2022

الإرهاب الإلكتروني والأمن القومي
في ظل جائحة كورونا (كوفيد-19)

وفاء لطفي حسين عبد الواحد

مدرس العلوم السياسية

كلية الاقتصاد والإدارة – جامعة 6 أكتوبر

ملخص

أصبحت ظاهرة الإرهاب الإلكتروني منذ وقت مبكر حقلاً للدراسة والبحث، واستطاعت العديد من الدول أن تراكم كماً علمياً ومعرفياً عن أسباب الإرهاب الإلكتروني، وتتّضح خطورة الإرهاب الإلكتروني من خلال النظر إلى حجم التهديدات التي يفرضها على الأمن القومي للدول وأكثر التهديدات التي زاد خطرها بشكل مطرد مع التقدم التكنولوجي والتقني، هي طريقة إدارة الإرهاب أكثر، حيث صار من الممكن تدمير البنى التحتية للدول دون إطلاق رصاصة من خلال استخدام الجماعات الإرهابية للفضاء الإلكتروني لشن هجمات إرهابية باستخدام بعض البرامج المعقدة، ومن ثم أصبحت أعمال الإرهابيين أكثر خطورة وتدميرًا، بينما أصبح مرتكبو هذه الأعمال أكثر مراوغة.

وعليه، ترصد هذه الورقة بالتحليل ظاهرة الإرهاب الإلكتروني عبر الإنترنت في ظل أزمة كورونا وتلقي مزيدًا من الضوء على المجال الافتراضي بوصفه ساحة قتال جديدة باتت تشكل تهديداً يضاف إلى قائمة التهديدات التقليدية التي تواجه العالم، وتتجاوز في أبعادها وآثارها الحدود الجغرافيَة والسياسية، وتلقي بتداعياتها على مستقبل الأمن القومي والحيوي للدول.

الكلمات الدالة: الإرهاب الإلكتروني، الأمن القومي، جائحة كورونا (كوفيد 19)، الدولة.

Abstract

The phenomenon of electronic terrorism has become from an early age a field of study and research, and many countries have been able to accumulate a scientific and knowledgeable amount about the causes of electronic terrorism. And the technical is the way to manage terrorism more, as it became possible to destroy the infrastructure of countries without firing a bullet through the use of cyberspace by terrorist groups to launch terrorist attacks using some complex programs, and then the terrorists' actions became more dangerous and destructive, while the perpetrators of these acts became more elusive.

Accordingly, this paper analyzes the phenomenon of electronic terrorism via the Internet in light of the Corona crisis and sheds more light on the virtual field as a new battlefield that has become a threat added to the list

of traditional threats facing the world, and its dimensions and effects exceed geographical and political borders and have repercussions on the future of the national and vital security of states.

Key words: Cyber terrorism, national security of countries, Corona virus (Covid 19), the state.

مقدمة

ظهرت في القرن العشرين مجموعة من التحولات أفرزتها معطيات الثورة التكنولوجية الهائلة التي ساهمت في نقل المجتمعات التقليدية إلى مجتمعات حديثة ذكية تقوم على التكنولوجيا المتطورة، كما أدت هذه الأخيرة إلى ظهور مفاهيم جديدة في العلاقات الدولية أهمها مفهوم الإرهاب الإلكتروني كتهديد أمني جديد للدولة والمجتمعات عابر للحدود يقوم على استخدام التقنيات الحديثة لشن هجمات إرهابية بهدف نشر الخوف والرعب.

وقد ازداد خطر الإرهاب الإلكتروني؛ نتيجة لاستخدام الدولة للتكنولوجيا المتطورة في مختلف الميادين، بهدف تحقيق الرخاء والتقدم البشري، لكن الجماعات الإرهابية استغلت الظروف وبدأت تشن هجمات على مختلف القطاعات: السياسية، الاقتصادية، العسكرية والاجتماعية من خلال اختراقها للمواقع الإلكترونية لرؤساء الدول والحكومات والوزارات والتجسس عليها وتدميرها، والاطلاع على مختلف المعلومات الأساسية للدولة خاصة الأمنية منها، إضافة إلى المؤسسات الاقتصادية كالبنوك والبورصات العالمية.

الأمر الذي أثر سلباً على الأمن الاقتصادي للدولة، فلم تقتصر الهجمات على الجوانب السياسية والأمنية والاقتصادية فقط، بل أيضاً الجوانب الاجتماعية والثقافية وتدمير مواقع المستشفيات ومصانع توليد الطاقة: الكهرباء، الماء، الغاز، فضلا عن نشر ثقافة التطرف الديني في أوساط الشباب ومحاولة طمس الهوية واجتذابهم إلى المنظمات الإرهابية؛ ما يهدد الأمن الاجتماعي للدولة.

وعلى الرغم من أن أزمة كورونا (كوفيد 19) فرضت تحديات كثيرة على الدول من قبيل سبل التعامل مع العدوى وآليات الوقاية والعلاج، إلا أن ذلك لم يمنع الدول والتنظيمات المتطرفة عن ممارسة الأعمال الإرهابية. فقد فرض تحدياً أمنياً مرتبطاً بالإرهاب الإلكتروني، حيث شهدت العديد من دول العالم هجمات إلكترونية شكلت تهديدا لأمن واستقرار الدول. إذ قامت العديد من التنظيمات

المتطرفة في استخدام الإنترنت في بث خطابات الكراهية ونشر الآراء المتطرفة. إذ تشير المعطيات إلى أن الجماعات الإرهابية استغلت المزايا التكنولوجية كعنصر حيوي لدعم وتحقيق أهدافها، ومنفذ لوجستي داعم للنشاط الإعلامي لها في مناطق مختلفة من العالم.

من هذا المنطلق، تحاول هذه الدراسة أن ترصد بالتحليل تأثير ظاهرة الإرهاب الإلكتروني على الأمن القومي في ظل جائحة كورونا وتلقي مزيدًا من الضوء على المجال الافتراضي بوصفه ساحة قتال جديدة باتت تشكل تهديدا يضاف إلى قائمة التهديدات التقليدية التي تواجه العالم، وتتجاوز في أبعادها وآثارها الحدود الجغرافيَة والسياسية، وتلقي بتداعياتها على مستقبل الأمن القومي والحيوي للدول.

المشكلة البحثية

تكمن المشكلة البحثية في تحديد الأسلوب المتبع لتعريف الإرهاب الإلكتروني وكذا الأمن القومي. فمن ناحية تُعد ظاهرة الإرهاب الإلكتروني من أخطر الظواهر التي تواجه الدول لما لها من تداعيات خطيرة على الأمن القومي، فقد انتشرت مؤخَّرًا نوعية خطيرة من الهجمات والجرائم الإلكترونية تعتمد على تقنيات متقدمة تدمر البنية التحتية والحيوية للدول. ومن ناحية أخرى تعتبر جائحة كورونا من أبرز التحديات التي تواجه العديد من الدول لما لها من تأثير خطير على جميع الأصعدة، فقد أبدت التيارات الإرهابية بمختلف أيديولوجياتها قدرات ملحوظة على التأقلم السريع مع تلك التغيرات الناجمة وتوظيف الجائحة كأداة لتحقيق أهدافها.

وعليه، يمكن طرح السؤال الرئيسي للبحث على النحو التالي: ما أثر الإرهاب الإلكتروني على الأمن القومي؟ وما تداعيات جائحة كورونا على الإرهاب الإلكتروني؟

وينبثق عن هذا السؤال بعض الأسئلة الفرعية على النحو التالي:

1. ما تعريف الإرهاب الإلكتروني؟
2. ما مفهوم الأمن القومي؟ وما أبعاد الأمن القومي؟
3. ما تداعيات الإرهاب الإلكتروني على الأمن القومي؟
4. ما تداعيات فيروس كورونا على الإرهاب الإلكتروني؟
5. كيف تستغل الجماعات الإرهابية جائحة كورونا؟
6. ما الجهود الدولية في مكافحة جرائم الإرهاب الإلكتروني؟

أهمية الدراسة

تكتسي ظاهرة الإرهاب الإلكتروني أهمية بالغة بسبب ما ينجم عنه من مخاطر وخسائر بوصفه اعتداءً سافراً على الأفراد، وتهديدا ظاهرا على الأمن القومي للدول واستقرار المجتمع وتماسكه، فالنمو السريع في انتشار تكنولوجيا المعلومات والتطور التكنولوجي –مثل إنترنت الأشياء، والحوسبة السحابية والذكاء الاصطناعي وخدمات من قبيل برنامج حماية الخصوصية "أونيون روتر"، والشبكة الخفية– فتح مجالاً حيوياً للأنشطة التي تقودها الجماعات الإرهابية.

