



الإرهاب الإلكتروني والأمن السيبراني: دراسة مفاهيمية وتحليلية للحركات السببية

Cyber terrorism and cyber security conceptual and analytical study of causal movements

د. فؤاد جدو

جامعة محمد خيضر بسكرة، (الجزائر)

البريد الإلكتروني: foued.djeddou@univ-biskra.dz

ملخص

يعتبر الإرهاب من بين التهديدات التي أصبحت جزء من التحولات الدولية والتي تخص التهديدات اللامثالية، وذلك في ظل تزايد درجات الانكشافية الإعلامية وإفرازات العولمة خاصة مع تزايد تدفقات الأنترنت وتحول الدول إلى ما يعرف بالحكومات الإلكترونية والإعتماد على التواصل الإلكتروني عبر فضاءات مواقع التواصل الاجتماعي، أين أصبح الإرهاب الإلكتروني أحد التهديدات التي تمس أمن الدول والمواطنين والتي أصبحت تتطلب استراتيجيات لمواجهةها في إطار ما يعرف بالأمن السيبراني. ولهذا أصبح ضبط هذه المفاهيم وتحديد الحركات السببية مهم من أجل ضبط آليات المواجهة والاستباقية لهذا الإرهاب الإلكتروني الذي أسهم فيه التطور التكنولوجي بشكل سريع، وهذا يتطلب تقاطع مستويات الأمن منها السيبراني والديني والثقافي والإعلامي من أجل الوصول إلى تحقيق فعالية في مواجهة الإرهاب الإلكتروني.

كلمات مفتاحية: الإرهاب الإلكتروني؛ الأمن السيبراني؛ الأمن الإعلامي؛ الانكشافية الإعلامية.

Abstract

Terrorism is one of the threats that has become part of the international transformations that constitutes asymmetric threats in view of the increasing media exposure and the disruptions of globalization, especially as Internet flows increase and countries turn into so-called electronic governments and the reliance on electronic communication through social media spaces, where cyberterrorism has become one of the most important threats to the security of states and citizens and

which require strategies to confront it within the framework of what is known as cybersecurity, and therefore determine these concepts and the identification of causal movements is important in order to control the mechanisms of confrontation and proactiveness of this cyberterrorism in which technological development has contributed rapidly, this requires intersecting levels of security, including cyber, religious, cultural and media-related, in order to achieve effectiveness in the face of cyberterrorism.

Keywords: Cyber terrorism; cyber security; media security; media exposure.

مقدمة

منذ نهاية الحرب الباردة أصبح مفهوم الإرهاب له دلالات أخرى تختلف عن المفاهيم التي كانت سائدة في تلك الفترة، أين هيمن البعد الأيديولوجي على مفهوم الإرهاب ببعده الكلاسيكي والتقليدي وارتباطه بالتهديدات التماثلية من حروب ومواجهات مسلحة ضمن أمن الدولة. ومع التطور التكنولوجي الذي يعرفه العالم تغيرت التهديدات الأمنية أين أصبح الأمن مرتبط بتهديدات أخرى والتي تعرف باللاماثلية مثل الإرهاب عابر للأوطان والهجرة غير الشرعية والإرهاب الإلكتروني، مما استلزم استراتيجيات جديدة ومتجددة لمواجهته وإن كانت إشكالية ضبط الاستراتيجية مرتبطة أساسا بفهم الخصائص والماهية من أجل وضع هذه الظواهر وفق مقاربة تفكيكية-تركيبية حتى تعطينا تصورا شاملا لمواجهته، وهذا ما سنتطرق إليه في هذا المقال من خلال معالجة إشكالية رئيسية وهي: ما محددات الإرهاب الإلكتروني في ظل سياق التهديدات الأمنية اللاماثلية؟

وتندرج تحت هذه الإشكالية مجموعة من التساؤلات التالية: ما هو مفهوم الإرهاب الإلكتروني؟ ما هي خصائص الإرهاب الإلكتروني؟ وما هي محددات العلاقة ما بين الأمن السيبراني والإرهاب الإلكتروني؟

كما يهدف هذا المقال إلى تحديد خصائص وماهية الإرهاب الدولي وفق التحولات الدولية الراهنة إلى جانب تحليل خصائص الإرهاب الإلكتروني ضمن سياق تحقيق الأمن السيبراني وتزايد درجات الانكشافية الإعلامية.

في مقالنا هذا استخدمنا المنهج الاستقرائي من أجل تحليل المفاهيم المرتبطة بالإرهاب الإلكتروني والمفاهيم المتقاطعة من أجل تفكيك وإعادة تركيب هذه المفردات. وقد اعتمدنا على الخطة التالية:

- مفهوم الإرهاب الإلكتروني؛
- خصائص ومحددات الإرهاب الإلكتروني؛
- محددات العلاقة ما بين الأمن السيبراني والإرهاب الإلكتروني.

