الحرب والإرهاب الإلكترونى فى ظل الذكاء الإصطناعى: التهديدات وآليات المواجهة

د. أمانى عصام محمد عبد الحميد

أستاذ العلوم السياسية المساعد– كلية التجارة– بجامعة حلوان

ملخص البحث:

تعد قضية الإرهاب الإلكتروني من القضايا الصاعدة في الاهتمام الدولي في ظل ارتباطها بالتطور التقني المتسارع من جهة، وتحول المصالح الإستراتيجية إلى الفضاء السيبراني من جهة أخرى، ويأتي ذلك مع توجه العديد من الحكومات نحو التحول الرقمي، وتضاعف معدلات الانتشار والنفاذ لتكنولوجيا الاتصالات والمعلومات، وارتبط بتلك المتغيرات الجديدة حدوث تحول كمي ترافق معه تحول كيفي آخر كان لهما بالغ الأثر في القيم والسلوك للفاعلين سواء من الدول أو من غير الدول. وقد مثلت الجماعات الإرهابية والمتطرفة مصدراً لتهديد الأمن القومي من خلال قدرتها على التوظيف السياسي والأمني للقوة السيبرانية لتحقيق أهدافها لنشر عدم الاستقرار في بيئة امنية ودولية مغيرة.

الكلمات المفتاحية: الإرهاب الإلكترونى– الذكاء الإصطناعى– الحرب السيبرانية.

Research Summary:

The issue of cyberterrorism is one of the emerging issues of international attention in light of its link to the rapid technical development on the one hand, and the shift of strategic interests to cyberspace on the other hand, and this comes with the orientation of many governments towards digital transformation, and the doubling of the rates of spread and access to communications and information technology, and associated with these new variables is a quantitative transformation accompanied by another qualitative transformation that had a great impact on the values and behavior of actors, whether from countries or non-states. Terrorist and extremist groups have posed a source of threat to national security through their ability to politically and securely employ cyber power to achieve their goals of spreading instability in a changing security and international environment.

(ISSN: 2536 - 9555)

مقدمة

يشهد العالم تهديدات أمنية غير تقليدية ترتبط في أغلبها بالتطورات التكنولوجية المتسارعة، حيث ساهمت التكنولوجيا في تغيير المفاهيم بطبيعة التهديدات ودرجة تأثيرها على الأمن والاستقرار على الصعيدين الداخلي والدولي، فقد ساهمت القفزات التكنولوجية في بروز ساحة جديدة للتفاعلات الدولية تعتمد على شبكات رقمية ذات صلة بأجهزة الحواسيب بمختلف دول العالم لتشكل الفضاء السيبراني الذي اضفى بعداً جديداً على نوعية الصراعات من حيث طبيعة الفاعلين وأساليب إدارة الصراع.

وعزز التنازع حول هذه القوة التأثيرية الجديدة حدوث تغيرات متزامنة في السياقات العالمية، حيث أصبحت القوة السيبرانية شكل من أشكال القوة، مما فرض واقعاً جديداً تشارك فيه فواعل من غير الدول، وقد أنتج التطور التكنولوجي الذي نعيشه نقلة نوعية في أسلوب عمل وتكتيكات الجماعات الإرهابية، وهو ما عبر عنه "جون اركويلا" أحد أبرز الباحثين بمؤسسة راند في مجال عمل التنظيمات الإرهابية بقوله "إن التكنولوجيا في عصر المعلومات ساهمت في تعظيم قدرات الجماعات الإرهابية من حيث نوعية الأسلحة المستخدمة، والأهداف التي يمكن الوصول إليها، بل منحت تلك الجماعات القدرة على هيكلة تركيبها الداخلي وتطوير قدراتها العملياتية، وتعكس هذه العبارة تأثير التقنيات على قدرات الجماعات الإرهابية وزيادة حجم التهديدات التي قد تشكلها من خلال مزج أنشطتها في الواقعين المادي والافتراضي، فلقد لعبت التكنولوجيا دوراً بارزاً في ظهور نمط جديد من أنماط الارهاب يختلف في استراتيجيته وتكتيكاته عما سبقها من أنماط، ويمتزج فيه استخدام التكنولوجيا بمختلف صورها داخل البيئة الافتراضية "الفضاء الالكتروني" مع العمل على أرض الواقع، ويزيد الأمر تعقيداً على الأجهزة الاستخباراتية والأمنية في متابعة الأنشطة الإرهابية الإلكترونية.

أهمية البحث:

يمثل الإرهاب جريمة العصر، وقد أصبح التاريخ يسجل العمليات الإرهابية وتاريخ حدوثها، وتتجلى أهمية هذا البحث فى اختيارنا لأحد اهم الظواهر الإجتماعية والقضايا السياسية، وحتى الفكرية التي يجري الحديث عنها أو تحليلها الآن في كل ميادين الحياة العامة، فضلاً عن الخطورة التي تنطوي عليها جريمة الإرهاب، واثاره على الفرد والجماعة والمؤسسات والمنظمات الدولية والمجتمع الدولي.

وتبرز أهمية دراسة الإرهاب الإلكترونى من زوايا عدة، مثل إلقاء الضوء على الذكاء الاصطناعى، وكيف يستفيد منه الإرهاب، وظهور ما سمى بالإرهاب الإلكترونى، وظهور الحروب السيبرانية، حيث مع انتشار تقنية نظم الاتصالات وشيوع شبكة الإنترنت نشأت مفاهيم وأبعاد جديدة للإرهاب تعتمد على التقنية أكثر منه على الفعل المادي، مما أفرز أسلوباً جديداً للإرهاب الإلكترونى. كما تبرز أهمية الدراسة بشكل عام من خطورة جريمة الإرهاب الإلكتروني، حيث أن التقنية وحدها لم تعد قادرة على حماية الأفراد من عمليات الإرهاب الإلكتروني، والتي تترك غالباً آثاراً وأضراراً تمس الأفراد والمجتمعات، الأمر الذي يتطلب من الدول إيجاد تشريعات لمواجهة هذه الظاهرة الخطيرة.

أهداف البحث:

يهدف البحث إلى تلسيط الضوء على الذكاء الإصطناعى- والإرهاب الإلكترونى، كما يهدف إلى:

- توضيح العلاقة بين الارهاب بالذكاء الاصطناعى.
- التركيز على الدوافع الرئيسية لتنامي ظاهرة الاستخدامات الإرهابية للذكاء الاصطناعي.
- توضيح أنواع القدرات الارهابية التي يمكن استخدامها عن طريق الذكاء الاصطناعي.

(ISSN: 2536 - 9555)

- إلقاء الضوء على أدوات مكافحة الإرهاب المتاحة لجهات إنفاذ القانون باستخدام الذكاء الاصطناعي.
- توضيح الحرب السيبرانية، وتبيان أشكالها، وتسليط الضوء على استراتيجيات مواجهتها.

إشكالية الدراسة:

تعكس المخاوف المثارة حول العلاقة بين التكنولوجيا والإرهاب الطبيعة المعقدة للواقع الذي يهدد فيه الارهاب المجتمعات بشكل يختلف عن الماضي، خاصة على مستوى الانتشار والانعكاسات البشرية والمادية، وفي حين يتسبب الإرهاب في خسائر عديدة ومتنوعة في العالم المادي، يصيب عدداً متزايداً عبر العالم الافتراضي بفعل التكنولوجيا التي تستحضر الخوف والرعب إلى المنازل عبر الأجهزة الحديثة، بما فيها التليفونات المحمولة، وبشكل عام يعد الفضاء السيبراني بيئة بدون حدود، ومساحة مميزة يجد فيها الإرهاب موارد، ويتم فيها القيام بأنشطة دعائية لتلك التنظيمات، ويمكن من خلالها شن هجمات على الأعداء في كل مكان في العالم، ويعمق من اشكالية الدراسة المخاطر الناجمة عن طريقة تعامل العناصر والتنظيمات المتطرفة والإرهابية مع النماذج الرقمية الجديدة للقرن الحادي والعشرين، وكيف قامت بتعلم استخدام تقنية المعلومات والاتصالات، خاصة في الإنترنت والعديد من المنصات التفاعلية، ومنصات التواصل الاجتماعي من أجل تعزيز أهدافها مثل نشر ايديولوجية الكراهية والحصول على الدعم المالي، وإدارة الدعم عبر مجتمع الانترنت، بالاضافة الى تكييف وتوظيف تلك التقنيات وفقاً للمجتمع المحلي والجمهور المستهدف من حيث اللغة والمحتوى والأدوات المستخدمة بما يساعد في عملية الانتشار والتجنيد.

تساؤلات البحث:

يدور البحث حول تساؤل رئيسى وهو ما علاقة الارهاب الالكترونى بالذكاء الاصطناعى؟

وينبثق عن التساؤل الرئيسى عدة تساؤلات، تتمثل فيما يلى:

- ما هو الذكاء الاصطناعى، وما هى دورته؟
- كيف يستفيد الارهاب بالذكاء الاصطناعى؟
- ما هى الدوافع الرئيسية لتنامي ظاهرة الاستخدامات الإرهابية للذكاء الاصطناعي؟
- ما أنواع القدرات الارهابية التي يمكن استخدامها عن طريق الذكاء الاصطناعي؟
- ما هى أدوات مكافحة الإرهاب المتاحة لجهات إنفاذ القانون باستخدام الذكاء الاصطناعي؟
- ما المقصود بالحرب السيبرانية، وما هى أشكالها؟
- ما هى استراتيجيات مواجهة الهجمات السيبرانية؟

منهج الدراسة:

تعتمد الدراسة على:

المنهج الوصفي التحليلي: حيث يهدف هذا المنهج إلى تحقيق الفهم الدقيق والإحاطة بالأبعاد الواقعية للظواهر والموضوعات. ومن هنا فالقواعد الأساسية التي يقوم عليها المنهج الوصفي هي تحديد الظواهر المراد بحثها، وجمع المعلومات الدقيقة عنها وفحصها ودراستها، ومحاولة الإحاطة بعدد كبير من الأبعاد والعلاقات المرتبطة بالظاهرة للإنتقال من مستوى الفهم البسيط إلى المستوى المركب، وما يرتبط بذلك من صياغة عدد من النتائج والتعميمات والتوصيات التي ترشد عملية البحث، وذلك من خلال محاولة وصف وتحليل مفهوم الارهاب الالكترونى، وأدواته من خلال الذكاء الاصطناعى، وكيفية مواجهته، وكذلك الحرب السيبرانية واستراتيجيات مواجهتها.

تقسيم البحث:

ينقسم البحث الى النقاط الأساسية التالية:

(ISSN: 2536 - 9555)

أولاً: الذكاء الاصطناعى.. الفمهوم ودورته.

ثانياً: الإرهاب الإلكترونى– والذكاء الاصطناعى.

أ. الدوافع الرئيسية لتنامي ظاهرة الاستخدامات الإرهابية للذكاء الاصطناعي. والتى تتمثل فى:

ب. انواع القدرات الارهابية التي يمكن استخدامها عن طريق الذكاء الاصطناعي.

ج. العلامات الافتراضية– والإرهاب الإلكترونى.

د. أدوات مكافحة الإرهاب المتاحة لجهات إنفاذ القانون باستخدام الذكاء الاصطناعي.

ثالثاً: الحرب السيبرانية– والذكاء الإصطناعى.

(أولاً) مفهوم الحرب السيبرانية.

(ثانياً) أشكال الحرب السيبرانية.

(ثالثا) استراتيجيات مواجهة الهجمات السيبرانية.

الحرب والإرهاب الإلكترونى فى ظل الذكاء الإصطناعى: التهديدات وآليات المواجهة

يعد الذكاء الاصطناعي Artificial Intelligence- AI أحد أنواع العلوم الحديثة التي انتشرت على نطاق واسع خاصة مع دخوله في كثير من المجالات الصناعية والبحثية، ومنها الروبوتات والخدمات الذكية للحكومات والشركات، ويكمن جزء أساسي من جاذبية الذكاء الاصطناعي في قدرته على تحليل كميات هائلة من البيانات يطلق عليها البيانات الضخمة والعثور على الأنماط والعلاقات بينها بسرعة، واستقراء النتائج المحتملة لسيناريو معين بناء على تلك البيانات، ورغم الانتشار، لا يوجد تعريف عالمي للذكاء الاصطناعي الذي يتم التعامل معه بوصفه تقنية متطورة تحاكي الذكاء البشري عبر خوارزميات معقدة تتعامل مع

معلومات تسهل في النهاية من تقديم مخرجات تتشابه مع السلوك الإنساني بما يجعل منها أداة مهمة لتنفيذ الكثير من المهام دون الحاجة لوجود البشر[١].

فى هذا الإطار، يستهدف هذا التحليل **أولاً تحديد مفهوم الذكاء الاصطناعى وتطوراته، ثانياً: الإرهاب الإلكترونى- والذكاء الاصطناعى، ثالثاً: الحرب السيبرانية- والذكاء الإصطناعى.**

أولاً: الذكاء الاصطناعى.. الفمهوم ودورته:

تطور مفهوم الذكاء الاصطناعى (AL)، بشكل ملحوظ منذ عام ١٩٥٠، عندما طرح آلان تورينج لأول مرة مسألة ما إذا كان بإمكان آلات التفكير أم لا، ثم تمت صياغة ذلك المفهوم كمصطلح فى عام ١٩٥٦، لتبرز لاحقاً أنظمة آلية قائمة على المنطق فى سبعينيات القرن العشرين. ثم ازدات الطفرة بشكل أكبر فى عقد التسعينيات، إثر بناء كمبيوتر يمارس لعبة الشطرنج "ديب لو". ومنذ عام ٢٠١١، أدى التقدم فى "التعلم الآلى" "Machine Learning" إلى تحسين قدرة الآلآت على إجراء تنبؤات من البيانات التاريخية، وساعد على ذلك نضج تقنية نمذجة التعلم الآلى (ML) المسماة "الشبكات العصبية" جنباً إلى جنب مع اتساع قوة الحوسبة والبيانات الكبيرة، مما قد أسهم فى تطوير الذكاء الاصطناعى.