فرضية الدراسة

تنطلق الدراسة من فرضية تتناول تأثير الإرهاب الإلكتروني على الأمن القومي في ظل جائحة كورونا، اعتمادا على رؤية مفادها أن ظاهرة الإرهاب الإلكتروني من أخطر الظواهر الذي يشهدها العالم المعاصر، نظراً لما تتسم به هذه الظاهرة من القدرة على توظيف التكنولوجيا في اختراق أنظمة المعلومات للدول وتدمير البنى التحتية والحيوية، هذا بالإضافة إلى سعي الجماعات الإرهابية للاستفادة من التقنيات الحديثة واستخدام الشبكات المعلوماتية في اختراق المواقع العسكرية والمدنية بالدولة.

تقسيم الدراسة

تُقسم الدراسة إلى أربعة محاور وهي كالتالي:

المحور الأول: يتناول التأصيل النظري لمفاهيم الدراسة، والذي يتناول تعريف الإرهاب الإلكتروني، وآلياته وأدواته.

المحور الثاني: ويتحدث عن تداعيات الإرهاب الإلكتروني على الأمن القومي، وتناول مفهوم الأمن القومي، والتمييز بين مفهوم الأمن القومي وبعض المفاهيم المشابهة له، وأبعاد الأمن القومي، وتهديدات الإرهاب الإلكتروني على الأمن القومي.

المحور الثالث: تداعيات جائحة كورونا على الإرهاب الإلكتروني، وتناول الكيفية التي استغلت بها الجماعات الإرهابية جائحة كورونا، والجهود الدولية في مكافحة الإرهاب الإلكتروني.

المحور الأول

التأصيل النظري لمفاهيم الدراسة

أولًا: مفهوم الإرهاب الإلكتروني

الإرهاب ظاهرة عالمية، قديمة حديثة، لا دين له ولا وطن له، تتغير أشكاله وأساليبه بتغير الزمان والمكان، ولكنه يظل دائماً مرتبطا بالإنسان أياً كان عقيدته أو مذهبه الفكرى، لقد أصبح الإرهاب واقعنا الأليم الذي نعانيه كأفراد ومؤسسات ودول، وتحاول الدول بقدر الإمكان أن تعمل على اقتلاع هذه الظاهرة من جذورها، ولقد تعددت وسائل الإرهاب وأثبت الإرهابيون قدرتهم على استخدام كل وسائل العلم الحديث لتحقيق أهدافهم.

"الإرهاب في الأساس هو إنكار لحقوق الإنسان وتدمير لها، والحرب ضد الإرهاب لن تنجح أبدا بإدامة الإنكار والتدمير نفسه. يجب أن نحارب الإرهاب بلا هوادة لحماية حقوق الإنسان. وفي الوقت نفسه عندما نحمي حقوق الإنسان، فإننا نعالج الأسباب الجذرية للإرهاب". (الأمم المتحدة، news.UN.org)

- **الإرهاب في اللغة:** الإرهاب كلمة مشتقة من الفعل رهب بمعنى خاف وكلمة الإرهاب هي مصدر الفعل أرهب وأرهبه بمعنى خوَّفه. (أحمد الصياد، 2002، 14)
- **الموسوعة السياسية تعرف الإرهاب:** "استخدام العنف غير القانوني، أو التهديد به بأشكاله المختلفة مثل الاغتيال والتشويه والتعذيب والتخريب والنسف، بغية تحقيق هدف سياسي معين مثل كسر روح المقاومة والالتزام عند الأفراد وهدم المعنويات عند الهيئات والمؤسسات، أو كوسيلة من وسائل الحصول على المعلومات أو مال، وبشكل عام هو استخدام الإكراه لإخضاع طرف مناوئ لمشيئة الجهة الإرهابية". (الكيالي، 1994، ص 153)
- **الإرهاب في المعجم السياسي:** "محاولة نشر الذعر والفزع لأغراض سياسية، وهو وسيلة تستخدمها حكومة استبدادية أو دكتاتورية لإجبار وإرغام الشعب على الاستسلام لها. (زيتون، 2006، ص 21)
- **الإرهاب دولياً:** اعتداء يصل إلى حد العمل الإجرامي، ولكن المستهدف من هذا الإرهاب هو الذي يحدد إذا كان هذا العمل جريمة سياسية أو جريمة إرهابية. وتجدر الإشارة أن الإرهاب

الدولي ركنان: الأول مادي يتمثل في العنف المستخدم والموجه ضد شخص، ومعنوي مجموعة من الأشخاص أو الرهائن أو المنشآت أو الممتلكات. أما الركن المعنوي في توافر قصد العنف لتخويف المستهدفين بذلك العنف وترويعهم وإرهابهم. (مصطفى علوي،2005)

- **تعريف علم الاجتماع السياسي للإرهاب:** هو كل تصرف أو سلوك بشرى ينزع إلى استخدام القوة والإكراه والاستخدام غير المشروع للسلاح بهدف تحقيق غايات في شتى المجالات: "السياسية- الاقتصادية- الاجتماعية" وقد يطال هذا الإرهاب آخرين غير مستهدفين. وفى النهاية قد يكون الإرهاب فعلاً أو رد فعل، وفى الحالتين هو يستهدف أفراد جماعة معينة أو أشخاصا بعينهم بهدف إيقاع الرعب والفزع فى نفوسهم. (المركز الديمقراطي العربي، 2016)
- **الإرهاب في اتفاقية جنيف 1937** نجدها تتحدث عن الإرهاب باعتباره نوعاً واحداً، وهو الإرهاب الفردي الموجه ضد الدولة وحددت جرائم معينة تعتبرها إرهاباً، وعرفت الإرهاب بأنه: "الأعمال الإجرامية الموجهة ضد الدولة والتى يكون من شأنها إثارة الفزع والرعب بين الأفراد". (المكتبة الرقمية العالمية، 11579)
- **الإرهاب عند "بريان جنكيز":** هو "مجموعة أفعال معينة يقصد بها إحداث رعب وخوف"، ولكن مفهوم الإرهاب لا يجب أن يتوقف عند الإرهاب الذي يمارسه الأفراد وإنما لابد من التوسع في المفهوم حتى نصل إلى الإرهاب الذي تمارسه الدول.
- **الإرهاب في قانون العقوبات المصرى رقم 97 لسنة 1992:** هو استخدام القوة، أو العنف، أو التهديد، أو الترويع ويلجأ إليه الجاني تنفيذاً لمشروع وإجرام فردى أو جماعي بهدف الإخلال بالنظام العام وتعريض سلامة المجتمع وأمنه للخطر. (نهاد سمير، 2013، 46288).

ثانيًا: تعريف الإرهاب الإلكتروني

بالرغم أن الإرهاب السيبراني لا يزال ظاهرة وليدة إلا أنه يشكل تهديدًا كبيرًا ومتزايدًا للمجتمع الحديث، وتجدر الإشارة إلى أنه لم يتم التوصل لمفهوم محدد للإرهاب وبالتالي لم يتم الوصول إلى مفهوم محدد ودقيق للإرهاب الإلكتروني نظراً لانتشار الحواسب الآلية وتنوع الأهداف والوسائل والأشخاص وسوف نعرض لعدد من المفاهيم كما يلي: (المرصد المصري، 2021)

- **تعريف "دينينج"**

يعبر عن التقاء الإرهاب وعالم الكمبيوتر وأنه الاستخدام غير المشروع للقوة والتهديدات بضرب أجهزة الكمبيوتر والشبكات والمعلومات المختزنة فيها من أجل ترويع وإكراه الحكومات وشعوبها من أجل تحقيق أهداف سياسية واجتماعية، ولكي يعتبر ذلك إرهاباً فلابد أن يؤدى إلى ترويع وإكراه الحكومات والأشخاص والممتلكات، أو على الأقل التسبب في الضرر والخوف، وكذلك إيذاء بدني وانفجار وأضرار اقتصادية جسيمة والهجوم على البنية الأساسية وإعاقة عمل الخدمات الأساسية. (بكر أبو بكر، 2018)

- **تعريف وزارة الدفاع الأمريكية**

عمل إجرامي يتم الإعداد له باستخدام الحاسبات ووسائل الاتصالات وينتج عنه عنف وتدمير أو بث الخوف تجاه متلقي الخدمات بما يسبب الارتباك وعدم اليقين؛ وذلك بهدف التأثير على الحكومة أو السكان لكي تمتثل لأجندة سياسية أو اجتماعية أو فكرية معينة.

