توظيف الفواعل مِن غير الدول للقوة السيبرانية وأثرها على الأَمن الدولي

الباحث/ محمد اكرم محسن أ.م.د. مروان سالم علي
جامعة الموصل/ كلية العلوم السياسية
dr-marwanalali82@uomosul.edu.iq

تاريخ استلام البحث 2023/5/1 تاريخ ارجاع البحث 2023/5/20 تاريخ قبول البحث 2023/6/4

أثرت الثورة العلمية والتكنولوجية والفضاء السيبراني (الإلكتروني) على تحولات مفهوم القوة لمواكبة التطور الحادث في السياسة العالمية ليبرز على الساحة مفهوم جديد أطلق عليه بالقوة السيبرانية، كما ساعدت على أنتِشار مفهوم القوة على المستويين (الداخلي والخارجي) وعلى الفاعلين المستخدمين لها، فلم تعد القوة حِكراً على الدولة، بل توزعت بين عدد أكبر مِن الفاعلين مِن غير الدول- بِما فيهم الفاعلين العنيفين وغير العنيفين- والأفراد، وذلك بعد أنْ كانت الدولة هي المحتكر الوحيد للقوة، بِما جعل قدرة الدولة على الهيمنة على هذا المجال موضع شك. بِما أدى إلى ظهور مصادر تهديد غير تقليدية على الأَمن الدولي، بعد أنَّ ارتبطت القوة التكنولوجية ارتباطاً وثيقاً بالصِراع الدولي في شكل جديد، فيما يُسمى(الصِراع السيبراني).

ومِن هُنا يهدف البحث إلى استِقراء العلاقة الترابُطية بين القوة السيبرانية والأَمن الدولي والتعرُف على كيفية توظيف البيئة الإلكترونية الجديدة مِن جانب الفواعل مِن غير الدول (العنيفين وغير العنيفين) وأثرها في تهديد منظومة الأَمن الدولي. ويقوم البحث على فرضيةٌ مفادها؛ إنهُ كُلما تزايد توظيف القوة السيبرانية مِن جانب الفواعل مِن غير الدول في تفاعُلاتهم كُلما أثر سلباً على الأَمن الدولي وتهديداً لهُ ثُم بروز أنماط جديدة مِن الصِراعات الدولية في ظل عجز الدول عموماً عن مواجهة التهديدات السيبرانية. وللوقوف على هذا الموضوع تم تقسيم البحث إلى مِحورين رئيسين تناول أولهما؛ توظيف الفاعلين مِن غير الدول للفضاء السيبراني وأثرهُ في الأَمن الدولي. أما المِحور الثاني فتطرق إلى توظيف الفاعلين العنيفين مِن غير الدول للفضاء السيبراني وأثرهُ في الأَمن الدولي.

The scientific, technological and cyberspace revolution has influenced the shifts in the concept of power to keep pace with the development of global politics to bring to the fore a new concept called cyber power, and has helped to spread the concept of power at the (internal and external) levels and to the actors employed, the force is no longer the preserve of the state, but has been divided among more non-State actors — including violent and non-violent actors — and individuals, after the state was the sole monopoly of power, making the ability of The state's dominance in this area is in doubt. This has led to the emergence of unconventional sources of threat to international security, after technological power has been closely linked to the international conflict in a new form, the so-called "cyber conflict."

The research aims to read the interconnection between cyber power and international security and to learn how the new electronic environment is employed by non-State actors (violent and non-violent) and their impact on the threat to the international security system. The research is based on the premise that the more non-State cyber-power is employed in their interactions, the more negatively and threatening international security will be, and new patterns of international conflicts will emerge as States generally are unable to respond to cyber threats. Thus, the research was divided into two main themes, the first of which was the recruitment of non-State cyberspace actors and its impact on international security. The second focus was on the recruitment of violent non-state cyberspace actors and its impact on international security.

الكلمات المفتاحية: الفواعل مِن غير الدول، القوة السيبرانية (الالكترونية)، الأَمن الدولي، الفاعلين العنيفين.

المُقدِمة

الدول عادةً ما تُترجم قدراتها على تحقيق أَهدافها الخارجية مِن خِلال استِخدامها لوسائل عدة، ومع ثورة المعلومات والقدرة على إِنتاج التكنولوجيا المتطورة عن طريق الاختِراع والإِبداع ظهر لدينا شكلٌ جديد مِن أَشكال القوة وهي القوة السيبرانية، التي وزعت القوة بين عدد أَكبر مِن الفاعلين ومكنت الفاعلين الأَصغر في السياسة الدولية، مِن امتلاك قدرةٌ كبيرةٌ على مُمارسة كُل مِن القوة الصلِبة والناعِمة في الفضاء السيبراني، وهو ما يعني تغير في رسم العلاقات السياسية الدولية، حيثُ ظهر مفهوم الفاعلين مِن غير الدول، وإِمكانية امتلاكهم قوة تدخل في مُنافسة قوة الدولة بل في بعض الأحيان التفوق على الدولة نفسها، حيثُ يتكون هذا النوع مِن الفاعلين مِن الشرِكات المتعددة الجنسيات والمنظمات الإِجرامية والتنظيمات الإِرهابية كذلك الأَفراد، التي صار بإِمكانهُم استِخدام القوة السيبرانية ولأَغراض هجومية ودفاعية بالأَساس. فالصِراعات بين الدول والحكومات والشرِكات والجِهات الإِجرامية أَو الأَفراد ليست جديدة؛ لكن انخِفاض تكاليف المعركة في الفضاء السيبراني مُقارنةً بالحرب التقليدية وإِمكانية عدم الكشف عن هوية الفاعل في الفضاء السيبراني يوَّلد الاطمئنان لدى الفاعلين في الفضاء السيبراني، الأَمر الذي ينتج عنهُ زيادة الدخول في تفاعُلات دولية وتركها أَثاراً سلبية على الأَمن الدولي.

أَهمية البحث :

تتجلى أَهمية البحث في أَنهُ يجمع بين الشقين: العلمي (النظري)، والعملي (التطبيقي)؛ إِذ تظهر الأَهمية النظرية للبحث في تناوله أَحد أَهم القضايا الحديثة في علم العلاقات الدولية، وهي القوة السيبرانية (الإِلكترونية) كأَحد أَهم المجالات التي تُمارس فيها التفاعُلات الدولية، بجانب تناولها لقضية باتت مُهِمة وهي الفاعلين العنيفين وغير العنيفين مِن غير الدول وتوظيفهم للفضاء السيبراني واثر ذلك في الأَمن الدولي. كما إِنَّ هذا البحث حاول تقديم وجهة نظر جديدة تُركز على دِراسة وتحليل مُهدِدات الأَمن الدولي بواسِطة التركيز على دِراسة توظيف الفواعل غير الدوليين للقوة السيبرانية في استراتيجياتهم وتفاعُلاتها التعاونية والتصارُعية، وعلى رأَسهم الشرِكات مُتعددة الجنسيات والتنظيمات الإِجرامية والإِرهابية والأَفراد.

أَما الأَهمية العملية للبحث فتأَتي في أَنَّ نتائج البحث يمكن أَنَّ تُسهِم في تقديم تجارب واستراتيجيات بعض الفواعل غير الدوليين في توظيفهم للفضاء السيبراني وبِما يُمكِّن الاستِفادة مِنها في واقعنا العربي، وتقديم رؤى وتحليل حقيقي لصناع القرار لمعرفة طبيعة التهديدات السيبرانية وكيفية تبني استراتيجية سيبرانية وطنية دفاعية وهجومية على نحوٍ يُقلل مِن تأَثيراتها السلبية على الأَمن الوطني والدولي.

إِشكالية البحث :

يتركز البحث حول مشكلة أَساسية مفادها؛ ساعدت تكنولوجيا المعلومات والاتصالات والأَنترنت فواعل النظام العالمي مِن غير الدول (العنيفين وغير العنيفين) على امتِلاك القوة السيبرانية (الإِلكترونية) واستِخدامها

في التفاعُلات الدولية وتهديد الأَمن الدولي، لتجد الدول نفسها عاجزةً عن مواجهة المهدِدات السيبرانية مُتسعة النِطاق والأَبعاد، ليُجسد ذلك أَبرز ملامح إِشكالية البحث، وبذلك تتمحور الإِشكالية حول التساؤل الرئيس الآتي: كيف يتم توظيف القوة السيبرانية مِن جانب الفواعل غير الدوليين في تفاعلاتهُم وتهديدهم للأَمن الدولي؟.

فرضية البحث :

يقوم البحث على فرضيةٌ مفادها؛ إِنَّ منظومة الأَمن الدولي اليوم تواجه جُملةٌ مِن التهديدات الاستراتيجية غير التقليدية التي أَفرزتها مُتغيرات البيئة الدولية، وتأَتي التهديدات السيبرانية (الإِلكترونية) على رأَس تِلك المهدِدات، في ظل سعي فواعل النِظام العالمي غير الدوليين إِلى توظيف القوة السيبرانية في تفاعُلاتهم الدولية، ومِن ثُم كُلما تزايد توظيف القوة السيبرانية مِن جانب هؤلاء الفواعل في تفاعُلاتهم كُلما أَثر سلباً على الأَمن الدولي وتهديداً لهُ ثُم بروز أَنماط جديدة مِن الصِراعات الدولية في ظل عجز الدول عموماً عن مواجهة التهديدات السيبرانية، ومِن ثُم تحول هذه الصِراعات مِن مُجرد مناورات إِلى حروب واقعية يكون ميدانها الرئيس الفضاء الرقمي وعسكرة الفضاء الإِلكتروني.

هدف البحث :

يهدف البحث إِلى تسليط الضوء على أَهم واخر تحولات القوة التي شهدها حقل العلاقات الدولية وانتقالها مِن القوة الصلبة ثُم الناعِمة ثُم الذكية وصولاً إِلى القوة السيبرانية، واستِقراء العلاقة الترابطية بين الأَخيرة والأَمن الدولي والتعرُف على كيفية توظيف البيئة الإِلكترونية الجديدة مِن جانب الفواعل مِن غير الدول (العنيفين وغير العنيفين) وأَثرها في تهديد منظومة الأَمن الدولي. فضلاً عن المساهمة في خلق وتطوير الوعي الجمعي بشأَنَّ ظاهرة السيبرانية وتهديدها للأَمن، فهي سلاحٌ ذو حدين.

مناهج البحث:

لسِعة الموضوع وشموليتهُ وتنوعهُ اعتمد الباحث مناهج عديدة، مِنها: (المنهج الوصفي) لما له من حاجة ماسة في وصف المفاهيم والاصطلاحات الاجرائية. فضلاً عن إِيلاء (المنهج التحليلي) أَهمية خاصة للوقوف برؤَية تحليلية على أَهم المدخلات الأَمنية المسبِبة لإِرباك الأَمن الدولي ومُخرجاتهُ في ظل تهديد الفواعل مِن غير الدول للأَمن الدولي عبر توظيفهم للفضاء السيبراني. كما تمت الاستعانة (بالمنهج (التاريخي) الذي مِن خِلاله يمكن الرجوع إِلى المحطات التاريخية والأَحداث المهِمة لِمُساعدتنا على فهم موضوع تطورات القوة وتوظيفها مِن قِبل الفواعل مِن غير الدول.

هيكلية البحث:

وللوقوف على توظيف الفاعلين مِن غير الدول للقوة السيبرانية وتأَثيرها على الأَمن الدولي ارتى الباحث تقسيم البحث إِلى مِحورين رئيسين جاءت على النحو الآتي :

المِحور الأَول:توظيف الفاعلين غير العنيفين مِن غير الدول للفضاء السيبراني وأَثرهُ في الأَمن الدولي.
المِحور الثاني : توظيف الفاعلين العنيفين مِن غير الدول للفضاء السيبراني وأَثرهُ في الأَمن الدولي.