ويعرف خبراء بمنظمة التعاون الاقتصادي والتنمية "الذكاء الاصطناعي" بأنه نظام قائم على الآله، إذ يمكنه وضع تنبؤات أو توصيات أو قرارات تؤثر في البيئات الحقيقية أو الافتراضية لمجموعه معينه من الاهداف المحدده من قبل الإنسان باستخدام مدخلات اليه و/أو بشرية، حيث يتم تجديد هذه التصورات في النماذج بطريقة آلية سواء باستخدام التعلم الآلي أو يدوياً او الاستدلال النموذجي لصياغه خيارات للمعلومات، وعادة ما يتم تصميم أنظمة الذكاء الاصطناعي للعمل بمستويات مختلفة من الاستقلالية.

---

[١] عبير ياسين، "التكنولوجيا فى عالم الإرهاب.. سلاح ذو أوجه متعددة"، **السياسة الدولية**، عدد ٢٢٧، يناير ٢٠٢٢، ص ٢٤١.

(ISSN: 2536 - 9555)

وفي عام ٢٠١٩ أوصت منظمة التعاون الاقتصادي والتنمية، الصادرة عن مجلس الذكاء الاصطناعي، بإنشاء ما يسمى دورة حياة نظام الذكاء الاصطناعي، حيث تتضمن أربع مراحل محددة غالباً ما تحدث بطريقة تكرارية وليست متسلسلة بالضرورة[٢]. **المرحلة الاولى** تتعلق بتصميم النموذج حيث تتضمن العديد من الأنشطة التي قد يختلف ترتيبها باختلاف أنظمة الذكاء الاصطناعي منها تخطيط وتصميم هذه الانظمه وتوضيح أهدافها، والافتراضات الأساسية لها والسياقات والمتطلبات، وذلك لبناء نموذج اولي مع جمع البيانات ومعالجتها وتنقيتها واجراء عمليات التحقق من الاكتمال والجودة وتوثيق البيانات الوصفية، وخصائص مجموعة البيانات Metadata وبناء او انشاء النماذج أو الخوارزميات ومعايرتها و/أو التدريب والتفسير.

أما المرحلة الثانية فهي التحقق، حيث تتضمن تنفيذ النماذج وضبطها مع اختبارات لتقييم الأداء عبر مختلف الابعاد والاعتبارات، بينما تحوي المرحله الثالثه والمتعلقة بالنشر، التجريب والتحقق من التوافق مع الأنظمة القديمة وضمان الامتثال التنظيمي وإدارة التغيير التنظيمي وتقييم تجربة المستخدم، فيما تنطوي المرحلة الرابعة والأخيرة على التشغيل والمراقبة، أي تفعيل نظام الذكاء الاصطناعي، والتقييم المستمر لتوصياتة وآثاره المقصودة وغير المقصودة في ضوء الأهداف والسلوكيات الاخلاقية وطبيعة القيم المجتمعية، وتحدد هذه المرحلة المشكلات وتعديلها من خلال الرجوع الى مراحل أخرى أو إذا لزم الأمر سحب نظام الذكاء الاصطناعي من الإنتاج[٣].

---

[٢] انظر:

OECD, Recommendation of the Council on Artificial Intelligence, OECD, Paris 2019.

[٣] د. أميرة تواضروس، "دور الذكاء الاصطناعى فى التنبؤات التنموية"، **السياسة الدولية**، (ملحق اتجاهات نظرية)، عدد ٢٢٢، اكتوبر ٢٠٢٠، ص ٢١.

وقد أدى الذكاء ودورته إلى التطور فى التطبيقات الرقمية، وإلى هجرة المواقع الإلكترونية والمنتديات وغرف الدردشة والمدونات، إلى تطبيقات الشبكات الاجتماعية والهواتف الذكية، والتي أحدثت بدورها تطوراً ملحوظا في الإستراتيجية الإعلامية للتنظيمات المتطرفة، وهو ما عمل على مضاعفة التأثير والانتشار وتضخيم الظاهرة الإرهابية في ظل عصر الشبكات الاجتماعية، وأتاحت البيئة الرقمية الجديدة الفرصة إلى أن تتمكن الجماعات المتطرفة من تطوير أساليب جديدة وتكتيكات تساهم في تعزيز قدراتها السيبرانية ، وذلك من اجل توظيفها في مواجهة أعدائها وفي مخاطبة مؤيديها وفي مخاطبة الكتلة الصامتة من مستخدمي تلك التطبيقات الرقمية من الشباب وبخاصة أنهم الأكبر استخدماً لها وأكثر معاناة في نفس الوقت من الظروف الاقتصادية[٤]، وهذا ما يجعلنا نتطرق الى النقطة التالية، حيث الإرهاب الإلكترونى واستخدامه للذكاء الاصطناعى..

ثانياً: الإرهاب الإلكترونى- والذكاء الاصطناعى.

على الرغم من العلاقة التاريخية بين التكنولوجيا والإرهاب إلا أنها اكتسبت أبعاداً جديدة في ظل تطبيقات العصر الرقمي، والتي على الرغم من حيادتها إلا أنها أخذت طابع ونمط استخدامها من ثقافة المستخدم وبيئته، والتي تشكل الأهداف التي تقف وراء ذلك. وكانت التنظيمات الإرهابية والمتطرفة الأكثر استفادة بقدرتها على التعبئة والحشد، وذلك مع إضفاء الغطاء الديني على ذلك الاستخدام، وهو ما كان من شأنه تعزيز عملية المزج بين مدلولات القوة المادية والقوة الروحية، وبخاصة في منطقة الشرق الأوسط وشمال إفريقيا، والتي يكتسب الدين فيها دوراً كبيراً في المجال العام، ناهيك عن التنوع العرقي والمذهبي فى المنطقة، والتي تعد كذلك مرتكزاً للصراع بين القوى الدولية على ثرواتها، وموقعها

[٤] د. عادل عبد الصادق، "الإرهاب السيبرانى والأمن القومى فى بيئة متغيرة"، **السياسة الدولية**، عدد ٢٢٧، يناير ٢٠٢٢، ص ٢٤٥.

(ISSN: 2536 - 9555)

الجغرافي المتميز، وشهدت المنطقة معدلات غير مسبوقة في انتشار الانترنت فاقت بكثير قدرة البنية الثقافية والاجتماعية على امتصاص تحدياتها[٥].

أ. **الدوافع الرئيسية لتنامي ظاهرة الاستخدامات الإرهابية للذكاء الاصطناعي. والتى تتمثل فى:**

١ – الرقمنة.

الواقع أن إدماج التكنولوجيات الرقمية في الحياة اليومية يتنامى يومياً بوتيرة غير عادية، خصوصاً بعد جائحة كورونا، وكما هو الحال مع الأجيال الشابة في جميع انحاء العالم فإن العديد منهم يطلق عليهم المواطنون الرقميون وهم الأفراد الذين ولدوا او أنشأوا خلال العصر الرقمي ويمتلكون مستويات عالية من الإلمام بالتكنولوجيا ولديهم قبول أعلى للخدمات المتعلقة بها وهم مستخدمون متحمسون لوسائل التواصل الاجتماعي، ولسوء الحظ فإن مزايا وسائل التواصل الاجتماعي تجعلها جذابة للجهات ذات النيات الخبيثة لنشر الأيديولوجيا الراديكالية والدعايه السيئة وتجنيد أعضاء جدد وتنظيم الدعم المالي والتكتيكات التشغيلية.

٢ – نمو تطبيقات الذكاء الاصطناعي.

من الجدير بالذكر أن الطلب المتزايد على تكنولوجيا الذكاء الاصطناعي في الاستخدامات التجارية يوفر ضغطاً مستمراً على مطوري تلك التكنولوجيات لتطويرها بشكل مفيد للبشرية مع توفير خوارزميات الذكاء الاصطناعي المفتوحة المصدر، أي متاحة بشكل كامل للتعديل والاستخدام لأي غرض على شبكات الانترنت، على صعيد آخر، فإن تطوير تلك التكنولوجيا بصفة دائمة يوفر الفرصة بشكل متساوي أحياناً امام الجماعات الارهابية لاستخدامات الذكاء الاصطناعي في القيام بعمليات إرهابية يصعب وقفها في حالة هجمات الذئاب المنفردة لأن جهات انفاذ القانون يتعين عليها أن تكون ناجحة في كل مرة في وقف تلك

[٥] المرجع السابق، ص ٢٥٤.

الهجمات، بينما يتعين على المهاجم المنفرد أن يجد ثغرة واحدة ينجح في استغلالها لمرة واحدة فقط لغرس الخوف، وهو أحد أهم الأغراض الدعائية للإرهاب، كما أن تنامي اعتماد البشرية على البيانات يوفر البيانات التسويقية والصحية والمالية التي تبدو غير حساسة والمتوافرة على الانترنت، ويمكن تغذيتها لانظمه الذكاء الاصطناعي وربط الخيوط معاً لانشاء هويات مزيفة تفيد في تلك الهجمات الإرهابية بشكل كبير[٦].

٣-تطوير تكتيكات الإرهاب.

أصبح الأرهاب أكثر تعقيداً، حيث أن تكتيكات الجماعات الارهابية أصبحت تختلف من مجموعة الى أخرى ومن فرض إلى آخر، لكن من الثابت أن التكنولوجيا تمثل إحدى أهم أدوات الإرهابيين، حيث أصبح الإنترنت ووسائل التواصل الاجتماعي فضلاً عن المنصات الأخرى مثل منصات الألعاب ومنصات التجارة الإلكترونية ومنصات العمل الحر ومنصات التواصل الصوتي والفيديو كونفرنس عبر الانترنت أدوات قوية للجماعات الإرهابية لنشر التطرف، والتحريض على العنف، وإعلان المسؤولية عن الهجمات والتجنيد وجمع الأموال خصوصاً مع انتشار العملات الرقميه ومنصات دارك ويب. وقد توسعت الترسانات الإرهابية توسعاً كبيراً، وأدت التطورات التكنولوجية إلى تحويل قدرات الجماعات الارهابية والاجرامية لوجستياً، ما سمح لها بزيادة سرعة عملياتها ومدى وصولها وحجمها، وجعلها تقدم على تهديدات عالمية وليست محلية[٧].

---

[٦] د. محمد خليف، "الارهاب المنفرد.. مخاطر الاستخدام الخبيث للذكاء الاصطناعى"، **السياسة الدولية**، عدد ٢٢٩، يوليو ٢٠٢٢، ص ٢١٩.

[٧] يمكن رصد هذه الظاهرة في الأحداث التالية كمثال في عام ٢٠١٦ أظهر شريط فيديو اعده تنظيم نسخة بدائية من سيارة ذاتية القيادة وتم التوصل لأدلة على أن التنظيم يعمل بالفعل على تطوير سيارات ذاتية القيادة لاستخدامها بدلا من الانتحاريين. استخدم داعش طائرات مسيرة في ٢٠١٧ في هجمات بشمال العراق ما أسفر عن مقتل اثنين من مقاتلي البشمركة

(ISSN: 2536 - 9555)

٤-تجنيد أتباع جدد ونشر الأفكار والمعتقدات.

مع تزايد اعتماد الفاعلين من غير الدول في تحركاتهم الخارجية على الجمع بين أدوات القوة الناعمة والصلبة، ارتفع الاعتماد على هذه الشبكات. فحتى الحركات المسلحة لم تعد تعتمد على القوة العسكرية فقط في تحقيق أهدافها، بل تلجأ إلى استخدام وسائل الاتصال والإعلام وشبكة الإنترنت بشكل واسع ودعائي لأفكارها وتحركاتها[٨]، وكأداة جديدة لنشر أفكارها ومعتقداتها وزيادة عدد المنتمين لها عبر تجنيدهم باستخدام تلك المواقع العابرة للحدود القومية، ومن دون استخدام تلك الأدوات لم يكن بمقدور هذه التنظيمات أن تحقق أهدافها مع توفير ذلك الوقت والجهد، بالإضافة لميزة الابتعاد والتخفي بعيداً عن قبضة الأجهزة الأمنية للدول المستهدفة[٩].

ويعتبر "فيسبوك" من أكثر وسائل التواصل الاجتماعى استخداماً في تجنيد المتطرفين، وغالباً ما تقوم الجماعات الإرهابية بإنشاء مجموعة Group على "فيسبوك" لإجتذاب المتوافقين فكرياً معها، حيث تركز المجموعة في أطروحاتها على فكرة إنسانية بالأساس، كدعم الفلسطينيين أو الإسلام بصفة عامة، ومع زيادة عدد الأعضاء المنتمين لهذه المجموعة، فإن المواد الجهادية يتم وضعها تدريجياً عليها بطريقة لا تستهجن الأفعال الجهادية أو تدينها في الوقت نفسه، حتى لا تنتهك سياسة "فيسبوك"، ثم يتم بعد ذلك توجيه أعضاء المجموعة مباشرة إلى المواقع أو المنتديات المرتبطة بالجماعة الإرهابية. ويمكن "فيسبوك" بهذه

الأكراد وإصابة جنديين من العمليات الخاصة الفرنسية ازال فيسبوك أكثر من ٢٦ مليون قطعة من المحتوى بستها جماعات إرهابية عام ٢٠٢٠

[8] Joseph Nye, "Smart Power and the War on Terror", Asia Pacific Review, Vol. 15, no. 1, 2008, p 11.

[٩] سماح عبد الصبور، "الإرهاب الرقمى: استخدامات الجماعات المسلحة لوسائل التواصل الاجتماعى"، **اتجاهات الأحداث**، عدد ٢، سبتمبر ٢٠١٤، ص ٤٣.

