الإرهاب السيبراني والتقنيات الناشئة:

تحديات الأمن الوطني السيبراني والسيادة الوطنية

الأستاذ الدكتور/ ذياب البداينة

عضو هيئة التدريس - كلية الدراسات العليا، أكاديمية الشرطة. دولة قطر.

الإرهاب السيبراني والتقنيات الناشئة:
تحديات الأمن الوطني السيبراني والسيادة الوطنية

الأستاذ الدكتور/ ذياب البداينة
عضو هيئة التدريس – كلية الدراسات العليا، أكاديمية الشرطة. دولة قطر.

المُلخَّص

تتناول هذه الدراسة الإرهاب السيبراني، والتقنيات الناشئة، وتحديات الأمن الوطني والسيادة الوطنية السيبرانية، والدولة المحايدة في الفضاء السيبراني. كما تتناول مكونات الفضاء السيبراني وتطوره وخصائصه كحاضنة للإرهاب السيبراني. وتركز المراجعة (دراسة مكتب (Desk research)) على الإرهاب السيبراني؛ من حيث مفهوم الإرهاب السيبراني، وتطوره، وأشكاله، والطرق الشائعة في الهجمات الإرهابية السيبرانية، والحرب السيبرانية، والأساطير الشائعة حول الإرهاب التقليدي والسيبراني. وتناقش الدراسة في المضامين الأمنية الإرهاب السيبراني وعلاقته بالتقنيات الناشئة كالذكاء الاصطناعي وإنترنت الأشياء، وإنترنت الأجسام، وإنترنت كل شيء، وذكاء التهديد السيبراني، والأمن السيبراني. كما تناولت الورقة استعراض تحديات الإرهاب السيبراني لقضايا الأمن الوطني السيبراني والسيادة الوطنية.

الكلمات المفتاحية: الفضاء السيبراني، الإرهاب السيبراني، الحرب السيبرانية، الهجمات السيبرانية، إنترنت الأشياء، الذكاء الاصطناعي، إنترنت الأجسام، استخبارات التهديدات السيبرانية، الأمن السيبراني.

ABSTRACT

Cyberterrorism and Emerging Technologies: the Challenges of National Cyber Securityand National Sovereignty

Prof. Dhieb ALbadeina
Graduate College, Police Academy, MOI Qatar

The issues of national cyber security, cyber sovereignty and the neutral state in cyberspace are examined, along with cyberterrorism and developing technology. It covers cyberspace's elements, evolution, and traits that make it an incubator for cyberterrorism as well. Cyberterrorism is the main topic of the review (Desk Research study), which covers its definition, evolution, forms, typical cyber techniques, cyber warfare tactics, and popular myths regarding both traditional and cyberterrorism—examining the security implications of cyberterrorism and the emerging technologies like AI, IoT, IoB, IoE, cyber threat intelligence, and cyber security. Moreover, the study also discusses the challenges of cyberterrorism on issues of national cybersecurity and national sovereignty.

Key words: Cyberspace, Cyberterrorism cyberwarfare, cyber-attacks, IoT, AI, IoB, cyber threat intelligence, Cybersecurity

المقدمة

يعد الفضاء السيبراني (Cyberspace) الحاضنة الأساسية للتفاعل الإنساني على المستوى الشخصي أو الجماعي محليًا وكونيًا. وكما يوفر هذا الفضاء مجالًا سيبرانيًا رحبًا للنشاطات الإنسانية والاجتماعية والثقافية والعلمية والمالية، وغيرها مما يسر حياة الناس في التفاعل والتبادل الثقافي للأفكار والمنتوجات المادية والفكرية، إلا أن هذا الفضاء لا يخلو من سلبيات وتهديدات لأعمال الناس وحياتهم، تتمثل في توفير بيئة حاضنة لحوادث الإرهاب السيبراني نظرًا لما تشكله البيئة السيبرانية من خصائص مسهلة وميسرة (مثل إخفاء الهوية وسرقتها، وسهولة وصعوبة الاكتشاف، وتعدد المستهدفين، وصعوبة التعقب، وانخفاض الخطورة) لمثل هذه الحوادث الإرهابية السيبرانية. كما أن هذا الفضاء مصمم لاستخدام الجميع، وإن موضوع تيسير استخدام هذا الفضاء من قبل الجميع قد طغى على موضوع أمنه (Cross, 2008). والبيئة السيبرانية بما تملكه من خصائص فريدة ومسؤولة عن زيادة الإنتاجية على مستوى الاقتصاد الدولي، فهي ذاتها المسؤولة عن الإمكانيات العالية في إلحاق الأذى بمستويات متعددة في المجتمع.