وعرفه جيمس لويس James Lewiss على أنه: "استخدام أدوات شبكات الحاسوب في تدمير أو تعطيل البنى التحتية الوطنية المهمة مثل: الطاقة والنقل، أو بهدف ترهيب الحكومة والمدنيين". (ريهام عبد الرحمن، 2021)

هناك تداخل بين مفهوم الإرهاب الإلكترونى وبين عدد من المفاهيم الأخرى سنتعرض لها بإيجاز وهي:

- **الفضاء الإلكتروني**

يقصد به الفضاء الذي أوجدته تكنولوجيا المعلومات والاتصالات، وفي مقدمتها الإنترنت ويرتبط هذا الفضاء ارتباطاً وثيقاً بالعالم المادي، عبر البنى التحتية المختلفة للاتصالات، والأنظمة المعلوماتية، وعبر العديد من الخدمات، التي لم يكن بالإمكان الحصول عليها، من دونه، بما في ذلك الوصول إلى البيانات والمعلومات. (جامعة الدول العربية، ص16)

- **الصراع**

يشيع تداول اصطلاح الصراع في كل مجالات الحياة، حيث إنه يعد سمة لكل المجتمعات البشرية، فضلا عن أنه سمة غالبة يفرضها واقع الحياة المتغيرة، إذ إننا لا نجد مجتمعاً يخلو من صراع بغض النظر عن طبيعة هذا المجتمع أو نوع ذلك الصراع. (محمد علام،2014، ص70)

- **الصراع الإلكتروني**

اتخذ الصراع الإلكتروني أدوات وأشكالاً جديدة في عصر الثورة المعلوماتية، ومثل الفضاء الإلكتروني ساحة لنقل الصراعات من خلاله أو استخدامه كوسيلة من وسائل الصراع، وبالتالي فالصراع الإلكتروني هو الذي يمكن أن ينشب في بيئة الفضاء الإلكتروني، ويمتد الصراع عبر الفضاء الإلكتروني إلى شتى المجالات، ويتجاوز الصراع الإلكتروني الحدود التقليدية وسيادة الدول وذلك يؤثر على امتداد الصراع ونطاقه ومن ثم تفاقم تداعياته وآثاره. (عبد الصادق، 2018، ص42)

- **الجريمة الإلكترونية**

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. (البشيري، 2005، 6)

- **التجسس الإلكتروني**

هو التلصص وسرقة المعلومات من الأفراد، أو المؤسسات، أو الدول، أو المنظمات، والتجسس على هذه المعلومات أياً كان نوعها يأخذ أبعاداً جديدة، فتعددت أهدافه من معلومات شخصية إلى معلومات اقتصادية وسياسية وعسكرية. (بشير، 2012، 92)

ثالثًا: آليات الإرهاب الإلكتروني

- **البريد الإلكتروني**

يعتبر البريد الإلكتروني من أهم الخدمات التي تقدمها شبكة الإنترنت، كصندوق للبريد بحيث يستطيع المستخدم إرسال الرسائل الإلكترونية إلى شخص أو عدة أشخاص من مستخدمي الإنترنت، فهو يسمح بتبادل الرسائل والمعلومات مع الآخرين عبر شبكة للمعلومات، تتميز بالسرعة في إيصال الرسالة وسهولة الاطلاع عليها في أي مكان، فهي لا ترتبط بمكان معين. (عطوة الزنط، 2010، ص3)

ونتيجة لذلك تعد من أبرز وسائل الإرهاب الإلكتروني من خلال استخدام البريد الإلكتروني في التواصل بين الإرهابيين وتبادل المعلومات بينهم، بل إن كثيرًا من العمليات الإرهابية التي حدثت في الآونة الأخيرة كان البريد الإلكتروني فيها وسيلة من وسائل تبادل المعلومات وتناقلها بين القائمين بالعمليات الإرهابية والمخططين لها. (إبراهيم، 2008، ص19)

- **إنشاء مواقع على الإنترنت**

يعرف الموقع بأنه: "مجموعة مصادر للمعلومات متضمنة في وثائق متمركزة في الحاسبات والشبكات حول العالم"، كما عرفه أيضاً بأنه "مجموعة صفحات إلكترونية مرتبطة مع بعضها البعض يمكن مشاهدتها والتفاعل معها عبر برامج حاسوبية تدعى المتصفحات. كما يمكن عرضها بواسطة الهواتف النقالة عبر تقنية نظام التطبيقات الكلاسيكية وهذه الصفحات موجودة فيما يسمى بالخادم". (محمد أل زيران، 2011، ص1)

فالمواقع الإلكترونية سهلت على المنظمات الإرهابية توسيع أنشطتها لأبعد الحدود من خلال تبادل الآراء والأفكار والمعلومات، إذ يمكن أن يلتقي عدة أشخاص في أماكن متعددة في وقت واحد، كما ساعدتهم أيضاً 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 مثل قنوات التليفزيون والإذاعة صعباً، فإن إنشاء مواقع على الإنترنت، واستغلال منتديات الحوار وغيرها لخدمة أهداف الإرهابيين غدا سهلًا ممكنًا، 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. (عطية، 2014، ص16)

- **اختراق الموقع**

تتم عملية الاختراق الإلكتروني عن طريق تسريب البيانات الرئيسة والرموز الخاصة ببرامج شبكة الإنترنت، وهي عملية تتم من أي مكان في العالم دون الحاجة إلى وجود الشخص المخترق في الدولة التي اخترقت فيها المواقع، فالبعد الجغرافي لا أهمية له في الحد من الاختراقات الإلكترونية ولا تزال نسبة كبيرة من الاختراقات لم تكتشف بعد بسبب التعقيد الذي يتصف به نظام تشغيل الحاسب الآلي. أما تدمير المواقع فهو الدخول غير المشروع على نقطة ارتباط أساسية أو فرعية متصلة بالإنترنت من خلال نظام آلي أو مجموعة نظم مترابطة شَبَكِيًّا بهدف تخريب نقطة الاتصال أو النظام.

رابعًا: أدوات الإرهاب الإلكتروني

يتم استخدام الفضاء الإلكتروني في الإرهاب بصورة غير مباشرة عن طريق تسهيل عملية تنفيذ العمل الإرهابي من خلال توفير المعلومات والحصول على التمويل، وكذلك يتم استخدامه لنشر الخوف والفزع والرعب وبث الكراهية، أو عن طريق استخدام أدوات ذات طابع إلكتروني في الصراع

ويكون الفضاء الإلكتروني هو مسرح ذلك الصراع، وهذه الأدوات يصعب الفصل بينها بمعنى أنه قد يتم استخدام كل هذه الأدوات في عملية واحده ويصعب الفصل بين الأدوات المستخدمة فيها وسوف نتعرض تفصيلا لهذه الآليات كما يلي:

- **اختراق المواقع الإلكترونية**

يتم اختراق المواقع الإلكترونية لتغيير محتوياتها أو سرقة معلومات سرية أو تعطيل الموقع عن العمل والسيطرة عليه بشكل كامل، وبعد نجاح اختراق الموقع يضع المهاجمون رسائل في الموقع تعلن اختراقه وكأنه بمثابة رفع راية النصر.