الطريقة من تجنيد الأعضاء من أنحاء العالم كافة من دون أن يمثل ذلك تهديداً لأمن المنظمة.

وتعتبر وسائل التواصل الإجتماعى من الوسائل المهمة للتنظيمات المسلحة لنشر أفكارها وكسب متعاطفين وأتباع جدد، وتجنيد الشباب للإنضمام لصفوف المقاتلين في تلك الجماعات، ومن ثم، تولى تلك الجماعات اهتماماً متزايداً لحساباتها على مواقع التواصل الإجتماعى للتواصل مع الآخرين عبر مبرمجين متخصصين لحثهم على تنفيذ أجندتها.

ومن بين أنشطة الجماعات في هذا الصدد تنظيم داعش، من خلال قيامه بنشر الصور والفيديوهات، عبر "تويتر" بصورة خاصة لسهولة استخدامه عبر الهواتف. وقد ذكرت بعض المصادر أن التنظيم يمتلك ما يقارب ٢٠ حساباً على "تويتر"، بجانب حسابات غير رسمية تابعه لأنصاره، ويعمل مبرمجو "داعش" على ابتكار تطبيقات مثل التطبيق الذي يتيح إرسال منشورات "داعش" للمشترك مباشرة لدى نشرها وإعادة النشر التلقائي لمتابعي المشترك. ويرجع اهتمام تلك التنظيمات المسلحة بوسائل التواصل الإجتماعى **لعدة أسباب هي**[١٠]:

- البعد عن سيادة الدول، كما هي الحال في وسائل الإعلام التقليدي.
- إتاحتها للجميع وصعوبة السيطرة عليها عبر الأجهزة الأمنية، إضافة إلى قدرة تلك الجماعات على التحايل على المراقبة الأمنية، وفتح مواقع وحسابات أخرى بسهولة.
- تقدم هذه الشبكات خدمة الاتصال والتواصل السريع بين الأعضاء والمؤيدين بطرق شتى.

[١٠] المرجع السابق، ص ٤٥.

(ISSN: 2536 - 9555)

- توفر مواقع التواصل لهذه التنظيمات منصات إعلامية للدعاية لأنشطتها وأفكارها، كما تساعد التنظيمات في حربها النفسية ضد خصومها من المنظمات المسلحة الأخرى والحكومات.
- إمكانية النشر المكثف للصور والأفلام والوثائق التي تدعم الأفكار التي تروج لها.

وبجانب نشر الأفكار والدعاية للتنظيمات، تستهدف التنظيمات المسلحة تجنيد أعضاء جدد للقتال في صفوفها، **وتستهدف هذه الجماعات ثلاث فئات هي:**

- **الفئة الأولى:** المتعاطفون مع الفكر الجهادي وغالبيتهم من الشباب لاستمرار الحصول على دعمهم.
- **الفئة الثانية:** الرأي العام من أجل تأكيد نفوذ التنظيمات الجهادية في المجتمع، إما بغرض الحشد والتأييد أو التخويف من مواجهتها.
- **الفئة الثالثة:** الخصوم من أجهزة الدولة ومؤسساتها، وذلك بهدف إضعاف موقفهم، والتأثير على هيبتهم، وإظهارهم بمظهر العاجز في مقابل قوتها.

وقد صرح أيمن الظواهري، زعيم تنظيم القاعدة بالقول: "نحن في معركة، وأكثر من نصف المعركة يدور في ساحات الإعلام، نحن في معركة إعلامية لكسب عقول وقلوب أمتنا"(١١).

وقد نشطت تلك التنظيمات في البلدان العربية اعتماداً مواقع التواصل الإجتماعى، ففي تونس توجد مؤسسة "القيروان الإعلامية"، وهي مؤسسة إعلامية افتراضية في شكل صفحة رسمية على "فيسبوك"، تقوم ببث ونشر بيانات تنظيم "أنصار الشريعة"، الذي يضم شباب التيار الجهادي التونسي، ونشر المواد المرئية

(11) eorge Michael, The New media and the rise of exhortatory terrorism, **Strategic Studies Quarterly**, Vol. 7, Issue 1, Spring 2013, pp 50 – 52.

والصوتيات والفتاوى والكتابات التي أصدرتها مؤسسات إعلامية جهادية عالمية والمتعلقة بالشأن التونسي.

وفي العراق وسوريا، ينشط تنظيم داعش اعتماداً على تلك الوسائل الإتصالية لدعم أهداف التنظيم، والتي يتم الترويج لها من خلال الإعلام المركزي للتنظيم، ومنها "مركز الفجر للإعلام"، ومؤسسة "الفرقان الإعلامية"، والتي تعد وسيلة أساسية وشبه وحيدة في الترويج والنشر لأفكارهم ومنهجهم. أما فى سوريا، فقد وجد نحو ٤٠ حساباً معظمها يرتبط بالتوجهات الجهادية ومؤيدي "تنظيم القاعدة"، و"جبهة النصرة"، و"تنظيم داعش"، وتهدف إلى الدعاية والترويج لأفكارها، ويتمتع "داعش" بوجود ٨٧ ألف متابع، وقد حصلت فيديوهاته على مشاهدة ١.٧ مليون شخص حول العالم لنحو ألف شريط فيديو[١٢].

٥-<u>التنسيق عبر وسائل التواصل الاجتماعى.</u>

يعتبر "تويتر" أحد أهم وسائل التواصل الاجتماعى التي تستخدم للتفاعل والتنسيق أثناء العمليات الإرهابية، وتكمن الميزة الأساسية في "تويتر" بالنسبة إلى الجماعات الجهادية في أنه يوفر مجتمعات افتراضية متغيرة، تتكون بصورة تلقائية خلال الأحداث الكبرى، وهو ما تستفيد منه تلك الجماعات من خلال متابعة أحدث المعلومات عن أي قضية تظهر في المجال العام، ولعل المثل البارز على ذلك هو الهجوم الإرهابى في مومباي في ٢٦ نوفمبر٢٠٠٨، والذي راح ضحيته نحو ١٦٤ شخصاً وجرح أكثر من ٣٠٠ شخص. وقد كشفت التحقيقات أن جماعة "عسكر طيبة" الباكستانية كانت تقوم بالتنسيق مع منفذي الهجوم من باكستان، وإبلاغهم بالتطورات التي تحدث كافة من خلال الاعتماد على أحدث

[١٢] سماح عبد الصبور، "الإرهاب الرقمى: استخدامات الجماعات المسلحة لوسائل التواصل الاجتماعى"، مرجع سابق، ص ٤٥.

(ISSN: 2536 - 9555)

الأخبار المنشورة على تويتر، مثل تحركات وتمركز وحدات مكافحة الإرهاب الهندية، التي خططت للهجوم على الفندق(١٣).

ومن الأمثلة الأخرى على نجاح ذلك الإرهاب الرقمي، ما قامت به حركة "الشباب الإسلامية" الصومالية التي استقطبت أشخاصاً للجهاد عبر تلك الشبكات من أجل مهاجمة مركز تجاري في العاصمة الكينية نيروبي في مارس ٢٠١٢، الأمر الذي نتج عنه مقتل ٦٢ شخصاً، واحتجاز عدد من الرهائن، وكان بعض منفذي تلك العمليات مواطنين أمريكيين، جندتهم الحركة عبر الإنترنت، وكانت منشورات تلك الجماعة على "تويتر" خلال الهجوم مصدراً لأخبار وسائل الإعلام، ووكالات الأنباء العالمية.

وبالإضافة إلى ما سبق، فإن الجماعات الإرهابية تستخدم مواقع التواصل الاجتماعى كأداة لتحديد أهدافها والتعرف عليها ومراقبة تحركاتها، خاصة في إطار عمليات الاغتيالات التي تطال بعض رموز الأجهزة الأمنية أو السياسية في الدول المستهدفة، وذلك إما بمراقبة من يمتلك حسابات على تلك المواقع، أو مراقبة دائرة أصدقائهم ومعارفهم للوصول إليهم، وجمع البيانات اللازمة عن تحركاتهم، وتوفير الوقت والجهد اللازمين للقيام بذلك على أرض الواقع، وأيضاً ضمان سرية المراقبة، ومن ثم، تعد وسائل التواصل الاجتماعى مهمة لتلك الجماعات في إطار ما أسماه البعض "شبكات الكوادر"، التي تعد أحد أساليب استخدامها كمساحات افتراضية مغلقة، تعمل على التواصل بين كوادر التنظيم المسلح كأداة عابرة لقيود المكان، وذلك من أجل مهام عدة، منها التدريب على تكوين خلايا تنظيمية، واستقطاب مزيد من الكوادر وتدريبهم على استخدام

(١٣) انظر فى ذلك:

Geoff Dean, Peter Bell, Jack Newan, The Dark Side of Social Media: Review of Online Terrorism, **Pakistan Journal of Criminology,** Vol. 3, No. 4, April – July 2012, pp 194 – 195.

الأسلحة، والتنسيق للعمليات المسلحة وتوقيتها، والتدريب على صنع القنابل البدائية.

والجدير بالذكر، أنه إلى جانب استخدام الإنترنت كوسيلة لتنسيق العمليات المسلحة التي تتم على أرض الواقع، فإنها تستخدم كذلك لتنفيذ هجمات إرهابية افتراضية على المواقع الإلكترونية المهمة، ولسرقة أرقام بطاقات الائتمان أو استهداف البنية التحتية للدولة التي تعتمد على أجهزة الحاسوب الرقمي بهدف تعطيلها أو مهاجمة أهداف اقتصادية إليقافها عن العمل[١٤].

٦-ساحة افتراضية للتدريب.

يستخدم "يوتيوب" بصورة أساسية من جانب الجماعات الجهادية بهدف التدريب، فالوظيفة الأساسية للموقع هي استضافة الفيديوهات التي يقوم المشتركون بتحميلها على الموقع (Upload) وبعد ذلك تصبح متاحة للرؤية من قبل الجميع. وعلى الرغم من وجود عدد من القيود على الفيديوهات التي يمكن وضعها على الموقع، فإن نظام المراقبة في الموقع يتم بعد وضع الفيديو على الموقع، وهو ما يعني أنه لا يتم حذف الفيديو، إلا إذا قام المشاهدون على الموقع بالإبلاغ عنه، ثم تتم بعد ذلك مراجعته وإزالته من قبل القائمين على الموقع، ما يجعل هناك إمكانية لتوظيفه من قبل الجماعات الإرهابية، إذ يمكن تحميل فيديو لكيفية تصنيع قنبلة، وتتم مشاهدته مئات المرات قبل أن يتم حذفه من قبل إدارة الموقع. وعلى سبيل المثال تستخدم الجماعات المسلحة "فيسبوك" لنشر رسائلها، كما تستخدم الجماعات المسلحة "يوتيوب" من أجل شرح كيفية القيام بهجمات أو استخدام الأسلحة مثل الكلاشينكوف.

---

[١٤] سماح عبد الصبور، "الإرهاب الرقمى: استخدامات الجماعات المسلحة لوسائل التواصل الاجتماعى"، مرجع سابق، ص ٤٤.

(ISSN: 2536 - 9555)

٧-الحصول على الدعم المعنوى والمادى.

استخدمت الجماعات الإرهابية مواقع التواصل الإجتماعى لتسهيل التحويلات المالية فيما بينها، بجانب الحصول على التبرعات المالية، في ظل سهولة استخدام تلك المواقع لتحويل التبرعات والدعم المالي، مع عدم إمكانية التحقق من هوية متلقى تلك التبرعات في بعض الأحيان. وقد اعتمد التنظيم على بعض الفتاوى التي يتم بثها من بعض الدعاة على "تويتر" للتضحية بالأموال والأنفس، خاصة منذ أن انتقلت القاعدة إلى سوريا، فكانت بعض تبرعات السعوديين لحسابات مجهولة تحت دعاوى مساعدة الشعب السوري تصل إلى التنظيم، الأمر الذي حدا بالسلطات السعودية إلى التحذير من الدولة التبرع للجهات غير المصرح بها رسمياً.

وبجانب الدعم المادي، تحصل تلك الجماعات على الدعم المعنوى أيضاً من خلال مواقع التواصل الإجتماعى، فقد شهدت بعض الصفحات الإلكترونية ما أسماه البعض "البيعة الافتراضية" لزعيم تنظيم داعش من جانب آلاف السلفيين الجهاديين، وجاء ذلك على أثر إعلان الناطق باسم التنظيم عن تأسيس "دولة الخلافة"، في المناطق التي يوجد فيها التنظيم في العراق وسوريا، وظهرت صفحات على شبكات التواصل الإجتماعى من بينها "بيعة أمير المؤمنين أبوبكر البغدادي"، و"إعلان الولاء الشرعي لأمير المؤمنين أبوبكر البغدادي" وغيرها، وهو الأمر الذي ساهم فى انتشار التنظيم وتوسيع مؤيديه عبر العالم الافتراضى، وبالتالى ساهمت مواقع التواصل الاجتماعى بشكل كبير في تقديم الدعم للجماعات المسلحة والمساهمة في اتساع تأثيرها ووجودها.

وتلجأ تك الجماعات إلى استخدام شبكات التواصل الاجتماعى للأسباب التالية:

- تقليل العبء المادي، حيث إن الاعتماد على آلية منخفضة التكلفة يتيح نشر المعلومات عن التنظيمات وكيفية التواصل مع أعضائها، بالإضافة إلى إتاحة تدفق المعلومات وتسهيل تشكيل المجموعات وتقليل تكلفة تجنيد الأعضاء وإيجاد حوافز حماسية للمشاركة.

