

الإرهاب الإلكتروني والأمن القومي للدول: نمط جديد وتهديدات مختلفة  
The electronic terrorism and national security: a new pattern and various threats



صليحة محمدي

جامعة باتنة1، الجزائر. [mohamedi\\_saliha@yahoo.fr](mailto:mohamedi_saliha@yahoo.fr)

شفيعة حداد

جامعة باتنة1، الجزائر. [chafiaahaddad@gmail.com](mailto:chafiaahaddad@gmail.com)

تاريخ قبول النشر: 2019/06/22

تاريخ الإستلام: 2019/05/28

ملخص:

يعد الإرهاب الإلكتروني أحد أهم الموضوعات التي تحتل حيزا مهما في الدراسات والنقاشات المثارة على الساحة الدولية خلال الفترة الأخيرة، وهو من أخطر أنواع الجرائم التي ترتكب عبر شبكة الإنترنت، وتتضح خطورة هذا الإرهاب من خلال النظر إلى حجم التهديدات التي يفرضها على الأمن القومي للدول.

الكلمات المفتاحية:

الإرهاب الإلكتروني؛ الأمن المعلوماتي؛ الأمن القومي للدول.

**Abstract:**

The electronic terrorism is one of the most important topics that occupy an important place in the studies and discussions that have been raised in the international arena in recent period, which is one of the most serious types of crimes committed through the Internet, and the seriousness of this terrorism is revealed by considering the size of the threats it poses to the national security of states.

**:Keywords**

Electronic terrorism; Information security; The national security of states.

\* المؤلف المرسل: صليحة محمدي. [mohamedi\\_saliha@yahoo.fr](mailto:mohamedi_saliha@yahoo.fr)

## مقدمة:

أدت ثورة المعلومات والاتصالات والإعلام المتعددة الوسائط إلى بروز نمط مختلف من المخاطر ارتبط بها وبعمليات العولمة وصيرورتها على نحو أسفر عن تهديدات أمنية جديدة .، وترتب على ظهور الفضاءات الإلكترونية تغيير في طبيعة الإرهاب الدولي، حيث ظهر نمط جديد يتراوح بين التقنية وجماعات الإرهابية، يعرف بالإرهاب الإلكتروني، والذي يعد من أخطر أنواع الإرهاب في العصر الحاضر .

إن دراسة ظاهرة الإرهاب الإلكتروني تكتسي أهمية بالغة بسبب ما قد ينجم عنه من مخاطر وخسائر، بوصفه اعتداء سافرا على الأفراد وتهديدا ظاهرا على الأمن القومي للدول و السيادة الوطنية وزعزعة استقرار المجتمع وتماسكه. فالنمو السريع في انتشار تكنولوجيا الاتصال والمعلومات فتح مجالا حيويا للأنشطة التي تقودها الجماعات الإرهابية، إذ بات مؤكدا اليوم العلاقة الوطيدة بين الإرهاب واستخدام الوسائل التكنولوجية، حيث استفادت الجماعات الإرهابية من مكتسبات الثورة المعلوماتية والتقنية ووظفتها في تحقيق أهدافها.

إذ تشير معطيات إلى أن التوسع في استخدام الانترنت مكن التنظيمات الإرهابية من التحرك بمرونة عالية وإبراز دورها وإدارة إمكانياتها من مختلف أنحاء العالم، إذ أصبحت شبكة الانترنت منبرا للجماعات الإرهابية في التواصل مع المولدين والمساندين والمؤيدين لهم، بل ذهبوا إلى أكثر من ذلك فتح عبر الشبكة العنكبوتية تجنيد الإرهابيين، وبث الأفكار الضالة والتدميرية . علاوة على ذلك يتم في هذه المواقع التخطيط والتنسيق وتبادل الخبرات في مجالات عملياتهم الإرهابية، إضافة إلى استحداث التعليم الإلكتروني الإرهابي عبر الشبكة، ليس هذا فحسب بل أصبح الإرهاب الإلكتروني خطرا يهدد البنى التحتية للدول. وهو ما ستحاول هذه الدراسة إلقاء الضوء عليه من خلال الإجابة على الإشكالية التالية: ما مدى تأثير الإرهاب الإلكتروني على الأمن القومي للدول ؟.

## المحور الأول: الإرهاب الإلكتروني: مقارنة مفهوماتية

### أولا: تعريف الإرهاب الإلكتروني:

هناك العديد من المفاهيم للإرهاب الإلكتروني حيث أنه لا يوجد اتفاق تام حول تعريف الإرهاب بشكل عام ومن ثم عدم وجود مفهوم محدد للإرهاب الإلكتروني، ويمكن القول أن الإرهاب الإلكتروني يعتمد على استخدام إمكانيات أو مقدرات الحاسوب الآلي في الترويع أو إكراه. ومن هنا يعد الإرهاب الإلكتروني نمطا جديدا من الحروب التي لا تعتمد على استخدامات الأسلحة والمتفجرات وينطوي على استخدام أو استغلال المجرمين لعدم حماية أو قابلية الأنظمة المدنية والعسكرية للمخاطر على النحو الذي يؤدي إلى التأثير على الأمن الوطني والعالمي، لذلك فيشهد مستقبل الإرهاب في القرن الحالي أسوأ أنواع الحروب. ( أحمد، ف، ع ( 2006). ص.81.

ويعرفه "دينينج": "يعبر عن التقاء الإرهاب وعالم الكمبيوتر وأنه الاستخدام غير المشروع للقوة والتهديدات بضرب أجهزة الكمبيوتر والشبكات والمعلومات المخزنة فيها من أجل ترويع وإكراه الحكومات وشعوبها من أجل تحقيق أهداف سياسية واجتماعية، ولكي يعتبر ذلك إرهاب لابد أن يؤدي إلى ترويع وإكراه الحكومات والأشخاص والممتلكات أو على الأقل التسبب في الضرر والخوف، وكذلك أحداث ضحايا وإيذاء بدني وانفجار وأضرار اقتصادية جسيمة والهجوم على البنية الأساسية وإعاقة عمل الخدمات الأساسية.

