2024 تشرين1 مجلة دراسات في الإنسانيات والعلوم التربوية العدد 7
October 2024 Journal of Studies in Humanities and Educational Sciences No. 7
Print ISSN 3006-3256 Online ISSN 3006-3264

تداعيات التهديدات الإلكترونية للجماعات الإرهابية تنظيم ـداعش أنموذجاً

م. م. ياسين مارد كاظم الدحيدحاوي
جامعة الكوفة – كلية الهندسة
yaseenm.alduhaidahawi@uokufa.edu.iq

المُلخص

إن الثورة التكنولوجية مطلع العقد الأول من القرن الحادي والعشرين، والتي تعتمد على المعلوماتية والمعرفية والقدرة على استخدامها، استثمرت في الاتجاه السلبي بالتزامن مع التطور الملحوظ في المفهوم التقليدي للأمن الدولي ليضم الدول والفاعلين الدوليين وظهور الأمن الإلكتروني على صعيد العلاقات الدولية، إذ توسعت التهديدات الأمنية الإلكترونية التي تتسم بتغيرها وتطورها واتساع نطاقها العالمي، وفي ظل الانفتاح التكنومعلوماتي أخذت الجماعات الإرهابية، خاصة تنظيم "داعش"، يستخدم الأدوات الإعلامية والإلكترونية في الترويج لأفكاره ومبادئه من خلال المواقع الإلكترونية والصحف الصادرة بلغات مختلفة، أو لتخطيط وتنفيذ العمليات الإرهابية، أو لأغراض هجومية، مثل: "اختراق المواقع الإلكترونية، شبكات المعلومات، التجسس، نشر الفيروسات في أجهزة الدولة، نشر الأعمال الإرهابية بتقنية عالية الجودة لتضخيم بأنه الأقوى والأخطر عالمياً، والترويج لنمط حياة الأفراد في مناطق سيطرة التنظيم".

الكلمات المفتاحية: الإرهاب الإلكتروني، الجماعات الإرهابية، داعش، الهيئة الإعلامية، الانتشار الإلكتروني.

The repercussions of electronic threats to terrorist groups ISIS is a model

Assistant teacher: Yassin Mard Kazem Al – Dahidhawi
University of Kufa – College of Engineering

Abstract

The technological revolution at the beginning of the first decade of the twenty – first century, which depends on information and knowledge and the ability to use them, was invested in a negative direction in conjunction with the noticeable development in the traditional concept of international security to include states and international actors and the emergence of cybersecurity at the level of international relations, as cybersecurity threats expanded. Which is characterized by its change, development, and wide global scope, and in light of technological and informational openness, terrorist groups have taken. Especially ISIS, which uses media and electronic tools to promote its ideas and principles through websites and newspapers published in different languages, or to plan and implement terrorist operations, or for offensive purposes, such as: “hacking websites, information networks, espionage, or spreading viruses in state agencies”. “Disseminating terrorist acts with high – quality technology to amplify that it is the strongest and most dangerous in the world, and to promote the lifestyle of individuals in the areas under the organization’s control”.

Keywords: electronic terrorism, terrorist groups, ISIS, the Media Authority, electronic proliferation.

مقدمة

يعد المجال الافتراضي ميداناً رحباً للجماعات الإرهابية حيث أسهم التطور في الميدان المعلوماتي بتعزيز الهجمات الإرهابية الأنفرادية والقيادة الافتراضية عن بعد، وتأتي التهديدات الإلكترونية في مقدمة

الهجمات التي بدأت تثير قلق الدول والحكومات، بسبب تعدد الجهات التي تستطيع الانخراط فيها، وتعقيد تتبع مصادرها أو تحديد مكان انطلاقها، وأصبحت شبكة الإنترنيت ساحة للنزاعات والصراعات التي يدخل في سياقها التجسس والاختراق والتحكم في بيانات تمس الأمن القومي للدول، مما انعكس على السلم والأمن الدوليين الذي أصبح عرضة لمخاطر الإرهاب الإلكتروني. وقد أوجدت التحولات في النظام الدولي فرصة مواتية للتنظيمات الإرهابية لتطوير آليات عملها، لا سيما بعد تعزيز الخطاب الأصولي المتجاوز لحدود الدولة، وإزالة الهوية الثقافية المحلية لتحقيق طموح عالمي، وهذا الخطاب المتأثر بأيديولوجي متشددة وجد صداه عند التنظيمات والجماعات الإرهابية، وكشفت عن هشاشة بنيوية في بعض الدول حيث تراجع دور الدولة في ضبط أمنها وحدودها.

إشكالية البحث

يتمحور البحث حول إشكالية مفادها: **"طبيعة تداعيات التهديدات الإلكترونية للجماعات الإرهابية تنظيم داعش أنموذجاً"**، إذ أصبحت التنظيمات والجماعات الإرهابية في توجهها العام تعتمد على الإرهاب الإلكتروني للاضرار بالمنظومة النفسية من وراء عمليات العنف لإشاعة الخوف والقلق بين مواطنين الدول المستهدفة. وعليه تتبين التساؤلات التالية:

- ماهية طبية التهديدات الإلكترونية وأنماطها؟
- ما هي آليات استثمار تنظيم داعش الإرهابي للمسارين الإعلامي والإلكتروني؟

فرضية البحث

تنطلق فرضية البحث من إدراك أن التهديدات الإلكترونية أصبحت أحد أسهل السبل التي تستخدمها الجماعات الإرهابية للتأثير في قوة الخصم، ومن دون تكاليف كبيرة إذ بإمكانها إلحاق أضرار بمصالح الأفراد والمؤسسات والدول عن طريق اختراق المواقع الإلكترونية الحيوية.

منهج البحث

اعتمد البحث على المنهج التاريخي والمنهج الوصفي التحليلي، بغية استنباط الحقائق وتتبع التطورات في مسار التقدم الإلكتروني الذي استخدم من قبل الجماعات الإرهابية سواء لتنفيذ العمليات أو استقطاب الأعضاء الجدد أو جمع التبرعات المالية.

هيكلية البحث

اشتمل البحث على ملخص، ومقدمة، وخاتمة، كما تضمن مطلبين، إذ في المطلب الأول: **"ماهية التهديدات الإلكترونية وأنماطها"**. والمطلب الثاني: **"استثمار تنظيم داعش الإرهابي للمسارين الإعلامي والإلكتروني"**.