- تدعم وتعزيز وجود هوية جماعية ووجود إحساس وانتماء بين أفراد المجموعة الواحدة، حيث تربطهم قضية واحدة، وهدف مشترك، وقيم متماثلة.
- إيجاد مجتمعات للتواصل الإلكترونى يتشارك أعضاؤها الأفكار والنقاش، وتتيح تأسيس علاقات واسعة، وتمكن من قيام علاقات وجهاً لوجه، على الرغم من بعد المسافات الجغرافية(١٥).

ونخلص مما سبق إلى أن توظيف وسائل التواصل الاجتماعى أصبح مكثفاً من قبل الجماعات المسلحة، لتجاوز حاجز الزمان والمكان والرقابة الأمنية، وتوفير الوقت والجهد، وتعددت أساليب توظيف تلك الجماعات لهذه الوسائل ما بين الحصول على الدعم، وتجنيد الأفراد، ونشر الأفكار، حتى أصبحت هناك حروب غير تقليدية تدار عبر شبكات التواصل الاجتماعى، وقد ظهرت في المقابل الرقابة على تلك الوسائل من قبل الأجهزة الأمنية، وأصبح هناك نوع من الحروب غير التقليدية بين تلك الجماعات والأجهزة الأمنية للدول التي أصبح لديها متخصصون في التعامل مع تلك القضايا، ولذلك أصبح الجانب الأمنى أكثر تغلغلاً في المجالات التكنولوجية والمعلوماتية والإتصالية، وذلك من أجل التعامل مع المستجدات التكنولوجية التي تهدد الأمن القومي للدول(١٦).

ب. <u>انواع القدرات الارهابية التي يمكن استخدامها عن طريق الذكاء الاصطناعي.</u>

١ – التهديدات السيبرانية.

تعد مجالا مثيراً للقلق بالنظر الى نقاط الضعف المتأصلة في الفضاء السيبراني وتشمل التهديدات التصيد الاحتيالي وبرامج الفديه بالاضافه الى تشويه

(١٥) لمزيد من التفصيل انظر:

Garrett, R. K., "Protest in an Information Society: A Review of Literature on Social Movements and New ICTs Information", **Communication and Society**, Vol. 9, No. 2, 2006, pp 5 – 8.

(١٦) سماح عبد الصبور، "الإرهاب الرقمى: استخدامات الجماعات المسلحة لوسائل التواصل الاجتماعى"، مرجع سابق، ص ٤٦.

(ISSN: 2536 - 9555)

مواقع الويب واستخدام وسائل التواصل الاجتماعي لنشر الاخبار المضللة بغرض ارتكاب اعمال ارهابية او التحريض عليها أو التجنيد او التمويل او التخطيط لها.

٢-الهجمات الإرهابية باستخدام الآليات الذاتية القيادة.

كثيرا ما استخدمت المركبات خاصة السيارات والشاحنات الصغيره في الهجمات الارهابية، وهناك عدد لا يحصى من الأمثلة البارزة على استخدامها. ولكن الذكاء الاصطناعى أضفى عنصراً جديداً على تلك الآليات، وأصبح ممكناً استخدامها ذاتياً بدون سائق للقيام بهجمات تشمل السيارات الذاتية القيادة والطائرات المسيرة والمركبات تحت السطحية عن طريق محاكاة عمليات صنع القرار للسائق للتحكم في تصرفات السيارة، والتوجيه، والتسارع، والتشغيل. وتتوافر الخوارزميات اللازمة لذلك بشكل تجاري ما يسمح للارهابي بالهجوم عن بعد دون الحاجة للمخاطرة بإلقاء القبض عليه[١٧].

---

[١٧] وبشكل عام مثلت الطائرات المسيرة واحدة من التقنيات التي استرعت انتباه المتخصصين بقوة مع رصد تطوير عناصر من داعش لها بعد استخدامها من قبل قوات التحالف في عمليات استهدفت شخصيات مهمة في التنظيم مثل محمد اموازي الشهير بالجهادي جون وجنيد حسين مسؤول ملف التجنيد الإلكتروني بالتنظيم عام ٢٠١٥ وتم التحذير بشكل خاص من فرص امتلاك التنظيمات الإرهابية لطائرات بدون طيار من الطائرات الرخيصة التي تعكف الولايات المتحدة الأمريكية والصين على تطويرها والخوف أن يؤدي سباق التسلح في الذكاء الاصطناعي إلى زيادة استخدام الطائرات الموجهة الذكية من التنظيمات الإرهابية وتتجاوز المخاوف من الدرونز عمليات الاستهداف المباشر الى استخدامها في نشر السموم والأوبئة في حرب بيولوجيه تتزايد احتمالاتها والمخاوف منها في ظل زيادة الاستثمار في تلك التكنولوجيا وبالتالي فرص الانتشار والاستخدام كما حدث مع الديناميت والكلاشنكوف

انظر: عبير ياسين، "التكنولوجيا فى عالم الإرهاب.. سلاح ذو أوجه متعددة"، **السياسة الدولية**، عدد ٢٢٧، يناير ٢٠٢٢، ص ٢٤١.

٣-صناعة المحتوى المزيف.

وتشمل التزييف العميق للمحتوى المرئي او الصوتي لتقديم رسائل مسجلة مسبقا غالبا من قبل الجماعات الإرهابية والأفراد ويمكن استخدام محتوى مزيف على سبيل المثال لا الحصر لاقناع الافراد بأنهم يتواصلون مع شخص يعرفونه ويتم تدريب خوارزميات الذكاء الاصطناعي على نسخ أنماط الصوت والصوره للافراد المستهدفين ثم إنشاء أنماط جديدة بالخصائص نفسها ما يصعب كشف التزييف ويمكن القول أن التزييف العميق اصبح احدى اكثر حالات سوء الاستخدام وضوحا للذكاء الاصطناعي اليوم.

ومن المرجح ان يؤدي الى اعاقة ثقة الناس بوسائل الإعلام الموثوق بها تقليديا بعد أن غمرتهم الاخبار المزيفة التي يتم إنشائها بشكل متزايد بواسطة الذكاء الاصطناعي على منصات التواصل الاجتماعي.

٤-الهندسة الاجتماعية عبر الانترنت.

تعتمد على التفاعل البشري لاستغلال نقاط الضعف، وغالباً ما تنطوي على التلاعب وتستخدمها الذئاب المنفردة وغيرهم من الجامعه من الجهات الإرهابية في عمليات الاحتيال للحصول على أموال أو معلومات سرية أو لإقناع الضحايا بفعل شيء ما كانوا ليفعلوه بطريقة أخرى[١٨] وتعد روبوتات الدردشة chat bots أحد أكثر الاستخدامات وضوحاً للذكاء الاصطناعي في مجتمع العصر الحديث وغني عن القول أن المنظمات الارهابية تستغل تكتيكات الهندسة الاجتماعية عبر الانترنت في مساعدتها في تحديد وتجنيد أعضاء جدد ومتعاطفين معهم[١٩].

---

(18) Joseph M. Hatfield, "Social engineering in cybersecurity: The evolution of a concept", Computers & Security, Volume 73, March 2018, Pages 102-113.

[١٩] د. محمد خليف، "الارهاب المنفرد.. مخاطر الاستخدام الخبيث للذكاء الاصطناعى"، مرجع سابق، ص ٢٢١.

(ISSN: 2536 - 9555)

ج. العلامات الافتراضية– والإرهاب الإلكتروني.

تختلف نوعية التعاملات بالعملات الافتراضية، ففيما يستخدمها العديد من الأفراد والشركات في معاملات تجارية مشروعة، فثمة تعاملات أخرى غير مشروعة تتم عبر ما يعرف باسم "الشبكات الداكنة Dark Net، يتم فيها الإتجار بالمخدرات والأسلحة أو تمويل تنظيمات إرهابية.

١–وتتمثل أبرز أنواع العملات الافتراضية فيما يلي:

- **البتكوين:** هو نظام دفع عبر الإنترنت يعتمد على برنامج حاسب آلي مصمم لإيجاد وإدارة عرض من عملة افتراضية تسمى "بتكوين وتسيير عمليات الدفع بين مستخدمين يقومون بخصم أو إيداع حساباتهم الرقمية بوحدات "بتكوين" من دون الإفصاح عن هويتهم. وبالتالي فإن "بتكوين" هي عملة افتراضية "رقمية" لا يتم إصدارها من جهة رسمية مثل البنوك المركزية، وتعمل كوسيلة للدفع ومن دون وجود إدارة مركزية، وتعتمد على التحويلات من شخص إلى شخص من دون وسطاء (Networks Peer to Peer). ويمكن شراء أو بيع البتكوين بعملات عديدة من قبل أفراد وشركات، إما عن طريق شراء من شخص أو ماكينة صرف ألى ATM خاصة بالبتكوين فى مقابل مبلغ نقدى.
- **ليندن دولار Linden dollars :** وهي على النقيض من "البتكوين"، لا يمكن تداولها إلا في العالم الافتراضي، ممثلة في لعبة "الحياة الثانية" Second Life، والتي قام مختبر ليندن (Linden Labs) بتطويرها، وتعد أحد أكثر الألعاب الافتراضية شيوعاً، إذ بلغ عدد أعضائها نحو ١١ مليون عضو ، ووصلت قيمة تداول هذه العملة الافتراضية في عام ٢٠١٠ إلى٥٦٧ مليون دولار أمريكى.

ومن الملاحظ أن بعض الأفراد في هذه اللعبة يستطيعون توليد دخل في العالم الحقيقي real world من الأرباح المولدة في اللعبة، أى البيئة الافتراضية، ونذلك نظراً لأته يمكن تحويل "ليندن دولار لأى عملة حقيقية في أي دولة في

العالم من خلال استخدام شركة الصرافة Exchange business والقيام بتعاملات اقتصادية خارج العالم الافتراضى(٢٠).

٢-**أسباب الإقبال على العملات الإفتراضية:**

- **الحافظ على السرية:** يتضمن نظام "بتكوين" درجة عالية من إخفاء هوية المستخدمين
- **إمكانية اللجوء إلى البتكوين خلال أوقات الأزمات الاقتصادية:** فخلال أوقات الأزمات الاقتصادية، وانهيار قيمة العملة الوطنية أو تراجعها، لا تفقد العملات الافتراضية قيمتها؛ ما يجعلها تمثل بديلاً عن العملة الوطنية.
- **انخفاض تكلفة المعاملات نتيجة غياب الوسطاء:** إذ تعد "بتكوين" أول وسيلة للتجارة الإلكترونية تقترب تكلفة المعاملات فيها من الصفر، فلا توجد حاجة للاعتماد على البنوك لتسهيل المعاملات المالية.
- **سهولة الإستخدام:** إن سهولة الإستخدام تمكن من إجراء المعاملات وإدارة العملات.
- **الأمان:** درجة الأمان التي وصلت إليها البنية التحتية للعملات المشفرة لسرية وسلامة ودقة المعاملات وحسابات المستخدمين.
- **القبول:** درجة قبول العملة من قبل مجتمع المستخدمين، كذلك حجم مجتمع المستخدمين.
- **الموثوقية:** سرعة وتوافر المعاملات وفق إحتياجات المستخدمين.
- **الحجم:** الحجم الإجمالي المتوسط للعمليات المتعلقة بالعملات المشفرة.

(٢٠) د. علا السيد، "العملات الإفتراضية: التدفقات المالية الإلكترونية فى مرحلة المخاطر اللامحدودة"، **اتجاهات الاحداث**، العدد ٢، سبتمبر ٢٠١٤، ص ٥٥.

(ISSN: 2536 - 9555)

هذا وتستخدم بعض الجماعات الإرهابية العملات الافتراضية لتجنب كل الأنظمة المعروفة لمكافحة الإرهاب وغسيل الأموال، خاصة أنه يمكن من خلال العملات الافتراضية القيام بتحويلات مالية من دون الإفصاح عن هوية المتعاملين في ظل غياب هيئة مركزية تقوم بالمراقبة.

وقد أثبت تقرير صادر عن مكتب التحقيقات الفيدرالي الأمريكي في عام ٢٠١٣ أن "بتكوين هي الأداة المفضلة للمجرمين والجماعات غير الرسمية لاستخدامها في سرقة العملات الافتراضية وكذلك المضاربة وتكوين عملات افتراضية أخرى وهمية لا توجد لها قيمة أو أصل حقيقي"، وأقر بأنه "كلما زاد استخدام وتداول بتكوين سوف يزيد سوء استخدامها بسبب القابلية للقيام بمعاملة من دون ترك أي أثر"، لاسيما أن هناك شركات قامت بإنشاء سوق سوداء لتداول "بتكوين" مثل سيلك رود التي تم إغلاقها من قبل الحكومة الأمريكية[٢١].

وتجدر الإشارة إلى أن الشبكات الإجرامية تسعى لإيجاد طرق لإخفاء مصدر وهدف التمويل غير الشرعي للأنشطة الإجرامية، ومن المسلم به أن غسيل الأموال في الاقتصاد الواقعي يصعب اكتشافه، وهو الأمر الذي يعني أن اكتشافه في الفضاء الافتراضي أمر أشد تعقيداً بالطبع. وعلى سبيل المثال، فإن المستخدمين في لعبة "الحياة الثانية" قد يقومون بإنشاء حساب بأسماء وهمية أو حتى سرقة هوية شخص آخر، والقيام بأنشطة غير شرعية في الفضاء الإلكتروني، ويقومون بعد ذلك بتحويلها إلى عملة واقعية ،ثم تحويلها إلى حساب بنكي.

وينطبق الأمر نفسه على بتكوين، إذ يمكن أن يقوم تاجر مخدرات مثلاً ببيع المخدرات إلى عميل بنحو ٢.٥٠٠ بتكوين من خلال الإنترنت، ثم يقوم هذا التاجر بأخذ هذه الأموال واستخدامها في لعبة مثل البوكر على الإنترنت، ثم يقوم

---

[٢١] المرجع السابق، ص ٥٥.

بسحب الأموال من "البتكوين" وتحويلها من خلال الكازينو إلى الدولار، ثم تحويلها إلى حساب بنكي تابع لهذا الشخص.