I- مفهوم الإرهاب الإلكتروني

قبل التطرق لضبط وتحليل مفهوم الإرهاب الإلكتروني لابد من تعريف الإرهاب في عمومته، فهذا المصطلح عرف تحولات وتطورات منذ نهاية الحرب العالمية الثانية وإن كان موجوداً منذ وجود الإنسان لأنه مرتبط بالأمن الذي يعتبر أهم أسس الحياة.

يعتبر تحديد مفهوم الإرهاب أمراً معقداً، كونه يبين أبعاد وانعكاسات هذه الظاهرة، أين يعرف هذا المصطلح تمايزاً من حيث تحديد الإطار المفاهيمي من جهة ومن دولة إلى أخرى من جهة أخرى نتيجة لعدة عوامل أهمها:

1. مشكلة على مستوى التنظير تتصل بالمفاهيم والمصطلحات على النحو التالي: (أحمد، 2011، صفحة 36)

- عدم وجود إجماع بين الباحثين حول تحديد المصطلح وذلك يرجع إلى التنوع الثقافي المرتبط بتفسير الفعل الإرهابي؛
- تداخل مفهوم الإرهاب مع المفاهيم الأخرى ذات صلة بالمعنى؛
- إن مصطلح الإرهاب يثير لأول وهلة حكماً ينطوي على رفض الأعمال الإرهابية؛
- إن مصطلح الإرهاب مفهوم ديناميكي وليس ثابتاً وتباين أشكاله وأهدافه من دولة لأخرى؛
- غياب تأصيل نظري على مستوى النظرية العلمية تحدد هذا المصطلح.

2. مشكلة غياب الموضوعية والحياد القيمي في التحليل المرتبط بظاهرة الإرهاب بحيث لا توجد محددات علمية ونظرية حيادية لهذه الظاهرة.

3. مشكلة المناهج المستخدمة التي في أغلبها وصفية ولهذا لا توجد مناهج موجهة لدراسة هذه الظاهرة.

إذا أردنا تعريف الإرهاب لغة نجد في مختار الصحاح أن الإرهاب كلمة مشتقة أقرها مجمع اللغة العربية في الفعل "رهب" بمعنى أخاف، وكلمة إرهاب هي مصدر الفعل "أرهب" وأرهبه بمعنى خوفه، أما في المعجم الوسيط "مشتقة من معنى الرعب والفزع والخوف وإن كانت الرهبة في اللغة العربية لفظا يستخدم عادة عند التعبير عن الخوف المشوب بالاحترام لا خوف الفزع الناجم عن تهديد قوى مادية أو حيوانية أو طبيعية (أحمد، 2011، صفحة 40).

وحسب الباحث جروجري لوكوفيتز إن تعريف الإرهاب لم يلق إجماع حيث تم حصر في الثمانينات من القرن الماضي حوالي 109 تعريف للإرهاب حول تهديد الدولة باستخدام العنف كاختطاف الطائرات وقتل رجال الأمن، وفي التسعينات من القرن الماضي تم تحديد أكثر من 212 تعريف للإرهاب حيث أصبح يعرف بأنه استخدام العنف والترويع لتحقيق أغراض لجهة ما (Lewkowicz, 2006, p. 28).

أما تعريف الإرهاب حسب الاتفاقية العربية لمكافحة الإرهاب، فهي كل فعل من أفعال العنف والتهديد أيا كانت بواعثه أو أغراضه ويتبع تنفيذا لمشروع إجرامي فردي أو جماعي بهدف إلقاء الرعب بين الناس أو إلحاق الضرر بالبيئة أو بأحد المواقف أو الأملاك العامة أو الخاصة أو الاستيلاء عليها أو تعريض أحد الموارد الوطنية للخطر (الراوشدة، 2010، صفحة 38).

وبالعودة إلى تعريف الإرهاب الإلكتروني فقد ظهر هذا المصطلح بعد الطفرة الكبيرة في استخدام التكنولوجيا وانتشارها بشكل كبير مما دعا أكثر من 30 دولة حول العالم للتوقيع على "الاتفاقية الدولية الأولى لمكافحة الإجمام عبر الأنترنت" في بودابست عام 2001، والذي يعتبر وبحق من أخطر أنواع الجرائم والإرهاب والذي يؤدي إلى خسائر فادحة من كل النواحي الاقتصادية والعسكرية والبشرية (عبدالرحمان، 2016).

في حين تشير بعض الدراسات إلى أن أول استخدام لكلمة الإرهاب الإلكتروني في فترة الثمانينات في دراسة باري كولين Barry Collin التي خلص فيها إلى صعوبة تعريف ظاهرة الإرهاب التكنولوجي أو الإلكتروني بدقة، وأيضا الأساليب والحلول المطلوبة لمواجهة وتحديد دور الكمبيوتر والأنترنت في العمل الإرهابي. وقد عرّف مركز حماية البنية التحتية القومية الأمريكية الإرهاب الإلكتروني بأنه "عمل إجرامي يتم تحضيره عن طريق استخدام أجهزة الكمبيوتر وبرامجه والاتصالات السلكية واللاسلكية، ينتج عنه تدمير أو تعطيل الخدمات لبث الخوف، بهدف إرباك وزرع الشك لدى السكان أو لخدمة أجندة سياسية