المطلب الأول
ماهية التهديدات الإلكترونية وأنماطها

إن المجتمع الدولي في القرن الحادي والعشرين يواجه تحديات أمنية تتسم بالتطور المستمر، أبرزها انتشاراً هي "التهديدات الإلكترونية" التي لا يقتصر ضررها على أمن فواعل محددة، وإنما يتسع ليؤثر على الأمن العالمي، إذ بات من الصعب حصر التهديدات الإلكترونية أو تنمية استراتيجيات محكمة لمواجهتها، فالتطورات التكنولوجية انعكست على تعدد أشكال التهديدات الإلكترونية ومصادرها. وبناء عليه، نقسم هذا المطلب على ثلاثة فقرات، هي: الفقرة الأولى، مفهوم التهديدات الإلكترونية الناشئة. والفقرة الثانية، أسباب التهديدات الإلكترونية. والفقرة الثالثة، أنماط التهديدات الإلكترونية.

الفقرة الأولى: مفهوم التهديدات الإلكترونية الناشئة

تعرف التهديدات الإلكترونية بأنها: استهداف المواقع الإلكترونية عن طريق الوسائل الإلكترونية الاتصالية، ويرى "مايكل شميت" **(Michael Schmitt)** بأنها: "مجموعة من الإجراءات التي تتخذها

الدولة للهجوم على نظم المعلومات المعادية بهدف التأثير والإضرار بها، وفي الوقت نفسه للدفاع عن نظم المعلومات الخاصة بالدولة المهاجِمة"[1]، كما عرفها "إليهو زيميت وتشارلز باري" **(Elihu Zimet and Charles L. Barry)** بأنها: "استهداف شبكة تواصل العدو العسكرية وعملياته الأمنية الإلكترونية"[2]، ويرى "ماركو روسيني" **(Marco Roscini)** بأنها: "تطويع الإمكانيات الإلكترونية العسكرية لأجل التأثير في مواقع الكترونية أخرى وتعطيلها أو تدميرها سواء أكانت تقدم خدمات مدنية أم عسكرية"[3]، ويعتقد "مايكل فويرتس" **(Micheal Fuertes)** بأنها: "هجوم عبر الإنترنت يقوم على التسلل إلى مواقع الكترونية غير مرخص بالدخول إليها، بهدف تعطيل أو إتلاف البيانات المتوفرة فيها أو الاستحواذ عليها، وهي عبارة عن سلسلة الهجمات الإلكترونية تقوم بها دولة ضد أخرى"[4].

وبناء عليه فأن التهديدات الإلكترونية هي هجمات آلية تتم عن طريق الشبكات الإلكترونية، مثل: الإنترنت وأجهزة الحاسب، وتهدف إلى الضرر بأجهزة، أو شبكات أخرى، أو سرقة المعلومات، فضلاً عن الهجمات الحركية غير المبرمجة التي يتم توجيهها للشبكات الإلكترونية الخاصة بالدول أو المنظمات عن طريق استخدام الأدوات العسكرية أو النبضات الكهرومغناطيسية التي تولد تيارات بإمكانها تعطيل خطوط وشبكات الكهرباء، أو أن تدمر مكونات رئيسية في أجهزة الحاسب الآلي[5].

إن نشأت التهديدات الإلكترونية يرتبط بحدثين في القرن العشرين، هما: الأول، تطوير أجهزة الكمبيوتر في منتصف الخمسينيات، بهدف معالجة وحفظ المعلومات رقمياً، إذ أصبحت أجهزة الكمبيوتر أساساً في عمل المؤسسات والأفراد، والثاني، ظهور شبكة المعلومات الدولية "الإنترنت" في بداية الثمانينيات الأمر الذي أحدث ثورة في حياة البشرية عن طريق التواصل ونقل المعلومات بسرعة فائقة عبر الأثير، لهذا يصف الفقهاء نشوء الثورة المعلوماتية بمثابة الجيل الثالث للثورات التقنية المتمثلة بالثورة الزراعية، الثورة الصناعية، والثورة المعلوماتية[6].

إن الجريمة الإلكترونية نشأت على هيئة هجمات طالت المؤسسات المالية والمصرفية، والشركات المتخصصة ببرمجة نظم الاتصالات، وفي الوقت نفسه اتخذت الدول من أجهزة الحاسب الآلي أداة لتطوير الجانب الأمني والعسكري، إذ ارتبطت الهجمات بحدثين مهمين، هما: الأول، الهجوم الإلكتروني الذي نفذته الولايات المتحدة عام ١٩٨٢، ضد منظومة التحكم العالية صناعياً في أنبوب نفط تابع للاتحاد السوفياتي، والثاني، اتهام روسيا الاتحادية بالهجوم الإلكتروني على الأنظمة الاتصالية التابعة لوزارة الدفاع الأمريكية ووكالة الطاقة الأمريكية ووكالة الفضاء الأمريكية خلال الأعوام 1998 – 2000، والذي أدى إلى السيطرة على الآلاف من الملفات المصنفة بأنها عالية السرية[7].

---

(1) Michael N. Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, Columbia Journal of Transnational Law, Institute for Information Technology Applications, Arlington, Vol. 37, 1998, P. 7.

(2) Elihu Zimet and Charles L. Barry, Military services Overview, Cyber power and National Security, National Defense University Press, Washington, DC, 2009, P. 291.

(3) Marco Roscini, World Wide Warfare – Jus ad bellum and the use of Cyber Force, Max Planck Yearbook of United Nations Law, Vol. 14, Brill NV, Leiden, 2010, P. 91.

(4) Micheal S. Fuertes, Cyber warfare, Unjust Actins in a just War, Florida International University, Florida, 2013, P. 1, 2.

(5) Mike McConnell, "Cyber Insecurities: The 21st Century Threat scape", In Kristin M. Lord and Travis Sharp (eds), Americas Cyber Future Security and Prosperity in the information Age, Vol. 2, Centre for new American Security, Washington, DC, 2011, P. 32, 33.

(6) Christopher c. joyner and Catherine Lotrionte, Information Warfare as International Coercion: Elements of a Legal Framework, European Journal for International Law, Vol. 12, London, 2001, P. 825, 826.

(7) Diego Rafael Canabarro and Thiago Borne, Reflection on the fog of Cyber War, National Center for Digital Government, Policy working Paper, Federal University of Rio Grande do Sul, Brasilia, 2013, P. 10.

ويعد الهجوم الإلكتروني على المواقع النووية الإيرانية هو الأخطر، إذ تعرضت إلى هجوم عبر الإنترنت حيث اخترقت المنشأة النووية الإيرانية في موقع "نطنز" عن طريق الدودة الحاسوبية الخبيثة "ستوكسنت" **(Stuxnet)** في حزيران/يونيو 2010، وقام هذا الهجوم على شقين، هما: الأول، استهداف أجهزة الطرد المركزية وخروجها عن السيطرة، والثاني، الإيحاء إلى أجهزة التحكم بأن عمليات تشغيل المنشأة النووية تعمل بصورة طبيعية، لكنها في الواقع معطلة[1].