كما يمكن للإرهابيين استخدام لعبة مثل "الحياة الثانية "والأرباح التي حققوها في اللعبة لتمويل أنشطة إرهابية، فمن الممكن أن يقوم أحد المتعاطفين مع منظمة إرهابية بشراء ليندن دولار، ويتصل بعضو الجماعة الإرهابية من خلال اللعبة، لشراء منتجات افتراضية منه، ثم يقوم هذا العضو بأخذ هذه الأموال وتحويلها لأموال واقعية لشراء المنتجات اللازمة للقيام بعملية إرهابية، كما قد تتم المعاملة نفسها باستخدام البتكوين، وفي كلتا الحالتين، فإن تعقب هذه المعاملات المالية أمر صعب[٢٢] ويسمح لمجرمي الإنترنت بالتحايل على المؤسسات المالية وأدواتها التشغيلية التي تم تصميمها لمكافحة تمويل الإرهاب وقد يؤدي ارتفاع معدل الربح وتقلب قيمة العملات المشفرة إلى اعتمادها على نطاق واسع من قبل الجماعات المتطرفة التي تحتاج الى آلية جديدة لجمع الأموال للحفاظ على أنشطتها[٢٣].

٣-تقييم قدرات العملات الافتراضية في تمويل الإرهاب:

كانت العملات الورقية هي الطريقة الفعالة الوحيدة للدفع لأغراض غير مشروعة بسبب عدم الكشف عن هويتها وتكتمها على طبيعة الصفقة، إلا أنها في المعاملات الدولية لا تتم آنياً، كما ان طريقه الدفع الرقميه لم تكن فعالة لأنها تترك أثراً للمال يتعين تعقبه فيما بعد. الأمر اختلف مع ظهور العملات الافتراضية التي تعتمد على بنية تحتية للدفع مبني على بروتوكولات البرامج، وفيها يستخدم أسلوبان تقنيان متماسكان هما العملات المشفرة Cryptocurrency، وتسلسل الكتل Blockchain، فمعظم العملات الافتراضية

---

[٢٢] المرجع السابق، ص ٥٦.

[٢٣] د. عبد الله عبد العزيز النجار، "التكنولوجيا وتمويل الإرهاب.. العملات المشفرة نموذجاً"، **السياسة الدولية**، عدد ٢٢٧، يناير ٢٠٢٢، ص ٢٤٨.

(ISSN: 2536 - 9555)

حالياً محمية بتكنولوجيا التشفير التي تم تصميمها باستخدام علوم الرياضيات، بينما تسلسل الكتل هي شبكات مفتوحة من الكتل المشفرة والتي تعمل كقاعدة بيانات للمعاملات المالية العامة، وكلاهما يدمج مبادئ التشفير لتحقيق اقتصاد معلومات موزع لا مركزي وآمن. ولزيادة ميزة اخفاء الهوية توفرت تكنولوجيا خلط العملات المشفرة Coin Mixer تعمل خلاطات العملة عن طريق أخذ العملة المشفرة المراد إرسالها ومزجها مع كومة عملاقة من العملات المشفرة الاخرى، ثم ارسال وحدات أصغر من العملة المشفره الى العنوان المطلوب، هذه الخدمه تجعل تتبع المعاملات في شبكة العملة المشفره أكثر صعوبة[٢٤].

على مدى الزمن كان هناك ابتكار مستمر في مجال العملة المشفرة وظهرت عملات جديدة يطلق عليها العملات البديلة Alt-Coins، بعضها معزز بخصوصية تعتبر اكثر ازعاجاً وحمايه من بيتكوين. وتمكن Zcash من إجراء المعاملات أثناء عدم الاتصال بالانترنت، ممن يجعل من الصعب على سلطات الدولة تتبع المعاملات غير المشروعة، وان كان التحقق من هوية المرسل وهوية المتلقي وعلاقته المحتملة بالإرهاب أمراً اساسياً لهيئات مكافحة الارهاب، فان التطورات التقنية الجديدة ستهدد مكافحة التمويل. وتوفر عملات الخصوصية مثل Monero حماية اكثر تعزيزاً لخصوصية المستخدم، كما أن المحافظ غير الحاضنة/ اللامركزية[٢٥]، والتبادلات، تسمح بمعاملة نظير إلى نظير P2P نقية دون توفير وسيط، وفي معاملات P2P البحت، لا يمكن ممارسة الرقابة التنظيمية المباشرة إلا من قبل السلطات التنظيمية وسلطات التحقيق. وسيتطلب هذا النهج

(24) "Coin mixer: What is it and how does it work?, https://www.okx.com/learn/what-is-coin-mixer, Jul 28, 2023.

(25) Pawan Nahar, "What is the difference between custodial and non-custodial crypto wallets?", The Economic Times, May 26, 2022, On: https://economictimes.indiatimes.com/markets/cryptocurrency/what-is-the-difference-between-custodial-and-non-custodial-crypto

تطوير قدرات تقنية جديدة وتوسيع قدرات الرصد المتخصصة داخل السلطات التنظيمية، الأمر الذي من شأنه أن يشكل تحديات هائلة للموارد المحدودة الموجودة.

نهاية القول.. تشكل التكنولوجيا والعملات المشفرة تحديات جديدة لأعمال مكافحة الإرهاب التى تقوم بها الدول والمنظمات الدولية. وحيث أن استخدام العملة المشفرة لتمويل المنظمات الإرهابية لا يزال فى مراحلة الأولية، فإن التدابير المضادة لا تزال فى مرحلة استكشافية كذلك، وتحتاج السلطات إلى تسخير إمكانات العملات المشفرة فى التنمية الاقتصاية للدولة، كما يلزمها فهم آلياتها لتسهيل الكشف المبكر عن تمويل الإرهاب، ومن شأن عدم القيام بذلك أن يسمح بتطوير جهاز مالى كبير محتمل دون قيود ينتظر الاستغلال الكامل من قبل الإرهاب الذى تحركه الإنترنت، لذلك فإن الرقابة التنظيمية المتزايدة والتدقيق المعزز لإنفاذ القانون فى استخدامها أمر واجب[٢٦].

د. أدوات مكافحة الإرهاب المتاحة لجهات إنفاذ القانون باستخدام الذكاء الاصطناعي.

في المقابل يمكن أن يكون الذكاء الاصطناعي اداه قويه في مكافحه الأرهاب وتمكين أجهزه إنفاذ القانون والمكافحة من تعزيز الفاعلية عبر خطوات[٢٧] حيث بدأت المنظمات في استخدام أنظمة دفاع قوية تستخدم التكنولوجيا لمواجهة الإرهاب الالكتروني، وهناك العديد من الطرق الواعدة للحد من هذه الهجمات الإرهابية، في الواقع، تنمو الهجمات الإلكترونية بنفس سرعة نمو الابتكار

[٢٦] د. عبد الله عبد العزيز النجار، "التكنولوجيا وتمويل الإرهاب.. العملات المشفرة نموذجاً"، مرجع سابق، ص ٢٥١.

[٢٧] عبير ياسين، "التكنولوجيا فى عالم الإرهاب.. سلاح ذو أوجه متعددة"، مرجع سابق، ص٢٤١.

(ISSN: 2536 - 9555)

التكنولوجي. لذلك فالتقنيات التي تمكن الإرهاب الإلكتروني مفيده أيضاً لتقليل مخاطر التهديدات، ومن هذه التقنيات على سبيل المثال لا الحصر[٢٨]:

١-شريحة الحاسوب عالية التقنية التي تمنع الهجمات بشكل استباقي.

أعلن الباحثون في جامعة ميتشيغان انهم توصلوا الى طريقة استباقية لردع أي هجوم الكتروني عن طريق شريحة تقوم بتشفير وتغيير بياناتها وترميزها ٢٠ مره في الثانية[٢٩]. حتى اذا اخترق احد المتطفلين جهاز حاسوب، فإن المعلومات التي يحتاجون إليها لاستغلال ثغرة أمنية تختفي في غضون أجزاء من الثانية وأكد الباحثون أن الشريحة نجحت في منع كل نوع من اختراق التحكم في التدفق وهو أحد أكثر الهجمات شيوعا وخطورة.

٢-تقنية البلوكتشين.

البلوكتشين blockchain هي التقنية التي تضمن صلاحية العملات الرقمية. وبشكل عام يمكن أن تساعد في مكافحة الهجمات الإلكترونية، لأنه لا يمكن تغييرها أو حذفها بمرور الوقت. تعد تقنية البلوكتشين أحد الاحتمالات القابلة للتطبيق للحفاظ على التفاصيل القيمة في مأمن من الارهابيين، ويتم التحقيق من المعلومات واضافتها بشكل دائم الى دفتر الاستاذ الرقمي. ولهذا من الصعب التلاعب بالمحتوى، خاصة أنها تعطي الشفافية لجميع الأطراف المعنية. يمكن البلوكتشين المؤسسات من التعامل الآمن مع المعلومات، هذا ما جعل شركات مثل Microsoft و IBM و Walmart و UPS تستخدمه لمنع العبث واكتشاف أي شكل من أشكال التخريب السيبراني.

---

[٢٨] د. غادة محمد عامر، "جهود الدول فى مكافحة الإرهاب الإلكترونى"، **السياسة الدولية**، عدد ٢٢٧، يناير ٢٠٢٢، ص ٢٥٥.

[29] university of Michigan News, "Unhackable: New Chip Stops Attacks Before They Start", SmithBucklin, Washington, May 6, 2019, On: https://cacm.acm.org/news/236672-unhackable-new-chip-stops-attacks-before-they-start/fulltext

٣-<u>الذكاء الاصطناعي.</u>

جمع باحثو معهد ماساتشوستس للتكنولوجيا بين المعرفة البشرية وأجهزة الحاسوب في منصة تسمى AL2، وأختبروها على ٣.٦ مليار قطعة من البيانات(٣٠)، اظهرت النتائج ان النظام توقع أحداث الأمن السيبراني بدقة ٨٥%، وهو ما يقرب من ثلاث مرات أفضل من السابق. كذلك يقوم الذكاء الاصطناعي بأتمتة عمليات تحديد الهوية، وتقوم الأساليب القائمة عليه بمسح النظام بكفاءة، ومقارنة مصادر المعلومات المختلفة لاكتشاف نقاط الضعف، كما يقوم بمنع الهجمات من خلال النظر في الأحداث السابقة (التعلم الآلي)، ويمكن استخدام الذكاء الاصطناعي لمحاربة الارهاب الالكتروني عن طريق:

- **مكافحة الفيروسات:** تكتشف برامج مكافحة الفيروسات ذات الذكاء الاصطناعي الشذوذ في الشبكة عن طريق متابعة العمليات التي تتصرف بشكل مريب وتمنعها عند إطلاقها.
- **نمذجة سلوك المستخدم:** يقيم الذكاء الاصطناعي سلوك مستخدمي الشبكة لتقييم كيفية تفاعلهم مع النظام واكتشاف محاولات الإطاحة به، ويمكن له كذلك تحديد الأنشطة المشبوهة، والاستجابه عن طريق تعطيل المستخدم، أو عن طريق إخطار مسؤولي النظام.
- **التحليل الالي للشبكه والنظام:** يضمن التحليل الآلي لمعلومات الشبكة التقييم المستمر والكشف المبكر للهجمات الإلكترونية المشتبه بها.

٤-<u>استخدام منصات متعددة الكيانات للكشف والاستجابة.</u>

من الحقائق الصعبة للأمن السيبراني ان المخاطر يمكن أن تأتي من مصادر متعددة، لذلك يستلزم نهج واحد للأمن السيبراني البحث عن انواع عديدة من

(30) Adam Conner-Simons, "ystem predicts 85 percent of cyber-attacks using input from human experts",
https://news.mit.edu/2016/ai-system-predicts-85-percent-cyber-attacks-using-input-human-experts-0418

(ISSN: 2536 - 9555)

التهديدات والحماية ضدها جميعاً، وهذا ما وهذا مثل ما اطلقته شركة تسمى Mistnet منتجاً يسمى CyberMist، وهو عباره عن أداة لنظام للكشف والاستجابة متعدد الكيانات، وتوفر هذه الأداة منعاً في الوقت الفعلي للتهديدات، وتوفر الرؤية المرتبطة بالمستخدمين أو الشبكات أو المضيفين. فهي تجمع بين الحوسبة المتطورة وتحليلات الذكاء الاصطناعي للعثور على التهديدات في اقل من ساعه. وتشير المقاييس المحدثة باستمرار على الصفحة الرئيسية للمنتج إلى أن CyberMist قد خفض الاختراقات بنسبة ٩٩% في خلال شهر[٣١].

٥-<u>الأدوات التقدمية لتحديد التهديد.</u>

هناك عدة أنواع من التقنيات يمكن استخدامها كجزء من خطة شاملة ضد التهديدات الإلكترونية، وهي تشمل تقنيات الخداع الدفاعي، التي تحدد الهجمات في وقت مبكر وتنقل البيانات المهمة قبل الوصول إليها او إتلافها. ويساعد استخدام الشراك الخداعية، بالإضافة إلى جدران الحماية لتطبيقات الويب، ونظام منع الاختراق IPS، وحلول الخداع المستندة الى الويب، في حماية البيانات من الهجمات.

ثالثاً: الحرب السيبرانية- والذكاء الإصطناعى.