أو اجتماعية أو أيديولوجية"، مثل ما حدث مع فيروس الحاسوب "I love you" عام 2000 الذي أدى إلى إتلاف معلومات قدرت بحوالي 10 مليار دولار. (رافعي، 2021، صفحة 73)

كما يعرف الإرهاب الإلكتروني بأنه أحد الاستخدامات غير السلمية للفضاء الإلكتروني، وهو نتيجة لتفاعل العالم المادي مع العالم الافتراضي، فحسب باري كولن الذي يشير إلى استخدام الفضاء الإلكتروني كأداة لإلحاق الضرر بالبنية التحتية سواء كانت "طاقة- مواصلات- خدمات حكومية"، أي يشير إلى الهجمات التي يستخدم فيها الكمبيوتر ضد الاقتصاد والحكومات.

إن أهداف الإرهاب الإلكتروني غالباً ما تكون سياسية، حيث قد يأتي في صورة تدمير نظم المعلومات لدى الخصم وافقاده القدرة على الحصول على المعلومات، شل قدرته على التواصل مع أعضائه عن طريق تدمير مواقعه الإلكترونية، اختراق شبكات المعلومات الرسمية للوزارات والحكومات بغرض تدميرها أو الحصول على معلومات سرية (عبدالرحمان، 2016).

وفي تعريف آخر للإرهاب الإلكتروني هو "إرهاب يستخدم الأنترنت وبإمكانه التسبب في إلحاق الضرر والشلل بأنظمة المعلومات والاتصالات المدنية والعسكرية وقطع الاتصال بين الشبكات المختلفة وتعطيل أنظمة الطيران والدفاع الجوي واختراق الأنظمة المصرفية وإرباك حركة المسافرين برا وجوا وشل محطات الطاقة الكهربائية ومهاجمة القواعد الاستراتيجية". وبأكثر دقة فإن الإرهاب الإلكتروني "استخدام التقنيات الرقمية لإخضاع الآخرين أو القيام بمهاجمة نظم المعلومات على خلفية سياسية أو عرقية أو دينية" (الشهري، 2015)

من خلال التعاريف السابقة نجد أن الإرهاب الإلكتروني يقوم على ثلاث عناصر أساسية وهي:

- الشبكة الافتراضية والتي تقوم على تسويق التهديد واستخدامها بشكل أساسي في عملية انشاء مواقع ذات محتوى تطرفي أو إحتيالي أو تخطيط ما هو صحيح؛
- المحتوى الذي غالبا ما يقوم على النصب والاحتيال أو استغلال المعلومات أو الضرر بجهة معينة؛
- الأفراد والمقصود بهم من يقومون بالعمل الإجرامي أو الإرهابي.

وبالتالي، أصبح الإرهاب الإلكتروني أحد الأشكال المتقدمة والتي تقوم على التأثير على الآخرين سواء في أمنهم أو سلامة الأنظمة والشبكات.

هناك بعض المصطلحات التي ترتبط بمفهوم الإرهاب الإلكتروني ومنها:

الفضاء السيبراني: وهو مفهوم أساسي ظهر قبل الإرهاب الإلكتروني، لأنه يرتبط بدلالات تبين أبعاد ومسارات انتشار الإرهاب الإلكتروني، حيث قدم الباحثان بيتر سينغر و آلان فريدمان تعريفا للفضاء السيبراني بأنه "عالم شبكات الكمبيوتر والمستخدمين الذين يقفون وراءها، حيث يتم تخزين المعلومات ومشاركتها ونقلها عبر الأنترنت" وفي المقابل نجد مايكل فانبوت يعرفه "بأنه مجموعة أجهزة الكمبيوتر والأشخاص المترابطين من خلال أنظمة الاتصالات ويتم تخزين كل تعليمات الكمبيوتر والبيانات ومعالجتها ونقلها في أي وقت على جهاز مادي أو يتم نقلها عبر وسيلة اتصالات" (حارك و رياض، 2022، صفحة 134)، وبالتالي نجد أن الفضاء السيبراني هو الفضاء الأوسع والذي يضم مختلف الشبكات والأنظمة التي تتفاعل فيها البيانات والمعلومات عبر أجهزة الكمبيوتر وأجهزة الاتصال متخطيا حدود الزمان والمكان.

الجريمة الإلكترونية: هذا المصطلح غالبا ما يستخدم كمترادف للإرهاب الإلكتروني، إلا أن الكثير من الدراسات تؤكد أن هناك فرق بينهما، ولهذا لا بد أن نعرف الجريمة الإلكترونية والتي تشير إلى نشاط غير شرعي من قبل أطراف معينة ويتم ارتكابها عن طريق الشبكات الإلكترونية العالمية، أي أنها جريمة ترتكب في بيئة الفضاء الإلكتروني (النت- شبكات الكمبيوتر)، وقد تكون الجريمة بمعنى سرقة البرمجيات أو أن يخضع الكمبيوتر للجريمة أو أن يكون الكمبيوتر هو أداة الجريمة (عبدالرحمان، 2016)، أي أن هدف الجريمة يكون غالبا مادي، من خلال الإحتيال على الأشخاص أو سرقة الحسابات البنكية وغيرها، ومنها ما يتم من خلاله الإبتزاز أو ممارسة نشاط غير مشروع كالدعارة أو بيع أشياء ممنوعة، وبالتالي فهي تختلف عن الإرهاب الإلكتروني الذي يقوم على أهداف أشمل وأكبر تستهدف الأفكار والأنظمة والدول.