المِحور الأَول : توظيف الفاعلين غير العنيفين مِن غير الدول للفضاء السيبراني وأَثرهُ في الأَمن الدولي

شهد العالم في العقود الأَخيرة ظهور تحولات مُهِمة على صعيد العلاقات الدولية وعلى مُسلماته الأساسية التي مِن أَبرزها "إِنَّ الدولة هي الفاعل الأَساسي في العلاقات الدولية"، إِذ أَصبحت الحركات السياسية الاجتماعية والتنظيمات الإِرهابية مِن الفواعل الأَساسية في العلاقات الدولية جنباً إِلى جنب مع الشركات المتعدِدة الجنسيات، والمنظمات العالمية غير الحكومية وغيرها. وتُعد التنظيمات الإِرهابية مُتمثلةً بتنظيم القاعِدة، تنظيم داعش، جبهة النصرة، وغيرها، الظاهرة الجديدة في سياق ظهور الجيل الثاني مِن الفواعل مِن غير الدول التي تتبنى العنف السياسي كوسيلة لتحقيق أَهدافها[1].

وقد تعددت تعريفات الفاعلين من غير الدول، فبموجب القانون الدولي ليس هُنالك تعريف مُحدد لِمُصطلح "الفاعلين مِن غير الدول" ولكن أَوسع تعريف مُمكن أَنَّ يشمل جميع الجِهات الفاعِلة مِن غير الدول، بِما في ذلك الأَفراد ومُنظمات المجتمع المدني والشرِكات والجماعات المسلحة [2].

وعرفها الباحثان الاسكتلنديين (ويليام دالاس وديفنى جوزلين) بأَنهُم "مُنظمات مُستقلة بصورة كبيرة أَو كُلية عن تمويل الحكومة المركزية وسيطرتها، وعن اقتصاد السوق والدوافع السياسية والمرتبطة بتوجيه الدولة، وتعمل في شبكات خارج حدود الدولة التي تنتمي إِليها بحكُم النشأَة، ومِن ثُم فهي طرف في علاقات مُتعدية الحدود، تربط بين نظُم سياسية واقتصادية ومُجتمعات متنوعة، وتعمل بطريقة تؤثر على المخرج السياسي، سواءً في دولة ما، أَو في مُنظمة دولية سِواءً كبُعد لنشاطها أَو كغاية رئيسة لها"[3].

كذلك عرفها بعض المفكرين على انها "الجماعات أَو المنظمات التي تتمتع بعدد مِن السِمات، وتتمثل في: الاستِقلال التام أَو بدرجة كبيرة عن تمويل الحكومة المركزية التي تعمل على أَرضها، وامتِلاك موارد خاصة بِها، ولها هوية مُتميزة، ولها سياسة خارجية مُستقلة عن سياسات الدولة التي تنتمي اليها، سِواءً عن قصد أَو غير قصد وسِواءً كان ذلك غاية للمُنظمة أَو أَحد أَبعاد أَنشطتها"[4] .

غير أَنَّ البعض الآخر عرفهم بأَنهم، فواعل سياسية مُنظمة ليس لهُم علاقة مُباشِرة بالدولة، لكن لديهم أَهدافهم التي تؤثر على مصالح الدولة[5]. ومِن أَجل توضيح دور الفاعلين مِن غير الدول وتوظيفها للقوة والفضاء السيبراني وتهديدهم للأَمن الدولي ارتى الباحث تقسيم هذا المِحور على النحو الآتي:

أَولاً: توظيف الشرِكات الإِلكترونية المُتعددة الجنسيات للقوة السيبرانية

الشرِكات المتعددة الجنسيات هي الشرِكات التي تُدير الإِنتاج أَو تقدم الخدمات في بلدين على الأَقل وتقليدياً إِنَّ إِحدى نماذج هذه الشرِكات هي شرِكة خاصة مقرها في دولة واحِدة ولها فروع في دول أَخرى جميعها تعمل وفقاً لاستراتيجية عالمية مُنسقة لكسب الحصة الأَكبر مِن السوق العالمية وتحقيق أَكبر قدر مُمكِن مِن الأَرباح[6].

كذلك عرفها الباحث الأَمريكي (دافيد ليلينثال) بانها "هي الشرِكات التي مركزها الرئيسي في دولة ما وتعمل وتعيش في ظل قانون دولة أَخرى"[7].

إذ تمتلك بعض الشرِكات الإِلكترونية موارد للقوة والتأَثير في الفضاء السيبراني تفوق قدرة العديد من البُلدان، مِن قبيل ذلك "شركة Google وFacebook وMicrosoft، التي تسمح لها بامتلاك قواعد البيانات العملاقة التي مِن خِلالها تستكشف وتستغل الأَسواق، وتؤَثر في الاقتصاد العالمي. وهذا ما حدث في فضيحة تسريب بيانات مُستخدمي فيسبوك لصالح شركة "كامبردج أناليتيكا"، وهي شرِكة الكترونية أَمريكية مُختصة بجمع البيانات الخاصة بالأَشخاص وتحليلها لمعرفة ميولهم واهتماماتهم التي تم الاستِعانة بِها لصالح حملة المرشح الجمهوري دونالد ترامب في الانتخابات الرئاسية للولايات المتحدة الأَمريكية عام2016 إِذ استطاعت قناة 4channel البريطانية مِن تصوير مُدير الشركة "اليكسندر نيس" وهو يتكلم عن مُساعدة المرشح (دونالد ترامب) في الانتخابات عن طريق مُستخدمي فيسبوك مِن خِلال استِغلال بياناتهُم التي حصلت عليها الشركة التي مكنتها مِن تحليل ميولهم وتوجيههُم للتصويت لصالح ترامب ذلك مِن خِلال إِرسال رسائل ترغيبية ومُناهِضة لهيلاري كلنتون المنافِسة لترامب[8].

ثانياً : توظيف المنظمات الإِجرامية للقوة السيبرانية

يتوقع مختصون أَنَّ النتائج التي ستترتب على الثورة العلمية والتكنولوجية، هي تزايد القلق بسبب كثرة التهديدات وفقدان الأَمن، ونتيجة تراجع الدولة وتنامي حركة الاقتصاد العالمي، فأَنَّ الأَموال تنتقل بسرعة عبر الحدود، وتصل إِلى جهات خطرة كالأَنظمة الدكتاتورية، أَو الجماعات الإِرهابية على سبيل المِثال[9].

فحروب الفضاء يمكن أَنَّ ينتج عنها أَثاراً مُدمِرة مِن شأَنها تدمير الأَقمار الصِناعية بشكلٍ عشوائي، وان أَجزاءً مِن هذا الحطام قد ينتشر في مدارات أَرضية قريبة بسرعة فائقة وتسبب بحوادث على سطح الأَرض يمتد أَثارها إِلى عقوداً طويلة[10].

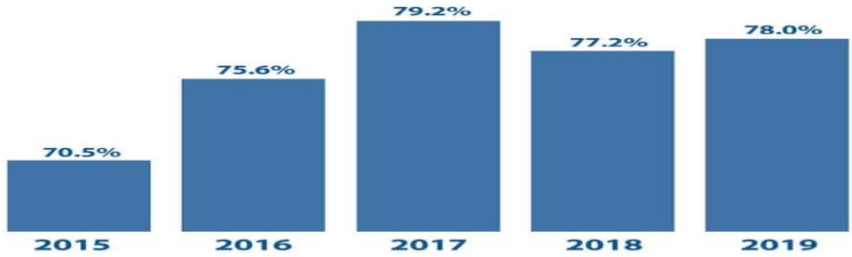
ولعل من أَهم العوامل التي تُعزِز أَنتِشار الأَنشطة غير السلمية في الفضاء السيبراني، هي[11]:

1. تزايد الارتباط العالمي بالإِنترنت والأَنظمة الإِلكترونية وزيادة احتمالية تعرض البُنى التحتية المكونة للمعلومات إِلى هجمات سيبرانية تُهدد الأَمن الدولي.
2. استِخدام الفواعل الجدُّد مِن غير الدول للفضاء السيبراني بشكلٍ مُتزايد لردم الفجوة بينهم وبين الدول في مجال القوة لغرض تحقيق أَهدافهم التي يسعون مِن أَجلها.
3. تراجُع دور الدولة وانسحابها مِن قطاعات استراتيجية مُهِمة لصالح الفواعل الجدُّد مِن غير الدول.
4. بروز تحديات جديدة تكمنُ مِن كيفية تعامُل الدول مع الشركات مُتعددة الجنسيات المختصة بالتكنولوجيا، إِذ تتفوق في قدرتها التكنولوجية على الدول، مثل مواقع لشبكات الاجتماعية كالفيس بوك وتويتر واليوتيوب وغيرها، التي مهدت لظهور فواعل الشبكات كفواعل جدُّد في الساحة العالمية.

https://doi.org/10.61353/ma.0150535

وتقوم الجماعات الإجرامية بعمليات القرصنة السيبرانية واختِراق الحاسبات البنكية وتحويل الأموال. وتقوم بدور مؤثر في التفاعُلات الدولية، ففي الغالب ما تقوم الحكومات الضعيفة بحمايتها، كذلك تعمل هذه المنظمات الإجرامية ببيع معلومات مالية مُتعلقة بكلمات مرور شخصية وحسابات بنكية وأرقام كروت وبطاقات ائتمان وذلك مِن خِلال وجود سوق سوداء على الانترنت. إذ تُكلف الجرائم السيبرانية الشرِكات أكثر مِن ترليون دولار سنوياً[12]. والشكل ذو الرقم (1) يوضح زيادة الهجمات السيبرانية التي تقوم بها المنظمات الإجرامية للمُدة 2015-2019.

الشكل (1): زيادة فعالية هجمات المُنظمات الإجرامية السيبرانية للمُدة 2015 – 2019



الشكل مِن إعداد الباحث بالاستِناد إلى: أَضواء للبحوث والدِراسات، اثر التهديدات السيبرانية على الأَمن القومي : دِراسة حالة ماليزيا 2015-2022، رسالة ماجستير منشورة على الرابط : https://adhwaa.net

يوضح الشكل أعلاه أنَّ عام2017 هو أعلى هجمات سيبرانية قامت بها المنظمات الإجرامية مِما يؤكد بان هذا النوع مِن الفواعل الدولية في زيادة نشاطها المتمثل في الابتزاز والقرصنة الإلكترونية ونشر المعلومات الكاذبة وغيرها مِن الأَعمال لتحقيق أَهدافها.

إذ إنَّ مِن الصعب الكشف عن هوية هذه المنظمات، ذلك راجع للميزة التي يتمتع بِها الفضاء السيبراني مِن قابلية التخفي، فضلاً عما سبق، فأنَّ هُناك أَنواع مِن الجرائم التي يمكن أنَّ تتم بواسطة الفضاء السيبراني وقد يتعرض لها المستخدم أَو يكون طرفاً فيها وهو لا يعلم ومِنها[13]:

1. عملية انتِحال شخصيات سياسية أَو اقتصادية معروفة، أَو انتحال شخصية الموقع.
2. القيام بهجوم على مواقع الانترنت والتعديل فيها، إذ بإمكان أَحد المنافسين أَن يدخل إلى موقع الشركة المنافسة عند عرض سلعها ويتلاعب بأَسعارها المعروضة.
3. التلاعُب في التجارة الإلكترونية. إذ يتم استخدام بطاقات الائتمان استِخداماً غير مسموح به، وقد لا يعرف صاحب البطاقة ان بطاقتهُ أَصبحت متداوله بين مجموعه مِن المجرمين.