## "الإرهاب الإلكتروني والأمن القومي للدول: نمط جديد وتهديدات مختلفة" صليحة محمدي و شفيعة حداد

في الحين تعريف وزارة الدفاع الأمريكي بأنه: عمل إجرامي يتم الاعداد له باستخدام الحاسبات ووسائل الاتصالات وينتج عنه عنف وتدمير أو بث الخوف تجاه متلقى الخدمات بما يسبب الارتباك وعدم اليقين وذلك بهدف على الحكومة أو السكان لكي تمثل لأجندة سياسية أو اجتماعية أو فكرية معينة ( المركز العربي (24-06-2016).

إن الإرهاب الإلكتروني هو أحد الاستخدامات غير سلمية للفضاء الإلكتروني، وهو نتيجة لتفاعل العالم المادي مع العالم الافتراضي، وكانت بداية استخدام كلمة (Cyber Terrorism) في دراسة لباري كولن والذي توصل فيها إلى أنه من الصعب الوصول إلى تعريف محدد لظاهرة الإرهاب الإلكتروني، وهذا المفهوم يشير إلى استخدام الفضاء الإلكتروني كأداة لإلحاق الضرر بالبنية التحتية سواء كانت " طاقة – موصلات- خدمات حكومية" أي يشير إلى الهجمات التي يستخدم فيها الكمبيوتر ضد الاقتصاد والحكومات. أهداف الإرهاب الإلكتروني تكون غالبا سياسية وقد يأتي الإرهاب الإلكتروني في صورة: تدمير نظم المعلومات لدى الخصم وافتقاده على الحصول على المعلومات، شل قدرته على التواصل مع أعضائه عن طريق تدمير مواقعها الإلكترونية، اختراق شبكات المعلومات الرسمية للوزارات والحكومات بغرض تدميرها أو الحصول على معلومات سرية. (كازيز.ص. و كزيز.أ. (2018). ص. 314 .

على هذا الأساس يمكن تعريف الإرهاب الإلكتروني بأنه: " التخويف أو التهديد أو العدوان المادي أو المعنوي باستخدام الغير مشروع للوسائل الإلكترونية الصادرة من الدول أو الجماعات أو الأفراد على الفرد وممتلكاته".

### ثانيا: خصائص الإرهاب الإلكتروني:

ينفرد الإرهاب الإلكتروني بعدد من الخصائص وهي:

- ✓ لا يحتاج الإرهاب الإلكتروني في ارتكابه إلى العنف والقوة، بل يتطلب وجود حاسب إلى متصل بالشبكة المعلوماتية فقط ومزود ببعض البرامج اللازمة.
- ✓ ينسم الإرهاب الإلكترونية بأنه عابر للقارات والدول.
- ✓ صعوبة اكتشاف جرائم الإرهاب الإلكتروني .
- ✓ صعوبة إثبات جرائم الإرهاب الإلكتروني، لغياب الدليل الرقمي من ناحية، وسهولة إتلافه وتدميره من ناحية أخرى.
- ✓ يكون مرتكب الإرهاب الإلكتروني في العادة من المتخصصين في مجال تقنية المعلومات، أو لديه – على الأقل – قدر من المعرفة والخبرة في التعامل مع الشبكات المعلوماتية. (يوسف كافي م. (2011). ص. 441).
- ✓ ترتكب الجرائم عبر الشبكة العالمية للإنترنت بدقة بالغة نتيجة دقة أدوات الجريمة.
- ✓ الإرهاب الإلكتروني لا حدود جغرافية له، حيث ألغت شبكة الإنترنت أي حدود جغرافية فيما بين الدول فالجاني قد يكون في بلد وضحيته في بلد أخرى. (حسن. أ.ش. (يناير 2015). ص. 08).

### ثالثا : آليات الإرهاب الإلكتروني:

#### 1- البريد الإلكتروني:

خدمة تسمح بتبادل الرسائل والمعلومات مع الآخرين عبر شبكة للمعلومات، وتعد هذه الخدمة من أبرز الخدمات التي تقدمها شبكة الإنترنت، لما تمثله من سرعة في إيصال الرسالة وسهولة الإطلاع عليها وقراءتها في أي مكان من العالم. يستخدم البريد الإلكتروني في التواصل بين الإرهابيين وتبادل المعلومات بينهم، بل إن كثيرا من العمليات الإرهابية التي تحدث في الآونة الأخيرة كان البريد الإلكتروني فيها وسيلة من وسائل تبادل المعلومات وتناقلها بين القائمين بالعمليات الإرهابية والمخططين له. (الهاشمي، ر.ع. (2018). ص 07)

#### 2- إنشاء مواقع على الإنترنت:

يقوم الإرهابيون بإنشاء وتصميم مواقع لهم على شبكة المعلومات العالمية الإنترنت لنشر أفكارهم والدعوة إلى مبادئهم، بل تعليم الطرق والوسائل التي تساعد على القيام بالعمليات الإرهابية، فقد أنشئت مواقع لتعليم صناعة المتفجرات، وكيفية اختراق وتدمير المواقع، وطرق اختراق البريد الإلكتروني، وكيفية الدخول على المواقع المحجوبة، وطريقة شر الفيروسات وغير ذلك.