- **الفيروسات**

فيروسات الحاسب الآلي تنتشر بسرعة كبيرة عن طريق شبكة الإنترنت، وذلك يرجع إلى عدد الملفات الهائل التي يتم تبادلها بين مستخدمي الشبكة العنكبوتية، وهذه الفيروسات هى عبارة عن برامج تستنسخ نفسها في الجهاز وعندما تنشط هذه الفيروسات تحدث تغييرات في البرامج أو في البيئة التي تعمل فيها ولها أضرار مختلفة تتمثل في فقد الملفات المخزنة وقد تصل تلك الأضرار إلى تحطم نظام التشغيل في الجهاز. (مهران، 2013، ص 118)

- **الحرب الإعلامية**

للفضاء الإلكتروني تأثير كبير على الرأي العام، إذ إنه يخاطب الملايين من مستخدمي الشبكة العنكبوتية في شتى دول العالم بوسائل مختلفة كالصوت أو الصورة أو النص، وبالتالي أي جماعة أو منظمة يمكن لها إنشاء مواقع إلكترونية نشر الأفكار، أو المعلومات، أو الشائعات التي من شأنها إلحاق الضرر بالدول. (Vladimir,2008,3)

- **التجسس الإلكتروني**

التجسس الإلكتروني في أبسط معانيه هو عبارة عن عدة طرق تتمركز على التقنية التكنولوجية البرمجية للحصول على المعلومات غير المعلنة. (Cyber one,2021)

يعتبر التجسس الإلكتروني أحد أبرز التهديدات الأمنية الحديثة التي تتعرض لها الحكومات والمواطنون، ومع التطور التكنولوجي تضاعفت عمليات التجسس الحاصل في خوادم الإنترنت.

وقد نجحت العديد من الحكومات في استخدام تقنيات متطورة للتجسس من خلال الشبكة العنكبوتية على الدول أو المنظمات ومراقبة المعلومات التي يتم تداولها عالميا. (المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات، 2020)

- **التهديد الإلكتروني**

نتج عن التطور والتقدم العلمي والتقني في مجال الاتصالات وتكنولوجيا المعلومات وشبكة الإنترنت أنماط مستحدثة من التهديدات مثل التهديدات المرتبطة باغتيال شخصيات سياسية، تهديدات بتفجيرات في مراكز سياسية أو هيئات حكومية، أو التهديد بإطلاق الفيروسات التي من شأنها تدمير أنظمة المعلومات، وعليه لابد من التوعية والتطرق للأفعال التي تعرّض من يرتكبها للمُساءلة القانونية وتطبيق العقوبة التي تتناسب مع جسامة الفعل المرتكب. (هيئة تنظيم الاتصالات والحكومة الرقمية، 2021)

المحور الثاني

تداعيات الإرهاب الإلكتروني على الأمن القومي

يعتبر الإرهاب الإلكتروني تهديداً لأمن واستقرار الدول؛ وذلك نتيجة لاستخدام الدول للتكنولوجيا المتطورة في البنية التحتية وتطوير المؤسسات الرسمية وغير الرسمية وجعلها إلكترونية، فهذا ما سهل على الجماعات الإرهابية اختراق هذه المواقع وتهديدها ونشر الرعب والخوف لتحقيق أهدافها، باستخدام الإنترنت، للاتصال والتلقين وكسب أكبر عدد ممكن من المتعاطفين معهم. فسنحاول في هذا المحور التطرق إلى نقطتين أساسيتين: استخدام الجماعات الإرهابية للإنترنت، وأثر ذلك على أمن الدول.

أولًا: ضبط مفهوم الأمن القومي

الأمن في اللغة هو نقيض الخوف. والفعل الثلاثي أمِن أي حقق الأمان. قال ابن منظور: "أمنت فأنا آمن، وأمنت غيري أي ضد أخفته، فالأمن ضد الخوف، والأمانة ضد الخيانة، والإيمان ضد الكفر، والإيمان بمعنى التصديق، وضده التكذيب، فيقال آمن به قوم وكذب به قوم. (ابن منظور، 2014، 140)

تعرف الموسوعة السياسية الأمن القومي على أنه "تأمين سلامة الدولة ضد أخطار خارجية وداخلية قد تؤدي بها إلى الوقوع تحت سيطرة أجنبية نتيجة ضغوط خارجية أو انهيار داخلي". (السياسة، 1990، 331)

وتعرفه الموسوعة العالمية للعلوم الاجتماعية على أنه "قدرة الأمة على حماية قيمها الداخلية من التهديدات الخارجية بدفع العدوان عن الدولة وضمان استقلالها". (سعيد، 2006، ص35)

فيما **يعرفه قاموس وزارة الدفاع الأمريكية على** أنه "مصطلح جماعي يشمل كلا من الدفاع الوطني والعلاقات الخارجية بغرض كسب ميزة وأفضلية دفاعية (عسكرية)، أعلى من أي دولة أجنبية أو مجموعة دول، علاقات خارجية مواتية، وضعية دفاعية قادرة بنجاح على مقاومة أي عمل عدائي أو مدمر من الداخل أو الخارج، علني أو سري". (Joint Publication, 2010, 211)

يعرف تريجر وكرنبرج الأمن القومي بأنه "ذلك الجزء من سياسة الحكومة الذي يستهدف خلق الظروف المواتية لحماية القيم الحيوية". (Frank Trager, 1973, 35-36)

التمييز بين مفهوم الأمن القومي وبعض المفاهيم المشابهة له

يُعد مفهوما المصلحة القومية والإستراتيجية القومية من أكثر المفاهيم التي يتم الخلط بينها وبين مفهوم الأمن القومي ولذلك يسعى الجزء التالي من الدراسة إلى وضع حدود بين مفهوم الأمن القومي ومفهومي المصلحة القومية والإستراتيجية القومية.

الأمن القومي والمصلحة القومية

تُستخدم المصلحة القومية كأداة تحليلية لوصف وشرح وتقويم مصادر السياسة الخارجية للدولة، ومدى كفاءتها. ويتم توظيف المصلحة القومية كأداة للعمل السياسي في تبرير أو استنكار أو اقتراح سياسة ما. وغالباً ما يتم الربط بين المصلحة القومية والقوة، والنظر إلى المصلحة القومية على أنها هي التي تقرر السياسة الخارجية، وذلك أن تلك السياسة يتم رسمها بهدف تعزيز المصالح القومية وليس فقط مصالح كل فرد على حدة. (Keith Krause, 1987)

إن المصلحة القومية، وفقاً لما سبق، هي الأوضاع التي ترى الدولة في وجودها واستمرارها ما يحقق أهدافها، وهي تتضمن الحفاظ على قيم الدولة وصيانة استقلالها وكيانها وحرياتها في علاقاتها الخارجية ودعم هيمنتها الاقتصادية. وغالباً ما تستخدم الدولة هذا المفهوم في محاولتها للتأثير على البيئة الدولية لصالحها.

كما أن هناك من يرفض قبول مفهوم المصلحة القومية كأداة تحليلية في مجال السياسة الخارجية على أساس ضخامة المفهوم وافتقاره إلى التحديد الكلي والتصنيف الجزئي لمكوناته، بالإضافة إلى غياب الوسائل الإجرائية لتجسيد المفهوم بعد تحديده. كما أن ارتباط المفهوم بالقيم يجعله كياناً أضخم من مكوناته. (Keith Krause,1987)

الأمن القومي والإستراتيجية القومية

المقصود بالإستراتيجية أساساً فن القيادة، وهي مفهوم عسكري أساساً تطور وأصبحت له مضامين سياسية واجتماعية، فصارت الإستراتيجية هي تلك العملية التي يتم فيها الصهر الكامل لكل مصادر القوة في الجسد السياسي والاقتصادي والاجتماعي للدولة من أجل تحقيق المصلحة القومية العليا، والأهداف المطلوب إنجازها في إطار فلسفة الأمن القومي.

يصعب تحديد كيفية تشكيل الإستراتيجية القومية وتنفيذها. وتتبع المصالح القومية من التفاعل بين القيم والبيئتين المحلية والدولية. (Daniel J. Kaufman, 1985, 15)

ثانيًا: أبعاد الأمن القومي

- **البعد السياسي**

من أهم عوامل التهديد ذات الطبيعة السياسية فصل الدولة أو تجميد عضويتها في المنظمات السياسية الدولية وقطع العلاقات الدبلوماسية مع دول ذات أهمية دولية وفرض العقوبات الرادعة على الدولة ووجود أحلاف وتكتلات تتعارض ومصلحة الدولة، على أن أخطر المؤشرات هي عمليات التجسس وهي عبارة عن محاولات للحصول بطريقة سرية أو بوسائل التزييف على معلومات حكومية ما لصالح حكومة أخرى. وبعبارة أخرى هي تلك الجهود التي تضطلع بها أجهزة مخابرات الدولة، بهدف التفتيش السري على جهود الدولة الأخرى للتأكد من حقيقة قوتها، وتحركها وخططها المستقبلية.