4. كذلك هُنالك الفيروسات التي تعبث بالأَنظمة العامة، وتقوم بتحطيم الأَعمال وتُساعد على خلق البلبلة والاضطراب وعدم الامان في استخدامات الفضاء الإلكتروني مِن قِبل روادهُ.
5. ناهيك عن الجرائم الأَخلاقية والإعلانات عن الرذائل وابتزاز بعض الشخصيات العامة.

ومِن اجل فهم دور هذه المنظمات الإجرامية وأَثرها في الأَمن الدولي ارتى الباحث إلى ذكر بعض النماذج ومِن أَهمُها:

- **نادي كايوس للحاسوب Chaos Computer Clubk** : تكونت المجموعة في برلين عام1981 لكنها حظيت بشهرة كبيره بعد قيام افرادها باختراق شبكة الكمبيوتر الالمانية الرسمية "Bildschirmtext"، وتمكنوا مِن الحصول على مبلغ(134,000) مارك ألماني مِن أَحد البنوك في هامبورغ الأَلمانية، كان هدف هذه العملية هو إثبات أَنَّ النِظام الأَمني الإلكتروني في المانيا يحتوي على ثغرات، وقامت المجموعة بإعادة المبلغ المالي في اليوم التالي. كذلك قامت المجموعة باختراق عدد مِن حواسيب الشرِكات والحكومة الأَمريكية عام1989 بعملية أُطلق عليها اسم "cuberespionage" ومِن ثُم قامت ببيع المعلومات التي حصلت عليها إلى جِهاز مُخابرات الاتحاد السوفيتي السابق[14].
- **طاقم المرحلة السابعةThe Level Seven Crew**:في عام1999 تمكن فريق مِن هذِه المجموعة مِن اختِراق(60) نظاماً حاسوبياً لشخصيات رسمية وشركات حكومية في الولايات المتحدة مثل نِظام وكالة الفضاء الأَمريكية ناسا، وفنادق الشيراتون، وبنك (First American National)[15].
- **كلوبل هيلGlobal Hell** : اشترك في إنشاء هذه المجموعة شخص يُدعى Patrick Gregory، وهو أَحد أَفراد العصابات في هيوستن تكساس، يُقال أن هذه المجموعة مسؤولة عن تدمير المعطيات و المعلومات الخاصة بـ (155) موقعاً إلكترونياً، فضلاً عن تجارة المعلومات غير الشرعية، وتقدر الأَضرار الناجِمة عن أَفعالها بملايين الدولارات، قام فريق غريغوري أَيضاً بابتزاز وتخريب موقع الجيش الأَمريكي على شبكة الإنترنت، وكتب عبارة لن يموت "global hell will not die" على الموقع الإلكتروني للجيش الأَمريكي[16].
- **New Crack Program Hacker Group(NCPH Group)** : نشأت هذه المجموعة في الصين عام1994، بقيادة هكر يدعى Tan Dailin، الذي يُقال أَنهُ كان يعمل لصالح الجيش الصيني، لا يعرف عدد أفراد هذه المجموعة بدقة، لكن يُقال أنها مكونة مِن (10) أَشخاص إضافة إلى ثلاثة أَشخاص آخرين في القيادة، استخدمت GinWui وهي الـ rootkit التي طورها Dailin في مُهاجمة وزارة الدفاع الأَمريكية عام2006[17].
- **Lulz Sec** : تم انشائها عام2011 وشِعار هذه المجموعة Laughing at your security since، قامت المجموعة بِمُهاجمة Fox.com، وقاعدة بيانات X-Factor، وSony، وFBI،

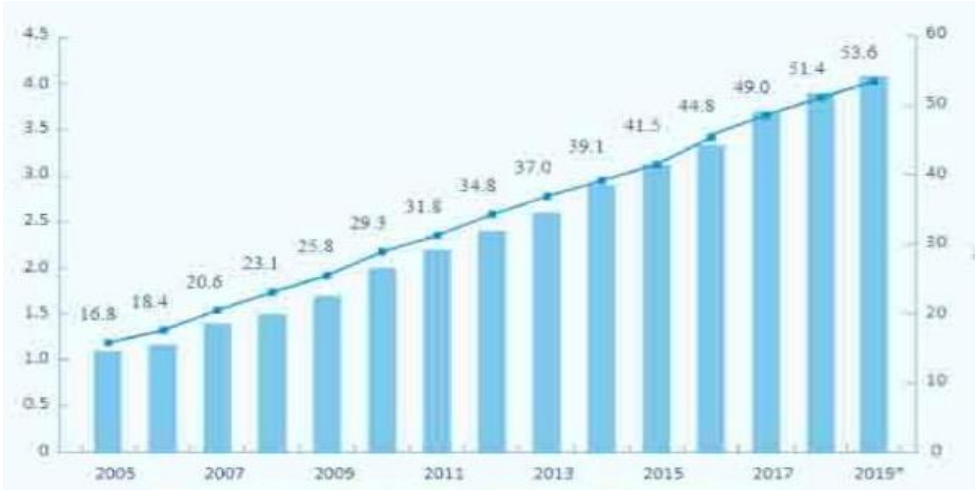
وCIA، وتسببت المجموعة بأضرار تُقدر بمليارات الدولارات. وكشفت LulzSec المعلومات الشخصية الخاصة بـ (73000) مُتسابق عند اختراقها لقاعدة بيانات X-Factor، اعتقل مكتب التحقيقات الفدرالي أَهم أَعضاء المجموعة عام 2012[18].

- **Milw0rm** : هي مجموعة مِن النُشطاء، شُكِلت عام 1998، كان هدفها الرئيس مركز الأَبحاث والدِراسات النووية في Bhabha في الهند، تمكنت المجموعة مِن الحصول على (5) ميغابايت مِن المعلومات السرية المتعلقة بالتجارب النووية الهندية، وحذفت المعلومات مِن مُخدمين في المركز، فضلاً عن ذلك اخترقت المجموعة الموقع الإلكتروني لشرِكة Easyspace التي تستضيف المواقع الإلكترونية، ونشرت رسائل مُناهضة للأَسلحة النووية على (300) موقع إلكتروني[19].

ثالثاً: توظيف الأَفراد للقوة السيبرانية

يُعد الفرد اليوم فاعِلاً مُهِماً في الفضاء السيبراني، لامتلاكهُ القدرة على إِحداث الثورة في المعلومات، وتصبح هذه الثورة مجال تستخدمهُ الدول نفسها[20]، ومِثال على ذلك ما قام بِه (جوليان اسانج) بتأَسيس موقع (ويكليكس) الخاص بنشر الوثائق السرية، ويتلقى الموقع معلومات وثائق مِن أَماكن حول العالم مِمن يرغبون في الكشف عن سلوكيات غير أَخلاقية في الحكومات والشرِكات[21]. كما لا يمكن إِخفاء الدور المهِم الذي قام بِه أَحد عُملاء وكالة الاستخبارات الأَمريكية (إِدوارد سنودن) إِذ قام بتسخير المعلومات التي حصل عليها بحكُم عمله في كشف مُمارسات المخابرات الدولية بشكلٍ عام والأَمريكية بشكلٍ خاص، ونشر الكثير مِن هذه الفضائح على موقع ويكليكس الذي أَشتهر بفضح الجرائم والانتهاكات التي يقوم بها الجيش الأَمريكي، حيثُ قام سنودن بتسليط الضوء على أَساليب الاستخبارات الأَمريكية وطرق التجسُس الإِلكتروني على دول العالم وأَنظمتها وكانت بداية ظهورهُ في عام2013 عندما سرب معلومات مُصنفة على أَنها سرية للغاية مِن وكالة الأَمن القومي الأَمريكي، على رأَسها برامج "بريزم" إِلى صحيفة "كارديانيا" و"واشنطن بوست" وهو برنامج سري تابع لوكالة الأَمن القومي الأَمريكي يعمل على استِخراج بيانات المستخدمين المخزونة ضمن أَجهزة خوادم شرِكات الانترنت الأَمريكية الكُبرى، وتنزيلها على أَنظمة شرِكات لكي تتمكن الوكالة مِن الوصول المباشر إِلى خوادم مركزية للموقع مثل كوكل وفيسبوك وياهو لاستِخراج رسائل البريد الإِلكتروني والمكالمات الصوتية ومقاطع الفيديو والصور والاتصالات الاخرى لمستخدمي تلك الشركات دون الحاجة إِلى الأَمر القضائي[22]. والشكل ذو الرقم (2) يوضح زيادة مُستخدمي الإِنترنت والمواقع الإِلكترونية عام2005 إِلى عام2019.

الشكل (2): زيادة عدد مُستخدمي المواقع الإلكترونية مِن عام 2005 إلى عام 2019



الشكل من إعداد الباحث بالاستناد إلى: بيانات الاتحاد الدولي للاتصالات2020.

يتضح مِن الشكل أعلاهُ أنَّ عدد مُستخدمي مواقع التواصل الاجتماعي والمواقع الإلكترونية حقق زيادة كبيرة مِن 2005- 2019 مِما يعني زيادة في دخول الفضاء الإلكتروني في الحياة اليومية للفواعل الدولية ودخولهُ في تكوين البُنية التحتية للدول، الأمر الذي انتج عنه سهولة اختراق هذه المواقع عن طريق هجمات الكترونية مِن خِلال برامج مُصنعة خصيصاً لهذا الغرض.

فضلاً عن كُل ما سبق، لم يقتصر دور الفرد في الفضاء الإلكتروني على ذلك انما هُنالك أفراد مُنفردين كانوا أم مُجتمعين لهم تأثير مُباشر أو غير مُباشر على الفضاء السيبراني ويُطلق عليهم أسم الهاكرز ويمكن تصنيفهم حسب درجة خطورتهم وتأثيرهم على الأمن الدولي إلى ما يأتي[23]:

- **الهاكر ذو القبعة البيضاء White hat hacker أو الهاكر الأخلاقي Ethical**: وهو ذلك الشخص الذي يستخدم قدراتهُ في مجال الكمبيوتر بصورة شرعية، ولا يترتب عليها الإضرار بمصالح الغير، ويحاول أنَّ يجد الثغرات في أنظمة الكمبيوتر لتأمينها مِن محاولة الاختراق الخارجية. وغالباً ما يلجأ كثير مِن الدول إلى تجنيد هذا النوع مِن القراصنة، بِما يمتلكهُ مِن قدرات مُتقدِمة في استِخدام التكنولوجيا الحديثة، ويحاول توظيفه في أعمال أخلاقية وشرعية، مثل ضبط الجرائم الإلكترونية، أو تجنيده في القوات المسلحة في وحدات إدارة الحروب الإلكترونية Cyber warfare[24].
- **الهاكر ذو القبعة السوداء Black hat hacker ويُسمى أيضاً Cracker**: وهو ذلك الشخص الذي يستغل قدراتهُ للإضرار بمصالح الآخرين، أو لتحقيق أهداف غير شرعية، مثل سرقة البنوك والبطاقات الائتمانية، واختراق الهواتف المحمولة ومواقع الإنترنت، حيثُ يتسم بقدرته على استخدام أدوات الاختراق

https://doi.org/10.61353/ma.0150535

والقرصنة الإلكترونية، بهدف السرقة والتدمير والتخريب، ويكثر وجود هؤلاء في "الإنترنت المظلم" Darknet، وهو جزء من الإنترنت، لكنهُ لا يظهر على مواقع البحث، ويتطلب برامج ومُتصفحات مُعينة لكي يمكن الولوج إليه مثل مُتصفح تور TOR، ويتم فيه بيع كُل ما هو ممنوع ومحظور قانوناً.

- **الهاكر ذو القبعة الرمادية Grey hat hacker**: وهو الشخص الذي يقوم تارةً بتأمين وحماية أَنظمة الكمبيوتر، وتارةً أُخرى يقوم باختِراقها لتحقيق أَهداف شخصية[25].