والموقع هو: معلومات مخزنة بشكل صفحات، وكل صفحة تشتمل على معلومات معينة تشكلت بواسطة مصمم الصفحة باستعمال مجموعة من الرموز تسمى لغة تحديد النص الأفضل Hyper text mark up language (HTML) ولأجل رؤية هذه الصفحات يتم طلب استعراض شبكة المعلومات العنكبوتية (WWW) (Browser) ويقوم بحل رموز (HTML) وإصدار التعليمات لإظهار الصفحات المتكونة. (عبد الرحمن. (2009). ص 14). فالمواقع الإلكترونية سهلت على المنظمات الإرهابية توسيع أنشطتهم لأبعد الحدود من خلال تبادل الآراء والأفكار والمعلومات، إذ يمكن أن يلتقي عدة أشخاص في أماكن متعددة في وقت واحد، كما ساعدتهم أيضا على جمع أكبر عدد ممكن من الأتباع والأنصار عبر إشاعة أفكارهم ومبادئهم من خلال هذه المواقع ومنتديات الحوار، وغرف الدردشة، فإذا كان الحصول على وسائل إعلامية كالقنوات التلفزيونية والإذاعية صعبا، فإن إنشاء مواقع على الإنترنت، واستغلال منتديات الحوار وغيرها لخدمة أهداف الإرهابيين غدا سهلاً ممكناً، بل تجد لبعض المنظمات الإرهابية آلاف المواقع، لضمان الانتشار الواسع، وحتى لو تم منع الدخول على بعض هذه المواقع أو تعرضت للتدمير تبقى المواقع الأخرى يمكن الوصول إليها. (أيسر محمد عطية، "دور الآليات الحديثة للحد من الجرائم المستحدثة وطرق مواجهته". (أيسر، م.ع). أيام 04-02 /2014/09، ص 16).

#### 3- اختراق الموقع:

يستطيع قرصنة الحاسوب الآلي Hackers التوصل إلى المعلومات السرية والشخصية واختراق الخصوصية وسرية المعلومات بسهولة، ومن ثم تتم عملية الاختراق الإلكتروني عن طريق تسريب البيانات الرئيسية والرموز الخاصة ببرامج شبكة الإنترنت، أو عن طريق نشر الفيروسات وهي عملية تتم من أي مكان في العالم دون حاجة إلى وجود شخص المخترق في الدولة التي اخترقت فيها المواقع فالبعد الجغرافي لا أهمية له في الحد من الاختراقات الإلكترونية ولا تزال نسبة كبيرة من الاختراقات لم تكشف بعد بسبب التعقيد الذي يتصف به نظام تشغيل الحاسوب الآلي. (الهاشمي، ر. المرجع السابق، ص 10).



مخطط يوضح ادوات الإرهاب الإلكتروني المصدر: (المرجع نفسه، ص 11).

#### المحور الثاني: تداعيات الإرهاب الإلكتروني على الأمن القومي للدول: المخاطر والإجراءات المضادة

##### أولاً: ضبط مفهوم الأمن القومي:

يعرف تريجر وكرننبرج الأمن القومي بأنه "ذلك الجزء من سياسة الحكومة الذي يستهدف خلق الظروف المواتية لحماية القيم الحيوية". ويعرفه هنري كيسنجر بأنه يعني "أية تصرفات يسعى المجتمع - عن طريقها - إلى حفظ حقه في البقاء. أما روبرت ماكنمارا فيرى أن "الأمن هو التنمية، وبدون تنمية لا يمكن أن يوجد أمن، والدول التي لا تنمو في الواقع، لا يمكن ببساطة أن تظل آمنة.

ويوضح تنوع تعريفات مفهوم الأمن القومي أن هناك قدرًا من التخلف النظري للمفهوم. ويذكر باري بوزان عدة أسباب لذلك التخلف، وهي: (عبد الحفيظ، ع. م).

- ✓ الأمن القومي مفهوم معقد ومركب لدرجة يصعب معها جذب الدارسين إليه، حيث انصرفوا إلى مفاهيم أكثر مرونة، أي أنه مفهوم مثير للخلاف والاختلاف.
- ✓ التشابك بين الأمن القومي ومفهوم القوة، لاسيما بعد بروز المدرسة الواقعية التي رسمت فكرة التنافس من أجل القوة في العلاقات الدولية، وبحيث يُنظر للأمن على أنه مشتق من القوة وأنه أداة لتعظيمها.
- ✓ ظهور موجة من المثاليين ترفض المدرسة الواقعية وتطرح هدفاً بديلاً للأمن القومي وهو السلام.
- ✓ غلبة الدراسات الإستراتيجية في مجال الأمن القومي واهتمامها بالجوانب العسكرية للأمن، وتكريسه لخدمة المتطلبات الدفاعية والحفاظ على الوضع القائم، مما أسهم في تحجيم الأفق التحليلي والبعد النظري للمفهوم.
- ✓ دور رجال السياسة في تكريس غموض المفهوم، لتوفير فرصة أكبر من المناورة عليه سواء في أغراض الاستهلاك الداخلي أم الصراع الخارجي.

## 2- أبعاد الأمن القومي:

استخدام اصطلاح الأمن القومي للتعبير عن مجموعة سياسات تتخذ لضمان سلامة إقليم الدولة والدفاع عن مكتسباتها في مواجهة الأعداء، سواء في الداخل أو الخارج، واتسع مفهوم الأمن في العقود الأخيرة ليشمل قضايا ليست بالضرورة ذات طابع عسكري أو أمني، ليشمل مجموعة من الإجراءات الاقتصادية والثقافية والاجتماعية، بعد أن ثبت أن هناك مهددات للأمن القومي بخلاف العدوان والمهددات الخارجية. مثل صراع الفروق الطبقية وسوء توزيع الدخل وغياب العدالة الاجتماعية، ومن هنا. فإن شمولية الأمن تعني أن له أبعاداً متعددة لها خصائصها التي تثبت ترابطها وتكاملها، وهي:

### أ: البعد السياسي:

ويتمثل في الحفاظ على الكيان السياسي للدولة وهو ذو شقين داخلي وخارجي. يتعلق البعد الداخلي بتماسك الجبهة الداخلية وبالسلام الاجتماعي والوحدة الوطنية. أما البعد الخارجي فيتصل بتقدير أطماع الدول العظمى والكبرى والقوى الإقليمية في أراضي الدولة ومواردها، ومدى تطابق أو تعارض مصالحها مع الدولة سياسياً واقتصادياً واجتماعياً، وتحكمه مجموعة من المبادئ الاستراتيجية التي تحدد أولويات المصالح الأمنية وأسبقياتها. (زكي. عبد م. ( 02-09-2016 ). ص. ص (02-01).