وقد اتسعت مجالات الجاسوسية إلى كل من: الجاسوسية العسكرية، والتي تتركز حول معرفة القدرات العسكرية للدولة، وما تقتضيه من محاولة الحصول على معلومات عن طريق التنظيم والتدريب والتسليح والنظريات الإستراتيجية التكتيكية للقيادات، والجاسوسية السياسية التي تهدف إلى التعرف على النوايا الخفية للقادة السياسيين وطبيعة القوى الداخلية ومدى الصراع بينها، والجاسوسية الاقتصادية التي تهدف لمعرفة القدرات المالية والإنتاجية للدولة وقدراتها الصناعية ومراكز الإنتاج

الاقتصادي المؤثرة، التي تهدف إلى توضيح المستوى العلمي للدولة ومعرفة أنواع الأبحاث الإنتاجية وأهدافها. (فيكتور مارسيل، 27،1984)

- **البعد الاقتصادي**

يقصد بالبعد الاقتصادي كل ما يرتبط بالجانب الاقتصادى، وتهدف عملية التنمية إلى تحقيق الرفاهية، وتأمين الحياة الكريمة لأفراد الدولة، وذلك من خلال الوسائل الاقتصادية والتكنولوجية المتباينة –والتى تستهدف التبادل التجارى والسلعى– وذلك من أجل تحريك المؤشرات الاقتصادية، وإضافةً إلى ذلك اتفاقيات التبادل المشتركة بين الدول بما تتضمنه من انتقال لحركآت رؤوس الأموال والسلع، فضلاً عن ذلك انتقال التكنولوجيا المرتبطة بعمليات التصنيع. (Triumphias,2018)

- **البعد العسكري**

يُعَد البعد العسكري أقدم أبعاد الأمن القومي، حيث يتعين أن توفره الدولة، فمن أجل أن تحمي الدولة حدودها ومصالحها الداخلية والخارجية يتعين أن يتوفر لديها بعد عسكرى غاية فى القوة بما يتضمنه من بناء القدرة العسكرية للدولة حتى يتحقق التوازن الاستراتيجى العسكرى من خلال التوازن بين المقدرات العسكرية وأفراد القوات المسلحة.

وحتى على صعيد الاتفاقيات العسكرية التى تستهدف التحالفات العسكرية أو حتى أنظمة الدفاع المشتركة، ناهيك عن القدرة والكفاءة التى يتعين أن تتوافر بين القوات المسلحة بالإضافة لدرجة الاستعداد التى تتطلب أن تكون فى أقصى قدرة لها؛ وذلك لمجابهة أى مخاطر قد تطرأ فجأة وتهدد أمن أى دولة، كما سبق أن أشار الباحث أن القوة العسكرية هى أداة فعالة من أدوات السياسة الخارجية للدولة؛ لأنها تضمن لها الفاعلية الدولية وتيسر من عملية تحقيق البرامج والطموحات الخاصة بأى دولة.

ويجدر بالذكر أن البعد العسكري هو البعد الاكثر أهمية نظراً لأن تهديد الأمن القومي كان غير ممكن بغير الأداة العسكرية تقريباً؛ لذا حاز هذا البعد أهمية قصوى لدى الدول. (حسني النحال، 2020، 163-199)

- **البعد الاجتماعي والثقافي**

يقصد بهذا البعد توفير الأمن للمواطنين بالقدر الذي يزيد من تنمية الشعور بالانتماء والولاء، فبغير إقامة عدالة اجتماعية من خلال الحرص على تقريب الفوارق بين الطبقات وتطوير الخدمات يتعرض الأمن القومي للخطر.

كما يرتبط هذا البعد أيضاً بتعزيز الوحدة الوطنية كمتطلب رئيسي لسلامة الكتلة الحيوية للدولة ودعم الإرادة القومية وإجماع شعبها على مصالح وأهداف الأمن القومي والالتفاف حول قيادته السياسية.

ويؤدي الظلم الاجتماعي لطبقات معينة أو تزايد نسبة المواطنين تحت خط الفقر إلى تهديد داخلي حقيقي للأمن القومي تصعب السيطرة عليه، وبخاصة في ظل تفاقم مشاكل البطالة والإسكان والصحة والتعليم والتأمينات الاجتماعية. (political encyclopedia, 2021)

ثالثًا: تهديدات الإرهاب الإلكتروني على الأمن القومي

ثمَّة تهديدات كثيرة رتبتها ثورة الاتصالات الحديثة التي نشهدها في الوقت الحالي ليس أقلها إمكانية استهداف العديد من منشآت الدولة الحيوية من خلال هجوم إلكتروني بما يعنيه ذلك من إمكانية تعطل عمل أجهزة رئيسية في الدولة.

وقد شهدت كل دول العالم ذلك النوع من الهجوم وكانت خسائره بملايين الدولارات، بما يعنيه ذلك من أن هذا التهديد قد تجاوز كونه تحديا تقنيا بل يرتبط بالأمن الوطني للدول بشكل كبير. (أخبار الخليج، 2019)

وكلما شهدت البنية التحتية للدول تقدما ملحوظا في مجال تكنولوجيا المعلومات، فإن أمنها الوطني سوف يظل عرضة للمخاطر، إلا أن الأمر الذي يجب أن توليه الدول اهتماماً هو مدى قدرة الجماعات الإرهابية على شن هجمات إلكترونية على قطاعي الدفاع والأمن.

الخبراء يؤكدون حتى الآن أن أنظمة الجيوش لا تزال في مأمن من تلك المخاطر إلا أنه تجدر الإشارة إلى أنها مستهدفة والأمثلة على ذلك عديدة ومنها إعلان وزير الدفاع الفرنسي أن الأنظمة الأمنية الفرنسية قد أحبطت 24 ألف هجوم إلكتروني خارجي استهدف أجهزة الدفاع خلال عام 2016.

وفي عام 2017 تعرضت العديد من الدول لسلسلة من الهجمات الإلكترونية، حيث وقع أكثر من 45 ألف هجمة إلكترونية لأكثر من 99 دولة، وذلك وفقًا لخبراء في الأمن المعلوماتي، وأعلنت شركة "كاسبرسكاي لابس" Kaspersky Labs، أن من ضمن الدول التي تعرضت لذلك الهجوم من خلال "الفيروس العالمي الذي يطلق عليه انتزاع الفدية " Grab the Ransom، بريطانيا، ألمانيا، تركيا، اليابان، الهند، مصر، الصين، فرنسا، إسبانيا، والفلبين، المكسيك، روسيا. (عبد الدايم، 2017، 9)

وفي العام 2018، اتهم وزير الخارجية البريطاني جيريمي هانت الاستخبارات العسكرية الروسية بالوقوف خلف هجمات إلكترونية في جميع أنحاء العالم واستهداف وسائل إعلامية وسياسية كالدخول في الانتخابات الأميركية في العام 2016 بناء على نتائج المركز الوطني البريطاني للأمن السيبراني.

كما تعرضت بريطانيا في عام 2018 كذلك لهجمات الفدية، استهدفت قطاع الصحة، بهدف جمع الأموال، وقد اتهمت روسيا وكوريا الشمالية. سبق ذلك في عام 2012 تعرض شركة أرامكو السعودية لأكبر هجوم إلكتروني عندما تم تدمير أكثر من 30 ألف جهاز باستخدام فيروس شامون. (سكاي نيوز عربية، 2021)

وفي نهاية عام 2020 تعرضت الولايات المتحدة لأكبر هجوم إلكتروني وأكثرها تعقيداً، وذلك عن طريق استخدام برنامج شركة سولار ويندز كقاعدة لاختراق جهات أميركية ذات طابع حساس، وقد شمل الاختراق أكثر من 18 ألف عميل من عملاء الشركة حسب تصريح شركة مايكروسوفت، ووجهت الولايات المتحدة أصابع الاتهام إلى روسيا فيما رفضت موسكو هذا الاتهام.

وتتمثل التهديدات الاقتصادية في الاستخدام غير الشرعي للمعلومات السرية أو نظم التشغيل، فضلا عن التهديدات الإلكترونية من قبل المجموعات الإرهابية، والتعدي على أموال الغير بالوسائل الإلكترونية، والسطو على أموال البنوك. (موسى، 2006، 13)

كما يهدد الإرهاب الإلكتروني الحياة الاجتماعية والثقافية للمواطنين مثل توجيه المنظمات الإرهابية رسائلها للإعلام في المجتمعات التي تقوم بترويعها وإرهابها وذلك بهدف شن حملات نفسية ضد الدول المستهدفة.