الفضاء السيبراني ليس بلا جانب مظلم، فقد استغل من قبل الإرهابيين كأداة اتصال بين المجموعات الإرهابية، وأداة تجنيد وتنفيذ، كما استخدم هذا الفضاء كأداة تدمير وتعطيل للبنية التحتية والحرمان من الخدمة، كما أنه يشكل حيزًا ووسيطًا لتوزيع الرسائل والمعلومات الإرهابية (Taylor,2007). ومع انتشار التقنيات الناشئة مثل الذكاء الاصطناعي وإنترنت الأشياء والأجسام، وذكاء التهديد السيبراني، ومع وجود الذئب المنفرد السيبراني جنبًا إلى جنب مع الخصائص المسهلة للإرهاب في البيئة السيبرانية، يبقى السؤال الكبير الذي يطرح نفسه هنا: هل يستطيع أحد أن يطلق هجومًا إرهابيًا سيبرانيًا كارثي النتائج؟ وإذا كان ذلك، فما هي احتمالات حدوث مثل هذا الهجوم؟ في الواقع: لا يستطيع أحد الجزم بذلك. ومن السهل أن يعد الإنسان عددًا من السيناريوهات؛ مثل: «تعطل سوق الأسهم المالية بعد عبث أحد المتسللين المخربين بأجهزة كمبيوتر وول ستريت»، أو: «اصطدام طائرتين بعد أن قام أحد المخربين بالتسلل إلى نظام التوجيه الجوي وتغيير الطرق والمسارات الجوية للطائرات». ومن الصعب جدًا تقدير إمكانية حدوث مثل هذه السيناريوهات أو تنفيذها. ويجب أخذ عدد من العوامل بالحسبان، بما في ذلك نقاط الضعف الممكنة في التقنية والطرق التي يمكن استخدام التقنية بها، والإمكانيات اللازمة لاستغلال نقاط الضعف الموجودة فيها، وغير ذلك من عوامل الأمن التي يمكن أن تشكل نقاط ضعف بالنسبة للتقنية، وما إذا كان هناك أفراد لديهم النية أو الرغبة بالقيام بمثل هذه الأعمال العدوانية الشريرة المدمرة، والفرصة لتنفيذ هجماتهم المطلوبة (البداينة، 2002).

الفضاء السيبراني (Cyberspace) المفهوم والمكونات:

الفضاء السيبراني مجال كوني داخل بيئة المعلومات، يتكون من شبكة مترابطة من البنى التحتية لأنظمة المعلومات، بما في ذلك الإنترنت وشبكات الاتصالات وأنظمة الكمبيوتر والمعالجات ووحدات التحكم المدمجة (NIST SP 800-30 Rev. 1). ويشير الفضاء السيبراني بشكل أساسي إلى الكمبيوتر، وهو عبارة عن شبكة افتراضية، وهو وسيط مصمم إلكترونيًا للمساعدة في حدوث الاتصالات عبر الإنترنت، وهذا يسهل الاتصالات التي يمكن الوصول إليها في جميع أنحاء العالم. ويتكون الفضاء السيبراني بأكمله من شبكات كمبيوتر كبيرة فيها العديد من الشبكات الفرعية التي تتبع (TCP أو IP. TCP) بروتوكول التحكم في الإرسال، وهو معيار للاتصالات يسمح لبرامج التطبيق وأجهزة الحوسبة الأخرى بتبادل البيانات والرسائل عبر شبكة الإنترنت، تم تصميمها لإرسال البيانات عبر الإنترنت، والتي تتأكد بعد ذلك من تسليم البيانات المرسلة بنجاح عبر الشبكات. وهي المعايير المستخدمة في الغالب لتحديد قواعد الإنترنت التي يتم تحديدها من قبل فريق هندسة الإنترنت أو (IETF). إنه بروتوكول شائع الاستخدام ويضمن وجود تسليم شامل للبيانات. من ناحية أخرى، بروتوكول الإنترنت أو IP هو البروتوكول أو الطريقة التي تتضمن إرسال البيانات من جهاز إلى آخر باستخدام الإنترنت، فلكل جهاز عنوان IP خاص به، وهذا ما يمنحه هويته، ويتيح عنوان IP الاتصال وتبادل البيانات إلى الأجهزة الأخرى عبر الإنترنت، كما يحدد كيف ستتبادل الأجهزة وتطبيقاتها حزم البيانات مع بعضها البعض والشبكات المتصلة. وتحدث جميع عمليات النقل من خلال أي من مجموعة بروتوكول الإنترنت أو البروتوكولات؛ مثل TCP أو IP. إنَّ الفضاء السيبراني هو الفضاء الذي يشارك فيه المستخدمون المعلومات ويتفاعلون مع بعضهم البعض، وينخرطون في المناقشات أو منصات التواصل الاجتماعي والعديد من الأنشطة الأخرى (Vedantu, 2023). ويطلق على الفضاء السيبراني اسم «البعد الخامس» أو «المجال الخامس Fifth Dimension «. [مجالات الحرب: البرية والبحرية والجوية، الفضاء السيبراني] (Garibaldi & Deane, 2023).

لماذا سمي بالفضاء السيبراني؟

كلمة سايبر Cyber مشتقة من Cybernetic وأصلها يوناني، وتعني التوجيه والسيطرة، وعرفها Norbert Wiener في عام 1984م بأنها: «الدراسة العلمية للسيطرة على الأحياء والآلات وآلية التواصل بينها»، ومن هذا التعريف نصل لمفهوم الفضاء السيبراني. (Marinescu, 2017). تختلف استخدامات وأشكال السيطرة على الفضاء السيبراني أو السيادة السيبرانية

(cyber sovereignty) من دولة إلى أخرى؛ تبعًا لأولويات هذه الدول، فمنها الأمني والسياسي والاستخباراتي والمدني والمهني أو قد يكون معلوماتيًا بحتًا، ويتشكل كيان الفضاء السيبراني بشكل عام بوجود ثلاثة مركبات أساسية تضم الأدوات التقنية المستخدمة، والإجراءات، والعامل البشري من مبرمجين ومستخدمين (Clark, & Csail, 2010). استخدم المؤلف الأمريكي الكندي ويليام جيبسون (Gibson) مصطلح الفضاء السيبراني (cyberspace) لأول مرة في عام 1982 في قصة نشرت في مجلة أومني (Omni)، ثم في كتابه سرطان الأعصاب نيورومانسر(Neuromancer). في رواية الخيال العلمي هذه وصف جيبسون الفضاء السيبراني بأنه إنشاء شبكة كمبيوتر في عالم مليء بكائنات ذكية اصطناعية(Bussell, 2013). ولا يزال هذا المصطلح مستخدمًا على نطاق واسع بين الجميع لأنه ينمو بسرعة ويستخدمه الفرد لأغراض مختلفة. وفقًا لمعنى الفضاء السيبراني، يعد الفضاء السيبراني مساحة افتراضية بلا كتلة أو جاذبية أو حدود.

مكونات الفضاء السيبراني Cyberspace layers:

عرف الفضاء السيبراني (Cyberspace) بأنه: «مجال عالمي داخل بيئة المعلومات يتكون من شبكة مترابطة من البنى التحتية لتكنولوجيا المعلومات، بما في ذلك الإنترنت وشبكات الاتصالات وأنظمة الكمبيوتر والمعالجات المدمجة ووحدات التحكم». وهناك وجهة نظر مفادها أنه: «ليس مكانًا ماديًا – إنه يتحدى القياس في أي بعد مادي أو مساحة زمنية متصلة». ومع ذلك، فإن الفضاء السيبراني أكبر من الإنترنت، بما في ذلك – ليس فقط الأجهزة والبرامج وأنظمة المعلومات– الناس والتفاعل الاجتماعي داخل هذه الشبكات أيضًا. والطبقات المهمة من الأعلى إلى الأسفل هي:

- الناس (People): الذين يشاركون في التجربة السيبرانية، والذين يتواصلون ويعملون بالمعلومات واتخاذ القرارات وتنفيذ الخطط، وهم أنفسهم يحولون طبيعة الفضاء السيبراني من خلال العمل مع الخدمات المكونة له وقدرات.
- المعلومات (Information): التي يتم تخزينها ونقلها وتحويلها في الفضاء السيبراني.
- البناء المنطقي (Logical Building): التي تشكل الخدمات وتدعم النظام الأساسي لطبيعة الفضاء السيبراني.
- الأسس المادية (Physical foundations): التي تدعم العناصر المنطقية (Clark, & Csail, 2010).

ليس الكمبيوتر هو الذي يخلق الظاهرة التي نسميها الفضاء السيبراني، إنما هي الاتصالات البينية التي تصنع الفضاء السيبراني، والربط البيني يؤثر على جميع الطبقات. في كتابه الإنترنت الفيكتوري (The Victorian Internet) يجادل توم ستاندج (Standage, 1999) بأن وضع الاتصال البيني الذي تم إنشاؤه بواسطة التلغراف كان تحويليًا في عصره مثل الإنترنت اليوم.

الجدول (1) : الطبقات الثلاث الأفقية للفضاء السيبراني

البيئة	الوصف
شبكات وأنظمة الفضاء القريب (Near Space)	الشبكات والأنظمة المحلية، وهي حيوية لدعم البنية التحتية والخدمات الوطنية الهامة، ويفترض أن تخضع للرقابة والحماية من قبل الوكالات الوطنية أو الحكومية.
شبكات وأنظمة الفضاء المتوسط (Mid Space)	تعد بالغة الأهمية للوصول إلى الفضاء السيبراني العالمي، ولكن لا توجد سيطرة أو حماية محلية عليها. وعادةً ما تكون هذه الأصول بعيدة جغرافيًا ومملوكة من قبل شركات أجنبية أو أطراف ثالثة.
شبكات وأنظمة الفضاء البعيد (Far Space)	تشكل الفضاء القريب لمنافس أو لخصم، ويجب أن يتم التأثير عليه أو التحكم فيه كجزء من حملة لإبراز القوة والتأثير في الفضاء السيبراني.

Venables, Shaikh, & Shuttleworth, (2015). p.5

يتكون النموذج الموحد للفضاء السيبراني من سبع طبقات من الأسفل إلى الأعلى: (1) طبقة الخدمات (services layer)، (2) طبقة البنية التحتية (infrastructure layer)، (3) الطبقة المادية (physical layer)، (4) طبقة النحو (syntactic layer)، (5) الطبقة الدلالية (semantic layer)، (6) الطبقة البشرية (human layer)، (7) طبقة المهمة (mission layer). وتقع طبقة الخدمات أسفل طبقة البنية التحتية، وتؤكد التبعيات بين مكونات طبقة البنية التحتية التي تمكن الفضاء السيبراني من الوجود والعمل. وتتضمن موارد مثل الطاقة، والمياه، والمواد، والأمن المادي. وتشمل هذه الطبقة أيضًا الأنظمة والمكونات الصناعية التي تدعم البنية التحتية. (Venables, Shaikh, & Shuttleworth, 2015).