### ب- البعد الاقتصادي للأمن القومي:

برز البعد الاقتصادي للأمن القومي مع ازدياد عتبة الخيار العسكري وارتفاع تكلفته خاصة على الدول الكبرى في ظل الردع النووي الذي صار مكبلاً للأداة العسكرية لأن استخدامها قد يؤدي إلى فناء الجميع، ومن ثم بدأت الدول وعلى رأسهم الولايات المتحدة في الاتجاه نحو الجانب الاقتصادي في علاقاتها مع باقي دول العالم؛ ما جعل البعد الاقتصادي واحداً من أهم أبعاد الأمن القومي، نظراً للجوء الدول الكبرى إلى إتباع العقوبات الاقتصادية على الدول التي ترغب في تغيير توجهاتها الخارجية دون استخدام القوة العسكرية، وقد كان العراق خير مثال على ذلك حينما تعرض لحصار اقتصادي دولي أدى إلى إضعاف قدراته وخفض من المستوى المعيشي داخل العراق بشدة وكان من نتيجته أن توفي نحو 567 ألف طفل، ومع تزايد أهمية الأداة الاقتصادية وتزايد الاعتماد المتبادل في عالم اليوم، صارت القوة الاقتصادية أحد العوامل شديدة الأهمية بالنسبة لقوة الدولة لتثبت صدق المقولة القديمة القائلة بذهبي أعد الجند وبجندي أجمع مزيداً من الذهب، فبالفعل تساعد قوة الدولة الاقتصادية على تدعيم قدراتها العسكرية والسياسية وتساهم في تدعيم نفوذها الخارجي؛ حيث تمكن القوة الاقتصادية للدولة من أن تغري الدول الأخرى برعاية مصالحها من خلال المساعدات الاقتصادية المختلفة، ولا يفوتنا هنا الحديث عن أثر المساعدات الاقتصادية الضخمة التي قدمت لدول أوروبا الشرقية بهدف التعجيل بتحولها من النظام الاشتراكي المنهار إلى النظام الرأسمالي، وليس أدل من أهمية البعد الاقتصادي للأمن القومي ما حدث للاتحاد السوفيتي؛ فعلى الرغم من اهتمام قيادات السوفييت بالبعد العسكري التقليدي للأمن القومي، إلا أن تراجع مستوى المعيشة داخله أدى إلى تعريض وحدة الدولة للخطر فتصاعدت الاحتجاجات المختلفة في شرق أوروبا بشكل رئيسي نهاية الثمانينيات احتجاجاً على الوضع الاقتصادي المتدهور في الداخل السوفيتي ما أدى في النهاية إلى زوال الاتحاد السوفيتي كقوة عظمى من الخريطة السياسية وذلك بفضل تركيز اهتمامه فقط على البعد العسكري وإهمال البعد الاقتصادي تماماً. (C. R. Charles Wolf, 1994, pp: 25-27).

## "الإرهاب الإلكتروني والأمن القومي للدول: نمط جديد وتهديدات مختلفة" صليحة محمدي و شفيعة حداد

ويرمي البعد لاقصادي إلى توفير المناخ المناسب للوفاء باحتياجات الشعب وتوفير سبل التقدم والرفاهية له. فمجال الأمن القومي هو الإستراتيجية العليا الوطنية التي تهتم بتنمية واستخدام كافة موارد الدولة لتحقيق أهدافها السياسية، كذلك فالنمو الاقتصادي والتقدم التكنولوجي هما الوسيلتان الرئيسيتان والحاسمتان لتحقيق المصالح الأمنية للدولة وبناء قوة الردع الإستراتيجية وتنمية التبادل التجاري وتصدير العمالة والنقل الأفقي للتكنولوجيا وتوطينها وبخاصة التكنولوجيا العالية والحيوية. ( زكي. عبد م ( المرجع السابق، ص02).

ح- البعد العسكري: يعتبر من اخطر أبعاد الأمن القومي لأنه إذا لم تمتلك الدولة القوة العسكرية، لا تستطع الدفاع عن أمنها القومى وسادتها، وتتعرض للمخاطر والتهديدات التي تؤدي إلى انهيارها ووقوعها تحت النفوذ أو الاحتلال العسكري، أو حتى إلى اقتسامها مع دول أخرى،

د- البعد الاجتماعي: وهتم هذا البعد بالإنسان والمجتمع، وحماته من الأوقات الاجتماعية كالمخدرات وغيرها، والحفاظ على النسج الاجتماعي من التفكك، وبخاصة إذا كان في الدولة طوائف متعددة وتوفر الخدمات والاحتياجات الضرورية، كالصحة والتعلم، ودراسة أسباب الهجرة الداخلة والخارجة، ووضع الحلول الملائمة لها. (منصور.م. ذ.، 2011). ص. ص 51-52).

### ثانيا: استخدام الجماعات الإرهابية للشبكة العالمية:

بين ويمن كيف يستخدم الإرهابيون شبكة الإنترنت في أغراضهم الإرهابية كما يلي:

1- التنقيب عن المعلومات: إن شبكة الإنترنت في حد ذاتها تعتبر مكتبة إلكترونية هائلة الحجم وتكتظ بالمعلومات الحساسة التي يسعى الإرهابيين للحصول عليها مثل أماكن المنشآت النووية، والمطارات الدولية والمعلومات الخاصة بسبل مكافحة الإرهاب وبذلك يكون 80% من مخزونهم المعلوماتي معتمدا في الأساس على مواقع الانترنت متاحة لكل دون خرق لأي قوانين أو بروتوكولات للشبكة.