يتبين مما سبق أن الهجمات الإلكترونية تمتلك قدرة فعالة على تدمير الأهداف المدنية والعسكرية لا تقل خطورة عن الأسلحة التقليدية أو غير التقليدية من حيث حجم الدمار والآثار، إذ يمكن أن تستهدف منشآت توليد الطاقة والمحطات والوحدات الصناعة.

الفقرة الثانية: أسباب التهديدات الإلكترونية

أولاً: "الأسباب السياسية"، إذ إن أغلب الصراعات الدولية تتبلور نتيجة السعي إلى تحقيق المصالح السياسية، الأمر الذي يدفع الدول إلى إيجاد وسائل معينة لتحقيق أهدافها، لذلك فأن الهجوم الإلكتروني يهدف إلى عزلة الدولة خارجياً، وعلى سبيل المثال: فأن الحرب الروسية – الجورجية عام 2008، اعتمدت على الهجمات الإلكترونية التي قام بها القوميين الروس في جورجيا لاختراق المواقع الإلكترونية الحكومية السياسية والمالية، مثل: موقع رئيس الجمهورية، وزارة الخارجية، البنك القومي الجورجي، بهدف التشهير بالحكومة الجورجية، فضلاً عن الهجمات الإلكترونية لحرمان المواطنين في جورجيا من خدمة المواقع الحكومية، فقد طالت الهجمات الإلكترونية مواقع الأخبار ووسائل الإعلام[2].

ثانياً: "الأسباب الأمنية"، إن الدول تتخذ الوسائل الاستباقية وسيلة للحفاظ على أمنها القومي، وأن أي تحرك من الدولة يخرج عن النطاق المقبول يواجه من الدولة الأخرى التي يهدد أمنها مواجهة تتناسب ودرجة التهديد، مما يدفع الدول الساعية لتحقيق الأمن إلى اللجوء إلى الهجمات الإلكترونية ضد الخصم، فقد قامت الولايات المتحدة وإسرائيل بالهجوم الإلكتروني الاستباقي لتعطيل المفاعل النووي الإيراني عن طريق الدودة الحاسوبية الخبيثة عام 2010، وهي من أبرز البرامج الخبيثة تعقيداً فهي مصممة لاختراق الأجهزة والحواسيب عن طريق التفتيش عن علامة فارقة لتدمر نظم التحكم في إدارة المصانع، والشبكات الكهربائية، ومحطات الطاقة، والمحطات النووية[3].

ثالثاً: "الأسباب الإقتصادية"، إن المصالح الإقتصادية العالمية ارتبطت بالجانب التكنولوجي والمعلوماتي، حيث التحول إلى الاقتصاديات الرقمية المستندة على عنصر المعرفة والمعلوماتية، والقائمة على العمل التقني وشبكات الإنترنيت، ووسائل التواصل الرقمي، مثل: البورصات، صكوك الاكتتاب الإلكترونية، والتجارة الدولية، الأمر الذي جعل الاقتصاد الدولي عرضة للهجمات الإلكترونية، فعلى سبيل المثال: تعرضت شركة النفط السعودية "ارامكوا" **(aramco)** إلى هجوم إلكتروني عن طريق فيروس "شمعون" **(Shamoon)** عام 2012، وتمكن الفيروس من تعطيل الشبكة الإلكترونية للشركة ومسح البيانات عشوائياً، وأثر على عمليات الإنتاج والعمليات التجارية للشركة[4].

رابعاً: "الأسباب الشخصية"، إن بعض الجرائم الإلكترونية التي يرتكبها الشباب تكون بسبب التحدي، وحب الظهور في الإعلام، فقد وفرت التقنيات الحديثة فرصاً غير مسبوقة لتحقيق المنفعة السريعة، إذ أن سرقة المعلومات الشخصية من الأهداف السهلة المنال والتي يمكن استخدامها ضد الشخص، كما أن

---

(1) عادل عبد الصادق، الفضاء الإلكتروني والعلاقات الدولية: دراسة في النظرية والتطبيق، ط2، المركز العربي لأبحاث الفضاء الإلكتروني، القاهرة، 2016، ص269.

(2) أنمار موسى جواد، الحرب في السياسة الخارجية الأمريكية بعد الحرب الباردة، الأكاديميون للنشر والتوزيع، عمان، 2021، ص257.

(3) Bruce Middleton, History of Cyber Security Attacks 1980 to Present, Taylor & Francis Group, LLC, England, 2017, P. 9.

(4) Christopher Bronk and Eneken Tikk – Ringas, Hack or Attack? Shamoon and the Evoluation of Cyber Conflict, The James A. Baker III Institute for Public Policy, Rice University, Houston, 2013, P. 3.

تكنولوجيا المعلومات الحديثة يسرت نمو الجريمة الإلكترونية عن طريق الإنترنت، وفي ظل السلوك الطائش يتأكد احتمال انخراط الأفراد في الفعل الإجرامي لتغيير الفعاليات الروتينية[1].

الفقرة الثالثة: أنماط التهديدات الإلكترونية

أولاً: "الجريمة الإلكترونية"، هي الجريمة التي يستخدم فيها الآليات الإلكترونية للقيام بالهجوم الإلكتروني بغية تحقيق المكاسب المالية، إذ وفرت التطورات التكنولوجية آليات تمكن الأفراد من القيام بالجرائم بتكلفة ومخاطر أقل، وأصبحت الجرائم التقليدية تتم في صورة إلكترونية، لا سيما مع زيادة مستخدمي الإنترنت، وتأخذ الجرائم الإلكترونية أشكال متعددة، أبرزها: "سرقة الهوية" حيث يتم سرقة المعلومات الشخصية للقيام بأعمال الاحتيال أو غير قانونية لتحقيق المكاسب، مثل: الاسم، العنوان، مكان الميلاد، رقم الهاتف، رقم بطاقة الهوية، أرقام بطاقات الائتمان. بالإضافة إلى جرائم "الاحتيال عبر الإنترنت" حيث يتم استخدام المواقع الإلكترونية والبريد الإلكتروني للقيام بعمليات احتيالية لتحقيق المكاسب أو الابتزاز السياسي، أو بيع سلح وهمية، أو توجيه المستخدم إلى موقع خاطئ لغرض التحايل. فضلاً عن جرائم "هجمات الاختراق" إذ يتم الدخول غير المشروع إلى الأنظمة الآلية، وتخطي نظام التأمين، ومن ثم السيطرة الكاملة على الحاسب الآلي، وتغيير البيانات أو تبديلها، أو زرع برامج خبيثة في الجهاز[2].