والتصنيفات السابِقة هي للهاكرز المحترفين بصورة أَساسية، الذين تكون أَسعارهم في سوق القراصِنة مُرتفعة. ولكن توجد أَيضاً درجة أَقل مِن القراصنة، فهُناك "الهاكر المنفرد" Lone Hacker الذي يمكن تسميتهُ أَيضاً YouTube Hacker، وهو يعتمد على تطوير قدراتهُ مِن خِلال مُشاهدة فيديوهات أَو قراءة مقالات حول الاختراق، وغالباً ما تكون قدراتهُ محدودة تعتمد على استِخدام الهندسة الاجتماعية Social Engineering أَو فن اختراق العقول، لتحفيز الضحية على فتح رابط مُعين به فيروس أَو برنامج ضار بِما يُطلق عليه "التصيُد" Phishing. وعلى الرغم مِن كونه أَشهر أَنواع القرصنة البدائية، فإِنهُ مِن أَكثر الأَنواع خطورة لأَنهُ يعتمد على إِثارة الميول الشخصية للضحية بهدف الإِيقاع به[26] . ونتيجة لكثرة الأَنظمة الإِلكترونية وتعددُها بين نظُم مالية خاصة بالمؤسسات المالية والبنوك، وأُخرى إِدارية مُتعلقة بإِدارة الشركات والمؤسسات، وثالثة أَمنية ذات صلة بتأمين المعلومات وحمايتها، ورابعة استراتيجية خاصة بإِدارة البُنية التحتية مثل محطات الطاقة والوقود، وخامِسة ذات صلة بنظم الملاحة وتحديد المواقع، وسادِسة مُتعلقة بالهواتف المحمولة، كانت هُناك حاجة تلقائية لتخصص الهاكرز في أَحد هذه الأَنظمة بهدف تغطية جوانبها كافة[27].

ومِن ثُم ظهر الهاكرز المتخصصون في سرقة بطاقات الائتمان والحسابات البنكية، وآخرون وظيفتهم اختراق البريد الإِلكتروني والحسابات والصفحات الشخصية على مواقع التواصل الاجتماعي، وغيرهم مُتخصصون في تطوير فيروسات تُستخدم كأَسلحة إِلكترونية[28] والشكل ذو الرقم(3): يوضح الفرق بين الدول، والمنظمات الإِجرامية، والأَفراد في استِخدام الفضاء الإِلكتروني.

https://doi.org/10.61353/ma.0150535

الشكل(3): الفرق بين الدول، والمُنظمات الإجرامية، والأَفراد في استخدام الفضاء الإلكترونية

الجهة التي تقف وراء التهديد	الدوافع	الأهداف	الأمثلة
 دول قومية، مجموعات ترعاها دول	جغرافية–سياسية، أيديولوجية	الاضطراب، التدمير، الضرر، السرقة، التجسس، الكسب المالي	تلف البيانات الدائم، الضرر المادي المستهدف، تعطيل شبكة الكهرباء، تعطيل نظام الدفع، التحويلات الاحتيالية، التجسس
 مرتكبو الجرائم الإلكترونية	الإثراء	السرقة، الكسب المالي	سرقة الأموال النقدية، التحويلات الاحتيالية، سرقة بيانات الاعتماد
 الجماعات الإرهابية، القراصنة، التهديدات الداخلية	أيديولوجية، الاستياء	الاضطراب	التسريبات، التشهير، الهجمات الموزعة لتعطيل تقديم الخدمة

المصدر: تيم مورر وآرثر نيلسون، التهديد السيبراني العالمي، (واشنطن: صندوق النقد الدولي،2021)، ص25.

يتضح مِن الجدول أَعلاه بان الهجمات الإلكترونية التي تقوم بِها الدول تختلف مِن حيثُ الدوافع والأَهداف عن الهجمات التي تقوم بها المنظمات الإجرامية والأَفراد.

نخلص مِن كُل ذلك بأنَّ الفضاء الإلكتروني فتح المجال لظهور فواعل جديدة في العلاقات الدولية وتمكينها مِن امتِلاك القوة التي كانت حِكراً على الدول القومية فظهر فواعل جدَّد مِن الشركات والمنظمات الإجرامية بل أَكثر مِن ذلك ليُمكن الأَفراد بان يكون لهُم دوراً مؤثِراً في التفاعُلات الدولية مِن خِلال الاستِفادة مِن الخصائص التي يمنحها لهم الفضاء الإلكتروني مِن سهولة امتلاك مقوماتهُ والتخفي وعدم الكشف عن الهوية بِما شكل ذلك تهديداً جديداً للأَمن الدولي.

المِحور الثاني: توظيف الفاعلين العنيفين مِن غير الدول للقوة السيبرانية وأَثرها في الأَمن الدولي

زاد الاهتِمام في الآونة الاخيرة بدِراسة الفاعلين مِن غير الدول بِمن فيهم الفاعلين العنيفين في حقل العلاقات الدولية، على الرغم من أنَّ هذا الاهتِمام جاء مُتأخراً بالمُقارنة بالاهتِمام بباقي الأَنواع. إذ يقصد بالفاعلين العنيفين مِن غير الدول بأَنهم الجماعات أَو التنظيمات التي تلجأَ إلى استخدام أَدوات العنف المادي والنفسي بطريقة جماعية، ذلك مِن أَجل تحقيق غايات مُعينة، فهم لا ينتمون لأَجهزة الدولة الرسمية [29] وكما يُشير

المفهوم إلى المنظمات أو الجماعات المسلحة التي تتبنى العنف غير الشرعي لتحقيق أهدافها، ومِن ثُم تتحدى احتِكار العنف للدولة [30].

وتتمثل أهم أساليب التنظيمات الإرهابية (كذلك باقي التنظيمات العنيفة العابِرة للحدود) للتأثير في الأمن العالمي بإحدى أو أكثر مِن الأساليب التالية: "عمليات التفجير، الاختطاف، احتجاز الرهائن، المصادر والابتزاز، تخريب وتدمير المنشآت العامة، الاغتيالات، خطف الطائرات، التهديد بالعمليات الكاذِبة، القرصنة السيبرانية والإرهاب السيبراني...."[31]. فأنشطة التنظيمات الإرهابية قد شهدت تحولات كبيره ومُثيرة للقلق وتميزت بخصائص جديدة عديدة أهمُها انتشار رقعة الإرهاب لتشمل جميع مناطق العالم بدلاً مِن حصرها بمنطقة مُعينة، كما حققت العمليات الإرهابية اقصى درجات التأثير في الأمن الدولي عن طريق انتِشار التقنية الحديثة في وسائل الإعلام، إذ ساعدت الملايين مِن البشر على مُتابعة الأحداث كافة بصورة مُباشِرة على الهواء في كُل أنحاء العالم، مِما كان لهُ الأثر الكبير في زيادة تأثير هذه الهجمات على أمن واستِقرار الدول وهو ما يُشكل بالنتيجة نجاحاً للعمليات الإرهابية ومِن ثُم تهديداً للأمن الدولي عبر توظيف حروب الجيل الخامس، وبهذا فقد شكلت التحولات الأخيرة في نشاط المجموعات الإرهابية والمجموعات العنيفة المسلحة المختلفة نقطة تحول في مسيرتها، إذَّ تعاظم تأثيرها عبر تحولها إلى مجموعات مُنتشِرة في كُل أنحاء العالم وتهديد الاستقرار الأمني للدول والمجتمعات[32].

فالتكنولوجيا تُمثل أحد الأدوات الاستراتيجية التي تُمكن المنظمات الإرهابية مِن توظيف الأنترنت وسائر التطبيقات في مجموعة واسِعة ومتنوعة مِن الأغراض لتشمل التجنيد، والتمويل، والدعاية والتدريب. فضلاً عن تحريض الأخرين على القيام بأعمال إرهابية أو جمع المعلومات ونشرها لنفس الغرض وبقصد الاضرار بالأمن الدولي[33].

كما أنَّ تنامي ثورة التكنولوجيا والاتصالات وتسارُع تأثيرها في نشاط التنظيمات الإرهابية في العقود الأخيرة أدى إلى تبلور نمط جديد مِن الإرهاب هو الإرهاب المعولم. الذي تشترك فيه التنظيمات الإرهابية المحلية في مُختلف أنحاء العالم ونتيجة توسع النشاط في ظل العولمة أخذت تنتج شبكة مِن العلاقات العابرة للحدود فيما بينها، وقد وحدت في سابقة تنظيمات إرهابية مثل "القاعدة" أو "داعش" لزيادة قوتها وتأثيرها وانتشارها عالمياً عبر الانقياد إلى سياقات في التجنيد والتمويل تتجاوز النطاق المحلي. ومِن هذا المنطلق أصبح "الإرهاب المعولم" يُمارس نشاطهُ داخل دولة أو اقليم مُعين، لكي يستمد دعمهُ وأسبابهُ وذرائعهُ مِن شبكة عالمية مِن التنظيمات ذات صيغة عالمية[34].

وهُناك أشكال عديدة من الفاعلين العنيفين مِن غير الدول وأهمُها أُمراء الحروب، التنظيمات الإرهابية، الجماعات المتمرِدة، جماعات الجريمة المنظمة العابِرة للحدود، وشرِكات الأمن الخاصة، وتجنُباً للإطالة ارتى الباحث الأخذ النماذج الآتية:

أولاً: توظيف تنظيم القاعدة للقوة السيبرانية في التفاعُلات الدولية

أدرك تنظيم القاعدة مِنذُ فترة مُبكِرة أهمية القوة الإلكترونية، في الاشتباك مع الخصوم على جبهات عدة في وقت واحد، وضرورة نشر أفكارهُ، فتبلور لديه مفهوم الحرب الإلكترونية، إذ يرى البعض أنَّ بداية توجه تنظيم القاعدة للقوة الإلكترونية بدأ مِنذُ عام2000، ذلك بإطلاق أول موقع لهُ باسم معالم الجهاد[35]. لكن البعض الأخر يرى أنَّ التنظيم قد بدأ في استِخدام القوة الإلكترونية بالفعل بعد أحداث11 أيلول/سبتمبر 2001، بتوظيف الفضاء الإلكتروني مِن خِلال (13) موقع، وصلت في2012 إلى (4800) موقع، أهمُها موقع مؤسسة السحاب الإعلامية والتي كانت مُهمتها بث بيانات قيادات التنظيم. بعد أنَّ أيقن تنظيم القاعِدة أهمية الفضاء الإلكتروني، وبالأخص بعد تعرضهُ لخسائر كبيرة على أرض الواقع، وتشديد القيود المفروضة علية للحد مِن استخدامهُ القوة التقليدية مِن خِلال هجماتهُ باستِخدام الأسلحة التقليدية على أرض الواقع[36]. فسعى إلى أنَّ يكون لدية قوة إلكترونية تعمل جنباً إلى جنب مع القوة الصلبة وتزيد مِن فاعليتها، في ظل المميزات العديدة للفضاء السيبراني والتي مِن أهمُها[37]:

1. انخفاض تكلفة استخدامهُ، بنشر المعلومات عن التنظيم والتواصل مع أعضائه وتجنيد عناصر جدُّد.
2. يعمل الفضاء الإلكتروني على تقوية الشعور بالهوية الجماعية، وزيادة الانتِماء بين أفراد الجماعة الواحدة، ويزيل الفوارق بينهم، ويعتبرهُم أبناء مُجتمع واحد ويتشاركون قيماً واحِدة ويؤمنون بقضايا واحدة.
3. سايعد على قيام علاقات وجهاً لوجه، رغم وجود مسافات جغرافية، فتخلق مُجتمعات افتراضية[38].
4. كذلك بإمكان المجموعات الصغيرة من أنَّ يكون لها وجود الكتروني يُساعدها من تقديم أفكارها لملايين مِن الناس، بِما يُساعد على حشد المؤيدين مِن مُختلف بقاع الأرض.
5. امكانية استخدام الفضاء الإلكتروني لجمع الأموال، والمعلومات الاستخبارية.
6. سهولة التخفي بأسماء مُستعارة، وضعف رقابة الدول على المحتويات المقدمة على الانترنت[39].