2- الاتصالات: تساعد شبكة الإنترنت المنظمات الإرهابية المنفرقة في الاتصال بعضها البعض والتنسيق فيما بينها، وذلك نظرا لقللة التكاليف للاتصال باستخدام الإنترنت مقارنة بالوسائل الأخرى، كما أنها تمتاز بوفرة المعلومات التي يمكن تبادلها، وقد أصبح عدم وجود قائد ظاهر للجماعة الإرهابية سمة جوهرية للتنظيم الإرهابي الحديث مختلفا بذلك عن نمط الهرمي القديم للجماعات الإرهابية كل هذا بسبب سهولة الاتصال والتنسيق عبر الشبكة العالمية.

4- التعبئة وتجنيد الإرهابيين: إن انخراط عناصر جديدة داخل المنظمات الإرهابية يحافظ على بقائها واستمرارها وهم يستغلون تعاطف الآخرين من مستخدمي الإنترنت مع قضاياهم، ويجذبون السذج من الشباب بعبارات براقة حماسية من خلال غرف الدردشة الإلكترونية.

5- مهاجمة المنظمات الإرهابية الأخرى: تستخدم الإنترنت كحلبة مصارعة بين المنظمات الإرهابية وبعضها وبين أعضاء المنظمة الواحدة، وتكثر المناظرات والخلافات بين هذه المنظمات. ( حسن أ. الشهري (المرجع السابق. ص 16).

6- الحصول على التمويل: من خلال الشبكة المعلوماتية العالمية وعن طريق الاستعانة ببيانات إحصائية سكانية منتقاة من المعلومات الشخصية التي يدخلها المستخدمون على الشبكة المعلوماتية، من خلال الاستفسارات والاستطلاعات الموجودة على المواقع الإلكترونية، يقوم الإرهابيون بالتعرف على الأشخاص ذوي المشاعر الرقيقة، والقلوب الرحيمة، ومن ثم يتم استجوابهم لدفع تبرعات مالية لأشخاص اعتباريين يكونون واجهة لهؤلاء الإرهابيين، ويتم ذلك بواسطة رسائل البريد الإلكتروني أو من خلال ساحات الحوار الإلكترونية، بطريقة ذكية وأسلوب مخادع، بحيث لا يشك المتبرع بأنه سيساعد إحدى التنظيمات الإرهابية.

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

8- إصدار البيانات الإلكترونية: تقوم المنظمات الإرهابية باستخدام الشبكات المعلوماتية في نشر بياناتها الإرهابية المختلفة، وذلك عن طريق المواقع الإلكترونية أو بواسطة رسائل البريد الإلكتروني أو من خلال منتديات الحوار وساحاته، وقد ساعدت القنوات الفضائية التي تسارع في الحصول على مثل هذه البيانات الإرهابية ومن ثم تقوم بنشرها عبر وسائل الإعلام في مضاعفة انتشار تلك البيانات، ووصولها إلى مختلف شرائح المجتمع. وتأخذ البيانات الصادرة من قبل التنظيمات الإرهابية اتجاهات متنوعة، فتارة ترسم أهدافاً وخططاً عامة للتنظيم الإرهابي، وأحياناً تكون للتهديد والوعيد بشن هجمات إرهابية معينة، في حين تصدر معلنة عن تبني تنفيذ عمليات إرهابية محددة، كما تصدر تارة أخرى بالنفي أو التعليق على أخبار أو تصريحات صادرة من جهات أخرى. (فهد العجلان . (2-4 جوان 2008). ص. ص 16-19.)

ثالثاً: تداعيات الإرهاب الإلكتروني على الأمن القومي للدول: التهديدات غير التقليدية والإجراءات المضادة

تفاقمت ظاهرة الإرهاب الإلكتروني في الآونة الأخيرة وأثرت سلباً على أمن الدول في مختلف الميادين، حيث تستطيع الجماعات والمنظمات الإرهابية من خلال الضغط على لوحة المفاتيح تدمير البنية المعلوماتية، وتحقيق آثار تدميرية تفوق الآثار التي استخدمت فيها المتفجرات، مما يلحق أضراراً بالمؤسسات المالية، وأجهزة الاتصال والبنى التحتية والمؤسسات الحكومية وغيرها من الكيانات التي تعتمد بشكل كبير على شبكة الانترنت، والذي يؤدي بدوره إلى تعطيل المحركات الرئيسية للدولة والإضرار بمواطنيها وأمنها القومي. ومن تداعيات الإرهاب الإلكتروني على أمن الدول ما يلي:

1- تهديد أمني سياسي: تعمل المنظمات الإرهابية على إلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات، أو قطع شبكات الاتصال بين الوحدات والقيادات المركزية، أو تعطيل أنظمة الدفاع الجوي، أو إخراج الصواريخ عن مسارها. مما يهدد أمن الدول، كما تهدد شخصيات سياسية بارزة في المجتمع بالقتل، أو بالقيام بتفجير منشآت وطنية، أو بنشر فيروسات من أجل إلحاق الضرر والدمار بالشبكات المعلوماتية والأنظمة



## "الإرهاب الإلكتروني والأمن القومي للدول: نمط جديد وتهديدات مختلفة" صليحة محمدي و شفيعة حداد

الإلكترونية، إضافة لاختراق البريد الإلكتروني لرؤساء الدول وكبار الشخصيات السياسية وهتك أسرارهم والإطلاع على معلوماتهم وبياناتهم والتجسس عليها لمعرفة مراسلاتهم ومخاطباتهم والاستفادة منها في عملياتهم الإرهابية، أو تهديدهم لحملهم على إتيان أفعال معينة يخططون لاعتراقها.