ثانياً: "الإرهاب الإلكتروني"، إن الاتفاقية الدولية الأولى لمكافحة الإجرام عبر الإنترنت عام 2001، عرفت الإرهاب الإلكتروني بأنه: "هجمات غير مشروعة، أو تهديدات بهجمات ضد الحاسبات، أو الشبكات، أو المعلومات المخزنة إلكترونياً، توجه من أجل الانتقام، أو ابتزاز، أو إجبار، أو التأثير في الحكومات، أو الشعوب، أو المجتمع الدولي بأسره لتحقيق أهداف سياسية، أو دينية، أو اجتماعية معينة"، كما عرفته منظمة الأمم المتحدة عام 2012، بأنه: "استخدام الإنترنت لنشر أعمال إرهابية"[3].

إن الإرهاب الإلكتروني يؤدي إلى أضرار بالأفراد والممتلكات، ويخلق حالة من الذعر لدى الهدف المقصود، ويمكن اعتبار الهجمات غير المهمة خارج إطار مفهوم الإرهاب الإلكتروني، إذ ينبغي أن يكون الهدف حيوياً وهاماً بالنسبة إلى حياة المواطنين ووظائف الدولة، وأن تكون الهجمات مدبرة ومخططه مسبقاً، وتهدف إلى تدمير الهدف أو الحاقه بدرجة عالية من الضرر، وليس فقط إحداث خلل في عمله[4].

وهناك أسباب دفعت الجماعات الإرهابية إلى استخدام الإرهاب الإلكترونية، هي[5]:

1- تدن تكلفة الأدوات الإلكترونية مقارنة بالتقليدية لإحداث الضرر، مثل: الأسلحة المتطورة.
2- سهولة استخدام الأدوات الإلكترونية من قبل الجماعات الإرهابية لمهاجمة الأهداف المتعددة التابعة للأفراد أو الحكومات.
3- يصعب على أجهزة الدولة التعرف على هوية القائمين بالإرهاب الإلكتروني وملاحقتهم، بسبب الحواجز المكانية بين الدول.
4- إن الإرهاب الإلكتروني يتم عن بعد إذ لا يحتاج إلى تواجد المهاجم والهدف في نفس المكان، الأمر الذي يسهل جذب أعضاء جدد للمنظمات الإرهابية دون الحاجة إلى تدريبات بدنية أو نفسية.
5- تأخذ هجمات الإرهاب الإلكتروني الاهتمام الإعلامي على نحو يساعدها على تحقيق أهدافها.

---

(1) إيهاب خليفة، القوة الإلكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت؟ "الولايات المتحدة نموذجاً"، العربي للنشر والتوزيع، القاهرة، 2017، ص18.

(2) هاني خميس أحمد، الإرهاب الإلكتروني، المركز الدولي للدراسات المستقبلية والإستراتيجية، القاهرة، 2007، ص48.

(3) خالد مرزوق سراج العتيبي، الجوانب الإجرائية في الشروع في الجرائم المعلوماتية: دراسة مقارنة، مكتبة القانون والاقتصاد، الرياض، 2014، ص33.

(4) نوران شفيق، أثر التهديدات الإلكترونية على العلاقات الدولية: دراسة في أبعاد الأمن الإلكتروني، المكتب العربي للمعارف، القاهرة، 2016، ص195.

(5) Gabriel Weimann, Cyber Terrorism: How Real is the Threat?, United states Institute of Peace, Washington, DC, 2004, P. 2 – 6.

6- يسر الاتصال بين أفراد التنظيم الإرهابي الواحد دونما حاجة إلى الاجتماع، بالإضافة إلى سهولة التخفي، بسبب تنوع أساليب عمل الجماعات في إنشاء الحسابات والمواقع الوهمية وتجديدها[1].

7- يتميز الإرهاب الإلكتروني بالطبيعة العابرة للحدود من حيث الإعداد والتنفيذ، إذ يتم التخطيط للجريمة الإرهابية في دولة، ويتم جمع التمويل اللازم لتنفيذها في دولة أخرى، ويتم التنفيذ في دولة ثالثة[2].

8- صعوبة إثبات الإرهاب الإلكتروني بسبب سرعة غياب الدليل، إذ أن المعلومات في شبكة الإنترنت تكون في شكل رموز مخزنة على وسائط تخزين، وأن الجاني لا يترك وراءه أثر مادى خارجي.

يتضح مما سبق أن الإرهاب الإلكتروني يؤثر على الأفراد والدول، ويهدف إلى زعزعة الاستقرار والابتزاز، والتدمير لكل للمراكز الحيوي من خطوط الطاقة والاتصالات والمعلومات الرقمية.

ثالثاً: "الحرب الإلكترونية"، تستخدم مسبقاً لرصد حالات التشويش على أنظمة الاتصال، والرادار، وأجهزة الإنذار، ومع استخدام شبكات الاتصال والمعلومات في المجال الحربي وتعدد الأعمال العدائية الإلكترونية حمل مفهوم الحرب الإلكترونية مصطلح "الحرب السيبرانية" للتعبير عن التوجه الجديد في استخدام الإلكترونيات في الحروب، إذ أن المفهوم التقليدي للحرب يتضمن استخدام الجيوش في ميدان قتال محدد، بينما الهجمات الإلكترونية غير محددة المجال، ومبهمة الأهداف، كونها تتحرك عبر شبكات المعلومات والاتصالات العابرة للحدود الدولية، بالإضافة إلى ارتكازها على أدوات إلكترونية تلائم مع طبيعة المسار التكنولوجي في عصر الثورة المعلوماتية التي يتم توجيهها ضد المنشآت الحيوية للخصم[3].

وتوجد مستويات ثلاثة تفسر الحرب الإلكترونية، هي[4]:

1- الهجوم الإلكتروني المرافقة للحرب التقليدية بغية تحقيق التفوق المعرفي، مثل: الهجوم على نظام الدفاع الجوي، والذي يؤدي إلى إحداث خسائر استراتيجية واسعة النطاق.

2- الهجوم الإلكتروني المحدود ضد البنى التحتية والأهداف المدنية.

3- الهجوم الإلكترونية غير المحدودة لتعظيم الآثار التدميرية للبنى التحتية الاجتماعي للدولة، مثل: مهاجمة أسواق رأس المال، وخدمات الطوارئ.

رابعاً: "التجسس الإلكتروني"، القيام باختراق شبكة أو جهاز إلكتروني لسرقة المعلومات المتوفرة فيه، والتي تكون على درجة عالية من الأهمية سواء أكانت معلومات مدنية أم عسكرية، لإحداث آثار استراتيجية فادحة في الطرف المستهدف، إذ غيرت التطورات التكنولوجية من طبيعة عمليات التجسس، إذ توفر الآليات الإلكترونية فرص أقل تكلفة وأقل خطورة للفواعل من الدول وغيرها للقيام بالتجسس[5].