أحدث ظهور الحرب السيبرانية بشكل فعلي على الساحة الأمنية والمعلوماتية منذ منتصف العقد الأول من القرن الحالي نقلة نوعية في مفهوم الحرب التقليدية من حيث الوسائل والأهداف والنتائج أيضاً، فمن حيث الوسائل يتبين أن الحروب دائماً ما تتطور بتطور الآليات والأدوات المستخدمة في شنها، إذ أصبح اختراق قواعد البيانات والمعلومات او التلاعب بها أو تدميرها من خلال البرامج المعدة

---

(٣١) راجع فى ذلك:

Eastern Daylight Time, "MistNet Launches CyberMist Advanced Threat Detection Platform using Edge AI and Mist Computing, Closes Series A Funding Round", https://www.businesswire.com/news/home/20190521005248/en/MistNet-Launches-CyberMist-Advanced-Threat-Detection-Platform-using-Edge-AI-and-Mist-Computing-Closes-Series-A-Funding-Round

لذلك هو العنصر الاستراتيجي في شن الهجمات في عصر الثورة الرقمية، وذلك بعد أن أضافت الثورة التكنولوجية ساحة جديدة للصراع هي هجمات الفضاء السيبراني Cyberspace، والتي تؤذن ببداية ما يمكن تسميته الحرب السيبرانية Cyber War.

وفيما يتعلق بغايات تلك الحرب فإن الخسائر البشرية والمادية لم تعد هي الغاية المباشرة المتوقعة من شأن الحروب، وإنما تخطت الهجمات السيبرانية ذلك لغايات اخرى قد يكون من بينها تدمير قواعد البيانات والمعلومات الخاصة بالدول، أو سرقتها وإتاحتها على العلن بغرض إحداث الفضائح السياسية بالشكل الذي يسبب إحراجاً للقيادة السياسية لتلك الدول، والتأثير على شرعيتها، أو سرقة المعلومات التقنية والصناعية للدول بغرض تخريب البنية التحتية الحيوية، وهو الأمر الذي يعكس عمق الخطر الاستراتيجي لتلك الهجمات التي قد تصل لدرجة الحرب، ما دفع غالبية دول العالم الى وضع الأمن المعلوماتي والسيبراني في صدارة أولويات الأمن القومي[٣٢].

(أولاً) مفهوم الحرب السيبرانية.

تعرف الحرب السيبرانية بأنها "إجراء والإستعداد لإجراء العمليات العسكرية بالاعتماد على المبادئ والآليات المعلوماتية، ما يعني تعطيل– إن لم يكن تدمير– نظم المعلومات والاتصالات على اوسع نطاق لتشمل حتى العقيدة العسكرية للعدو، والتي يعتمد عليها لتحديد أهدافه والتحديات التي يواجهها[٣٣].

وقد تعددت التعريفات المطروحه للحرب السيبرانية دون وجود تعريف جامع تتفق عليه معظم الأدبيات، حيث تختلف في أغلب الاحيان حول محورين أساسيين، وهما: اقتصار تلك الحروب على الدول دون غيرها، وحجم التداعيات على تلك الحرب.

---

[٣٢] سارة عبد العزيز، "الحرب السيبرانية: التداعيات المحتملة لتصاعد الهجمات الإلكترونية على الساحة الدولية"، **اتجاهات الأحداث**، عدد ٢٠، مارس– إبريل ٢٠١٧، ص ٩.

[33] John Arquilla, David Ronfeldt, "Cyberwar is Coming!", **Comparative Strategy**, Vol. 12, No. 2, Spring 1993, pp. 141-150.

(ISSN: 2536 - 9555)

بالنسبة للمحور الأول، فإن بعض التعريفات المطروحة تقصر الحرب السيبرانية على الدول من حيث كونها الفاعل الرئيسى فى هذه الحرب، بينما ترى أطروحات أخرى ضرورة تضمين الفاعلين من غير الدول فى تعريف تلك الحرب نتيجة لدورهم فى إطلاق الهجمات السيبرانية سواء بشكل منفرد أو بالنيابة عن الدول. أما فيما يتعلق بالمحور الثاني وهو التداعيات المترتبة على الحرب السيبرانية، وتعكس هذه التعريفات المختلفة وجود مجموعة من الخصائص المميزة للحرب السيبرانية وللصراعات عبر الفضاء السيبراني، سواء من جانب الدول او الفاعلين من دون الدول[٣٤]، **وهو ما يمكن إيجازه في الآتي[٣٥]:**

- **انخفاض التكاليف** لا تحتاج الحرب السيبرانية إلى أعداد كبيرة من القوات والأسلحة ولا توجد تكاليف كبيرة لدخول المجال السيبراني باستثناء التكاليف الخاصه بعمليات التطوير وبناء الكفاءات في إطلاق الهجمات السيبرانية.
- **سهولة الاختراق** من الممكن أن يحدث الاختراق الإلكتروني نتيجة للتطور التكنولوجي السريع في المجال السيبراني حتى مع اتباع أكثر الأنظمة الدفاعية دقة.
- **الطبيعة غير المتماثلة للحروب السيبرانية** دائماً ما يحدث الهجوم نتيجة لتفوق المهاجم على الهدف أو وجود قصور في الدفاع السيبراني للجهة المستهدفة.
- **انتفاء أدلة الإدانة** يكتنف الحرب السيبرانية الكثير من الغموض، فالجهة التي تقوم بالهجمات السيبرانية غالباً ما تظل مجهولة، الأمر الذي يعتمد

---

[٣٤] انظر فى ذلك:

Shane Martin Coughlan, Is There A Common Understanding Of What Constitutes Cyber Warfare?, MA in International Studies (Globalisation and Governance) at the University of Birmingham, Second Edition March 2016, pp. 24-5.

[35] Fred Schreier, "on cyberwarfare", **Dcaf horizon working paper**, No. 7, 2015, pp. 27-28.

على مجرد تخمينات الدولة او الجهة المستهدفة، ومحاولة الربط بين الأحداث من دون وجود دليل قاطع بالضرورة.

- **إحداث نطاق واسع من التداعيات** في ظل الترابط بين الشبكات في القطاعات الحيوية بالدولة، يمكن للهجمات السيبرانية تعطيل وتدمير تلك الشبكات، وما يرتبط بها من بنية تحتية على أوسع نطاق ممكن، أي أن آثارها قد تتجاوز بذلك قدره الأسلحة التقليدية.
- **فعالية ودقة تحديد الأهداف** يمكن للهجمات السيبرانية تحديد الهدف بدقة، وتعطيله، أو تدميره.
- **عدم وجود مظلة قانونية** تجري الحرب السيبرانية في ظل ساحة مفتوحة، وما زالت تبذل الجهود لتنظيم العمليات التي تجري فيها من قبل القانون الدولي، ولكن لا توجد حتى الآن قواعد وقوانين تعمل على الحد من الإفراط في استخدام الهجمات السيبرانية أو تحديد نطاقها والتداعيات المترتبة عليها، أو خضوع مرتكبيها للعقوبة.

(ثانياً) أشكال الحرب السيبرانية.

تتمثل أهمية تصنيف الهجمات السيبرانية في توضيح المستويات المختلفة منها، بما يسمح بالتمييز بين الحرب السيبرانية وغيرها من العمليات الأخرى التي تتخذ من الفضاء السيبراني مجالاً لها، ويمكن بشكل عام تصنيف الهجمات السيبرانية وفقاً لمعيارى درجة الشدة Intensity، والغرض من تلك الهجمات، وذلك كما يلى:

١- **معيار درجة شدة الهجمات السيبرانية:** قسمت دراسة صادرة عن مجلة الناتو (NATO Review) تحت عنوان "مواجهة الحرب السيبرانية" الهجمات وفق هذا المعيار إلى ثلاثة مستويات، وهي:

أ. **الحرب السيبرانية المرتبطة بتحقيق أهداف عسكرية:** انطلاقاً من مبدأ كلاوزفي Clausewitz الخاص بإحداث "ضبابية الحرب" للعدو بما يصب فى صالح القوات المحاربة، فإن القوات العسكرية الحديثة تحاول الاستفادة من الهجمات السيبرانية في تحقيق التفوق المعلوماتى أو الهيمنة

(ISSN: 2536 - 9555)

المعلوماتية على ساحة المعركة، وهو ما يمكن تحقيقه من خلال استهداف نظم المعلومات والاتصالات الخاصة بالعدو، أو من خلال مهاجمة تلك الأنظمة داخلياً، ليس فقط لحرمانها من الخدمة، بل والحرمان من القدرة على استخدام أنظمتها الخاصة، ومن ثم فإن هذا الشكل من أشكال الحرب السيبرانية يركز على الأهداف العسكرية بالأساس(٣٦).

ب. **الحرب السيبرانية المحدودة:** يركز هذا النوع على أهداف محددة تتمثل في البنية التحتية المعلوماتية للدولة، أو الجهة المستهدفة، من دون أن يصاحبها القيام بأي عمليات على أرض الميدان، حيث تشكل تلك البنية التحتية في هذه الحاله الهدف والوسيلة بل وسلاح الهجوم أيضاً. وقد يتم استخدام الشبكات واسعة النطاق أو روابط مشاركة البيانات الخاصة بالدولة أو الجهة المستهدفة للقيام بهجمات سيبرانية على أهداف معلوماتية داخلها، كما قد يتم استهدافها مباشرة من خلال تقليل كفاءتها أو تدميرها، وذلك للتأثير على كفاءة وفاعلية الجهة المستهدفة، حيث يتم الاعتماد على تلك البنية التحتية في الأمور العملية والتنظيمية كافة، وتكشف طريقة تعامل الجهة المستهدفة مع الهجوم السيبراني عن مواطن الخلل في أنظمتها والبنية التحتية الخاصة بها بشكل كبير.

وواقعياً تحقق الحرب السيبرانية المحدودة مجموعة من المزايا فهي: **أولاً** تجنب الدولة النزول الى ساحة المعركة من البداية، حيث تشل حركة العدو وتحول دون تنفيذ العمليات التي تعتمد على تلك البنية التحتية، لأنها تتيح اختراق البنية التحتية المعلوماتية الخاصة بالعدو، **وثانياً** تحدث حالة من ارباك العدو والتشكيك في المعلومات الموجودة كافة التي يمكن اتخاذ القرار بناءً عليها، **وثالثا** تلجأ الدول إلى هذا النمط من الحرب السيبرانية لإبطاء استعدادات العدو للتدخل العسكري كجزء من المناورة التي ترافق عادة الأزمات والمواجهات المحتملة بين الدول(٣٧).

---

(36) Timothy Shimeall, "Countering cyber war", Nato Review, Vol. 49, No. 4, December 2001,

(٣٧) سارة عبد العزيز، "الحرب السيبرانية: التداعيات المحتملة لتصاعد الهجمات الإلكترونية على الساحة الدولية"، مرجع سابق، ص ٩.

ت. **الحرب السيبرانية غير المحدودة:** ربما يأتي هذا النوع على قمة التصنيف المتعلق بدرجة شدة الهجمات السيبرانية، وتتسم بثلاث خصائص رئيسية: أولها انها حرب شاملة من حيث النطاق والهدف من دون تمييز بين الأهداف العسكرية والمدنية، وثانيها أنها تسفر عن مجموعة واسعة من التداعيات المادية والبشرية حيث تعتمد على خلق حالة شاملة من الفوضى والدمار، الأمر الذي تتراجع معه قدرات الدولة على السيطرة وإدارة الأمور، وثالثها أنها تتجاوز الخسائر المادية والبشرية التي تحدثها لتخلف مجموعة من الآثار الاقتصادية والاجتماعية شديدة الوطأة، ومن ثم فهي نموذج للحرب السيبرانية شديدة التنظيم والتعقيد، والتي تماثل في آثارها النتائج المترتبة على الحروب التقليدية الشاملة، وإن كانت أسرع في إحداث الآثار التدميرية المباشرة.

٢-المعيار الثاني الهدف من الهجمات السيبرانية.

سمة ثلاث مجموعات أساسية تندرج تحتها العديد من الأسباب والدوافع التي تقع خلف شن الحروب السيبرانية **ومن بينها ما يلي:**

أ. **الهجمات السيبرانية ذات الأهداف الاستراتيجية:** وهي تلك الهجمات التي تستهدف مواقع نظم المعلومات والاتصالات وتهدد الأمن الداخلي للدول وذلك من خلال مجموعة من الاهداف الفرعية التي قد تتحقق منفرده أو مجتمعة ومن أبرزها[٣٨]:

- **هجمات الحرمان من الخدمة Denial Of Service Attack:** تهدف الهجمات السيبرانية في هذه الحالة إلى حرمان المستخدم الأصلي لأجهزة الحاسبات أوالشبكات أو المواقع من القدرة على استخدامها، وتعد هذه الاستراتيجية من أبسط الهجمات السيبرانية من حيث التكتيك من حيث التكتيك المستخدم في إحداثها وأكثرها شيوعاً، حيث يتم إغراق الهدف بعدد لا نهائي

(38) Sabrine SAAD, Stéphane BAZAN, Lorraine ETIENNE, Christophe VARIN, Asymmetric Cyber-warfare between Israel and Hezbollah The Web as a new strategic battlefield, **International Studies Perspectives,** Vol. 17, No. 3 (2016), pp. 307-321.

(ISSN: 2536 - 9555)

من البيانات الوهمية، ومن ثم لا يمكنه الاستجابة للطلبات الحقيقية من الخدمات أو المعلومات من جانب المستخدم الاصلي لها. وقد يتضمن هذا الشكل من الهجمات تجنيد مجموعة مئات أو آلاف من الأجهزة للمشاركة في الهجمات السيبرانية، وذلك بغرض التشويش و صعوبة تعقب الجهة التي قامت بالهجمة وتعقيد عملية إيقاف تلك الهجمات حيث تنبع من أكثر من مصدر (٣٩).