مثلا في إيطاليا عام 1998م تعرضت عدة وزارات وجهات حكومية ومؤسسات مالية لهجوم من جماعات الألوية الحمراء عن طريق تدمير مراكز المعلومات الخاصة بها، وفي عام 2010 ظهر ما عُرف باسم "إعصار ويكيليكس" إذ تم استغلال شبكة الإنترنت العالمية في تسريب وثائق تحوي معلومات سرية للغاية مُتداولة بين الإدارة الأمريكية وقنصلياتها الخارجية بدول العالم. وفي مارس 2014 هاجمت مجموعة "سايبير بيركوت" الأوكرانية المواقع الإلكترونية لحلف الناتو، ما أدى إلى تعطيل مواقع الحلف لعدة ساعات. كما أعلن الكرملن أن قرصنة حاسوب شنوا هجوماً "عنيفاً" على موقع الرئاسة الروسية، وعطلوا العمل بموقع البنك المركزي الروسي، وأقر مفتش وحدة الجرائم الإلكترونية الأمريكي في أوت 2014، بأن قرصنة أجنبية تمكنوا من اختراق حاسبات تابعة للهيئة الأمريكية لتنظيم الأنشطة النووية مرتين على الأقل خلال السنوات الثلاث الماضية ومؤخراً أكدت صحيفة نيويورك تايمز في تقرير لها في 26 إبريل 2015 أن قرصنة روسيين اطلعوا على رسائل إلكترونية للرئيس الأمريكي باراك أوباما العام الماضي، بعدما تمكنوا من اختراق الشبكة الإلكترونية غير السرية للبيت الأبيض، واطلعوا على أرشيف الرسائل الإلكترونية لموظفين في البيت الأبيض يتواصلون يومياً مع أوباما، ومن خلال هذا الأرشيف تمكن القرصنة من قراءة رسائل تلقاها أوباما، وهذا ما يهدد الأمن القومي الأمريكي.

أما أمنياً تعمل الجماعات الإرهابية على التسلسل الإلكتروني إلى الأنظمة الأمنية في دولة ما وشلها لصالحها، وفك الشفرات السرية للتحكم بتشغيل منصات إطلاق الصواريخ الإستراتيجية، والأسلحة الفتاكة، وتعطيل مراكز القيادة والسيطرة العسكرية ووسائل الاتصال للجيش بهدف عزلها عن قواتها، والنفوذ إلى النظم العسكرية واستخدامها لتوجيه الجنود إلى نقطة غير آمنة قبل قصفها أو تفجيرها. (بوحداته.س)

### 2- تهديد الاقتصادي:

أصبح لبرامج المعلومات قيمة غير تقليديه لاستخداماتها المتعددة في كافة المجالات الاجتماعية والاقتصادية فهذه القيمة المميزة لبرامج المعلومات تجعلها محلا للتداول، وهنا تبدو أهمية الإنترنت بصفتها مصدر للمعلوماتية، مما أدى إلى ظهور قيمة اقتصادية جديدة وأموال جديدة عرفت بالأموال المعلوماتية وصاحب ظهور هذا المال المعلوماتي جرائم جديدة عرفت بالجرائم المعلوماتية منها

أ- الاعتداء على الأموال الإلكترونية: وهي الأموال المتداولة الكترونياً سواء أكان ذلك في إطار التجارة الإلكترونية أو إلكتروني غيرها، مثل عمليات سحب وإيداع الأموال التي تقوم بواسطة أجهزة الصراف الآلي أو الهاتف المصرفي أو الخدمات المصرفية بواسطة الإنترنت للبنوك، إذ يمكن أن تتعرض هذه الأموال للسرقة والنصب وخيانة الأمانة، وذلك بواسطة بطاقات ائتمان مزورة أو انتهت صلاحيتها أو مسروقة، أو اختراق المواقع الإلكترونية للبنوك، أو اختراق أجهزة الحاسب الآلي للبنوك أو عملاء البنوك... الخ.

ب- التعدي على أموال غيره بالوسائل الإلكترونية مثل: الدخول لمواقع البنوك والدخول لحسابات العملاء وإدخال بيانات أو مسح بيانات بغرض اختلاس الأموال أو تحويلها من حساب لآخر

ج- السطو على أموال البنوك: أصبحت البنوك والمصارف هي هدف لمحترفي التلاعب واختراق شبكات الإنترنت والذين يتلاعبون في كشوف حسابات العملاء ونقل الأرصدة من حساب لآخر وقد تكون بصورة ثانية

## "الإرهاب الإلكتروني والأمن القومي للدول: نمط جديد وتهديدات مختلفة" صليحة محمدي و شفيعة حداد

كإضافة بضعة أرقام أو أصفار إلى رقم ما في هذا الحساب. (بوجلطية بوعلي، أ.، (جوان 2016). ص 186). كما مُنبت عدد من الشركات والمصارف العملاقة بخسائر اقتصادية فادحة نتيجة القرصنة الإلكترونية التي واجهتها. فحسبما أشارت أحدث دراسة أجرتها مؤسسة B2B International وشركة كاسبرسكي لاب، والتي أعلنت عنها في الخامس عشر من أبريل 2015. فإن 25 % من الشركات في منطقة الخليج تعتبر هجمات (DDoS) أحد أكبر ثلاثة تهديدات تواجه الشركات في المنطقة. وباعتبارها أحد أهم التقنيات الشائعة التي يستخدمها مجرمو الإنترنت لكسب الأموال، فإن عدد وتأثير هذه الهجمات يتزايد من عام لآخر، وهو ما جعل قضية حماية المستخدمين أمراً ولوليا لدى الشركات، وقبل السادس من فيفري 2015 أكدت شركة "كاسبرسكي" الرائدة في مجال الأمن المعموماتي أن مجموعة من "الهاكرز" تمكنوا من السيطرة على حسابات في مصارف عالمية، وسرقة نحو مليار دولار، إذ استخدموا تقنيات معقدة من أجل الوصول للحسابات، واستغل "الهاكرز" ثغرة بأنظمة أجهزة الحاسوب في المصارف تمكنوا خلالها من نسخ بيانات الحسابات في مدة لا تتجاوز 20 ثانية واستغلوها من أجل تحويل الأموال بسرعة فائقة. (الإرهاب الإلكتروني... هل يتحول إلى مصدر التهديد الأول في العالم. ) (2015/05/04).