يتطلب الفضاء السيبراني تدخلًا بشريًا من أجل إنشائه وصيانته واستغلاله و(حتى) تدميره. وبالتالي، يتم تضمين طبقة بشرية بشكل مباشر فوق الطبقة الدلالية التي توفر المعلومات المفيدة والمفهومة للمشغلين البشريين، ويتم توسيعه بالضرورة ليغطي الاحتياجات المحددة للمستخدمين النهائيين، وهذا يشمل اللغة والثقافة والمستخدمة في التفاعلات في الفضاء السيبراني. وتدرك أهمية هذا الجانب من التواصل في التعرف على المعلومات في مجال تحليل الشبكة الاجتماعية، والذي يبحث في خصائص الروابط العلائقية لاستخلاص استنتاجات حول الشبكة وكياناتها، وتعد الطبقة المهمة وحجر الزاوية لنموذج الفضاء السيبراني الموحد. إنه يؤكد حقيقة أن الفضاء السيبراني يخدم الاحتياجات البشرية باستمرار ويتطور ويتوسع، وأن الفضاء السيبراني ليس ظاهرة تحدث بشكل طبيعي. وكل تفاعل في الفضاء السيبراني له غرض ونتائج محددة، سواء كانت متعمدة أو غير مقصودة، بريئة أو خبيثة. بواسطة تحديد وإبراز فكرة المهمة في الجزء العلوي من النموذج، يمكن فهم أدوار جميع الطبقات الدنيا ووضعها في سياقها بشكل أفضل (Denning, 2000).

تم تعريف الفضاء السيبراني، من قبل أندرو كريبينيفيتش (Krepinevich, 2012) على النحو التالي: شبكات الكمبيوتر [في العالم]، المفتوحة والمغلقة، لتشمل أجهزة الكمبيوتر نفسها، وشبكات المعاملات التي ترسل البيانات المتعلقة بالمعاملات المالية، والشبكات التي تضم أنظمة التحكم التي تمكن الآلات من التفاعل مع بعضها البعض. على هذا النحو، يستخدم المجال السيبراني خطوط اتصال موسعة تتضمن شبكة عالمية، إلى جانب مراكز النشاط في مزارع الخوادم أو مواقع أجهزة الشبكة. (Klein, 2017) وتشمل الأنشطة السيبرانية التجارة والتمويل الدوليين.

السلوك المسؤول للدولة في الفضاء السيبراني:

اتفقت دول الأمم المتحدة على عملية جديدة لمجموعة العمل مفتوحة العضوية (OEWG) مدتها خمس سنوات لمواصلة تطوير المناقشات المتعلقة بالسلوك المسؤول للدولة في الفضاء السيبراني (الشكل 1)، وهي 11 قاعدة طوعية وغير ملزمة تصف ما ينبغي وما لا ينبغي للدول أن تفعله في الفضاء السيبراني. ويعكس محتوى القواعد الإحدى عشرة توقعات المجتمع الدولي الأوسع من كل دولة ومنظمة إقليمية. وهي تعبر عن رأي مشترك حول ما يعتبر سلوكًا مسؤولًا من قبل الدول. وبطبيعة الحال، يتطور هذا الرأي الجماعي حول ما هو السلوك المسؤول وما هو السلوك غير المسؤول مع مرور الوقت، مع تعمق فهم الأمن السيبراني، ووقوع الحوادث، ومساهمة المزيد من الحكومات في هذه العملية.

الشكل (1): أعراف الأمم المتحدة للسلوك المسؤول للدولة في الفضاء السيبراني

1. التعاون البين دولي في الأمن	2. خذ بالحسبان جميع المعلومات ذات الصلة	3. امنع سوء استخدام البنية التحتية الحساسة في منطقتك	4. تعاون في منع الجريمة والإرهاب
5. احترم حقوق الإنسان والخصوصية	6. لا تخرب البنية التحتية الحساسة	7. احم البنية التحتية الحساسة	8. استجب لطلبات المساعدة
9. تأكد من أمن سلسلة التزيد	10. بلغ عن الثغرات في البنية التحتية الحساسة	11. لا تؤذ فرق استجابة الطوارئ	

المصدر: Hogeveen, 2022, p. 14

تتمثل أغراض القواعد كما وردت في قرار الجمعية العامة للأمم المتحدة رقم 70/237 في الحد من المخاطر التي تهدد السلام والأمن الدوليين، والمساهمة في منع نشوب الصراعات. لقد تم تصميمها للتعامل مع الإجراءات التي تتم بين دولة ودولة، والتي يمكن أن تحمل أعلى المخاطر على السلام والأمن الدوليين ورفاهية المواطنين. القواعد في الشؤون الدولية هي اتفاقيات سياسية، وهي لا تنتهك سيادة الدولة أو تفرض التزامات قانونية على الدول. وفي الواقع، توفر القواعد أساسًا مشتركًا للدولة لتصميم الاتجاه الاستراتيجي وتطوير القدرات وتنفيذ الإجراءات بطريقة مسؤولة (Hogeveen, 2022).