المحور الثالث

تداعيات جائحة كورونا على الإرهاب الإلكتروني

دفعت جائحة كورونا إلى بروز أنماط جديدة من الإرهاب والتطرف، ما أثار تساؤلات حول تداعيات جائحة كورونا على هذه الظاهرة، ومدى تأثيرها في أجندات الجماعات الإرهابية وطبيعتها، بالإضافة إلى الاتجاهات المستقبلية المحتملة لها عقب انتهاء هذه الأزمة الوبائية الخطيرة للجماعات الإرهابية والمنظمات الإجرامية.

أولًا: كيف استغلت الجماعات الإرهابية جائحة كورونا

نحاول في هذا الجزء من الدراسة توضيح تأثيرات جائحة كورونا على خطابات وتوجهات بعض الجماعات الإرهابية كتنظيمَ داعش، القاعدة، الإخوان المسلمين، وذلك انطلاقاً من أن جائحة فيروس كورونا المستجد خلقت مناخاً داعماً وظروفاً موائمة للعديد من تلك الجماعات المختلفة والمتضادة فكرياً للتحرك ومحاولة استغلالها لتنفيذ أجندتها الخاصة، فقد أظهرت التنظيمات الإرهابية قدراً كبيراً من التكيف مع التغيرات الناجمة عن جائحة انتشار أزمة كورونا واتجهت أغلبها إلى توظيف الجائحة كأداة لتحقيق أهدافها المختلفة.

كما اتجهت التنظيمات المتطرفة للاستفادة من تكنولوجيا الإنترنت، واعتبر العديد منهم الفضاء الإلكتروني وسيلةً للاتصال وتبادل المعلومات ونشر الأفكار الهدامة، وبث خطابات الكراهية والآراء المتطرفة عبر مواقع التواصل الاجتماعي.

وبعد الإعلان عن تفشي وباء كورونا المستجد في مدينة "ووهان" الصينية في ديسمبر 2019 قامت التنظيمات الإرهابية على "تديين" هذا الفيروس، وإسباغه بمبررات دينية تخدم مصالحها.

1.تنظيم داعش

فسر تنظيم داعش انتشار الفيروس على أنه "عقاب من الله"، وحاول تأويل بعض الآيات القرآنية التي تتوافق مع فكره المغلوط، وقد ترجم تنظيم "داعش" هذه الرؤية الدينية لفيروس كورونا المستجد في إصداراته الإعلامية، وخاصة في مجلته الأسبوعية "النبأ"، فقد وصفت افتتاحية العدد رقم (226) الذي صدر في 19 مارس 2020 فيروسَ كورونا المستجد بأنه "عذاب أرسله الله إلى أعدائه".

كما نشرت قناة "جرين بيردز" التابعة للتنظيم صورة للفيروس مع تعليق مكتوب عليه "جندي الله". (العيسوي، 2020)

2.جماعة الإخوان المسلمين

تمثل جماعة الإخوان المسلمين منبعاً للتنظيمات الإرهابية التي تدعي الإسلام، فوفقاً لما أعلن عنه مرصد الفتاوى التكفيرية والآراء المتشددة التابع لدار الإفتاء المصرية، سعت جماعة الإخوان المسلمين إلى استحداث كيانات إلكترونية بهدف نشر الأفكار المتطرفة وتجنيد عناصر جدد مستغلة في ذلك تواجد الشباب في المنازل وقضاء المزيد من الوقت على مواقع التواصل الاجتماعي، كما قامت بإنشاء قنوات مغلقة عبر تطبيق تليجرام بهدف تكليف أفراد بنشر الفوضى وتعطيل قدرة الدولة على البناء والتنمية. (مرصد الإفتاء، 2020)

عملت الجماعة على توظيف جائحة كورونا (كوفيد- 19) من خلال اتجاهين، الأول من خلال انتقاد الدولة المصرية والإضرار بصورتها القومية وصورة النظام، والثاني عن طريق التقرب للمواطنين وإظهار التعاون.

ولا شك أن جماعة الإخوان تعاملت مع جائحة كورونا بانتهازية، حيث وضعت مصالحها الأيديولوجية والسياسية قبل الاعتبارات الدينية والوطنية. (دلال محمود، 2020)

3.اليمين المتطرف

لعل أبرز الأفكار التي روجها هذا التيار تجاه أزمة كورونا تمثلت في صياغة ونشر نظريات المؤامرة، والدعوة إلى الكراهية، وفي بعض الأحيان العنف ضد الأقليات، كل ذلك عبر مواقع التواصل الاجتماعي، حيث تمت إعادة توظيف القضايا التي تشغل التيار سابقاً، كمكافحة الهجرة ومعاداة الإسلام والسامية ومناهضة الحكومات، لتتوافق مع الأزمة الحالية.

وتجدر الإشارة، أن أزمة فيروس كورونا أسهمت بشكل كبير في توفير بيئة خصبة لبث نظريات المؤامرة. فضلاً عن ادعاء بعض مواقع النازيين الجدد، بأن هذا الفيروس لا وجود له، بل هو "خدعة" تستخدمه بعض الجهات للتربح (dw-akademie, 2020)

4.تنظيم القاعدة

اعتبر تنظيم القاعدة فيروس كورونا عقابا من الله، ولا يخفِي سعادته لإضراره بالاقتصاد الأمريكي، وأنه من الواجب على المجاهدين اتخاذ الخطوات العملية لتحريرهم، واتخاذ هذه الأزمة

فرصة للتوبة والعودة إلى الله. كما دعا البيان مواطني الدول الغربية إلى التفكر في أزمة فيروس كورونا، ومعرفة أن أسبابه الحقيقية تكمن في فسادهم الأخلاقي، واقتصادياتهم المبنية على الربا، والظلم والقمع اللذين تسببت فيهما حكوماتهم ضد المسلمين والعالم أجمع، (فاليريو مازوني، 2020) وقد اختلفت طرق تعامل أفرع التنظيم مع الجائحة وتباينت طريقة تعامل أفرع التنظيم مع جائحة كورونا. (Smtcenter, 2020)

ثانيًا: الجهود الدولية في مكافحة الإرهاب الإلكتروني

تعددت الجهود التي يبذلها كل الفاعلين في مجتمع المعلومات العالمي من أجل العمل على تنظيم عملية وضع السياسات المثلى للتعامل مع قضايا الإرهاب الإلكتروني من قبل الحكومات، فقد يمثل الإرهاب الإلكتروني تهديدًا مباشرًا لأمن الدول، لذلك تعمل الدول على استخدام استراتيجيات تغطي تدابير الأمن الإلكتروني بما في ذلك الدفاع الإلكتروني والردع ضد التهديدات الإلكترونية.

وتختلف جهود الدول في مواجهة الإرهاب الإلكتروني من دولة لأخرى حسب طبيعتها السياسية، والاقتصادية، والاجتماعية على المستوى الوطني ولكن على الرغم من تلك الجهود المبذولة من كل دولة على حدة، فإنها لا تكفي ويتطلب الأمر جهودًا دولية بالتعاون مع الدول بعضها البعض، من خلال عقد المؤتمرات والاتفاقيات.

تم إنشاء العديد من مواقع الإنترنت لمكافحة الإرهاب الإلكتروني والأمن الرقمي، حيث أصبحت بمثابة مؤسسات فكرية وفنية لدعم الأمن الرقمي، وكانت تلك المواقع إما بمبادرة حكومية أو من القطاع الخاص أو من المجتمع المدني، فضلا عن مواقع الشركات العاملة في تكنولوجيا الاتصال والمعلومات.

على الجانب الآخر هناك العديد من المنظمات الدولية عملت على التعاون فيما بينها لمواجهة الإرهاب بصفة عامة حيث إن هناك العديد من الاتفاقيات والمعاهدات العالمية المخصصة لمواجهة الإرهاب.

وتجدر الإشارة، إلى انه لا يوجد معاهدات أو قوانين تختص بتناول الإرهاب الإلكتروني، وعلى الرغم من ذلك تناول عدد من المنظمات والهيئات دراسة الإرهاب وكيفية مكافحته ومنها الأمم المتحدة وعلى رأسها الاتحاد الدولي للاتصالات (ITU)، حيث تعد الهيئة الوحيدة المسئولة عن مكافحة الإرهاب الإلكتروني من بين هيئات الأمم المتحدة، والإنتربول، واللجنة الأوروبية المعنية بالجرائم

الإلكترونية، ومجموعة الثمانية (G8)، والمجلس الأوروبي لمكافحة الإرهاب، والاتفاقية الأوروبية لمنع الإرهاب، والشراكة الدولية متعددة الأطراف لمكافحة الإرهاب السيبراني (IMPACT)، ورابطة أمم جنوب شرق آسيا (ASEAN)، ومنظمة التعاون الاقتصادي لمنطقة آسيا والمحيط الهادي (APEC).