إن عمليات التجسس تستطيع إحداث خسائر كبيرة في وقت محدود، أصبح العديدٌ من الدول تلجأ إليها الدول في خلال أوقات النزاعات والتوترات السياسية، أو في وقت الحروب بالتزامن مع العمليات العسكرية التقليدية، ومن أبرز أمثلة التجسس الإلكتروني الذي جاء في تقرير لجنة التحقيقات التي شكلها البرلمان الأوروبي عام 2001، والذي اتهم الولايات المتحدة باستخدام شبكة تجسس إلكترونية باسم "شبكة أيشلون" **(Echelon network)** خلال الحرب الباردة للتجسس وسرقة المعلومات الصناعية الأوروبية، بالإضافة إلى اتهام الصين بالتجسس ضد وزارتي الدفاعي في المملكة المتحدة البريطانية

---

(1) خالد حنفي علي، الإنترنت وتصدير الإرهاب، مجلة السياسة الدولية، مؤسسة الأهرام، القاهرة، السنة الحادية والأربعون، المجلد 40، العدد 162، تشرين الأول/أكتوبر، 2005، ص137.

(2) موسى مسعود أرحومة، الإرهاب والإنترنت، مجلة دراسات وأبحاث، جامعة زيان عاشور الجلفة، الجزائر، العدد 4، كانون الأول/ديسمبر، 2011، ص168.

(3) عادل عبد الصادق، الإرهاب الإلكتروني: القوة في العلاقات الدولية.. نمط جديد وتحديات مختلفة، مركز الدراسات السياسية والإستراتيجية بالأهرام، القاهرة، 2009، ص155.

(4) Kenneth Geers, Strategic Cyber Security, NATO Cooperative Cyber Defense Centre of Excellence, Tallinn, Estonia, 2011, P. 26.

(5) Clay Wilson, "Cyber Crime", In Franklin D Kramer et al (eds), Cyber power and National Security, Potomac Books Inc, Nebraska, 2009, P. 418.

والولايات المتحدة الأمريكية في عملية باسم "هجمات تيتان المطر" **(Titan Rain attacks)** عام 2002[1].

إن عمليات التجسس لا تطال الدول أو أن تركز الهجمات على المؤسسات الحكومية فحسب، وإنما تطال الشركات سواء أكانت التجارية أم الإعلانية والمنظمات غير الحكومية، ولا يقتصر هدف التجسس الإلكتروني على التخريب فحسب، وإنما يهدف إلى مراقبة الخصم وتحركاته، واقتناص الفرص.

المطلب الثاني

استثمار تنظيم داعش الإرهابي للمسارين الإعلامي والإلكتروني

إن الإرهاب بطبيعته يعول على الجانب الدعائي والإلكتروني في توصيل أفكاره، وترسيخ صورة نمطية عن الأهداف التي يسعى إلى تحقيقها، فضلاً عن استقطاب المزيد من الداعمين له، وتأسيساً على هذه الرؤية فقد سعى تنظيم الدولة الإسلامية في العراق والشام "داعش" الإرهابي بعد السيطرة على مناطقة شاسعة من المحافظات العراقية نينوى، صلاح الدين، الأنبار، وديالى في حزيران/يونيو 2014، إلى استخدام حركة الإرهاب الإلكتروني لإثبات الخلافة الافتراضية القائمة على تجنيد الأشخاص المحبطين. وبناء عليه، سوف نقسم هذا المطلب على فقرتين، هما: الفقرة الأولى، الإستراتيجية الإعلامية للتنظيم. والفقرة الثانية، استغلال التنظيم للإرهاب الإلكتروني.

الفقرة الأولى: الإستراتيجية الإعلامية للتنظيم

إن تطور تقنيات الاتصال أدت إلى ظهور الشبكات اللا سلكي، وتطور تقنيات الإعلام الآلي التي أنبعث عنها الإنترنت، حيث أصبح من السهل اختراق السيادة الوطنية، إذ أن عنصران المكان والزمان لا يؤثران على أنشطة تبادل المعلومات في بيئة الإنترنت، حيث تنقل المعلومات على شكل حزم توجه إلى عنوان افتراضي ينتقل عشوائياً لا صلة له بالمكان والزمان، وأصبح الإنترنيت عابر للأوطان وغير مركزي ومفتوح بالمطلق، ولن يستطيع الفاعلون التقليديون ضبطه والتحكم به، لذلك أصبح من السهل اجتذاب الشباب إلى التطرف من خلال نشر الأفكار المتشددة والفتاوى التكفيرية[2].

إن تطور وسائل الاتصال أدى إلى توزيع القوة بين عدد من الفاعلين من غير الدول، وأعطتهم القدرة على ممارسة القوة الصلبة والناعمة عبر الفضاء الإلكتروني، مما جعل قدرة الدولة على السيطرة موضع شك، وأن أبرز ما يعزز انتشار الأنشطة غير السلمية في الفضاء الالكتروني، هي: استخدام الفاعلين من غير الدول الفضاء الإلكتروني لتحقيق أهدافهم المؤثرة على السيادة، وتزايد ارتباط العالم بالفضاء الإلكتروني مع تنامي خطر التعرض للهجمات الإلكترونية، فضلاً عن صعوبة تعامل الدول مع الشركات التكنولوجية متعددة الجنسيات[3]، لذلك أصبح الفضاء الإلكتروني ساحة للصراع الذي يعكس نزاعات الدول أو الفاعلين على خلفيات دينية، أو أثنية، أو أيديولوجية، أو سياسية، أو اقتصادية.

وتعد وسائل الإعلام والتواصل الاجتماعي، مثل: "شبكات التواصل الاجتماعي، اليوتيوب، كوكل" وسائل هامة للتنظيمات الإرهابية، خاصة تنظيم "داعش" الإرهابي، إذ تتيح هذه الوسائل إمكانية التخطيط، والقيادة، والسيطرة، والاتصال بين جماعات منتشرة في مناطق مختلفة، والحصول على الدعم المادي والبشري، فضلاً عن أضفاء الغطاء الأخلاقي على عملياتها، بالإضافة إلى خلق حالة من الفوضى والذعر

---

(1) Paul Cornish, Cyberspace and the National Security of the United Kingdom: Threats and Responses, A Chatham House Report, Royal Institute of International Affairs, London, 2009, P. 8.

(2) حاج بشير جيدور، أثر الثورة الرقمية والاستخدام المكثف لشبكات التواصل الاجتماعي في رسم الصورة الجديدة لمفهوم المواطنة: من المواطن العادي إلى المواطن الرقمي، مجلة دفاتر السياسة والقانون، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، الجزائر، العدد 15، حزيران/يونيو، 2016، ص416.

(3) عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، الإسكندرية، 2016، ص17، 18.