II- خصائص ومحددات الإرهاب الإلكتروني

للإرهاب الإلكتروني خصائص ومحددات تختلف عن الأنواع الأخرى من الإرهاب خاصة بعد أحداث 11 سبتمبر 2001. ويمكن أن نستعرض قبل ذلك تطورات ما يعرف بالإرهاب الإلكتروني كما قدمته الباحثة ديننغ Denning المتخصصة في الحاسب الآلي بجامعة جورج تاون من خلال المراحل التالية: (الشهري، 2015، صفحة 10)

- سنة 1997، استطاع الآلاف من المكسيكيين تدمير أحد المواقع الإلكترونية المتخصصة في بيع الفيديوهات على الأنترنت؛
- سنة 1998، استطاعت منظمة "مور تامل" في سيرلانكا من تدمير المواقع الإلكترونية لسفارات سيرلانكا في العالم؛
- سنة 1999، تدمير الحاسب الآلي الخاص بالناتو بواسطة ما يعرف بقنابل البريد الإلكتروني

- التي أرسلها محتجون على الحرب في كوسوفو؛
- سنة 2001، تدمير العديد من المواقع الإلكترونية الأمريكية منها موقعي وزارة الخارجية والدفاع من طرف قراصنة صينيين؛
- سنة 2007، تعرضت استونيا إلى أكبر هجوم الكتروني على المواقع الرسمية للدولة.

كما نجد أن الإرهاب الإلكتروني، من خلال هذه التطورات، يعتبر مواكبا للتغيرات التي يعرفها قطاع التكنولوجيات بشكل يومي، بالإضافة إلى تطور قطاع البرمجيات والفيروسات وأنظمة التجسس والأنظمة المضادة، وبالتالي هذا التهديد أصبح يشكل مجالا غير محدود ومفتوح ويصعب ضبطه بآليات قانونية فقط، بل يتطلب سياسات فعالة وميزانيات ضخمة لمواجهة.

يمكن أن نلخص خصائص ومحددات الإرهاب الإلكتروني كما يلي: (أحمد، 2011)

- سرعة الإستهداف لأنه يعتمد على الأنترنت والحواسيب؛
- البيئة الهادئة أي أن الإرهاب الإلكتروني لا يحتاج إلى العنف والقوة؛
- ينفذ عن بعد؛
- تأثيره يكون أحيانا مدمراً وقوياً.

من جانب آخر، نجد أن هناك خصائص أخرى مرتبطة باستخدام وسائل الاتصال كالأنترنت ومواقع التواصل الاجتماعي خاصة من طرف الجماعات المتطرفة والتنظيمات الإرهابية، ويمكن أن نستعرض كيفية عمل هذه الوسائل من خلال ثلاثة أجيال: (بلعدي، 2017)

الجيل الأول: يعتمد على وسائل الاتصال التقليدية؛

الجيل الثاني: ظهر في التسعينات من القرن الماضي والذي تزامن مع انشاء المواقع المتطرفة؛

الجيل الثالث: يعتمد على الشبكة العنكبوتية ومواقع التواصل الاجتماعي.

وبالتالي، يمكن أن نستخلص مما سبق، أن الإرهاب الإلكتروني يعتمد أساسا على التقنيات الاتصالية العالية المتاحة مع التقدم التكنولوجي، كما استخدمته التنظيم الإرهابي ما يعرف بـ "داعش"، الذي كان يروج ويستقطب أفراد من دول العالم بواسطة الفيديوهات التي تبث عبر المواقع التابعة له أو عبر مواقع التواصل الاجتماعي مثل فايسبوك واليوتيوب، وبالتالي سهولة الانتشار عبر مواقع التواصل الاجتماعي، حيث يتم استهداف فئات معينة من

مستخدمي هذه الشبكات وهم في الغالب شباب. والخاصية الأخرى العالمية هي استخدام اللغة التي أصبحت وسيلة سهلة في نشر الأفكار المتطرفة سواء عبر لغة الصورة أو تصميم أنفوغرافي والفيديوهات القصيرة.

أما فيما يخص الآليات فيمكن تحديدها كما يلي: (أحمد، 2011)

أولاً: اختراق المواقع الإلكترونية: يتم اختراق المواقع الإلكترونية لتغيير محتواها أو سرقة معلومات سرية أو تعطيل الموقع عن العمل والسيطرة عليه بشكل كامل.