جميع هذه المميزات جعلت من الفضاء الإلكتروني، أداةً استراتيجيةً لدى تنظيم القاعِدة، بهدف تحقيق غايات وأهدف عديدة مِن أهمُها[40]:

- التجسُس والحصول على المعلومات الاستخبارية، ولاسيما أنَّ الانترنت مُكتظ بمثل هذه المعلومات.
- نقل الأخبار مع أعضاء التنظيم والتواصل معهُم.
- إرسال الوثائق والبيانات الخاصة بهم أو بالعمليات التي يستهدفونها، بعيداً عن رقابة السلطات.
- تجنيد الشباب واستِقطابهم للتنظيم، مِن خِلال نشر الحماس، ذلك للحفاظ على استمراريه التنظيم.
- إصدار المعلومات والتلقين الإلكتروني، عن طريق توفير المواقع والمُنتديات الخاصة بالتنظيم.
- جمع الدعم المادي، نظراً للمُراقبة الشديدة على التحويلات المالية بالأخص بعد أحداث سبتمبر2001[41].

- تقديم الغرب بأنه المُعتدي في المواجهة بين الشرق والغرب.
- خلق صورة نمطية حول الجِهاد العالمي باعتبارهُ استراتيجية دفاعية للحِفاظ على الإسلام.
- تصوير قدرة التنظيم بأنها أقوى مِما هو عليه في الواقع، من أَجل تحميس المتعاطفين والراغبين في الانضمام ومحاولة إرباك الخصم.
- أَيضاً الحفاظ على شرعية التنظيم مِن خِلال التربية الدينية، على أَساس النصوص الانتقالية ونشر الفتاوى التي تُجيز أَعمال العنُف.

كما أثر الفضاء الإلكتروني الذي دعمتهُ العولمة وثورة الاتصالات، في حدوث تحولات كبيرة في بُنية تنظيم القاعدة بشكلٍ عام، وعلى صعيد الوعي الأيديولوجي والعمليات الحركية. حيثُ اعتمد تنظيم القاعدة في توظيف القوة الإلكترونية على أَدوات عدة مِنها ما يلي[42]:

1.المواقع الإلكترونية: وهي مجموعه صفحات على الويب مُرتبطة ببعضها ومخزونة على نفس الخادم، وتختلف أهدافها حيثُ هُناك مواقع تجارية، ومواقع خاصة بالمحادثات أَو مُنتديات للنِقاش، بالإضافة إِلى المدونات الإلكترونية وهي مواقع ويب يكتب فيها مُستخدمها عن آرائه في المجالات المختلفة.

2. شبكة التواصل الاجتماعي: شبكة اجتماعية تتيح لمستخدميها التواصل في أَي وقت كان ومكان في العالم، وأَهمُها فيسبوك وتويتر واليوتيوب. وتُقسم مواقع تنظيم القاعِدة في مواقع التواصل الاجتماعي إِلى مواقع مُتعدِدة وتشمل مواقع رِجال الدين المؤَيدين للتنظيم أَو أَحد أَعضائه، الذين يضيفون شرعية على التنظيم مِن خِلال فتأَويهم، والمنتديات كمُنتدى الحسبة ومُنتدى الفلوجة الإِسلامي ومنبر التوحيد والجِهاد ومواقع خاصة بالتوزيع وهي غير ثابتة، لعدم تتبعها، ولا يقوم التنظيم بإدارتها بنفسهُ، لكنها تلتقي في الخطوط العامة معهُ، وتعمل تحت إِشراف مركز الفجر الإِسلامي، وهو مسؤَول عن استِلام المواد الإِعلامية مِن تِلك المؤَسسات وعمل المونتاج لها ونشرها المواقع المتعاطفة مع تنظيم القاعِدة؛ وهي مواقع سلفية الغرض والمحتوى ومُتعاطفة مع التنظيم رغم عدم تبعيتها لهُ.

وطُرِحت فكرة فقدان الملاذات الأَمنة على أَرض الواقع نتيجة ضرورة البحث عن اخرى أَمنة في المجال الافتراضي، فلجأَ تنظيم القاعِدة إِلى الاهتِمام بالقوة الإِلكترونية، وعمل على توظيف هذه القوة في التفاعُلات الدولية وبأَشكال مُتعدِدة وتركها أَثاراً كبيرة على الأَمن الدولي ومِنها:

أ- **استعمال الفضاء الإِلكتروني كمنصات إعلامية**: إِذ تتولى المواقع التابعة لتنظيم القاعدة بنشر الأَخبار عن التنظيم وعن العمليات التي قام بتنفيذها، أَو حتى نفي مسؤولية عن بعض الأَعمال والأَنشطة، إِذ تُعد مؤسسة السحاب الإِعلامية التابِعة للقاعِدة مِن أَبرز النماذج الإِعلامية في هذا الصدد[43].

https://doi.org/10.61353/ma.0150535

ب- **الدعاية والترويج لأفكار التنظيم**: يُعد الفضاء الإلكتروني مِن الوسائل المهمة لتنظيم القاعدة، لنشر أفكارهُ وكسب مُتعاطفين جدُّد، ايضاً كحرب نفسية على الأعداء، حيثُ نمت الآلة الإعلامية الإلكترونية للتنظيم مِنذُ هجمات 11 سبتمبر 2001 بشكلٍ مُطرد.

ت- **تجنيد أتباع جدُّد**: إذ اتاح الفضاء الإلكتروني لتنظيم القاعِدة فرصة تجنيد أعضاء جدُّد في التنظيم، مِما يضمن استمراريتهُ وبقائه، يتم ذلك مِن خِلال قدرتهُ على الدعاية وبث الأفكار، والعمل على تحسين صورتهُ خاصةً مع ظهور الفيسبوك وتويتر ويوتيوب، إذ أكدت صحيفة واشنطن بوست على أنَّ التجنيد في صفوف التنظيم قد تضاعفت بصورة كبيرة بعد ظهور هذه المواقع(44) .

ث- **التنسيق للعمليات المُسلحة عبر الوسائل التواصل الاجتماعي**: يُعد تويتر أحد أهم وسائل التواصل الاجتماعي التي تُستخدم للتواصل والتنسيق أثناء العمليات الإرهابية، فالميزة الأبرز لتويتر بالنسبة لتنظيم القاعِدة تكمنُ مِن أنهُ يخلق مُجتمعات افتراضية مُتغيرة، التي تتكون تلقائياً خِلال الأحداث والقضايا الكُبرى، ويقوم التنظيم بالاستِفادة مِن ذلك عبر مُتابعة أحداث المعلومات عن أي قضية تظهر في المجال العام.

ج- **استخدام الفضاء الإلكتروني كساحة تدريب افتراضية**: يستخدم تنظيم القاعِدة موقع يوتيوب بصورة أساسية بهدف التدريب، ذلك مِن خِلال نشر فيديوهات تكون مُتاحة للجميع، حيثُ أنَّ الوظيفة الرئيسية لليوتيوب هُنا هي استِضافة الفيديوهات التي تحمل مِن قِبل المشتركون على الموقع، لكن هناك قيود على الفيديوهات التي تنشر التنظيمات الإرهابية، إذ يمكن لإدارة الموقع حذفها تماماً، لكنهُ يتطلب قيام أشخاص إبلاغ عن هذه الفيديوهات ثُم يتم بعد ذلك مُراجعتها ثُم حذفها. هذا ما يتيح فرصة لسرعة نشرهُ على المواقع والمنتديات، ومِن ثُم تتم مُشاهدتهُ مئات المرات مع إمكانية عمل Download مِن قِبل رواد هذه الموقع على حواسيبهم الشخصية، ففي الغالب تكون هذه الفيديوهات المنشورة عِبارة عن محتوى كيفية صنع قنبلة وفيديوهات تدريب للقِتال وهكذا ومِن كُل ما سبق، فأنَّ وظيفة اليوتيوب مُكملة لوظيفة المنتديات وشبكات التواصل الاجتماعي، إذ يتم نشر وسائل تنظيم القاعِدة في الأخيرة وفي الأولى توضح شرح لكيفية عمل هجمات على أماكن مُحددة وكيفية استخدام الأسلحة وغيرها(45).

ح- **جمع الأموال**: استغل تنظيم القاعِدة الفضاء الإلكتروني لغرض تسهيل التحويلات المالية فيما بينهم، والحصول على التبرُعات المالية، مُستغلاً بذلك سهولة استخدام تلك المواقع لتحويل التبرعات والدعم المالي، مع ضعف الرقابة وانعِدام إمكانية التحقُق مِن هوية مُتلقي تلك التبرُعات في بعض الأحيان(46).

خ- **تشويه الخصوم**: عمل التنظيم على استخدام الفضاء الإلكتروني لتشوية خصومهُ، كنشر صور لعدوان وهجمات الولايات المتحدة على مدنيين، ومع اندِلاع حركة التغير في سوريا عام 2011 قام تنظيم

القاعدة بنشر وبث صور ومقاطع عن جرائم العنُف الجماعي ضد المدنيين التي قام بِها الرئيس السوري (بشار الأَسد)[47]. كذلك استخدم التنظيم الفضاء الإِلكتروني في الهجوم على ما يُسمى بتنظيم الدولة الإِسلامية في العِراق والشام (داعش) بعد الخِلافات معها، إذ اتهمها بالمغالاة في التكفير والقتل المفرط، وتم قتل (أبو خالد السوري) القيادي في تنظيم القاعدة وأَمير حركة أَحرار شام في حلب على يد تنظيم (داعش) عام2014، وانحرفت عن منهج التنظيم[48].

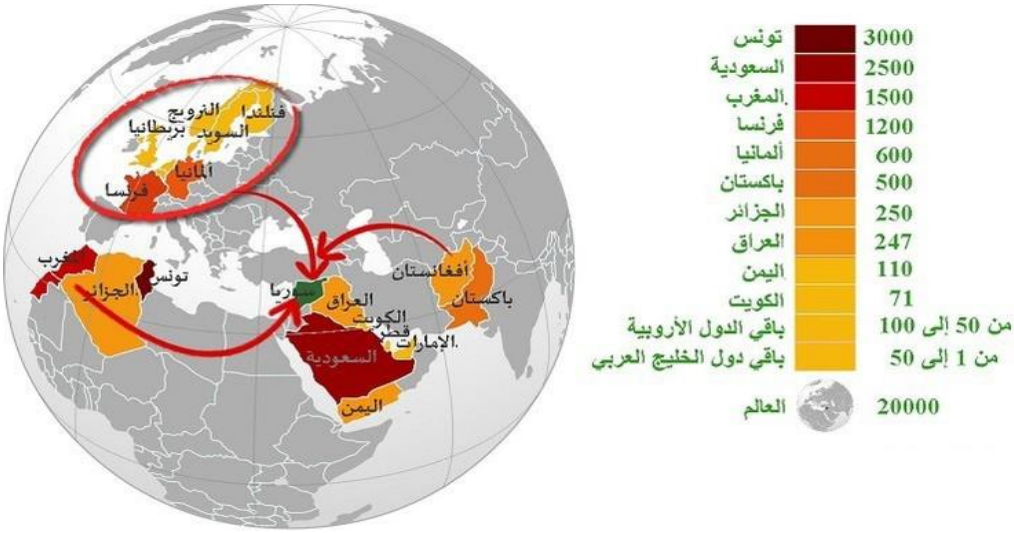
د- **القرصنة الإِلكترونية:** يتم استِخدام مواقع الانترنت مِن قِبل التنظيم لتنفيذ هجمات افتراضية على المواقع الإِلكترونية التابِعة للدول حول العالم، وبنوك بهدف تعطيلها، أَو الحصول على المعلومات التي تخدم أَهدافهُ، إِذ يوكد تنظيم القاعِدة على أَنَّ الحرب الإِلكترونية لا تقلُ أَهميةً عن الحرب على أَرض الواقع[49] .