مما سبق يتضح أن جائحة كورونا خلقت موجات من ردود الفعل المتباينة في أوساط الأفراد والمجتمعات، تراوحت بين الشعور بالغضب والحرمان والاستبعاد، الأمر الذي يُهدد بخلق أشكال جديدة من العنف السياسي والاجتماعي. كما قد تدفع ادعاءات بعض الجماعات الإرهابية بخصوص كون الفيروس "عقوبة إلهية" إلى ظهور موجات عنف أكثر وطأة من قِبل أعضائها ومؤيديها.

وعليه، من الصعب القول إن ظاهرة الإرهاب قد تتراجع أو تنتهي كما يعتقد البعض بعد انتهاء الجائحة، بل إنها قد تتطور وتأخذ أنماطاً أسوأ مما كانت عليه، سواء على مستوى العنف الداخلي أو على مستوى الإرهاب الدولي العابر للحدود الوطنية. (مركز الإمارات للسياسات، 2020)

الخاتمة

مما سبق يتضح أن أزمة كورونا فرضت تحديات عديدة تواجه دول العالم، فأصبح المجال الافتراضي بمنزلة ساحة قتال جديدة تشكل تهديدا يضاف إلى قائمة التهديدات التقليدية التي تواجه العالم، وتتجاوز في أبعادها وآثارها الحدود الجغرافية والسياسية، وتلقي بتداعياتها على مستقبل الأمن القومي والحيوي للدول، وأصبحت عمليات الاختراق التي يقوم بها "الهاكرز" قادرة على إغراق أجهزة خوادم برسائل من أنظمة متعددة تشل سير عملها وتوقف نظم الإنتاج.

أولًا: النتائج

1- لا يوجد تعريف واحد جامع مانع للإرهاب الإلكتروني، ولكن في النهاية تم التوصل إلى أن الإرهاب الإلكتروني يمكن تعريفه على أنه نشاط أو هجوم متعمَّد له دوافع سياسية بغرض التأثير على القرارات الحكومية أو الرأي العام باستغلال الفضاء الإلكتروني في عملية التنفيذ وذلك بقصد ترويع الأفراد من خلال تهديدهم أو إلحاق الضرر الفعلي بهم.

2- تتمثل الأساليب والوسائل التي تستخدمها الجماعات الإرهابية لاستغلال الفضاء الإلكتروني في تنفيذ أعمالها الإرهابية في التنسيق والاتصال، بالإضافة إلى الترويج الإعلامي، كذلك

التجسس على المواقع وتدميرها، وأخيرًا الحرب الدعائية التي تستهدف جذب العديد من الأفراد لها وتجنيدهم وخاصة القُصَّر والحصول على الدعم والموارد المالية.

3- قضايا الإرهاب الإلكتروني من أهم مصادر تهديد الأمن القومي، لما يمكن أن يترتب عليها من استثمار للمصادر الرئيسية للتهديد، وما يمكن أن تؤدى إليه من هدر للقدرات الوطنية والقومية.

4- صعوبة وضع خرائط جغرافية للخلايا الإرهابية النشطة وذلك بسبب حالة التحول والسيولة في هذه الخلايا كما تم تحليله في الجزء الأول من الدراسة.

5- أسهمت أزمة فيروس كورونا وتبعاتها الاقتصادية والاجتماعية في توفير بيئة خصبة لابتداع وانتشار نظريات المؤامرة.

ثانيا: التوصيات

1- تنظيم العديد من المؤتمرات العلمية والندوات التعريفية في الجامعات والمراكز البحثية المتخصصة تضم الخبراء والباحثين من مختلف المجالات لدراسة ظاهرة الإرهاب الإلكتروني ووضع الحلول المناسبة له.

2- استحداث مناهج دراسية في جميع المراحل الدراسية بما يساعد الطلبة على الاستخدام الأمن للفضاء الرقمي.

3- إنشاء مراكز للدراسات والأبحاث المتخصصة في الأمن المعلوماتي والبرمجيات بهدف تطوير استراتيجيات فاعلة لمكافحة جريمة الإرهاب الإلكتروني.

4- ضرورة وجود دور لعلماء الدين فى مكافحة التطرف والإرهاب عبر التركيز على آليات وطرق جديدة، والتخلى عن الطرق التقليدية التى لم تعد تواكب العصر، حيث يجب أن يتحول دور العالم من الناصح إلى المكافح، وذلك من خلال ممارسة دور أكثر إيجابية فى المجتمع، حيث يجب الانتقال من الدفاع عن الشريعة فقط إلى مهاجمة الأفكار المتطرفة، وتفنيدها، والرد عليها بشكل شرعى صحيح، يضع تلك الأفكار فى إطارها الشرعى الصحيح.

5- أهمية الأمن المجتمعي، باعتباره حجر الزاوية في القضاء على الإرهاب، من خلال حل مشكلات البطالة، والإسلام الشعبوي، والمظالم التي لا ينظر إليها.

6- أهمية الأمن الفكري بأن تكون هناك مجموعات تدخل سريعة من المتخصصين من رجال الدين، والمثقفين في المناطق، قبل وقوع الأحداث الإرهابية، وبعدها يتم التوضيح للمواطنين أن من يقدم الدعم اللوجيستي للإرهابيين هو شريك في العمل الإرهابي.

7- تأسيس وحدات للأمن الإلكتروني داخل المؤسسات العسكرية وتزويدها بكفاءات بشرية مدربة ولديها خبرة أسوة بتجارب الدول والمنظمات الدفاعية التي استطاعت التصدي لهذا النوع من التهديدات.

8- مراجعة أنظمة الاتصال في المؤسسات العسكرية من آن إلى آخر من خلال تأسيس كتائب دفاعية إلكترونية.

9- لا بد وأن تكون مواجهة الإرهاب الإلكتروني جزءًا أساسياً من المناورات العسكرية المشتركة التي تجريها الدول من آن لآخر بحيث يكون لدى أفراد القوات المسلحة القدرة على التصدي لأي إرهاب محتمل من هذا النوع.

10-لابد وأن تكون مواجهة التهديدات الإلكترونية جزءًا لا يتجزأ من استراتيجيات وخطط الأمن القومي للدول.

11-التعاون الدولي والإقليمي، حيث إن ذلك التهديد هو تهديد عابر للحدود، وليس بمقدور أي دولة مهما توافرت لديها الإمكانيات المادية والبشرية أن تدرأ ذلك الخطر سوى بالتعاون الإقليمي والدولي.

قائمة المراجع

أولا: المراجع العربية

- **الموسوعات**

1- ابن منظور (2014)، **لسان العرب**، تحقيق عبد الله علي الكبير، القاهرة، دار المعارف، د ت.

2- الكيالي، عبد الوهاب (1994)، **الموسوعة السياسية**، بيروت، المؤسسة العربية للدراسات والنشر، ج7.

3- زيتون، وضاح (2006)، **المعجم السياسي**، الأردن، دار أسامة المشرق الثقافي، ط1.

4- **موسوعة السياسة**، الجزء الأول، ط 3 بيروت، المؤسسة العربية للدراسات والنشر. (1990).

- **الكتب**

1- إبراهيم، خالد ممدوح (2008)، **حجية البريد الإلكتروني في الإثبات دراسة مقارنة**، القاهرة، دار الفكر العربي.

2- أحمد الصياد، عبد العاطي (2002)، **الإرهاب والعولمة**، الرياض، مركز الدراسات والبحوث الأكاديمية، جامعة نايف العربية للعلوم الأمنية، ط1.

3- سعيد، عبد الله محمود، مراد، على عباس (2006)، **الأمن والأمن القومي: مقاربة نظرية تطبيقية**، ط1، ليبيا، دار الكتب الوطنية، 2006.

4- ماركس، فيكتور مارشيل (1984)، **الجاسوسية تتحكم بمصائر الشعوب**، بيروت، الدار المتحدة للنشر، د ت.