عن طريق نشر فيديوهات توثق العمليات المرعبة التي يقوم بها تنظيم "داعش" الإرهابي، والتي تتضمن فيديوهات خاصة بعمليات القتل والتفجير والتعذيب[1].

واستخدم تنظيم "داعش" الإرهابي فكرة التمدد الجغرافي كونه رفض الاعتراف بالحدود الدولية عن طريق نشر عناصره وأعماله الإرهابية في دول عدة، وأزداد التنظيم خطورة حينما استخدم وسائل التواصل الاجتماعي لبث دعايته لأغراض التجنيد، وإذ شمل التجنيد الشباب الساعين إلى القتال والنساء، وبعض الأطباء والمهندسين واختصاصي تكنولوجيا المعلومات والاتصالات الذين التحقوا بالتنظيم من أغلب دول العالم من المقاتلين المتطرفين لإقامة خلافة "دائمة ومتوسعة"، وقد أشار وزير الداخلية الإسباني "خورخي فرناندیز دیاز" **(Jorge Fernandez Diaz)** قائلاً: "إن80 بالمئة من عمليات التجنيد تتم عبر شبكات التواصل الاجتماعي، بينما 20 بالمئة فقط تتم داخل السجون والمساجد، فيما كانت هذه النسبة معكوسة في عام 2012"، الأمر الذي يعكس الدور الذي لعبته الوسائل الإلكترونية في عمليات التجنيد[2].

وكان لتنظيم "داعش" الإرهابي هدفان من وسائل التواصل الاجتماعي، هما: الأول، "التنسيق بين الأعضاء" حيث تستخدم وسائل التواصل للتنسيق أثناء العمليات الإرهابية عن طريق مجتمعات افتراضية متغيرة بصورة تلقائية، والثاني، "تجنيد الأتباع الجدد" حيث تستخدم وسائل التواصل في تجنيد المتطرفين، واجتذاب المتوافقين فكرياً مع التنظيم، ومن أجل تحقيق البقاء والتمدد اعتمد تنظيم "داعش" على استراتيجية مزدوجة، هي: التوسع الجغرافي العسكري في الأراضي التي تحيط بالمناطق التي يسيطر عليها في العراق وسورية، بالإضافة إلى التوسع العالمي عبر اجتذاب المزيد من الأعضاء عن طريق وسائل التواصل[3].

وعلى الرغم من خسائر تنظيم "داعش" وانهيار بشكل كامل في العراق عام 2017، لكنه لا يزال يشكل تهديداً على الأمن العالمي، إذ يمتلك القدرة على بلورة تنظيمات إرهابية، وتشكيل خلايا عابرة للحدود عن طريق وسائل التواصل الاجتماعي، لا سيما أن التهديدات الإرهابية الإلكترونية غير مقيدة برقعة جغرافية، وأن واقع البيئة المعلوماتية التي تقع فيها التهديدات لا تعترف بالحدود الجغرافية، إذ لا توجد حدود تعرقل عمليات نقل المعلومات عبر الدول في ضوء شبكة الاتصالات، والتي تربط أعداد هائلة من أجهزة الحاسب الآلي عبر الدول، حيث أصبح التنقل والاتصال فيما بينها يسيراً، وهذه الميزة جعلت بالإمكان القيام بالتهديدات الإلكترونية دون الحاجة إلى التواجد الشخصي في موقع الحدث[4].

يتضح مما سبق أن التطورات التكنولوجية أفرزت تحولاً في مفهوم القوة حيث أدت الأدوات الإلكترونية دوراً في تعظيم القوة والاستحواذ على عناصرها، وأصبح التفوق في المجال الإلكتروني عنصراً في تنفيذ العمليات الإرهابية ذات الفاعلية، حيث دخل المجال الإلكتروني ضمن محددات القوة وأنماط استخدامها، مما أعطى فرصة للجماعات الإرهابية في توظيف التكنولوجيا في العمليات الإرهابية.

الفقرة الثانية: استغلال التنظيم للإرهاب الإلكتروني

يعد عنصر التخويف والترهيب من العناصر الأساسية للتنظيمات الإرهابية، إذ يتم توجه الهجمات الإرهابية إلى الخصوم المفترضين عن طريق الوسائل الإلكترونية، لا سيما أجهزة الدول المستهدفة ومواطنيها، بهدف إضعاف مواقف تلك الكيانات والتأثير على هيبتها، إذ تستهدف الهجمات الرأي العام في تلك الدول بغية بث الرعب والضغط على الجمهور عن طريق تقديم صورة مخيفة ومعلومات مغلوطة، بهدف إشاعة أسلوب الترهيب الذي يهدف إلى زرع الخوف. ويسعى ممارسو الإرهاب الإلكتروني إلى

---

(1) Daniel Byman and Jeremy Shapiro, be Afraid. Be A Little Afraid: The Threat Of Terrorism From Western Foreign Fighters In Syria And Iraq, Brookings, Washington, DC, November 2014, P. 5.

(2) Group of authors, Global Terrorism Index 2015: Measuring and Understanding the Impact of Terrorism, The Institute for Economics and Peace, Sydney, 2016, P. 76, 77.

(3) حارث حسن، السياسة الأمريكية تجاه تنظيم داعش، مجلة سياسات عربية، المركز العربي للأبحاث ودراسة السياسات، الدوحة، العدد 16، 2015، ص45.

(4) تشارلز ليستر، التنافس الجهادي: الدولة الإسلامية تتحدى تنظيم القاعدة، مركز بروكنجز، الدوحة، 2016، ص4.

الترويج لأفكارهم المتشددة، وكسب متعاطفين وأتباع جدد للانضمام لصفوف المقاتلين عن طريق خلق كتلة من الجمهور ينصهر معهم في اتجاهاتهم، وتنميط وعي الأفراد ليتوافق مع النظام الخاص بهم، إذ تمكن تنظيم "داعش" الإرهابي من تحويل مواقع التواصل الاجتماعي إلى عنوان لهويته ووسيلة للاختراق الأيديولوجي، بالإضافة إلى اختراق المؤسسات السيادية إلى اختراق المنظومة الثقافية للأفراد، وأن أبرز الوسائل الاتصالية لدعم أهداف التنظيم، هي: مركز الفجر للإعلام، مؤسسة الفرقان الإعلامية[1].