ثانياً: الفيروسات: فيروسات الحاسب الآلي تنتشر بسرعة كبيرة عن طريق شبكة الأنترنت وذلك يرجع إلى الكم الهائل من الملفات التي يتم تبادلها بين مستخدمي الشبكة العنكبوتية، وهذه الفيروسات هي عبارة عن برامج تستنسخ نفسها في الجهاز وعندما تنشط تحدث تغييرات في البرامج أو في البيئة التي تعمل فيها ولها أضرار مختلفة تتمثل في فقدان الملفات المخزنة وقد تصل تلك الأضرار إلى إتلاف نظام التشغيل في الجهاز.

ثالثاً: الحرب الإعلامية: الفضاء الإلكتروني له تأثير هائل على الرأي العام العالمي لأنه يخاطب ملايين المستخدمين للشبكة العنكبوتية من شتى أنحاء العالم وبوسائل مختلفة "الصوت- الصورة- النص"، وبالتالي أي جماعة أو منظمة يمكن لها انشاء مواقع الكترونية تروج أفكارها وتنشرها في مختلف أنحاء العالم.

رابعاً: التجسس الإلكتروني: لقد نجحت العديد من الحكومات في استخدام تقنيات متطورة للتجسس على الدول أو المنظمات ومراقبة المعلومات التي يتم تداولها حول العالم.

خامساً: التهديد الإلكتروني: يوجد العديد من الأساليب التي تستخدم في التهديد عبر الشبكة العنكبوتية، وتنوع تلك الأساليب بين تهديدات باغتيال شخصيات سياسية، تهديدات بتفجيرات في مراكز سياسية أو هيئات حكومية، أو التهديد بإطلاق الفيروسات التي من شأنها تدمير أنظمة معلومات بالكامل.

سادساً: تدمير أنظمة المعلومات: تشير إلى محاولة اختراق شبكة المعلومات الخاصة بالشركات العالمية أو بالأفراد بهدف تخريب نقطة الاتصال، وإطلاق أنواع جديدة من الفيروسات التي تسبب الدمار لأجهزة الكمبيوتر والمعلومات.

من جانب آخر يتم وضع تصنيف يحدد الأشكال التي تستخدم في عمليات الاستهداف الإلكتروني أو الإرهاب الإلكتروني من بينها:

- **المتطفل Hacker:** وهو عبارة عن قرصان يقتحم أنظمة الحاسب دون إذن؛

- **المخرب Crocker:** وهو قرصان لديه القدرة على اقتحام أنظمة الحاسب والتحكم فيه وإمكانية إلحاق الضرر به؛
 - **المتطفل النشط:** وهو الذي يجمع ما بين التطفل والتخريب؛
 - **المخرب النشط:** وهو الذي يقوم بعملية القرصنة لأهداف سياسية (الشهري، 2015) ويعمل أحيانا لصالح جهات معينة.
- وبالتالي نجد أن خصائص الإرهاب الإلكتروني تتحدد وفق الهدف من العملية الإلكترونية، إما تخريبية تجسسية تستهدف الأنظمة المعلوماتية أو أنها عملية تقوم على أهداف سياسية تعتمد عليها بالدرجة الأولى التنظيمات الإرهابية.
- وقد لخصنا هذه الخصائص في الجدول التالي: (من إعداد الباحث)

الجماعات السياسية والدول	التنظيمات الإرهابية	الهدف
- يستهدف الأمن الوطني والإعلامي؛ - إضعاف الخصوم؛ - سرقة البيانات والمعلومات الاستراتيجية والحساسة؛ - التجسس؛ - التأثير على الرأي العام؛ - الابتزاز والمساومة.	- يستهدف الأمن الفكري والديني؛ - استقطاب الشباب؛ - نشر الأفكار الخاصة بهم؛ - تقديم مغالطات والتأكيد على الصوابية الخاصة بهم؛ - تعزيز نفوذهم؛ - إرهاب وإرهاب الآخرين؛ - الابتزاز.	
- استخدام أنظمة الهاكر والتجسس؛ - استخدام فيروسات للقرصنة.	- وسائل التواصل الاجتماعي؛ - مواقع خاصة بالتنظيم؛ - تقنيات التصوير عالية ومتقدمة.	الوسائل
- يعتمد على تكنولوجيا متقدمة من أنظمة الحواسيب والبرمجيات؛ - اشتراك وزارات وأجهزة عديدة في عمليات الإستهداف؛ - تتميز بالسرية.	- موجهة ودقيقة في استهدافها وفق برنامج مسبق؛ - تتضمن محتوى مدروس وممنهج؛ - استخدام علم النفس في التأثير على الآخرين؛ - استخدام الدين والفكر كآليات لتبرير أعمالهم؛ - تتميز بالعلنية.	الخصائص

III- محددات العلاقة بين الأمن السيبراني والأمن الإعلامي والإرهاب الإلكتروني

من الضروري التطرق إلى الإرهاب الإلكتروني والأمن السيبراني خاصة أن التهديدات الأمنية في تزايد مستمر وأصبح الرأي العام أكبر المستهدفين (استهداف العقل وأمن الإنسان)، وذلك ضمن ثلاثة الأمن الفكري والديني والإعلامي وأيضا الوطني أو السياسي مجمله، ولهذا وجب تعريف الأمن السيبراني في المقام الأول وهو كما يلي:

يعرف الأمن السيبراني بأنه "هو النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات ويضمن إمكانات الحد من الخسائر والأضرار التي تترتب عنها في حال تحقق المخاطر والتهديدات. كما يتيح إعادة الوضع إلى ما كان عليه بأسرع وقت ممكن بحيث لا تتوقف عجلة الإنتاج ولا تتحول الأضرار إلى خسائر دائمة". وفي تعريف آخر "هو النشاط أو العملية أو نظم المعلومات واتصالات الدولة، حيث تكون المعلومات الواردة فيه محمية من التلف أو الاستخدام غير المصرح به أو التعديل أو الاستغلال" (سميرة، 2017، صفحة 257).

