، متاح على:

https://www.moi.gov.kw/main/content/docs/cybercrime/ar/law-establishing-cyber-crime-dept.pdf

- مخاطر الإرهاب الإلكتروني تتزايد، مركز الإمارات للدراسات والبحوث الاستراتيجية، بتاريخ ٢١ مارس ٢٠٠٤، متاح على:

https://www.ecssrae/reports_analysis/%D9%85%AE%D8%A%D8%A7%D9%84%D8%A7%D9%84%D8%A5%

- مراكز محاربة التطرف، البوابة الرسمية لحكومة الإمارات العربية، متاح على:

https://u.ae/ar-ae/about-the-uae/culture/tolerance/centers-for-countering-extremism

- مرسوم بقانون اتحادى رقم (٣٤) لسنة ٢٠٢١م في شأن مكافحة الشائعات والجرائم الإلكترونية، وزارة العدل لدولة الإمارات العربية المتحدة، متاح على:

https://www.moj.gov.ae/ar/laws-andlegislation/latest-legislations-and- laws.aspx=page=1

- مرسوم رقم ٣٧ لسنة ٢٠٢٢م بإنشاء المركز الوطني للأمن السيبراني، متاح على:

https://mesferlaw.com/archives/525

- منبر التوحيد والجهاد، متاح على: jahied.eba.com

- نص الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، موقع الجامعة العربية، متاح على:

https://www.courts.gov.ps/4serfiles/file/

- نظام مكافحة الجرائم المعلوماتية، هيئة الخبراء بمجلس الوزراء، المملكة العربية السعودية، بتاريخ ٣ أبريل ٢٠٢٣م ، متاح على :

https://laws.boe.gov.sa/boelaws/lawdetails/25df73d6-0f

ثانياً - المراجع الأجنبية:

1 - Cyber terrorism, Wegan council , Available at : https://www.wigan.gov.uk/resident/crime.emergencies/counter-terrorism/cyber-terrorism/cyber-terrorism.aspx.

2- Weiman,Gabiel.”New Terrorism and New Media” . Wilson international center for scholars,Washington D.C ,2014.

Abstract:

The tremendous development in information technology has left a counter-development at the level of performance of terrorist organizations, which have worked to develop their mechanisms in the face of the security measures followed towards them, as they worked to invest their presence in the electronic environment in the form of electronic terrorism to compensate for what they lost on the ground of camps, personnel, financing and operations through several mechanisms, which was confronted by countries, especially the countries of the Arab Gulf, by following counter-mechanisms that would reduce And facing the losses that resulted from the phenomenon of electronic terrorism, and then the strategic report seeks to analyze the various mechanisms used by the Gulf Cooperation Council countries in confronting the phenomenon of electronic terrorism and the effectiveness of these mechanisms in reducing the losses resulting from this phenomenon.

Key words: Cyberterrorism –Mechanism –Arab Gulf countries–Combating terrorism – Terrorist organizations.

جامعة الكويت
KUWAIT UNIVERSITY

مركز دراسات الخليج والجزيرة العربية

قواعد النشر في سلسلة (التقرير الاستراتيجي)

١ ـ أن يكون موضوع التقرير معنياً بالقضايا الاستراتيجية التي تهم دولة الكويت في المقام الأول، ودول منطقة الخليج والجزيرة العربية بشكل عام، أو يعالج قضايا دولية واقليمية من زاوية ارتباطها بمنطقة الخليج.

٢ ـ أن يغلب على التقرير التحليل والتفسير مع تقليص مساحة الوصف أو التأريخ.

٣ ـ لا يقل عدد كلمات التقرير عن (٣٧٥٠ كلمة).

٤ ـ يمنح الباحث مكافأة مالية مقدارها (١٥٠ دينار كويتي).

جامعة الكويت
KUWAIT UNIVERSITY

مركز دراسات الخليج والجزيرة العربية