- **الدوريات**

1- حسني النحال، مهاب (2020)، السياسة الخارجية والأمن القومي المصري.. حدود العلاقة في الفكر والممارسة، **مجلة السياسة والاقتصاد**، المجلد 8، العدد (7).

2- عبد الدايم، هبة أحمد وشعبان، منار محمد، (يوليو 2017)، "الهجمات السيبرانية"، **دراسات دورية**، بنك الاستثمار القومي، قطاع الاستثمار والموارد الدعم الفني للاستثمار.

3- عبد الصادق، عادل (2018)، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، الإسكندرية، **وحدة الدراسات المستقبلية**.

4- مهران، خالد وليد (2013)، الهجمات عبر الانترنت: ساحة الصراع الإلكتروني، **مجلة سياسات عربية**، العدد 5، ص 118.

- **تقارير ومؤتمرات وندوات**

1- البشيري، محمد الأمين (2005)، **التحقيق في جرائم الحاسب الآلي**، ورقة مقدمة لمؤتمر القانون والكمبيوتر والإنترنت، كلية الحقوق والشريعة، جامعة الإمارات.

2- عطوة الزنط، سعد (2010)، **الإرهاب الإلكتروني وإعادة صياغة استراتيجيات الأمن القومي**، ورقة علمية مقدمة) مؤتمر الجرائم المستحدثة-كيفية إثباتها ومواجهتها، المركز القومي للبحوث الاجتماعية والجنائية، مصر.

3- عطية، أيسر محمد، **"دور الآليات الحديثة للحد من الجرائم المستحدثة وطرق مواجهته"**، محاضرة ألقيت بملتقى دولي بعنوان الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، أيام 02-04 /09/ 2014.

4- موسى، ذياب (2006)، **دور الأجهزة الأمنية في مكافحة جرائم الإرهاب المعلوماتي**، ورقة مقدمة في الدورة التدريبية: مكافحة الجرائم المعلوماتية، كلية التدريب، جامعة نايف العربية للعلوم الأمنية.

5- **مذكرة الأسباب الموجبة لأمن وسلامة الفضاء السيبراني(الإنترنت)**، جامعة الدول العربية، المركز العربي للبحوث القانونية والقضائية.

- **رسائل علمية**

1- محمد علام، مها محمد (2014)، **ثورة المعلومات والأمن القومي: دراسة حالة الولايات المتحدة الامريكية**، رسالة ماجستير غير منشورة، كلية الاقتصاد والعلوم السياسية، جامعة القاهرة.

2- محمد أل زيران، مشبب ناصر (2011)، **المواقع الإلكترونية ودورها في نشر الغلو الديني وطرق مواجهتها من وجهة نظر المختصين**، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض.

ثانيًا: المراجع الاجنبية

- **Books.**

1- Daniel J. Kaufman& Jeffrey S. Mctrick& Thomas J. Leney (1985), U.S. National Security a Framework for Analysis, Toronto, Lexington Books.
2- Frank Trager and Philip Kronenberg (eds.) (1973), National Security and American Society, Kansas: Kansas University Press.
3- Keith Krause and Michael William, (ed.) (1987), Critical Security Studies: Concepts and Cases, Minneapolis, University of Minnesota Press.
4- Keith Krause and Michael William, (ed.) (1987). Critical Security Studies: Concepts and Cases, Minneapolis: University of Minnesota Press.

5- Vladimir Bratic (2008), " Examining peace-oriented media in areas of violent conflict", SFCG, Edited.

- **Periodicals: Articles and Papers.**

1- Joint Publication (2010) (JP) 1-02, Department of Defense dictionary of military and associated terms, Washington, Dc, Department of Defense, November.

- **Websites**

1- أشرف محمد كشك، **الأمن السيبراني والأمن الوطني: رؤية استراتيجية**، على الرابط التالي:
http://www.akhbar-alkhaleej.com/news/article/1182104

2- الأمين العام للأمم المتحدة أنطونيو غوتيريش، مكافحة الإرهاب والتطرف العنيف، على الرابط التالي: https://news.un.org/ar/focus/counter-terrorism

3- الموسوعة السياسية، على الرابط التالي:
https://politicalencyclopedia.org/dictionary/%D8%A7%D9%84%D8%A3%D9%85%D9%86%20%D8%A7%D9%84%D9%82%D9%88%D9%85%D9%8A

4- العيسوي، أشرف، التنظيمات المتطرفة والتوظيف الديني لـ "كوفيد-19": الأبعاد والتداعيات المحتملة على الإرهاب الدولي، على الرابط التالي: https://trendsresearch.org/ar

5- ابو بكر، بكر، الإرهاب الإلكتروني: من الدعاية والاستقطاب إلى اكتساح المجال الافتراضي، على الرابط التالي: https://www.europarabct.com

6- بشير، هشام، الإرهاب الإلكتروني في ظل ثورة المعلومات، على الرابط التالي:
https://araa.sa/index.php?option=com_content&view=article&id=244:2014-06-13-16-21-31&catid=132:articles&Itemid=294

7- عبد الرحمن، ريهام، أثر الإرهاب الالكترونى على تغير مفهوم القوة فى العلاقات الدولية دراسة حالة: تنظيم الدولة الاسلامية، على الرابط التالي: https://democraticac.de/?p=34528

8- عبد الله بن خالد بن سعود الكبير آل سعود، كيف تستغل الجماعات الإرهابية واليمين المتطرف أزمة "كورونا"؟، على الرابط التالي: https://smtcenter.net/archives/slider

9- _____، تداعيات أزمة "كورونا" على ظاهرة الإرهاب: الأنماط والتوقعات، على الرابط التالي:
https://epc.ae/ar/brief/the-impact-of-coronavirus-crisis-on-terrorism-patterns-and-expectations

10- فارس محمد العمارات، الاثار السياسية والأمنية للإرهاب، على الرابط التالي:
http://www.acrseg.org/41858

11- محمود دلال، التنظيمات الإرهابية تستخدم أسلحة جديدة وتتجه لتكون من الفاعلين السياسيين، على الرابط التالي:

https://araa.sa/index.php?option=com_content&view=article&id=4999&catid=4323&Itemid=172

12- مرصد الافتاء، جماعة الاخوان الإرهابية تسعى لنشر الفوضى في مصر عبر الإرهاب الإلكتروني، جريدة الرواق، 22 سبتمبر 2020، على الرابط التالي:
https://alruwaq.com/35875-31

13- مصطفى علوي، مستقبل الإرهاب: التنافس بين داعش والقاعدة، على الرابط التالي:
http://www.acrseg.com/39343

14- نسرين الشرقاوي، الإرهاب السيبراني وتداعياته النفسية والسياسية، على الرابط التالي:
/https://marsad.ecsstudies.com/57350

15- نهاد سمير، الإرهاب والعنف السياسي في مجال القانون الدولي وحقوق الإنسان، على الرابط التالي: https://gate.ahram.org.eg/daily/News

16- _____، أثر الإرهاب الإلكترونى على تغير مفهوم القوة فى العلاقات الدولية دراسة حالة: تنظيم "الدولة الاسلامية"، المركز الديمقراطي العربي، على الرابط التالي:
https://democraticac.de/?p=34528

17- https://www.wdl.org/ar/item/11579/

18- _____، ما هو التجسس الإلكتروني وما هي أساليبه وطرق مكافحتها؟، على الرابط التالي:
https://cyberone.co

19- _____، التجسس الإلكتروني.. كيف تقوم الاستخبارات باختراق الهواتف وأجهزة الكمبيوتر؟،، على الرابط التالي: https://www.europarabct.com/?p=72112

20- _____، الابتزاز الإلكتروني، على الرابط التالي:
https://www.tdra.gov.ae/ar/media-hub/cyber-blackmailing.aspx

21- https://triumphias.com/blog/concept-and-dimensions-of-national-security-difference-between-internal-and-external-security/

22- _____، جرائم القرصنة.. تهديد متزايد يستنفر جهود المجتمع الدولي، على الرابط التالي: https://www.skynewsarabia.com

23- _____، دراسة.. اليمين المتطرف يستغل كورونا للتمدد في أوروبا وأمريكا، على الرابط التالي: https://www.dw.com/ar

24- فاليريو مازوني، فيروس كورونا: ردود فعل المسلحين الإسلاميين على تفشي الوباء، عين أوروبية على التطرف، 30 مارس 2020، من خلال الرابط التالي: https://bit.ly/3eZMV50