وفي تعريف الأمم المتحدة للأمن السيبراني، جاء كما يلي "تعزيز قدرات الدول والأعضاء والمنظمات على منع استخدام الإرهابيين والمتطرفين التكنولوجيا المتطورة والتصدي لخطر الهجمات الإلكترونية"، وهو ما جاء أيضا في قرار 2371 الصادر عن مجلس الأمن بتاريخ 2017 (الأمم المتحدة، 2022). وبالتالي نجد أن الأمن السيبراني هو أحد أهم المجالات الحساسة التي أصبحت تقوم عليها أنظمة الدول والمؤسسات.

وفي المقابل نجد مفهوم أساسي وهو الأمن الفكري والذي يعرف كما يلي "الأمن الفكري هو أن يعيش الناس في بلدانهم وأوطانهم وبين مجتمعاتهم آمنين مطمئنين على مكونات أصالتهم، وثقافتهم النوعية ومنظومتهم الفكرية" (الواصل، 2022).

وفي تعريف آخر للأمن الفكري نجد أنه "هو سلامة فكر الإنسان وعقله وفهمه من الانحراف والخروج عن الوسطية والإعتدال في فهمه للأمور الدينية والسياسية والابتعاد عن الغلو والتطرف والإلحاد" (الطلحاوي، 2018).

إلى جانب الأمن الفكري لا بد أن نتطرق إلى الأمن الإعلامي، هذا المصطلح الذي تزامن مع ازدياد درجات الانكشاف الإعلامية التي تتزايد مع التطور التكنولوجي والإعلامي وهو "مجموعة الآليات والأفكار التي تقوم على جملة من المبادئ والتصورات سواء من خلال الدفاع عن هذه الركائز أو التأثير في الدائرة الإعلامية والسياسية الداخلية أو الخارجية لأي نظام سياسي" (جدو، 2017).

وقد ارتبط الأمن الإعلامي بمجموعة من العناصر من بينها:

- مواجهة الإرهاب الإلكتروني والذي يقوم على تجنيد الشباب ونشر التطرف عبر القنوات التي تبث عبر الأنترنت؛
- مواجهة الجرائم الإلكترونية التي تتزايد بشكل كبير مع التطور التكنولوجي؛
- مراقبة استخدام مواقع التواصل الاجتماعي التي تستخدم التهديد والضغط (الرجيحي، 2008، صفحة 50).

من خلال ما سبق، سنحاول تبيان محددات العلاقة ما بين الإرهاب الإلكتروني والأمن السيبراني والإعلامي والفكري من حيث فهم الحركات السببية وأبعاد العلاقة بينهم.

الدوافع والحركات السببية:

يمكن أن نلخص أهم الدوافع من الجانب الفكري فيما يلي: (الشهري، 2015، صفحة 169)

- الفراغ الفكري عند الكثير من الأشخاص لاسيما فئة الشباب؛
- الفهم الخاطئ للدين ومبادئه؛
- التشدد والغلو في الفكر والتطرف في الأفكار؛
- الانقسامات الفكرية المتباينة بين التيارات الفكرية والسياسية.

من جانب آخر نجد أن التيارات التطرفية والمنظمات الإرهابية تركز على البعد التطرفي في نشر أفكارها عبر مواقع الأنترنت حيث أطلق توماس هيغامر و برينجار ليا من مؤسسة الأبحاث الدفاعية النرويجية في أوصلو مصطلح "الدراسات الاستراتيجية الجهادية" بمعنى أن الأنترنت أصبحت مكانا حيويا للخلايا الإرهابية لتنظيم وتبادل الأفكار حول التكتيكات بطريقة لامركزية، إذ يسمح هذا المجال الافتراضي للخلايا النائمة التي تستمد نشاطها من الأفكار المتواجدة عبر هذه الشبكة (حسين، 2021، صفحة 118)، من نشر الأفكار والاستقطاب دون الحاجة إلى التواصل المباشر وذلك من خلال:

- الاعتماد على المنتديات النقاشية عبر مواقع التواصل الاجتماعي والصفحات الخاصة بها والدعاية والحرب النفسية أين يتم التسويق للأفكار والتنظيمات كما حدث مع تنظيم ما يسمى "داعش" الذي استغل مواقع التواصل الاجتماعي لعرض قوته كما حدث في 2017 وتغيير الإسم ونشره إلى ما يسمى "الدولة الإسلامية" مما يوحي بالقوة والبعد الديني وهذا ما انعكس على نسب التفاعل عبر حسابات التنظيم الإرهابي بواسطة فايسبوك وتويتر؛ (بلعدي، 2017، صفحة 192)