وعلى الرغم مِن كُل ما حققهُ تنظيم القاعدة مِن استغلال الفضاء الإِلكتروني لغرض تحقيق أَهدافهُ وتأَثيرهُ على الأَمن الدولي، لكن هُناك حدود وعوائق تقف أَمامهُ وتحدُ مِن قدرتهُ على التحرُك بحرية داخل هذا الفضاء الافتراضي، ذلك مِن خِلال الاستراتيجيات التي تتخذها الدول سِواءً للدفاع عن أَمنها الإِلكتروني، أَو لِمُراقبة أَعضاء التنظيم والقبض عليهم وايقاف مواقع التنظيم على الانترنت[50].

ثانياً: توظيف عصابات داعش الإِرهابية للقوة السيبرانية في التفاعُلات الدولية

استخدمت عصابات داعش الإِرهابية الفضاء الإِلكتروني بشكلٍ مُكثف وناجح، على نحوٍ غير مسبوق يتفوق فيه على كُل الجماعات الإِرهابية الأَخرى، إِذ يرى بعض الخُبراء أن توظيف داعش للفضاء الإِلكتروني يعكس قدراً كبيراً من الاحترافية والتعقيد في الأَداء، سِواءً فيما يتعلق بعدد المنصات الإِعلامية التابِعة له، أَو التقنيات التي يستخدمها، أَو الموضوعات التي يتناولها، أَو الجمهور الذي يستهدفه، إِذ يعد تنظيم داعش الإِعلام أَداة قتال رئيسة في معركته مع الأَعداء، مِما أَعطى التنظيم أَهمية كبيرة للفضاء الإِلكتروني، باعتبارهُ وسيلة أَساسية لنقل المخرجات الإِعلامية للتنظيم التي تتسع لتشمل المجلات والأَفلام الوثائقية والإِصدارات المرئية ووكالات الأَنباء والمحطات الإِذاعية وغيرها، إِذ يتم ترجمتها إِلى لُغات مُختلفة، كذلك نجح التنظيم بشكلٍ واسع في توظيف شبكات التواصل الاجتماعي التي لم تصبح فقط عنوان لهويتهُ الإِلكترونية بل منصة للسلطة والقوة[51]. والشكل ذو الرقم (4) يوضح عدد الوافدين لداعش.

الشكل(4) : عدد الوافدين إلى عصابات داعش لغاية عام2015، جلهم عبر الفضاء الإلكتروني

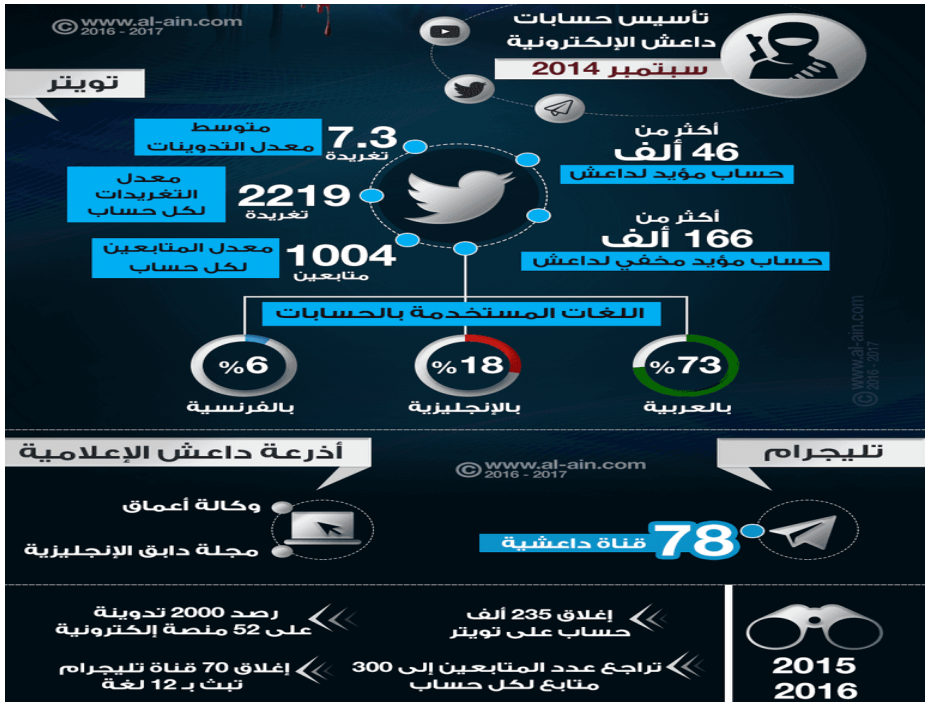


المصدر: نقلاً عن : قناة روسيا اليوم، بالأَرقام.. من أين جاء مقاتلو "داعش؟"، بحث منشور عبر شبكة المعلومات الدولية (الانترنت)، مُتاح على الرابط الآتي: https://www.arabic.rt.com

وأَصدرت عصابات داعش عدد مِن المجلات الدورية الشهرية والأَسبوعية تأَتي في مُقدمِتها مجلة النبأ ودابق وغيرها مِن المجلات التي تصدر باللغات الأَجنبية مثل دار السلام وعدد اخر مِن المجلات والقنوات التي تصدر بعدة لُغات، مثل مجلة الشباب الأَسبوعية، ومِن خِلال مُتابعة المحتوى الذي تبثهُ المنصات الإِلكترونية التابِعة لتلك العصابات نستطيع أَنَّ نُلحظ احترافية القائمين على استراتيجية عصابات داعش الإِعلامية، والأَمر الذي يظهر جلياً مِن خِلال استِخدام عناوين مؤثرة باقتباس بعض العناوين مِن القران الكريم أَو ربط هذه العناوين بتاريخ الإِسلام وبطولاتهُ[52]. والشكل ذو الرقم(5) يوضح نشاطات عصابات داعش الإِلكترونية.

https://doi.org/10.61353/ma.0150535

الشكل(5): نشاطات عصابات داعش الإلكترونية



المصدر: نقلاً عن شبكة العين الإخبارية، مُتاح على الرابط الآتي: https://www.al-ain.com

إذ يعمل التنظيم على تحديد المحتوى المنشور لهُ عبر قنواتهُ الإلكترونية، بالتركيز على الأخبار العاجِلة التي لا يتعدى مداها(48) ساعة، بغرض إعلام أفرادهُ بتحركاتهُ، ولتشتيت الخصوم، كذلك لتوصيل رسالة مفادها أنَّ التنظيم ما زال موجوداً، فضلاً عن نشر المعلومات عن العمليات التي يقوم بها، كذلك تبني العمليات الإرهابية التي يقوم بِها أعضائه[53]. وعِند مُتابعة المحتوى الإعلامي للتنظيم في الفضاء الإلكتروني يلحظ أنَّ لدى التنظيم نوعين مِن الرسائل حسب الجمهور المستهدف وهي[54]:

1. **الرسائل الايجابية التطمينية:** إن هذا النوع مِن الرسائل كان يستهدف المناطق التي كانت خاضِعة لسيطرته التامة، مثل مدينة الرقة والموصل على سبيل المثال، حيث تتضمن هذه الرسائل نجاحات داعش في تكوين مؤسسات وتوفير الخدمات الأساسية للمواطنين مِن الغذاء والسكن، وكيف أنَّ التنظيم، يوفر الأمن، وهذا ما كان يُمثل قُرابة (25%) مِن إجمالي دعاية التنظيم، إذ يحاول أنَّ يُظهر بأنهُ حركة اجتماعية عالمية تُطالب بالعدل والحق وليست مُنظمة إرهابية تُهدد الأمن الدولي.
2. **رسائل عنيفة أو ترهيبية:** في الغالب تتضمن هذه الرسائل الأعمال الوحشية ذات الطابع العنيف المصاغ بشكلٍ مسرحي استعراضي مُناسب للاتجاهات السائدة كشيء شائع بشكلٍ مألوف للأفراد من كُل أنحاء

العالم، يعتمد على تسهيل تقبلهم للأَحداث العنيفة التي يستهلكونها سواءً في العاب الفيديو أَو في أَفلام المسلسلات أَو يشاهدونها في الأَخبار، حيثُ يتم التركيز على المشاهد التي ينتصر فيها مقاتلو التنظيم والمشاهد التي يقاتلون فيها بشراسة وتصويرهم على أنهم لا يُهزمون.

فقد استثمر داعش الجهود والموارد في مُختلف وسائل الإِعلام إِذ تقوم مؤَسسة الحياة، ذِراع داعش الإِعلامي الرئيس، مِن خِلال إِنتاج الأَفلام التي تتراوح بين مقاطع الفيديو مُدتها (3) دقائق تصور عمليات قطع رؤوس الخصوم، كذلك نشر وثائق تزيد مدتها عن ساعة، والكثير مِنها عبارة عن مُنتجات عالية الجودة تتضمن تقنيات ومؤثرات خاصة على غِرار المستخدمة في هوليود. كذلك مجلة دابق التي تعد النشرة الإِخبارية الرئيسة لداعش، التي تجمع بين الأَبعاد العسكرية والسياسية، فضلاً عن التعليقات والتغيرات الدينية، جميعها يتم ترويجها بشكلٍ أَساسي باللغة الانجليزية بدلاً مِن اللُغة العربية، كما لديهم أَيضاً ترجمات إِلى اللُغات الغربية الاخرى، مثل الفرنسية والأَلمانية والروسية وحتى الالبانية.[55] وتعد مقاطع الفيديو التي يبثها تنظيم داعش والتي تم إِنتاجها باللغة العربية وتكون مصحوبة بترجمة باللغة الانكليزية واضِحة ومهنية، هذه ميزة لم يسبق لها مثيل في مقاطع الفيديو التي تم إِصدارها رسمياً مِن قِبل مجموعات مُتطرفة اخرى [56].

وبعد سلسلة الهزائم التي خسر خِلالها عصابات داعش الإِرهابية الأَراضي في العِراق وسوريا مِنذُ أَواخر عام2015، إِذ لجأت تِلك العصابات إِلى تصعيد حملتها لنشر العنف خارج نطاق الشرق الأَوسط، وعملت على حث وسائل الإِعلام الإِلكترونية التابعة لها والتي أُطلق عليهم تسمية (الذئاب أَو الأَسود المنفردة) على قتل أَعداء التنظيم في بُلدانهم الأَصلية، ففي صيف عام2016 أَصدر التنظيم العدد الأَول مِن مجلة الرمية التي تحث اتباع ومؤيدين داعش في الغرب على تنفيذ هجمات مُنفردة ضد الأَهداف السهلة مُهدِدة بذلك الأَمن الدولي، بِما في ذلك رُكاب المواصلات العامة وكذلك الشباب الذين في المنتزهات وغيرهم، فقد نجح التنظيم عبر الاستخدام الماهر والتخطيط الافتراضي في زيادة العنُف السياسي في الغرب، مثل الهجمات التي حصلت مِن عام2011 إِلى2015 في باريس وبروكسل وسان بيرناردينو وأَورلاندو مُهدِدة بذلك الأَمن الدولي[57].