وتتم عملية تجنيد أتباع جدد عبر الفضاء الافتراضي من خلال ثلاثة مراحل، هي: الأولى، "التأثير الوجداني" إذ يستهدف الشخص عن طريق إثارة العاطفة والنعرة الدينية بذريعة الدفاع عن القيم المقدسة. والثانية، "توظيف وسائل الإعلام" حيث يتم نقل المعلومات التي تعبر عن رؤية الجماعات القائمة بالاستقطاب، والثالثة، "التحول الفكري" إذ يتم تحويل الفكر إلى سلوك عن طريق تغيير سلوك الشخص المستهدف لتحويله من متعاطف إلى فاعل عبر إقناعه بالمشاركة في القتال، أو القيام بعمليات انتحارية، وتركز غالبية الجماعات الإرهابية على مجموعتين من الأشخاص المستهدفين، هما: الشباب والنساء[2].

ويستغل الإرهابيين الفضاء الشبكي للحصول على التمويلات المالي اللازمة لدعم نشاطاتهم، عن طريق جمع الأموال عبر دعوة الأنصار والمتعاطفين مع أفكارهم لمساندتهم مادياً، إذ توظف الجماعات المتطرفة الفتاوى التي تبيح التضحية بالأموال، فضلاً عن التبرعات التي تقدم إلى الجمعيات الخيرية والتي تقوم بأنشطة مالية غير مشروعة لتمويل الأنشطة الإرهابية، كما يستخدم الإرهاب الإلكتروني المنصات الشبكية لتسهيل تبادل التحويلات المالية في ضوء سهولة استخدام تلك المواقع لتحويل الأموال والعملات المشفرة مع عدم إمكانية التحقق من هوية متلقى تلك التحويلات المالية[3].

وتعد شبكة الإنترنت أداة للاتصال مهمة للمنظمات الإرهابية، إذ تتيح حرية التنسيق الدقيق لشن هجمات محددة، كما يعد التدريب الافتراضي والدعم الفني عبر الإنترنت من أبرز طرق التراكم المعرفي، إذ تسعى الجماعات الإرهابية عن طريقه إلى تقديم إرشادات لصنع القنابل والأسلحة الكيمياوية، وأساليب التفخيخ والتفجير، فقد نشر تنظيم "داعش" الإرهابي عام 2015، دليلاً بعنوان: "آليات البقاء على قيد الحياة في الغرب: دليل المجاهدين"، يهدف إلى تدريب الإرهابيين مع إخفاء هوياتهم، وتعلم أساليب البقاء على قيد الحياة، ونقل المتفجرات والهروب بعد الهجمات[4].

وتنامى دور المخططين الافتراضيين في تنسيق العمليات الإرهابية، عن طريق تقديم الإرشاد والدعم لمنفذي العمليات عن بعد، والتواصل مع عصابات الجريمة المنظمة لشراء الأسلحة، وتحديد المكان الذي تنفيذ العمليات فيه، والتواصل مع المنفذين لتسلم السلاح. ويستخدم الإرهابيون مواقع التواصل الاجتماعي للتجسس وتحديد الأشخاص المستهدفين ومراقبة تحركاتهم، بهدف القيام بعمليات الاغتيالات التي تطال بعض رموز الأجهزة الأمنية أو السياسية في الدول المستهدفة. كذلك يسعى الإرهابيون عن طريق الهجمات الإلكترونية إلى تحقيق الأضرار المباشرة عبر استهداف البنى التحتية للدول المستهدفة التي تعتمد على أجهزة الحاسب الرقمي، بهدف تعطيلها أو إيقافها عن العمل[5].

يتبين مما سبق أن الجماعات الإرهابية تستخدم الإرهاب الإلكترونية وسيلة لتحقيق دمار مادى بهدف إثارة الخوف، وإفساد وظائف النظم المعلوماتية والأخلاقية والقيمية في المجتمعات، وتدمير الأصول المادية والافتراضية من خلال التلاعب بالمعلومات الذي يؤدى إلى تقديم معلومات خاطئة، وإثارة الارتباك وعدم

---

(1) عمرو فاروق، داعش سفراء جهنم: الحياة في أحضان الدم، كنوز للنشر والتوزيع، القاهرة، 2015، ص123.

(2) عادل عبد الصادق، ٣ مراحل يستخدمها الإرهابيون لتجنيد الشباب، على الموقع الإلكتروني:
https://www.hafryat.comhttps://www.hafryat.com/ar/blog/. Visited 22/8/2024.

(3) Idahosa Stephen Osaherumwen, International Terrorism: The Influence of Social Media in Perspective, Vol. 10, WWJMRD, 2017, P. 86 – 91.

(4) Ahmet S. Yayla, How to Counter ISIS Wolf – pack, Modern Diplomacy, August 25, 2017, at: https://www.researchgate.net/publication/319291346_How_to_Counter_ISIS_Wolf-packs.

(5) مروة نظير، جماعات التطرف العنيف ومنصات التواصل الاجتماعي: قراءة في الاستخدامات والعوامل، المجلة الإجتماعية القومية، المركز القومي للبحوث الإجتماعية والجنائية، القاهرة، المجلد 57، العدد 1، كانون الثاني/يناير، ٢٠٢٠، ص103، 104.

الثقة في الأنظمة الحيوية، وقد ينخرط لإحداث أضرار مادية ضخمة وتخريب اقتصادي في البنية التحتية الحيوية، مثل: شبكات الكهرباء، وأنظمة توزيع النفط والتخزين.

الخاتمة

إن مفهوم التهديدات الإلكترونية يشير إلى أساليب تعتمد على تكنولوجيا الاتصال والمعلومات، وتستهدف أجهزة الحواسب أو المواقع الإلكترونية، وتشمل التسلل إلى أنظمة الحاسب الآلي، وجمع بيانات أو تصديرها أو اتلافها أو تغييرها، وأن التحكم في مسار المعلومات والاتصالات يمكن أن يؤثر على أمن الدولة، وبات الفضاء الإلكتروني وتعقيداته التكنولوجية محوراً مهماً للجماعات الإرهابية في تطوير أدوات الانتشار والاستمرار والاستقطاب، فلم تعد مصادر القوة التقليدية متغير مهم في إحداث الفرق بين الخصوم، وإنما انتقل الأمر إلى الفعل التكنولوجي.

الاستنتاجات

1- أصبح الفضاء الإلكتروني مجالاً لانتشار الجماعات الإرهابية، لا سيما تنظيم "داعش" الإرهابي بعد أن تطورت مفاهيم القوة والصراع، إذ تتميز التهديدات الإلكترونية للجماعات الإرهابية بالغموض وشدة وتنوعها كما تتزايد في الاحترافية والخطورة.

2- إن التنظيمات الإرهابية تسعى إلى توظيف التقدم الحاصل في المجال التكنولوجي والمعلوماتي، إذ أصبحت التهديدات الإلكترونية وسيلة أساسية للتأثير في المجتمعات من دون تكاليف باهظة.