- إصدار الفتاوى الدينية التي تسهل عملية التطرف حسب التوجهات السياسية، فهذا الفضاء مكن من إرسال خطابات عابرة للحدود وبدون حواجز أو عوائق، وبالتالي التأثير على توجهات الأفراد والشباب خاصة مع ضعف التكوين الديني والخطاب داخل بعض الدول؛
- الاعتماد على نشر أفكار متطرفة تهدد الولاء داخل الدولة لحساب أطراف خارجية؛
- ضعف المحتوى الإعلامي التقليدي والجديد في بعض الدول والذي لا يقوم على فكرة الاستباقية، خاصة مع افرازات العولمة والتطورات الرهيبة للتكنولوجيا، وبالتالي يعتبر ما يقدم عبر وسائل التواصل الاجتماعي أسرع وأكثر مواكبة لتوجهات الشباب خاصة؛
- استغلال ما يقدمه الآخر من أضرار للقيم والمعتقدات الدينية كما حدث مع الجريدة الفرنسية "شارلي ابيدو" التي نشرت صور مسيئة للرسول ﷺ وهذا ما يخلق ردود فعل مبررة للقيام بعمليات انتقامية؛
- أحداث 11 سبتمبر 2001 وما أفرزته من حرب على أفغانستان وغزو العراق سنة 2003 مما جعل هذه الأحداث مكانا ومنطلقا لنقاشات فكرية ضمن مقاربات ما يعرف بصراع الحضارات التي طرحها صامويل هنتغتون وما قبلها من أفكار جاء بها ما يسمى "تنظيم القاعدة"، وانتشار التنظيمات المتطرفة حتى داخل بعض الدول العربية، مما أتاح عمليات الاستقطاب والثقاف ضمن البيئة الرقمية والتكنولوجية، أي بروز ما يعرف بالإرهاب الرقمي أو الإلكتروني. إن عمليات الاستقطاب ظهرت بقوة مع ظهور ما يسمى "تنظيم داعش" في منطقة الشرق الأوسط، هذا "التنظيم" الذي استطاع أن يؤسس لأفكار جديدة من خلال تجنيد جنسيات عديدة للعمل المتطرف وفق برامج وفيديوهات متطورة ومخرجة بتقنيات عالية لتفعيل عمليات الاحتواء وغسل الأدمغة، مما أدى عملا وظيفيا مكن من تحقيق بناء ولاءات للتنظيم الإرهابي فوق الولاء للدولة والأمة، وهذا يعتبر مكنم الخطر في كيفية انتشار الفكر المتطرف عبر الفضاءات الإلكترونية؛
- تحويل العديد من مواقع التواصل الاجتماعي إلى عنوان للهوية الإلكترونية لدى الجماعات المتطرفة، والمقصود بها أن توظف مواقع التواصل الاجتماعي كبديل للمؤسسات والهيئات التي من المفروض أن تعمل على تحقيق الأمن الهوياتي، وهذا ما يسمح للتنظيمات المتطرفة باستغلال المواقع الإلكترونية للقيام ببرمجة حصص وبرامج خاصة تمكن من الاستقطاب وتحقيق المتابعة وتصبح سمة ثابتة ومرجعية دينية ومصدر للتحريض بشكل رئيسي؛
- اختراق المنظومة الثقافية والقيمية للفرد من طرف التنظيمات المتطرفة داخل المجتمعات وهذا يدخل في سياق تغير القيم العامة للمجتمعات عبر التسويق لأفكار جديدة هدامة،

عن طريق استخدام منصات تفاعلية تسهل عمليات الاختراق للأمن المجتمعي والهويات الجماعية والعمل على التشكيك في الموروث الديني ومنظومة القيم العامة والتسويق لأفكار بأسلوب علمي أحيانا وأحيانا أخرى بأسلوب التشكيك وأحيانا باستخدام الحجج العقلية؛ - استخدام لغة خطاب ومحتوى قوي مقارنة بما هو موجود في المضامين الرسمية (بلعدي، 2017، صفحة 195) والمقصود هنا أن اللغة المستخدمة في المحتوى الإلكتروني لدى القنوات الرسمية، خاصة عبر مواقع التواصل الاجتماعي، غالبا ما تكون نمطية وليست فعالة وموجهة حسب الفئات أي أن المضمون يكون واحد والمتلقي متنوع من فئات مجتمعية مختلفة إلا أنه في المقابل نجد أن الجماعات المتطرفة تستخدم لغة قوية ومؤثرة تمكن من الجذب والاستقطاب.