كُل ذلك أَدى إِلى ظهور مفهوم (الإِرهاب الموجه عن بُعد) إِذ يقصد به الهجمات التي يسبق لمنفذيها أَنَّ سافروا إِلى مناطق الصِراعات، أَو انظموا إِلى عصابات داعش الإِرهابية، ولكنهم كانوا على تواصل دائم مع عناصر التنظيم الإِرهابي ذلك مِن خِلال استِخدام منصات ووسائل الاتصال المشفرة، وذلك لتوفير الدعم والنصيحة للمهاجم في كُل مرحلة مِن مراحل الإِعداد[58]. كذلك المستفيدة تلك العصابات مِن الفضاء الإِلكتروني في توفير الدعم المالي للعناصر التابِعة لها للقيام بعملية إِرهابية، كذلك في انتقاء المناطق التي سيتم استهدافها، مِن خِلال التعريف السابق[59].

فقد خصص التنظيم مبالغ كبيرة لتمويل القنوات الفضائية والمحطات الإِذاعية والمواقع الرقمية عبر شبكة الانترنت، وأَعلن التنظيم إِصدار أَول صحيفة باسم دابق واستيديو أَجناد وقناة الفرقان وقناة الاعتصام وقناة

الحياة[60]. كذلك استِخدم التنظيم للفضاء الإلكتروني لتدريب أَعضائه عبر مُختلف أَنحاء العالم على كيفية صِناعة المتفجرات والقنابل وكيفية استخدامها، والترتيب للعمليات الإرهابية وتحديد وقتها، أَيضاً لتحفيز عناصرهُ ومؤَيدة مِن خِلال استِخدام الأَناشيد الحماسية، وإِظهار التنظيم بصورة المنتصر أمام أَعضائه مِن خِلال الخطب والبيانات التي ينشرها التنظيم الدائمة ونشر الوعود الكاذبة لأَعضائه بقدرته على امتداده الحتمي وهزيمة الدول الغربية والعربية التي تُحاربه[61].

فضلاً عن استغلالهُ لمواقع التواصل الاجتماعي كوسيلة لتحديد أَهدافهُ والتعرُف عليها ومُراقبة تحركاتهُ، وبالأَخص في إِطار عمليات الاغتيال التي تُطال بعض رموز الأَجهزة الأَمنية أَو السياسية في الدول المستهدفة، مِن خِلال مُراقبة من يمتلك حِسابات على تِلك المواقع أَو مُراقبة دائرة اصدقائهم ومعارفهم للوصول اليهم وجمع البيانات اللازمة عن تحركاتهم، مِما يوفر الجهد والوقت اللازمين للقيام بهذه المهام على أَرض الواقع كذلك ضمان سرية المراقبة[62] فقد ركز تنظيم داعش بدرجة كبيرة على الفضاء الإِلكتروني في فترة سيطرتهُ على مدينة الموصل عام2014-2017 وأَصبح يعمل بقوة في هذا المجال، إِذ فتح العديد مِن الحِسابات على مواقع التواصل الاجتماعي وتطبيقات الهواتف ومواقع نشر الأَخبار وكان يعمل بجِد لكي يقوم بنشر الفيديوهات المتنوعة الذي يُريد إِيصالها إِلى مُتابعيه ومُناصريه وهي أَغلبها رسائل فيها تطمينات عن أَنَّ التنظيم باقي ويتمدد وهو الشعار الذي رفعهُ التنظيم عند بداية احتلاله مدينة الموصل، أَيضاً توجيه الرسائل إِلى خصومه بنشر أَفلام الرعب مِن قتل وحرق كما فعل مع الطيار الأَردني (معاذ الكساسبة) عندما قام بتسجيل فيلم عن عملية حرقهُ[63].

وإِضافة إِلى كُل ما ذُكِر، فأَنَّ استِغلال التنظيمات الإِرهابية لمواقع الفضاء الإِلكتروني أَصبح أَمراً واضِحاً فأَنَّ المطلوب مِن الأَجهزة الأَمنية وشرِكات صِناعة المحتوى هو أَكبر مِن مُتابعة وحذف المحتوى المنشور مِن قِبل التنظيمات الإِرهابية عبر مواقع التواصل الاجتماعي بل زيادة دورها لغرض قطع الطريق أَمام هذه التنظيمات مِن النشاط في هذا المجال، وتفادي الأَضرار الناجمة عن ذلك مِن خِلال سن قوانين وشروط صارِمة على إِنشاء المحتوى لكي لا يكون الفضاء الإِلكتروني مُتاح بسهولة للتنظيمات الإِرهابية.

الخاتِمة

أَسهمت مُتغيرات القرن الحادي والعشرين وتحولاتهُ التكنو اقتصادية مِن تحول مسار القوة وانتشارها إِلى فاعلين مِن غير الدول، أثروا سلباً على الأَمن العالمي. فبجانب قوة الدولة الصلِبة والناعِمة ظهرت القوة السيبرانية التي أَصبح لها تأَثيرها على المستويين المحلي والدولي، إِذ أَدت إِلى تعدُد مستويات القوى بين الفاعلين دون حصرها بالدولة، كما مكنت الفاعلين الأَصغر في السياسة الدولية مِن مُمارسة كُل مِن القوة الصلِبة والناعِمة عبر الفضاء الإِلكتروني، وهو ما يعني تغيراً في علاقات القوى في السياسة الدولية. وفرض واقع الفضاء

السيبراني إعادة تعريف لبعض المفاهيم المهِمة: مثل الأَمن والصِراع والقوة، فبدأَ الاهتِمام المتصاعد بهذا الفضاء كتهديد أَمني. ومِن ضمن ما خرج به الباحث مِن استنتاجات:

- إنَّ التكنولوجيا الحديثة كان لها دوراً في ظهور فواعل جدُّد في النِظام الدولي مِن غير الدول، وساعدت على تخطي الحواجز الجُغرافية ما بين الدول، وكما ساهمت في انتِشار القوة بين الفاعلين المستخدمين لها فلم تعد القوة حكراً على الدولة، بل أَصبحت في متناول الفاعلين مِن غير الدول بِما فيهم الفاعلين العنيفين مِما أَدى إلى ظهور تحديات ومصادر تهديد للأَمن الدولي غير تقليدية، مثل الإِرهاب الإِلكتروني والتجسُس، وهذا قاد إلى تراجُع مفهوم سيادة الدولة، ذلك ما جعل مِن الضروري أن تمتلك الدول أَدوات وعناصر القوة السيبرانية التي تُمكِنها مِن مواجهة هذه المخاطر المحتملة بالدفاع أَو الهجوم الإِلكتروني.
- تتميز أَطرف الحروب السيبرانية بعدم الوضوح وتكون تداعياتها خطيرة سِواءً عن طريق تدمير المواقع على الإِنترنت ونسفها وقصفها بوابل مِن الفيروسات أَو العمل على استِخدام أَسلحة الفضاء السيبراني المتعدِدة.
- هُناك علاقة وثيقة ما بين الفضاء السيبراني والأَمن الدولي نتيجة التوسع في تبني الحكومات الإِلكترونية، واتِساع مُستخدمي وسائل الاتصال في العالم. فارتبطت التكنولوجيا بالتحولات في القوة.
- إنَّ استِخدام الفضاء الإِلكتروني يُعد مُتاحاً للفاعلين مِن غير الدول، والذي أَثر على سيادة الدولة وتحول الصِراع إلى صِراع إِلكتروني، وهو يقوم على التجسُس، والتسلُل، ثُم النسف، أَي تدمير المواقع على الإِنترنت، وقصفها بوابل مِن الفيروسات، للنيل مِن سلامتها. ومِن ثُم أَصبح تأَمين الفضاء الإِلكتروني جزء لا يتجزأَ مِن استراتيجيات الأَمن القومي للعديد مِن الدول.
- إنَّ الشبكات الإِلكترونية تسمح للجهاديين بالحفاظ على وجودهم والتنسيق فيما بينهم حول العمليات التي ستُنفِذها. وشبكة الأَنترنت هي واحِدة مِن هذه الشبكات. وهو مورد حيوي للإِرهاب العالمي ويعتقد الباحث؛ إنَّ الجماعات الإِسلامية ليست الأَولى في المنظمات الإِرهابية في اللجوء للإِنترنت، ولكنها تعلمت بسرعة قيمة التكنولوجيا الجديدة. فالأَنترنت وسيلة لتمكين الإِرهاب العالمي: فهو أَداة تنظيمية، ويوفر أَساساً للتخطيط والقيادة والسيطرة والاتصالات بين الجماعات كما أَنهُ وسيلة لجمع المعلومات الاستخباراتية، وتوفير الوصول إلى مجموعة واسِعة مِن المواد عن الأَهداف المحتملة، والوصول للخرائط عن طريق الصور الفوتوغرافية. وواحِدة مِن استِخداماتهُ الأَكثر قيمة هو الدعاية، ونقل الرسائل، والصور والأَفكار التي تُحفِز الجماعات الإِرهابية. على الرغم مِن كُل ذلك إلاَّ أَنَّ الأَسلحة الإِلكترونية أَقلُ فتكاً وفعالية وأَقل جاذبية مِن غيرها مِن الأَسلحة الملموسة في الترسانة الإِرهابية.. لذا فالحل كما يطرحهُ الباحث وضع سياسات فعالة لِمُكافحة استِخدام الإِرهابيين للإِنترنت وذلك يتطلب التركيز على شيئين: استِغلال ميزة احتِكار الوسائل الرسمية، والفوز في النِقاش بدلاً مِن محاولة قمعهُ.

المصادر والمراجع:

(1) مُراد بطل الشيشاني، **تنظيم القاعدة: الرؤية الجيوسياسية والاستراتيجية والبيئة الاجتماعية**، ط1، (أبو ظبي: مركز الإمارات للدِراسات والبحوث الاستراتيجية،2012)، ص7.

(2) إيمان رجب، اللاعبون الجدُد: أنماط وأدوار الفاعلين مِن غير الدول في المنطقة العربية، مقال مُتاح على الرابط الآتي: https://www.digital.ahram.org.eg

(3) إيمان رجب، **تأثير الهوية على سلوك الفاعلين من غير الدول في المنطقة العربية: دِراسة حالتي حزب الله وحماس**، رسالة ماجستير غير منشورة، (القاهِرة: جامِعة القاهِرة، كُلية الاقتصاد والعلوم السياسية،2014)، ص12.

(4) صباح عبد الصبور عبد الحي، **استخدام القوة الإلكترونية في التفاعُلات الدولية: تنظيم القاعِدة نموذجاً**، (مصر: المعهد المصري للدِراسات السياسية والاستراتيجية،2016)، ص51.

(5) MAI WILLIAM and Mai Troy, "Violent Non-State Actors: Countering Dynamic Systems", **strategic insights**, Volume III, Issue3, (March 2004), P.89-93.

(6) أمين السيد أحمد لُطفي، **المُحاسبة الدولية والشركات مُتعدِدة الجنسية**، ط1، (الاسكندرية: الدار الجامعية للطباعة والنشر،2004)، ص36.

(7) إيمان رجب، "القوة المُنافِسة: مداخل تحليل الفاعلين العنيفين مِن غير الدول في المراحل الانتقالية"، **مجلة السياسة الدولية**، العدد82، (القاهِرة: مركز الأهرام للدِراسات السياسية والاستراتيجية،2014)، ص57.

(8) حسن الحافظي، **الحماية القانونية للمُعطيات ذات الطابع الشخصي بين التشريع الوطني والاتفاقيات الدولية**، رسالة ماجستير غير منشورة، (الجزائر: جامِعة مولاي إسماعيل، كُلية العلوم القانونية والاقتصادية والاجتماعية،2018)،ص1-3.