وقد تصل الهجمات الشديدة إلى هدف تحقيق الحرمان الدائم من الخدمة Permanent Denial of Service، والتسبب في التدمير المادي لأجهزة الحاسبات، حيث يتم استخدام التداخل الكهرومغناطيسي لتدمير الإلكترونيات المكونة للأجهزة والشبكات. وتنطوي استراتيجية الحرمان من الخدمة على العديد من الآثار السلبية، فهي تسبب للدولة او الجهة المستهدفة خسائر مالية نتيجة توقف الخدمة التي تقدمها لفترة من الزمن، وارتفاع تكاليف إصلاح التدمير الذي أحدثته الهجمات. ومن جانب آخر يؤدي التعرض لذلك النوع من الهجمات الى اهتزاز ثقة المواطنين في قدرة الأنظمة المعلوماتية للدولة أو الجهة على مواجهة الهجمات السيبرانية(٤٠).

ويتفاقم الأمر في حالة مرور الدولة بحالة من عدم الاستقرار، حيث تفقد قطاعات الدولة القدرة على التواصل فيما بينها، أو التحكم في مجريات الأمور، ومن ثم تسود حالة من الفوضى بين المواطنين بما يهدد الأمن الداخلي للدولة ذاتها مثلما حدث في استونيا في عام ٢٠٠٧ أثناء احتقان العلاقات الدبلوماسية مع روسيا. هذا إلى جانب إمكانية استغلال تلك الحالة من جانب الدولة المعتدية

(39) Bello O. A., Aderbigbe F. M., "Cyberwar-The New Frontier of International Warfare", **International Journal of Sustainable Development Research**, Volume 1, Issue 1, September 2015, Pages: 1-6.

(40) Laone Moalosi, The New Battlefield: Cyberattacks Transforming Warfare, Solutions Global, Sep 26, 2023, On: https://www.linkedin.com/pulse/new-battlefield-cyberattacks-transforming-warfare-laone-moalosi

في القيام بعمل عسكري أو نشر حمل عدائية ضد الدولة لإثارة الاضطرابات والقلاقل بما يحقق أهدافها[٤١].

- **تغيير البيانات:** يعد هذا النوع من الهجمات السيبرانية على درجة كبيرة من الخطورة، حيث أن اختراق الاجهزة والشبكات الخاصة بالدولة أو الجهه المستهدفة، وتغيير البيانات الموجودة عليها هو أمر قد لا تنتبه له الجهه المستهدفة إلا بعد مرور فترة من الزمن، ومن ثم فإن قرارات مهمة قد تتخذ في تلك الفترة بناءً على معلومات مغلوطة. وتتراوح حدة هذه الهجمات بين مجرد تشويه المواقع بتغيير المحتوى الوارد عليها أو ما يمكن تسميته بـ الجرافيتي الالكتروني Electronic Graffiti، وتصل الى ذروتها في حال استهداف قواعد البيانات الخاصة بالأسلحة وأنظمة القيادة والتحكم.
- **التحكم في أنظمة البنية التحتية:** تعتبر البنية التحتية الحرجة Critical Infrastructure كل الأنظمة والأصول، سواء كانت مادية أو افتراضية، والتي قد يتسبب عدم القدرة على التحكم فيها أو تدميرها في الإضرار بالأمن القومي للدولة، والأمن الاقتصادي، وسلامة وصحة المواطنين وغيرها. وفي ظل الثورة الرقمية، فإن تلك البنية التحتية الحرجة تتم إدارتها من خلال شبكات إلكترونية، الأمر الذي يجعلها عرضة للهجمات السيبرانية التي تستهدف السيطرة عليها وإدارتها على نحو مخالف لرغبة الدولة أو حتى تدميرها، وهو ما يؤثر بشكل مباشر على الأمن القومي للدول، وتتعدد الأمثلة في هذا السياق وأبرزها على الإطلاق هو حادثة Stuxnet، ذلك البرنامج المخصص لاختراق أنظمة التحكم الصناعية، والذي تسبب في عام ٢٠١٠ في تدمير أجهزة طرد مركزية داخل مواقع تخصيب اليورانيوم ناطنز الإيرانية،

---

(٤١) ومن ابرز الامثلة على اقتران الحرمان من الخدمة بعمليات عسكرية ما قامت به روسيا أثناء حربها مع جورجيا في عام ٢٠٠٨ حيث تم توجيه مجموعة من الهجمات السيبرانية التي استهدفت موقع الرئاسة وعدد من الوزارات لحرمانها من الخدمات، الأمر الذي كان له بالغ الأثر في سهولة اقتحام جورجيا عسكريا وسرعة السيطرة على الأوضاع.

(ISSN: 2536 - 9555)

وفي أغسطس ٢٠١٢ تم توجيه سلسلة من الهجمات السيبرانية ضد شركة أرامكو السعودية أكبر منتج للنفط والغاز في العالم حيث تم حيث دمر حوالي ٣٠ ألف جهاز كمبيوتر، واستهدفت الهجمات بالأساس تعطيل أو وقف انتاج النفط والغاز، الأمر الذي كان سيتسبب في خسائر فادحة للمملكة العربية السعودية وللإقتصاد العالمي(٤٢).

ب. **الهجمات السيبرانية ذات الأهداف التقنية/ العسكرية:** تستهدف تلك الهجمات بشكل أساسي انظمة مراقبة الأسلحة ومواقع التواصل والتحكم العسكرية. ويدخل **التجسس السيبراني** Cyber Espionage في هذا السياق أيضاً، فعلى الرغم من أنه يمكن اعتبار التجسس السيبراني عملية مستقلة عن الحرب السيبرانية فان اقترانها بهجمات سيبرانية أخرى هو ما يضعها في نطاق أهداف الحرب السيبرانية حيث يتم استخدام القدرات السيبرانية في الحصول على المعلومات عن الجهة المستهدفة من الهجمات السيبرانية، وكيفية إصابتها بشكل دقيق. ومن الممكن الحصول على بيانات ومعلومات استخباراتية تخص البنية التحتية الحرجة، وكذلك الاتصالات والخطط السياسية والعسكرية الحساسة للغاية. وقد يهدف التجسس السيبراني أيضاً إلى إحداث خسائر اقتصاديه أو سرقه الابتكارات والأبحاث والمفاوضات السرية وغيرها(٤٣).

ج. **الهجمات السيبرانية ذات الأهداف السياسية:** هي تلك الهجمات التي تهدف الى تحقيق أهداف سياسية محددة، ويعتبر بعضها تدخلاً في

---

(٤٢) انظر فى ذلك:

Peter Trim, Yang-Im Lee, Strategic Cyber Security Management, 2023, On:
https://www.routledge.com/Strategic-Cyber-Security-Management/Trim-Lee/p/book/9781032154763

(٤٣) لمزيد من التفصيل انظر:

Peter W. Singer and Allan Friedman, **Cybersecurity and Cyberwar: What Everyone Needs to Know**, Oxford University Press, 2020, Oxford, pp. 90-91.

الشؤون الداخلية للدول، كما يمكن الاستعانة بـ الهجمات السيبرانية محدودة التكاليف في إحداث حملات شديدة التأثير من الدعاية والفضائح السياسية، وذلك من خلال اختراق الشبكات والأجهزة ونشر الوثائق الحساسة الموجودة بها على مواقع أخرى. وإتاحتها للجميع، الأمر الذي قد يتسبب وفقاً لطبيعة تلك التسريبات في الإحراج السياسي او اضطراب الساحة الداخلية أو توتر العلاقات الدبلوماسية بين الدول أو حتى اهتزاز الأوضاع الاقتصادية.

وقد شهد العالم خلال السنوات الأخيرة موجات كبيرة من التسريبات، منها موجة تسريبات "ويكيليكس" التي تضمنت نشر آلاف الوثائق السرية الرسمية المتبادلة بين وزارة الخارجية الامريكية وبعثاتها في دول العالم، وهو ما أحدثته تلك التسريبات من توتر حاد في العلاقات الدولية بين العديد من الدول التي مستها التسريبات، بالإضافة إلى حالة عدم الاستقرار الداخلي في بعض الدول، حيث انطلقت العديد من الاضطرابات والاحتجاجات نتيجة لما ورد بها، وأخيراً جاءت تسريبات أوراق بنما للأنشطة المشروعة وغير المشروعة للشركات المسجلة في الخارج، وهو ما تسبب في مشكلات لعدد كبير من المسؤولين السياسيين البارزين، وفي مقدمتهم ديفيد كاميرون، رئيس الوزراء البريطاني السابق[٤٤].

(ثالثا) استراتيجيات مواجهة الهجمات السيبرانية.

تستدعي مواجهة الهجمات السيبرانية من جانب الدول والفاعلين من غير الدول وجود سياسة واضحة المعالم تحتوي على مجموعة من العناصر الأساسية، لعل من بينها تحديد أهداف تلك السياسة السيبرانية، والخيارات الاستراتيجية المتاحة للتعامل مع الهجمات السيبرانية، ودرجة التوازن المطلوب تحقيقها في الاستراتيجية المستخدمة بين العدائية والدفاع، على أنه يستلزم في الوقت ذاته تطوير تلك السياسة بشكل مستمر في ضوء التطورات التكنولوجية وقدرات الفاعل

[٤٤] سارة عبد العزيز، "الحرب السيبرانية: التداعيات المحتملة لتصاعد الهجمات الإلكترونية على الساحة الدولية"، مرجع سابق، ص ١٢.

(ISSN: 2536 - 9555)

ذاته سواء كان دولة او غيرها في المجال السيبراني. وواقعياً، فإن عدم وجود تلك السياسة قبل حدوث هجوم سيبراني سيجعل قدرة الجهة المستهدفة على الرد محدودة وغير فعالة. وتتضمن الخيارات الاستراتيجية المطروحة أمام الدول في مواجهة تلك الحرب السيبرانية مجموعة من البدائل التي تتضمن الدفاع السيبراني، والردع السيبراني، علاوة على آليات تعتمد السياسة الخارجية التقليدية[٤٥]، **وهو ما يمكن تناوله بإيجاز في الآتي:**

١- **الدفاع السيبراني Cyber Defense:** في ظل ما تمثله الهجمات السيبرانية من تهديد لأمن الدول والفاعلين، أصبح لزاماً عليهم إعداد السياسات الدفاعية اللازمة لمواجهة تلك الهجمات وتأثيراتها، حيث يعبر الدفاع السيبراني في شكله التقليدي عن مجموعة التدابير التقنية وغير التقنية التي تتخذها الدولة بما يسمح لها بالدفاع عن نظم المعلومات في الفضاء السيبراني، ومن ثم تعتمد تلك الاستراتيجية على تطوير القدرات الدفاعية السيبرانية وتوفير الحماية والأمن السيبراني للأجهزه والشبكات الحكومية والخاصة، وكذلك البنية التحتية من التعرض للهجمات السيبرانية، في خطوة استباقية هدفها الوقاية من تلك الهجمات، وإن كان ذلك لا يمنع من وقوع تلك الهجمات في ظل التطور السريع والمتلاحق في الأسلحة السيبرانية وانتشار آلياتها بين العديد من الفاعلين[٤٦].

وإضافة لما سبق، فإن الدفاع السيبراني النشط والفعال يعني "استخدام التدابير الاستباقية للكشف أو الحصول على معلومات حول أي هجمات سيبرانية وشيكة، وكذلك تحديد مصدر أي هجمه سيبرانية محتملة لشن هجمة سيبرانية استباقية ووقائية ضد ذلك المصدر"، وعلى الرغم من صعوبة التنبؤ بالهجمات المحتملة

(45) Craig B. Greathouse, Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?, 2014, On: https://link.springer.com/chapter/10.1007/978-3-642-37481-4_2

(46) Cyber Defence, The NATO Cooperative Cyber Defense Centre of Excellence is a multinational and interdisciplinary cyber defense hub, https://ccdcoe.org/

وتحديد مصدرها، فإن بعض الدول طورت مفهومها عن الدفاع السيبراني ليشمل الدفاع والهجوم من خلال تطبيق التدابير الأمنية للحماية ضد الهجمات السيبرانية، والرد عليها، وتحصين البنية التحتية المعلوماتية للدولة، وبناءً عليه شملت خطط وميزانيات الدفاع في العديد من الدول تطوير القدرات السيبرانية الهجومية Offensive Cyber Capabilities.

٢- **الردع السيبراني Cyber Deterrence:** ربما تكون التسميه الافضل التي تعبر عن هذا الردع في إطار الفضاء السيبراني مصطلح "الهجمات السيبرانية المضادة Counter Cyber Attacks"، والذي يعني قيام الدولة أو الجهة التي تعرضت للإعتداء السيبراني بالرد من خلال هجمات سيبرانية سريعة وسرية ودقيقة بما يستهدف إرسال رسالة مفادها أنها قد حددت الدولة أو الجهة المعتدية، وأنها قادرة على الرد عليها بالاليه نفسها التي استخدمتها أو بصورة أشد وطأة. وهنا يلاحظ أن استخدام تلك الاستراتيجية على نحو فعال يعتمد على القدرات السيبرانية للدولة الهجومية والدفاعية، مدعومة بإطار قانوني دولي قوي.

وفي حقيقه الأمر، فإن هناك شبه اتفاق بين معظم الأدبيات أن الردع السيبراني لا يمكن الإعتماد عليه كآلية فعالة لمواجهة الهجمات السيبرانية نتيجة لصعوبة تحديد مصدر الهجوم وإمكانية الإستعانة بآخرين لتنفيذ الهجوم السيبراني، ولكن فكرة الردع لا تزال مسيطرة على العقلية الأمنية، حيث حذر وزير الدفاع البريطاني السابق "ديس براون" من أن الأسلحة النووية قد تم تجاوزها من قبل القراصنة، وأنه يستلزم إجراء تقييم شامل لهذه المخاطر على النظام النووي البريطاني "ترايدنت"، ورأى أن الحل يتمثل في وجود نظام ردع موثوق فيه. كما أن الاستراتيجية الأمريكية للفضاء السيبراني International Strategy for Cyberspace تضمنت الردع كإحدى آليات مواجهة الهجمات السيبرانية من

(ISSN: 2536 - 9555)

خلال الإقرار بأن الولايات المتحدة الأمريكية سترد على أي أعمال عدائية في الفضاء السيبراني كما نفعل مع أي تهديد آخر لبلادنا[٤٧].