المسؤولية الأخلاقية في العالم الرقمي: الوثيقة القطرية:

تقر الوثيقة الاستراتيجية لرؤية قطر الوطنية 2030 (الأمانة العامة للتخطيط التنموي، 2008) بأن المستقبل ملك للدول التي تسخر تكنولوجيا المعلومات والاتصالات للتنمية الاقتصادية وتنضج في اقتصادات قائمة على المعرفة. وللمضي قدمًا نحو هذا الهدف، أحرزت قطر بعض التقدم في تحويل اقتصادها القائم على الطاقة إلى مجتمع جيد التنوع وقائم على المعرفة. وتبرز قطر كواحدة من الدول الرائدة في العالم في التكيف والابتكار وأتمتة الأنظمة الجديدة. ويقدر سوق تكنولوجيا المعلومات والاتصالات في قطر حاليًا بنحو 4.4 مليار دولار أمريكي، ومن المتوقع أن ينمو بسرعة في المستقبل. في أواخر أكتوبر 2021، أصبح هناك وزارة المواصلات ووزارة الاتصالات وتكنولوجيا المعلومات، هذه الوزارة هي المنظم والميسر والمدافع عن التكنولوجيا للحكومة. وتركز على تحديث قطر من خلال برنامج دولة قطر الذكية، المعروف أيضًا باسم TASMU، وهي مبادرة مدتها خمس سنوات بقيمة 1.6

مليار دولار، تم إطلاقها في عام 2017 لتطوير البنية التحتية لتكنولوجيا المعلومات والاتصالات في قطر، وتحويل الدوحة إلى واحدة من أكثر المدن اتصالاً على مستوى العالم. يعد تحديث تكنولوجيا المعلومات والاتصالات ركيزة أساسية لرؤية 2030، لأنه يضع الأساس التكنولوجي اللازم لخلق وظائف ذات رواتب عالية في المستقبل، وتنويع الاقتصاد، وجذب الشركات العالمية. وتتمثل الدوافع الرئيسية الأخرى لهذا القطاع في الحصول على شركاء موثوقين لديهم معدات وأجهزة وبرامج جديرة بالثقة، وحماية الخصوصية للمواطنين، والتخفيف من مخاطر الأمن السيبراني. ومن الأمور المثيرة للقلق في قطاع تكنولوجيا المعلومات والاتصالات أيضًا منع الوصول غير المصرح به للبيانات التجارية والشخصية الحساسة، والتي يمكن استخدامها لتهديد الخصوصية والسيادة الاقتصادية والملكية الفكرية والأمن القومي العام للأمة. لقد نجحت قطر وكهدف قصير في تحديث وبناء ودمج بنيتها التحتية وقدراتها لتكنولوجيا المعلومات والاتصالات من أجل كأس العالم لكرة القدم 2022. وقد سبق ذلك القرار الأميري رقم (19) لسنة 2016 بإنشاء اللجنة الوطنية لأمن المعلومات.

دليل المسؤولية الأخلاقية في العالم الرقمي:

يلخص الجدول (2) القيم التي تبنتها الوثيقة القطرية كدليل للمسؤولية الأخلاقية في العالم الرقمي. ويلاحظ أن الوثيقة انطلقت من ثلاث قيم أساسية هي: الاحترام والأمانة والمسؤولية. وكل قيمة انبثق عنها ثلاث قيم أخرى (3X3) مع شرح مختصر لكل قيمة.