من خلال ما سبق، لا يمكن أن نفصل الإرهاب الإلكتروني عن التحولات التي تحدث داخل البيئة الرقمية وتزايد درجات الانكشاف الإعلامية، مما يضعنا أمام ثلاثية الأمن السيبراني والإعلامي والفكري، فكلما كان هناك تأمين ضد الإرهاب الإلكتروني كلما قلت التهديدات الإرهابية الإلكترونية من جهة، ومن جهة أخرى لا يمكن أن نواجه الإرهاب الإلكتروني بدون معرفة الأسباب والدوافع التي تؤدي إلى انتشاره ووضع استراتيجيات لمواجهة هذا النوع من الإرهاب وتحقيق الأمن السيبراني، وبالتالي فإن المعالجة الآلية والتصدي للآثار التي تنتج عن الإرهاب الإلكتروني لا تكون إلا بالإستباقية والإستشراف لمواجهة التحديات الأمنية وتفعيل المؤسسات والبرامج التي تحقق الأمن السيبراني على غرار الأمن الإعلامي والفكري والديني.

خاتمة

نخلص في هذا المقال إلى أن الإرهاب الإلكتروني من حيث المفهوم يختلف ليس مضامينا بل عموديا بسبب تزايد درجات التعقيد على مستوى الإعلام والتكنولوجيا وتطور وسائل التواصل الاجتماعي التي أصبحت جزءا من البيئة العامة للناس، بحكم توجه العالم إلى الرقمنة وزيادة استعمال المنصات الرقمية وشبكات التواصل الاجتماعي في مجال الترفيه كبديل للإعلام التقليدي. ليس هذا فقط، بل حتى نقل الأحداث من طرف الأشخاص عبر هواتفهم النقالة. ومن أجل تحقيق الأمن السيبراني ومواجهة الإرهاب الإلكتروني فيجب على الحكومات وصناع القرار تبني استراتيجيات ذات قدرة على مواجهة التهديدات الأمنية من خلال تطوير المحتوى الإعلامي عبر وسائل التواصل الاجتماعي أو الاعلام التقليدي، وذلك من خلال:

- تطوير المحتوى التعليمي والخطاب الديني الذي يمكن من المحافظة على الهوية الوطنية والاعتماد على المرجعية الدينية؛
- تطوير أنظمة الرقابة والدفاع في المجال السيبراني لمواجهة أي تهديد؛
- تحديث المنظومة القانونية والتشريعية حتى تتمكن من ردع الإرهاب الإلكتروني؛
- تفعيل دور مراكز البحث والجامعات في بناء سياسات واستراتيجيات لمواجهة الإرهاب الإلكتروني.

المراجع

1. Lewkowicz, G. (2006). Le problème de la définition du terrorisme. Belgique: Jletd.
2. الرجحي، م. (2008). الأمن الإعلامي في ظل الانفجار الإعلامي. الجزائر: دار اليسر. الشهري، ح. ب. (01، 2015). الإرهاب الإلكتروني حرب الشبكات. المجلة العربية الدولية للمعلوماتية، 4(8).
3. الطلحاي، ه. م. (1، 2018). الخطاب الديني وأثره على الأمن الفكري عند الشباب. مجلة كلية الأدب، 62(2)، 92-10.
4. الأمم المتحدة. (17، 07، 2022). أمن الفضاء السيبراني. الأمم المتحدة: www.un.org/counterterrorism/ar
5. الواصل، م. (17، 07، 2022). أهمية الأمن الفكري. جامعة الإمام سعود: <https://units.imamu.edu.sa/shis/malaz-inst/EduArticles/Pages/26-5-1439-m.aspx>
6. بلعدي، ن. (31، 12، 2017). توظيف تنظيم الدولة الإسلامية الأنظمة الرقمية في الاستراتيجية الاتصالية. المجلة الجزائرية للدراسات السياسية، 04(02)، 190.
7. جدو، ف. (25، 05، 2017). آليات تحقيق الأمن الإعلامي في ظل ثنائية الانكشافية الإعلامية ومنطق الأمانة. المجلة المغاربية للدراسات التاريخية والاجتماعية، 09(01)، 104.
8. حارك، ف.، و رياض، ح. (01، 2022). الدولة بين الهيمنة وتحقيق الأمن في الفضاء السيبراني. المجلة الجزائرية للأمن الإنساني، 07(01)، 134.
9. حسين، ق. (2021). دور الاستخبارات الإلكترونية في مكافحة الإرهاب السيبراني. مجلة الابحاث القانونية والسياسية، 3(1)، 118.
10. رافعي، ر. (03، 06، 2021). الارهاب الدولي وعلاقته بالجريمة المنظمة الإرهاب الإلكتروني نموذجاً. مجلة القانون والعلوم السياسية، 73.
11. عبدالرحمان رشاد رهان. (24، 07، 2016). المركز العربي الديمقراطي. <https://democraticac.de/?p=34528>

12. سميرة، ب. (07, 2017). الأمن السيبراني في الجزائر. المجلة الجزائرية للأمن الانساني (04)، 259.
13. الراوشدة، م. س. (2010). أثر قوانين مكافحة الإرهاب على الحرية الشخصية دراسة مقارنة. عمان: دار الثقافة.
14. هبة الله، أحمد. (2011). الإرهاب الدولي. الاسكندرية: منشأة المعارف.