٣- **الدبلوماسية السيبرانية Cyber Diplomacy:** يتمثل أحد الخيارات الاستراتيجية المتاحة أمام الدول- إلى جانب الدفاع والردع السيبراني- في اللجوء إلى الدبلوماسية السيبرانية التي تنطوي على استخدام الأدوات الدبلوماسية التقليدية مع الاستفادة من الفضاء السيبراني، وبالشكل الذي يعمل على احتواء التهديدات والهجمات السيبرانية وتحقيق الأمن السيبراني، علماً بأن الدبلوماسية السيبرانية يتم اتباعها من قبل الدول والفاعلين من غير الدول على حد سواء[٤٨].

وعلى الرغم من أهمية البعد الدبلوماسي للأمن السيبراني، فإن عدداً كبيراً من الدول ليست لديها ثقة في إمكانية مواجهة التهديدات السيبرانية من خلال الأدوات الدبلوماسية، ومع ذلك فقد ظهرت بعض الأمثلة البارزة على تصاعد دور الدبلوماسية في احتواء الصراعات السيبرانية، ومنها اتفاق الأمن السيبراني الذي تم توقيعه بين كل من الولايات المتحدة الأمريكية والصين في ٢٥ سبتمبر ٢٠١٥[٤٩]، حيث نصت الاتفاقية على التزام الطرفين بعدم المشاركة في أي نشاط سيبراني يستهدف التجسس الاقتصادي على أي منهما، والتعاون بينهما في اتخاذ الإجراءات اللازمة للحد من الجرائم السيبرانية. كما لعبت الأمم المتحدة دوراً بناء في هذا السياق، حيث انشأت فريق الخبراء الحكوميين Group of

---

[٤٧] انظر فى ذلك:

The Department of Defense cyber strategy, U.S. Department of Defense, April 2015, https://www.defense.gov/

(48) Franz-Stefan Gady and Greg Austin, **Russia, The United States, And Cyber Diplomacy Opening the Doors**, New York, The EastWest Institute, 2010, p. 1.

(49) Franz-Stefan Gady and Greg Austin, **Russia, The United States, And Cyber Diplomacy Opening the Doors**, New York, The EastWest Institute, 2010, p. 1.

Government Experts لتحقيق التعاون الدولي في دراسة قضايا الأمن السيبراني، وتقديم توصيات بشأن التدابير الرامية إلى تقليل التهديدات والمخاطر السيبرانية وزيادة الاسعار، وفي عام ٢٠١٣ تمكن الفريق من خلال الجهود الدبلوماسية من الاتفاق على اعتبار مبدأ السيادة الوطنية تطبق على الفضاء السيبراني بدرجة انطباقه على الأرض نفسها، كما تمكن الفريق في عام ٢٠١٥ من الاتفاق حول قائمة مطولة من قواعد وإجراءات بناء الثقة في الفضاء السيبراني(٥٠).

٤- **التدخل العسكري Military intervention**: قد يكون التدخل العسكري هو الخيار الاخير لمواجهة الحرب السيبرانية، لاسيما إذا كانت ذات طبيعة غير محدوده، وقد أبقت الولايات المتحدة الأمريكية في هذا الخيار قائماً ومطروحاً في إطار أدوات مواجهة الحرب السيبرانية(٥١).

وبناءً على ما سبق، يمكن القول أن الحرب السيبرانية قد فرضت واقعاً جديداً على الساحة الدولية، الأمر الذي يستلزم الاستعداد الجيد للتعامل معه من خلال إعداد استراتيجيات السياسة السيبرانية لكل من الدول والفاعلين من غير الدول، على أن تتضمن تلك الاستراتيجيات بناء القدرات الدفاعية السيبرانية، وإعداد بدائل الرد على الهجمات السيبرانية، وكيفية اعتماد نهج متكامل لتحقيق الأمن السيبراني، وإنشاء البرامج العامة للتعليم السيبراني، وكيفية الاستعداد لسيناريوهات الاستخدام المحدود للانترنت في حالة الهجمات السيبرانية.

---

(50) Dr. Hal Brands, Statement before the House Foreign Affairs CommitteeSubcommittee on Europe, Eurasia, Energy,and Environment, March26, 2019, https://csbaonline.org/research/publications/statement-before-the-house-foreign-affairs-committee-on-the-origins-and-end/publication/1

(٥١) سارة عبد العزيز، "الحرب السيبرانية: التداعيات المحتملة لتصاعد الهجمات الإلكترونية على الساحة الدولية"، مرجع سابق، ص ١٢.

(ISSN: 2536 - 9555)

خاتمة

لقد تعددت أساليب توظيف وقدره التنظيمات الإرهابية المتطرفة في استخدام منصات التواصل الاجتماعي، وبرزت من خلالها إمكاناتها الرقمية للوصول الى الجماهير وجمع المعلومات ونشر الأفكار والرسائل وتنسيق الانشطة، وأيضاً الحصول على الدعم وتجنيد الأفراد، وكذلك تشويه سمعة المنظمات في الفضاء الرقمي، مما وضع العالم دولاً وشعوباً أمام تحد كبير يتطلب تنسيقاً إلكترونياً عالي المستوى بين الأجهزة الامنية والجهات الفاعلة في مكافحة الارهاب والتطرف في الدول كافة، فضلاً عن تعزيز التعاون والتنسيق مع المؤسسات الدولية المعنية بمواجهة جميع أشكال جرائم الإرهاب على الإنترنت، من خلال دمج المنصات الرقمية، كمزايا للاتصال والتوعية، بجانب وضع تشريعات خاصة مع قدر كبير من الحرص والفعالية والتنفيذ السليم لمثل هذه التشريعات مما يمكن الدول وصانعي السياسات من تحقيق مكاسب ضد هذه التنظيمات، ومحاولة السيطرة على توسعها الرقمي بشكل كبير.

ومن ناحية أخرى تعتبر الحرب السيبرانية هي حرب المستقبل. وبعبارة أخرى فإن مدى خطورتها قد يصل لأن يتدمر كل شيء! وقد تكون نتائجها الوخيمة كارثية على كوكبنا العظيم. فالتسابق الالكتروني الذي بات يهددنا ونحن آمنين في بيوتنا، والنابع من العالم الرقمي الذي أصبح يعيش فينا. يتطلب منا اخذ تدابير الحماية بجدية أكثر من اللازم. ومن جهة أخرى عدم التهاون في أي تهديدات او اخطار قد نتعرض لها في هذا العالم الرقمي، الذي لا يقتصر ضرره على الافراد، بل انه قد يدمر أنظمة عالمية! ويتسبب في حروب نووية نحن بغنى عنها وعن المتاعب التي قد تتسبب بها. فهل يكون للحرب السيبرانية نهاية حتمية كما غيرها؟

المراجع

١- العربية:

١. د. أميرة تواضروس، "دور الذكاء الاصطناعى فى التنبؤات التنموية"، **السياسة الدولية**، (ملحق اتجاهات نظرية)، عدد ٢٢٢، اكتوبر ٢٠٢٠.
٢. عبير ياسين، "التكنولوجيا فى عالم الإرهاب.. سلاح ذو أوجه متعددة"، **السياسة الدولية**، عدد ٢٢٧، يناير ٢٠٢٢.
٣. د. عادل عبد الصادق، "الإرهاب السيبرانى والأمن القومى فى بيئة متغيرة"، **السياسة الدولية**، عدد ٢٢٧، يناير ٢٠٢٢.
٤. د. محمد خليف، "الارهاب المنفرد.. مخاطر الاستخدام الخبيث للذكاء الاصطناعى"، **السياسة الدولية**، عدد ٢٢٩، يوليو ٢٠٢٢.
٥. سارة عبد العزيز، "الحرب السيبرانية: التداعيات المحتملة لتصاعد الهجمات الإلكترونية على الساحة الدولية"، **اتجاهات الأحداث**، عدد ٢٠، مارس- إبريل ٢٠١٧.
٦. د. غادة محمد عامر، "جهود الدول فى مكافحة الإرهاب الإلكترونى"، **السياسة الدولية**، عدد ٢٢٧، يناير ٢٠٢٢.
٧. سماح عبد الصبور، "الإرهاب الرقمى: استخدامات الجماعات المسلحة لوسائل التواصل الاجتماعى"، **اتجاهات الأحداث**، عدد ٢، سبتمبر ٢٠١٤.
٨. د. علا السيد، "العملات الإفتراضية: التدفقات المالية الإلكترونية فى مرحلة المخاطر اللامحدودة"، **اتجاهات الاحداث**، العدد ٢، سبتمبر ٢٠١٤.
٩. د. عبد الله عبد العزيز النجار، "التكنولوجيا وتمويل الإرهاب.. العملات المشفرة نموذجاً"، **السياسة الدولية**، عدد ٢٢٧، يناير ٢٠٢٢.

٢-الأجنبية:

1. eorge Michael, The New media and the rise of exhortatory terrorism, **Strategic Studies Quarterly**, Vol. 7, Issue 1, Spring 2013.
2. Joseph Nye, "Smart Power and the War on Terror", Asia Pacific Review, Vol. 15, no. 1, 2008.

(ISSN: 2536 - 9555)

3. Geoff Dean, Peter Bell, Jack Newan, The Dark Side of Social Media: Review of Online Terrorism, **Pakistan Journal of Criminology,** Vol. 3, No. 4, April – July 2012, pp 194 – 195.
4. Garrett, R. K., "Protest in an Information Society: A Review of Literature on Social Movements and New ICTs Information", **Communication and Society**, Vol. 9, No. 2, 2006.
5. Joseph M. Hatfield, "Social engineering in cybersecurity: The evolution of a concept", **Computers & Security**, Volume 73, March 2018.
6. "Coin mixer: What is it and how does it work?, https://www.okx.com/learn/what-is-coin-mixer, Jul 28, 2023.
7. Pawan Nahar, **"**What is the difference between custodial and non-custodial crypto wallets?", The Economic Times, May 26, 2022, On: **https://economictimes.indiatimes.com/markets/cryptocurrency/what-is-the-difference-between-custodial-and-non-custodial-crypto**
8. OECD, Recommendation of the Council on Artificial Intelligence, OECD, Paris 2019.
9. university of Michigan News, "Unhackable: New Chip Stops Attacks Before They Start", SmithBucklin, Washington, May 6, 2019, On: **https://cacm.acm.org/news/236672-unhackable-new-chip-stops-attacks-before-they-start/fulltext**
10. Adam Conner-Simons, "ystem predicts 85 percent of cyber-attacks using input from human experts", **https://news.mit.edu/2016/ai-system-predicts-85-percent-cyber-attacks-using-input-human-experts-0418**

11. Eastern Daylight Time, "MistNet Launches CyberMist Advanced Threat Detection Platform using Edge AI and Mist Computing, Closes Series A Funding Round", **https://www.businesswire.com/news/home/20190521005248/en/MistNet-Launches-CyberMist-Advanced-Threat-Detection-Platform-using-Edge-AI-and-Mist-Computing-Closes-Series-A-Funding-Round**
12. John Arquilla, David Ronfeldt, "Cyberwar is Coming!", **Comparative Strategy**, Vol. 12, No. 2, Spring 1993.
13. Shane Martin Coughlan, Is There A Common Understanding Of What Constitutes Cyber Warfare?, MA in International Studies (Globalisation and Governance) at the University of Birmingham, Second Edition March 2016.
14. Fred Schreier, "on cyberwarfare", **Dcaf horizon working paper**, No. 7, 2015.
15. Timothy Shimeall, "Countering cyber war", **Nato Review**, Vol. 49, No. 4, December 2001.
16. Sabrine SAAD, Stéphane BAZAN, Lorraine ETIENNE, Christophe VARIN, Asymmetric Cyber-warfare between Israel and Hezbollah The Web as a new strategic battlefield, **International Studies Perspectives,** Vol. 17, No. 3 (2016).
17. Bello O. A., Aderbigbe F. M., "Cyberwar-The New Frontier of International Warfare", **International Journal of Sustainable Development Research**, Volume 1, Issue 1, September 2015.
18. Laone Moalosi, The New Battlefield: Cyberattacks Transforming Warfare, Solutions Global, Sep 26, 2023, On: **https://www.linkedin.com/pulse/new-battlefield-cyberattacks-transforming-warfare-laone-moalosi**
19. Peter Trim, Yang-Im Lee, **Strategic Cyber Security Management**, 2023, On**:**

(ISSN: 2536 - 9555)

https://www.routledge.com/Strategic-Cyber-Security-Management/Trim-Lee/p/book/9781032154763

20. Peter W. Singer and Allan Friedman, **Cybersecurity and Cyberwar: What Everyone Needs to Know**, Oxford University Press, 2020.
21. Craig B. Greathouse, Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?, 2014, On: **https://link.springer.com/chapter/10.1007/978-3-642-37481-4_2**
22. Cyber Defence, The NATO Cooperative Cyber Defense Centre of Excellence is a multinational and interdisciplinary cyber defense hub, https://ccdcoe.org/
23. The Department of Defense cyber strategy, U.S. Department of Defense, April 2015, **https://www.defense.gov/**
24. Franz-Stefan Gady and Greg Austin, **Russia, The United States, And Cyber Diplomacy Opening the Doors**, New York, The EastWest Institute, 2010.
25. Franz-Stefan Gady and Greg Austin, **Russia, The United States, And Cyber Diplomacy Opening the Doors**, New York, The EastWest Institute, 2010.
26. Dr. Hal Brands, Statement before the House Foreign Affairs CommitteeSubcommittee on Europe, Eurasia, Energy,and Environment, March26, 2019, **https://csbaonline.org/research/publications/statement-before-the-house-foreign-affairs-committee-on-the-origins-and-end/publication/1.**