إن التهديدات الإلكترونية هي تهديدات عابرة للحدود تنتهك السيادة الوطنية، وأن مواجهتها تتطلب جهود مكثفة في تطوير الجوانب المعلوماتية في إدارة مؤسسات الدولة وايجاد تشريعات قانونية كفيلة بالقضاء على هذه التهديدات.

قائمة المصادر والمراجع

أولاً: الكتب العربية

1. أنمار موسى جواد، الحرب في السياسة الخارجية الأمريكية بعد الحرب الباردة، الأكاديميون للنشر والتوزيع، عمان، 2021.
2. إيهاب خليفة، القوة الإلكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت؟ "الولايات المتحدة نموذجاً"، العربي للنشر والتوزيع، القاهرة، 2017.
3. تشارلز ليستر، التنافس الجهادي: الدولة الإسلامية تتحدى تنظيم القاعدة، مركز بروكنجز، الدوحة، 2016.
4. خالد مرزوق سراج العتيبي، الجوانب الإجرائية في الشروع في الجرائم المعلوماتية: دراسة مقارنة، مكتبة القانون والاقتصاد، الرياض، 2014.
5. عادل عبد الصادق، ٣ مراحل يستخدمها الإرهابيون لتجنيد الشباب، على الموقع الإلكتروني: https://www.hafryat.comhttps://www.hafryat.com/ar/blog/. Visited 22/8/202.
6. عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، الإسكندرية، 2016.
7. عادل عبد الصادق، الإرهاب الإلكتروني: القوة في العلاقات الدولية.. نمط جديد وتحديات مختلفة، مركز الدراسات السياسية والإستراتيجية بالأهرام، القاهرة، 2009.
8. عادل عبد الصادق، الفضاء الإلكتروني والعلاقات الدولية: دراسة في النظرية والتطبيق، ط2، المركز العربي لأبحاث الفضاء الإلكتروني، القاهرة، 2016.
9. عمرو فاروق، داعش سفراء جهنم: الحياة في أحضان الدم، كنوز للنشر والتوزيع، القاهرة، 2015.
10. نوران شفيق، أثر التهديدات الإلكترونية على العلاقات الدولية: دراسة في أبعاد الأمن الإلكتروني، المكتب العربي للمعارف، القاهرة، 2016.

11. هاني خميس أحمد، الإرهاب الإلكتروني، المركز الدولي للدراسات المستقبلية والإستراتيجية، القاهرة، 2007.

ثانياً: الدوريات

12. حاج بشير جيدور، أثر الثورة الرقمية والاستخدام المكثف لشبكات التواصل الاجتماعي في رسم الصورة الجديدة لمفهوم المواطنة: من المواطن العادي إلى المواطن الرقمي، مجلة دفاتر السياسة والقانون، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، الجزائر، العدد 15، حزيران/يونيو، 2016.

13. حارث حسن، السياسة الأمريكية تجاه تنظيم داعش، مجلة سياسات عربية، المركز العربي للأبحاث ودراسة السياسات، الدوحة، العدد 16، 2015.

14. خالد حنفي علي، الإنترنت وتصدير الإرهاب، مجلة السياسة الدولية، مؤسسة الأهرام، القاهرة، السنة الحادية والأربعون، المجلد 40، العدد 162، تشرين الأول/أكتوبر، 2005.

15. موسى مسعود أرحومة، الإرهاب والإنترنت، مجلة دراسات وأبحاث، جامعة زيان عاشور الجلفة، الجزائر، العدد 4، كانون الأول/ديسمبر، 2011.

16. مروة نظير، جماعات التطرف العنيف ومنصات التواصل الاجتماعي: قراءة في الاستخدامات والعوامل، المجلة الإجتماعية القومية، المركز القومي للبحوث الإجتماعية والجنائية، القاهرة، المجلد 57، العدد 1، كانون الثاني/يناير، ٢٠٢٠.

ثالثاً: الكتب الأجنبية

17. Bruce Middleton, History of Cyber Security Attacks 1980 to Present, Taylor & Francis Group, LLC, England, 2017.

18. Christopher Bronk and Eneken Tikk – Ringas, Hack or Attack? Shamoon and the Evoluation of Cyber Conflict, The James A. Baker III Institute for Public Policy, Rice University, Houston, 2013.

19. Christopher c. joyner and Catherine Lotrionte, Information Warfare as International Coercion: Elements of a Legal Framework, European Journal for International Law, Vol. 12, London, 2001.

20. Clay Wilson, "Cyber Crime", In Franklin D Kramer et al (eds), Cyber power and National Security, Potomac Books Inc, Nebraska, 2009.

21. Daniel Byman and Jeremy Shapiro, be Afraid. Be A Little Afraid: The Threat Of Terrorism From Western Foreign Fighters In Syria And Iraq, Brookings, Washington, DC, November 2014.

22. Diego Rafael Canabarro and Thiago Borne, Reflection on the fog of Cyber War, National Center for Digital Government, Policy working Paper, Federal University of Rio Grande do Sul, Brasilia, 2013.

23. Elihu Zimet and Charles L. Barry, Military services Overview, Cyber power and National Security, National Defense University Press, Washington, DC, 2009.

24. Gabriel Weimann, Cyber Terrorism: How Real is the Threat?, United states Institute of Peace, Washington, DC, 2004.

25. Group of authors, Global Terrorism Index 2015: Measuring and Understanding the Impact of Terrorism, The Institute for Economics and Peace, Sydney, 2016.

26. Kenneth Geers, Strategic Cyber Security, NATO Cooperative Cyber Defense Centre of Excellence, Tallinn, Estonia, 2011.
27. Marco Roscini, World Wide Warfare – Jus ad bellum and the use of Cyber Force, Max Planck Yearbook of United Nations Law, Vol. 14, Brill NV, Leiden, 2010.
28. Michael N. Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, Columbia Journal of Transnational Law, Institute for Information Technology Applications, Arlington, Vol. 37, 1998.
29. Micheal S. Fuertes, Cyber warfare, Unjust Actins in a just War, Florida International University, Florida, 2013.
30. Mike McConnell, "Cyber Insecurities: The 21st Century Threat scape", In Kristin M. Lord and Travis Sharp (eds), Americas Cyber Future Security and Prosperity in the information Age, Vol. 2, Centre for new American Security, Washington, DC, 2011.
31. Paul Cornish, Cyberspace and the National Security of the United Kingdom: Threats and Responses, A Chatham House Report, Royal Institute of International Affairs, London, 2009.
32. Idahosa Stephen Osaherumwen, International Terrorism: The Influence of Social Media in Perspective, Vol. 10, WWJMRD, 2017.
33. Ahmet S. Yayla, How to Counter ISIS Wolf – pack, Modern Diplomacy, August 25, 2017, at: https://www.researchgate.net/publication/319291346_How_to_Counter_ISIS_Wolf-packs.