(9) رتشارد واطسون، **ملفات المُستقبل**، ترجمة عمر الأيوبي،(الإمارات العربية المُتحدة: مشروع كلمة،2011)،ص ص8-10.

(10) مايكل كريبون، **الأمن أولاً قبل الندم مُفارقات التعايُش مع القنبلة**، ط1، (أبو ظبي: مركز الإمارات للدِراسات والبحوث الاستراتيجية،2012)، ص9.

(11) إسماعيل زروقة، "الفضاء السيبراني التحولات في مفاهيم القوة والصِراع"، **مجلة العلوم القانونية والسياسية**، المُجلد10، العدد1، (الجزائر: جامِعة محمد بو ضياف،2019)، ص1021.

(12) حسن طاهر داؤود، جرائم نظُم المعلومات، بحث مُتاح على الرابط الآتي: https://www.kenanonline.com

(13) الأمم المُتحدة، **الأمم المُتحدة المعين بالمُخدرات والجريمة: دِراسة شامِلة عن الجريمة السيبرانية**، (نيويورك: الأمم المُتحدة،2013)، ص66.

(14) هيئة التحرير، أشهر عشر فرق "Hackers" غيرت العالمين الافتراضي والواقعي، قدس نت، مقال مُتاح على الرابط الآتي: https://www.qudsn.net

(15) المصدر نفسهُ.

(16) Tim Maurer, **Cyber Mercenaries,** (Cambridge: University of Cambridge, 2018), P.112.

(17) Ibid, P.112.

(18) Weisenthal, Joe, "Notorious Hacker Group LulzSec Just Announced That It's Finished", **Business Insider.** Silicon Alley Insider. Archived from the original on 27 June 2011.

(19) Himma, Kenneth Einar, **Internet Security**, (USA: Jones & Bartlett Publishers,2019), P.92.

(20) رفد عيادة الهاشمي، الإرهاب الإلكتروني، بحث مُتاح على الرابط الآتي: https://www.Mizandz.com

(21) محمد شكو، ظاهرة ويكليكس: دِراسة تحليلية للمعركة الإلكترونية التي يخوضها الموقع، مقال مُتاح على الرابط الآتي: https://www.shacckow.wordpress.com

(22) دليل وكالة الاستخبارات المركزية، **تحليل التمرد**، (مصر: مركز حازم للترجمة والدِراسات الاستراتيجية، د.ت)، ص176.

(23) William Campbell and others, "Social Network Analysis with Content and Graphs", **Lincoln Laboratory Journal**, Vol.20 (USA: Lincoln Laboratory, 2013), P.P.61–81.

(24) Rita Boland, "Novel Big Data Reveals Global Human Behavior", Big Data eBook, **Fairfax,** (VA: AFCEA International, 2014), P. 13.

(25) David Pendall, **Global Operations and Biometrics: Next Generation Capabilities and Policy Implications, Carlisle,** (U.S.A: Army War College, 2013), P.4.

(26) جلني جيه، **صعود الحرب الإلكترونية: الهوية والمعلومات وخصائص الحرب الحديثة، ترجمة مركز حازم للترجمة والدِراسات الاستراتيجية**، (مصر: مركز حازم للترجمة والدِراسات الاستراتيجية،2018)، ص65.

(27) المصدر نفسهُ، ص67.

(28) إيمان رجب، "القوة المُنافِسة: مداخل تحليل الفاعلين العنيفين مِن غير الدول.."، مصدر سبق ذِكرهُ، ص67.

(29) إيمان رجب، "القوة المُنافِسة : مداخل تحليل الفاعلين العنيفين مِن غير الدول.."، مصدر سبق ذِكرهُ، ص68.

(30) Al Qaeda,"Propaganda and Media Strategy", **the Canadian Centre for Intelligence and Security Studies**,Vol.2, (Canada: the Canadian Centre for Intelligence and Security Studies, 2007), P.3.

(31) للاستزادة يُنظر: مُعتز محي عبد الحميد، **الإرهاب وتجدُّد الفكر الأَمني**، ط1، (عمان: دار زهران للنشر،2014)، ص ص37-39.

(32) صفية ادري، **آليات صيانة الأمن الإنساني بين مسؤولية الدولة وتمكين الفواعل غير الدول- منطقة الساحل الأفريقي أُنموذجاً**، أطروحة دكتوراه غير منشورة،(الجزائر: جامِعة باتنة، كُلية الحقوق والعلوم السياسية،2019)، ص145.

(33) مكتب الأُمم المُتحدة المعني بالمُخدرات والجريمة UNODC، **استِخدام الانترنت في أَغراض إرهابية**، (نيويورك: الأُمم المُتحدة،2013)، ص ص1-3.

(34) خالد حنفي علي، "مكافحة "الإرهابي المعولم" وبِناء ذهنيات بديلة، **مجلة السياسة الدولية، مُلحق اتجاهات نظرية**، العدد217، (القاهِرة: مركز الأَهرام للدِراسات السياسية والاستراتيجية،2019)، ص3.

(35) حسن جمو، **قراءة في انحياز الإعلام الجهادي على أَرض الشام**، (مصر: مركز دِراسات الجمهورية الديمقراطية، 2014)، ص2.

(36) David C. Gompert & Martin Libicki, "Waging Cyber War the American Way", **Survival,** Vol.57(4), (UK: Rutledge, 2015), P.P.7-28.

(37) ديفيد س. غومبرت، القدرة على الإرغام لمواجهة الأَعداء بدون الحرب، (كاليفورنيا: مؤسسة راند،2016)، ص26.

(38) Garrett, R.K, "Protest in an Information Society: Review of Literature on Social Movements and anaa NEW ICTs Information", **Communication and Society**, Vol.92, (2006), P.P.5-8.

(39) Irving Lachow and Courtney Richardson, "Terror Use of the internet: the Real Story", **JFQ**: Vol.45, (USA: National Defense University, 2007), P.27.

(40) لورانس رايت، **البروج المُشيدة: رحلة في تطور الفكر السلفي وأُصول تنظيم القاعِدة**، ط4،(القاهرة: كلِمات عربية للترجمة والنشر،2013)، ص ص15-24. كذلك يُنظر: مجموعة باحثين، **سر الجاذبية: داعش بالدعاية والتجنيد**، ط1، (عمان: مؤسسة فريد ريتش ايبرت الألمانية،2016)، ص ص12-19. كذلك يُنظر: جِهاد عودة، **عولمة الحركات الإسلامية الراديكالية**، ط1، (القاهِرة، مكتبة الأُسرة،2005)، ص ص15-27.

(41) الجِهاد الإلكتروني الزائف وآليات المواجهة، مقال مُتاح على الرابط الآتي: https://www.eipss-eg.org

(42) سماح عبد الصبور، "الإرهاب الرقمي استخدامات الجماعات المُسلحة لوسائل التواصل الاجتماعي"، **دورية اتجاهات الأَحداث"**، العدد2، (القاهِرة: مركز الأَهرام للدِراسات السياسية والاستراتيجية،2014)، ص25.

(43) فيفيان عقيقي، الإرهاب على مواقع التواصل الاجتماعي كُل ما يجب أَنَّ تعرفه، بحث مُتاح على الرابط الآتي: https://www.Annahar.com

(44) محمد عبد الله، **شبكات الاستقطاب: أبعاد وتداعيات تجنيد المُقاتلين الأجانب في سوريا عبر الانترنت**، (القاهِرة: المركز الاقليمي للدِراسات الاستراتيجية،2014)، ص33.

(45) Brian Principato, AL-QAEDA Jaeda Joins the Jihadist Movement on Facebook, twitter and YouTube, (MIC Policy,2013), P.65.

(46) إيهاب خليفة، "الكتائب الإلكترونية: الملامح العامة لحروب مواقع التواصل الاجتماعي في الشرق الأوسط"، **دورية اتجاهات الأحداث**، العدد4، (القاهرة: المركز الاقليمي للدِراسات الاستراتيجية،2014)، ص ص10-11.

(47) المصدر نفسهُ، ص14.

(48) محمد أبو رمان، تنظيم القاعِدة والانترنت: تدشين الجيل الثالث مِن الجهاديين، تقرير مُتاح على الرابط الآتي: https://www.assakina.com

(49) نوران شفيق، **السياسة الدولية والاستراتيجية: التهديدات الإلكترونية على العلاقات الدولية**، (القاهِرة: المكتب العربي للمعارف،2016)، ص57.

(50) أحمد الأحمد، التجنيد الإلكتروني الوسيلة الجديدة لداعش لاستِهداف الشباب السعودي والتنظيم ينقل التخطيط والتنسيق للعمليات الإرهابية إلى مواقع التواصل الاجتماعي، جريدة الرياض، مقال مُتاح على الرابط الآتي: http://www.alriyadh.com

(51) مكتب الأُمم المُتحدة المعني بالمُخدرات والجريمة في فيينا، **المقاتلون الإرهابيون الأجانب دليل لمعاهد التدريب القضائي في بُلدان الشرق الأوسط وشِمال أفريقيا**، (نيويورك: الأُمم المُتحدة،2021)، ص37.

(52) ريهام العباسي، أثر الإرهاب الإلكتروني على تغير مفهوم القوة في العلاقات الدولية دِراسة حالة: تنظيم الدولة الإسلامية، بحث مُتاح على الرابط الآتي: https://www.democraticac.de

(53) محمود رشدي، "الاتجاهات السيبرانية للمحتوي الإرهابي "داعش"، تقرير مُتاح على الرابط الآتي: http://www.smtcenter.net

(54) جِهاد فتحي، **كيف استخدمت التنظيمات الإرهابية التكنولوجيا في صِناعة الإرهاب؟**، (عمان: مركز البديل للتخطيط والدِراسات الاستراتيجية،2017)، ص35.

(55) مكتب الأُمم المُتحدة المعني بالمُخدرات والجريمة في فيينا، المقاتلون الإرهابيون..، مصدر سبق ذِكرهُ، ص40.

(56) Joanie chung Yin Yeung, "A critical analysis on ISIS propaganda and social media striges", **University of Sanford terrorism security studies,** (Sanford: 2015), P.91.

(57) George Michael, "DISTURBING TRENDS IN LONE WOLF TERRORISM: The convergence of Mental iiiness Marginality and Cyber Radicalism",(SKEPTIC MAGAZINE, 2017), P.P15-19.

(58) للاستزادة يُنظر: مكتب وزارة الخارجية الأَمريكية لِمُكافحة الإرهاب والتطرف العنيف، **تصنيفات المُقاتلين الإرهابيين الأجانب**، (واشنطن: دي سي، 29 سبتمبر/أيلول 2015).

(59) شادي عبد السلام، "الإرهاب عن بعد: نمط تنظيمي جديد لاستدام الدول الغربية والآسيوية"**, مجلة اتجاهات الأحداث**، العدد24، (أبو ظبي: مركز مُستقبل للأبحاث والدِراسات المُتقدمة،2017)، ص ص50-53.

(60) Cassandra Vinograd and Ammar Cheikh Omar, Syria, ISIS Have Been 'Ignoring' Each Other on Battlefield, Data Suggests, **NBC News,** available at: http://www.nbcnews.com.

(61) John Muller, the "Cyber coaching of terrorists: cause for Alarm? **CTC Sentinel combating Terrorism Center,** Vol.10, (2017), P.P. 30-32.

(62) محمد قيراط، "الإعلام الجديد والإرهاب الإلكتروني: آليات الاستخدام وتحديات المواجهة"، **مجلة الحِكمة للدِراسات الإعلامية**، (الجزائر: مركز الحِكمة للبحوث والدِراسات،2017)، ص ص24-27.

(63) مُجاهد الصُميدعي، أدوات داعش في الحرب الإلكترونية وأحلام الخِلافة السيبرانية، مقال مُتاح على الرابط الآتي: https://www.akhbaralaan.net