3-تهديد اجتماعي وثقافي : يهدد الإرهاب الإلكتروني حياة الاجتماعية والثقافي للأشخاص ورفاهيتهم كالتالي: - توجه المنظمات الإرهابية رسائلها للإعلام والدعاية الخاص بالمجتمعات التي تقوم بترويعها وإرهابها، وذلك بهدف شن حملات نفسية ضد الدول المستهدفة. وكذلك اختراق صفحة إلكترونية لمستشفى وتهديد حياة المرضى فيه عن طريق التلاعب بأنظمة العلاج عن بُعد بهدف قتل المرضى، وأيضا في مصانع غذاء الأطفال لتغيير مستويات نسب المواد الغذائية بهدف قتل الأطفال. (حسين، أ (2018-01-2).

### رابعا: الإجراءات المضادة للإرهاب :قراءة في أدوات المواجهة

1- الإجراءات السياسية والقانونية : فتح المجال لحرية الرأي والتعبير، وتوفير مبدأ تداول السلطة مما يساعد مختلف القوى على تشكيل أنفسها في منظومة سياسية تعبر عن توجهاته الفكرية. وكذلك قيام بالإصلاحات من شأنها حماية الأجهزة الرقابية من الآفات الخطيرة التي أصبحت تتكاثر بسرعة مذهلة مثل تبييض الأموال وغيرها.

2- الإجراءات الإعلامية: من خلال تجنيد كل وسائل الإعلام في شرح أنماط الإرهاب وأهدافه وما يتركه من آثار وخيمة على البنية التحتية للمجتمع، مما يقلص من الأثر الذي تحدثه المرجعيات الثقافية والدينية التي تعتمد عليها الجماعات الإرهابية في تجنيد الأفراد وتبرير نشاطاتها.

3- الإجراءات الأمنية: والتي تتجسد في تطوير وتحديث النظام المعلوماتي واللوجستي للأجهزة الأمنية مما يمكنها من إحداث الضرر بالجماعات الإرهابية عن طريق إحباط الكثير من العمليات الإرهابية.

4- الإجراءات الاقتصادية والاجتماعية: تحسين نمط المعيشي ورفع مستوى الدخل والقضاء على التهميش والبطالة، حتى لا تنزلق فئات المجتمع في دوامة الجماعات الإرهابية. عادة. ص. (2017). ص 130-131. ويمكن ذكر أهم الأدوات الاقتصادية والاجتماعية في النقاط التالية:

✓ المساواة بين طبقات المجتمع، ومعالجة ظاهري التخلف والبطالة التي تعد من مخلفات الحرمان الاقتصادي وتدايعيات القهر الاجتماعي.

## "الإرهاب الإلكتروني والأمن القومي للدول: نمط جديد وتهديدات مختلفة" صليحة محمدي و شفيعة حداد

- ✓ إعادة توزيع الثروة وتلبية مختلف الحاجات الأساسية للفرد المواطن، على نحو متوازن تجعله يمتلك القدرة على العطاء والبناء والابتعاد عن السلوك والأعمال العدوانية الملائمة لظاهرة الإرهاب، والشكل الذي يوجد حالة من الثقة المتبادلة بين المواطن والسلطة من جهة، وبين المواطن وأفراد المجتمع المحيطين به من جهة أخرى
- ✓ مكافحة عمليات الفساد المالي والإداري والرشوة في جميع مرافق وإدارات الدولة، وبناء قاعدة اقتصادية متطورة تؤمن الحاجات الأساسية والضرورية للمواطن. (عطية. إ. (2015) ص 32).

### الاستنتاجات والتوصيات:

#### أولاً: الاستنتاجات:

- أوضحت الدراسة أن الإرهاب الإلكتروني لا يحتاج إلى أدنى مجهود عضلي، بل يعتمد على الدراسة الذهنية والتفكير العلمي المدروس القائم على معرفة بتقنيات الحاسوب.
- الإرهاب الإلكتروني عابر للحدود؛ لأنه يقع بين أكثر من دولة؛ إذ غالب ما يكون الجاني في بلد والمجني عليه في بلد آخر، وقد يكون الضرر المتحصل في بلد ثالث، ما يؤدي إلى صعوبة إثبات هذا النوع من الإجرام والملاحقة
- القضائية، نظراً إلى ما استحدثته التطور التقني من وسائل جديدة في تطور الإرهاب الإلكتروني، مما صعب في العثور على الدليل المادي التقليدي.

#### ثانياً: التوصيات:

- ضرورة وجود تعاون دولي فاعل في مجال كشف ومكافحة وضبط نشاط الجماعات الإرهابية عبر شبكة الإنترنت، لأن هذا نوع من الإرهاب أصبح ذا صبغة دولية عابرة للمجتمعات والدول.
- ضرورة النفاق الدولي على تحديد طبيعة الإرهاب الإلكتروني وصوره، مع تحديد خطة عملية دولية لمكافحته ضمن صياغة اتفاقية دولية لمكافحة الإرهاب الإلكتروني.
- إجراء المزيد من الدراسات والبحوث للتعرف على حجم واتجاه الإرهاب عبر شبكة الإنترنت وأسبابه، ما يساعد على مزيد من الفهم الدقيق لهذا النوع من الإجرام، ووضع الأسس اللازمة للوقاية والعلاج.
- إنشاء مراكز الدراسات والأبحاث مختصة في الأمن المعلوماتي والبرمجيات بهدف تطوير إستراتيجيات فاعلة لمكافحة الإرهاب الإلكتروني.
- تأمين شبكات المعلومات وأنظمة الاتصال ومصادر الطاقة.
- استحداث مناهج دراسية في كل الأطوار الدراسية بما يساعد الطلبة على الاستخدام الآمن للسحوبات والفضاء الرقمي.
- تنظيم مؤتمرات علمية وندوات تعريفية في الجامعات والمراكز البحثية المتخصصة في مختلف دول العالم تضم الخبراء والباحثين ومن مختلف المجالات لدراسة ظاهرة الإرهاب الإلكتروني ووضع الحلول المناسبة له.
- ضرورة إصدار عدد من القوانين التشريعية الجديدة لتجريم أى استخدام غير آمن لتكنولوجيا المعلومات والاتصالات، بالإضافة إلى التعاون والتنسيق الدائم مع الإنترنت الدولي في مجال تبادل المعلومات والخبرات

## "الإرهاب الإلكتروني والأمن القومي للدول: نمط جديد وتهديدات مختلفة" صليحة محمدي و شفيعة حداد

الأمنية والفنية في رصد ومتابعة كافة الأنشطة الإجرامية والإرهابية، خاصة فيما يتعلق بالنشاط الإرهابي التكنولوجي لتزايد المستمر وارتباط هذا النشاط بشبكة المعلومات الدولية.

قائمة المراجع:

أولاً: المراجع باللغة العربية

أ- الكتب:

- 1- أحمد، ف، ع. (2006). مستقبل الإرهاب في هذا القرن. الرياض: جامعة نايف العربية للعلوم الأمنية
- 2- غادة، ص. (2017). الإرهاب والجريمة الإلكترونية. مصر: العربي للنشر والتوزيع.
- 3- الهاشمي، ر، ع. (2018). الإرهاب الإلكتروني القانوني. الأردن: دار أمجد للنشر والتوزيع
- 4- يوسف كافي، م. (2011). إدارة الإلكترونية: إدارة بلا أوراق، إدارة بلا مكان، إدارة بلا زمان. دمشق: دار مؤسسة رسلان للطباعة والنشر والتوزيع.

ب- المقالات:

- 1- أيسر، م، ع، "دور الآليات الحديثة للحد من الجرائم المستحدثة وطرق مواجهته". محاضرة أقيمت بملتقى دولي بعنوان الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، أيام 02-04/09/2014
- 2- أحمددي بوجلطية، ب. ( جوان 2016). الإرهاب الإلكتروني وطرق مواجهته على المستوى العربي، دراسة للتجربتين السعودية والقطرية، الأكاديمية للدراسات الاجتماعية والإنسانية. أ/ قسم العلوم الاقتصادية والقانونية. (16). 179-190
- 3- عبد المعطي، ز، ( 2016-02-09 ) الأمن القومي: قراءة في المفهوم والأبعاد. مصر: المعهد المصري للدراسات السياسية والإستراتيجية.
- 4- عبدالله، ع، اع، ف، العجلان، "الإرهاب الإلكتروني في عصر المعلومات" بحث مقدم إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت"، القاهرة في 2-4 جوان 2008 .
- 5- عطية، إ، ط. (2015). الظاهرة الإرهابية في زمن ما بعد الحداثة -دراسة تحليلية في الأشكال والأساليب والإجراءات المضادة. المجلة العربية للدراسات الأمنية والتدريب . (31) (3-42).
- 6- كازيز، ص . كزيز، أ. (2018). الإرهاب الإلكتروني وانعكاساته على الأمن الاجتماعي – دراسة تحليلية. مجلة الراث. (08) (01). 312-328.
- الشهري، ح، أ. (جانفي 2015). الإرهاب الإلكتروني- حرب الشبكات . المجلة العربية الدولية للمعلوماتية (4) (8). 1-23.

ج- مذكرات وأطروحات:

- 1- منصور، م، ذ. (2011) مفهوم الأمن القومي في ظل العولمة، رسالة ماجستير في الدراسات الدولية. فلسطين: جامعة بنزت .

د- الروابط الإلكترونية:

- 1- الإرهاب الإلكتروني... هل يتحول إلى مصدر التهديد الأول في العالم. (2015/05/04). تم تصفح المقال بتاريخ 2019-05-22. على الرابط التالي:

<http://alkhaleejonline.net/articles/1430728333185670700>

- 2- بوحادة، س. أثر الإرهاب الإلكتروني على أمن واستقرار الدول. تم تصفح المقال بتاريخ 2019-05-23 على الرابط التالي:

"الإرهاب الإلكتروني والأمن القومي للدول: نمط جديد وتهديدات مختلفة" صليحة محمدي و شفيعة حداد

<https://manifest.univ-ouargla.dz>

3- حسين. أ. (14-01-2017). الإرهاب الإلكتروني أخطر معارك حروب الفضاء. تم تصفح المقال بتاريخ 15-07-2018. على الرابط التالي:

<http://alwatan.com/details/166324>

4- عبد الرحمن بن عبد الله، س. (2009). سائل الإرهاب الإلكتروني حكمها في الإسلام وطرق مكافحتها. تم تصفح المقال بتاريخ 21-05-2019 على الرابط:

<http://shamela.ws/index.php/book/1244>

5- المركز العربي الديمقراطي. (جوان 2016). أثر الارهاب الإلكتروني على تغير مفهوم القوة في العلاقات الدولية . تم تصفح المقال بتاريخ 12-09-2018 على الرابط التالي: "دراسة حالة: تنظيم "الدولة الإسلامية

<https://democraticac.de/?p=34528>.

6- محمد، ع،، ع، ح. (13-09-2017). مفهوم الأمن القومي وتحديد أبعاده، المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات، تم تصفح المقال بتاريخ 12-04-2018. على الرابط التالي:

<https://www.europarabct.com>

ثانيا: المراجع باللغة الأجنبية:

1. Charles .W. C. R.,( 1994)The economic Dimensions o National Security", RAND .