الجدول (2): دليل المسؤولية الأخلاقية (القطري) في العالم الرقمي

الاحترام Patience	الأمانة Honesty	المسؤولية Responsibility
المساواة Equality	الجدارة بالثقة Trustworthiness	الكرامة Dignity
لا يوجد شخص أفضل أو أكثر قيمة من آخر - تعامل مع كل الناس بمستوى الاحترام والاعتبار نفسه. - دافع عن حقوق الإنسان والتحدث عنها علنًا في مواجهة القمع.	الصدق الخارجي والجدارة بالثقة - كن عضوًا موثوقًا ومعتبرًا في الإنترنت. - إنشاء بيئة آمنة وغير ضارة.	فهم قيمتنا في الجدارة والثقة الذاتية كما نعبر عنها ظاهريًا بالأخلاق العالية والمبادئ القوية - نحترم أنفسنا على الإنترنت كما نحن في الواقع. - تمثيل أمتنا وثقافتنا وقيمنا مع الاحترام.
الكياسة Courtesy	الأصالة Authenticity	التواضع Modesty
إظهار الأدب واللطف في مواقفك وسلوكياتك تجاه الآخرين - احترام وجهات نظر الآخرين وخصوصياتهم وممتلكاتهم. - امنح جميع المستخدمين الفرصة لسماع أصواتهم.	ابقَ أصيلًا ومباشرًا في كل تفاعلاتك عبر الإنترنت - كن صادقًا مع نفسك في كل تفاعلاتك على الإنترنت. - الحفاظ على التفاعلات والصدق واللياقة والأدب.	التصرف بطريقة تتجنب الفحش وعدم اللياقة - من حقنا أن نحتفظ ببعض الأشياء لأنفسنا. - يجب أن نحافظ على مستوى نسبي من الإنسانية.
الصبر Patience	النزاهة Integrity	الخصوصية Privacy
قدرة المرء على التسامح وفهم الفرق الزمني في وجهات النظر المختلفة - فكر جيدًا قبل أن تتصرف أو تستجيب. - لا يمكن التسرع في فهم الناس.	تقديم الحقيقة الكاملة غير المقسمة، وممارسة القدرة على أن تكون عادلًا ولائقًا، وكذلك الحفاظ على معايير الأخلاق العالية. - يجب ألا نحمل فخرنا بقيمنا أكبر مما لدينا من الصفات والعلاقات والشخصية. - يجب أن نولي قيمة كبيرة لكلمتنا ونتمسك بما نقول.	للحفاظ على بعض الأشياء بعيدة عن انتباه الجمهور - حماية تقديرنا على الإنترنت. - كن حذرًا مما ننشر.

Ministry of Transport and Communications (Qatar), 2018 Table: Author

بدأت الدراسات الأكاديمية في الفضاء السيبراني مع بداية تطور الحاسب واستخدامه في التعليم، وتركزت في دراسات الاتجاهات والخوف من الحاسوب (computer Phobia) (البداينة، 1993)، وتطورت إلى جرائم الحاسب وجرائم أمن المعلومات (البداينة،2007؛2003؛2013؛1999أ، 1999ب،)، والمشكلات الاجتماعية (البداينة، 2011، 2001أ،2020، 2001ب،2004،2010)، والإرهاب والتطرف (البداينة، 2000أ، 2000ب، 2006)، وقياس التطرف (Al-badayneh, 2023)، وضحايا التنمر السيبراني (Al-badayneh, et al., 2022, 2020, 2017,2016a, 2016bc)، والسلوك الإنساني في الفضاء السيبراني (Al-badayneh, 2016)، والخوف من الإرهاب (Al-badayneh, 20122011, 2011,2008).

الإرهاب السيبراني: التعريف:

تعريف الإرهاب السيبراني تعريف جدلي، وهو مثل تعريف الإرهاب التقليدي، وهناك محاولات عديدة لتحليل البناء المفاهيمي (construct) للإرهاب السيبراني من أجل الفهم والقياس والمكافحة، فالقوى الدافعة وراء الإرهاب السيبراني اجتماعية وسياسية وأيديولوجية واقتصادية (Yunos & Sulaman, 2017, p. 1). وقد تمت صياغة مصطلح «الإرهاب السيبراني» في عام 1996 من خلال الجمع بين مصطلحي الفضاء السيبراني والإرهاب، فالإرهاب السيبراني هو الجانب المظلم من عالم الويب، وهو ذو دافع سياسي وهجوم ضد المعلومات وأنظمة الكمبيوتر وبرامج الكمبيوتر والبيانات التي تؤدي إلى أعمال عنف ضد أهداف غير مقاتلة من قبل مجموعات وطنية فرعية أو عملاء سريين. وهو أيضًا استخدام الأنشطة التخريبية أو التهديد بها في الفضاء السيبراني، بقصد تعزيز أهداف اجتماعية أو أيديولوجية أو دينية أو سياسية أو أهداف مماثلة، أو لتخويف أي شخص لتعزيز هذه الأهداف (Surabhi, 2012). يطلق على الإرهاب السيبراني أيضًا (الإرهاب الناعم) (soft terrorism)، وهو استخدام الهجمات القائمة على الإنترنت في أنشطة الإرهابيين، بما في ذلك الأعمال المتعمدة؛ كالحرمان من الوصول واسع النطاق، أو تعطيل المعلومات، أو تدميرها، أو تخزينها ومعالجتها ونقلها في شبكات الكمبيوتر وإتلاف الشبكات. وتتضمن هذه الفكرة أيضًا استخدام أنظمة تكنولوجيا المعلومات للتضليل وشن الحرب النفسية. وغالبًا ما يكون الهدف من الهجوم هو معالجة المعلومات وليس النظام نفسه. (Kaźmierczak, 2017)

إن تعريف الإرهاب السيبراني الذي قدمته دوروثي دينينج (Denning) في عام 2000 أمام لجنة القوات المسلحة بمجلس النواب (الأمريكي) أثبت أنه مفيد؛ حيث عرفت دوروثي دينينج (Dorothy Denning) الإرهاب السيبراني بأنه: «هجمات غير مشروعة وتهديدات بالهجوم ضد أجهزة الكمبيوتر والشبكات والمعلومات المخزنة فيها، وذلك لترهيب أو إكراه الحكومة أو شعبها من أجل تحقيق أهداف سياسية أو اجتماعية». علاوة على ذلك، لكي يتم تصنيف الهجوم على أنه إرهاب سيبراني، يجب أن يؤدي إلى أعمال عنف ضد الأشخاص أو الممتلكات، أو على الأقل يسبب ضررًا كافيًا لتوليد الخوف، ومن الأمثلة على ذلك الهجمات التي تؤدي إلى الوفاة أو الإصابة الجسدية أو الانفجارات أو الخسارة الاقتصادية الجسيمة، ويمكن أن تكون الهجمات الخطيرة ضد البنى التحتية الحيوية بمثابة أعمال إرهابية عبر الإنترنت، اعتمادًا على تأثيرها، فالهجمات التي تعطل الخدمات غير الأساسية أو التي تمثل إزعاجًا مكلفًا بشكل أساسي لن تفعل ذلك (Denning, 2000). ويعد تعريف دوروثي داينج من أكثر التعاريف الشائعة، وخاصة أنها من أوائل الذي استخدموا هذا المصطلح. وتعرف الإرهاب السيبراني بأنه: «التقاء للإرهاب مع الفضاء السيبراني». ويمكن تصنيف الجمهور المستهدف في ثلاث فئات هي: الأفراد والممتلكات والحكومات (Stark, 1999).

لا يزال الفهم الضيق للإرهاب السيبراني مثل اتجاه دينينج سائدًا في الأدبيات أكثر بكثير من الاتجاهات الأخرى من نظرائهم الأكثر اتساعًا، ويمان (Weimann) - على سبيل المثال- يقصر المصطلح على: «استخدام أدوات شبكة الكمبيوتر للإضرار أو إيقاف تشغيل البنى التحتية الوطنية الحيوية (مثل الطاقة والنقل والعمليات الحكومية)» (Weimann, 2005). ويعرف هوا وبابنا (Hua and Bapna) المصطلح بالمثل، وذلك بأنه: «نشاط تم تنفيذه بواسطة الكمبيوتر والشبكة والإنترنت وتكنولوجيا المعلومات التي تهدف إلى التدخل في الشؤون السياسية والاجتماعية أو الأداء الاقتصادي لمجموعة أو منظمة أو دولة، أو إحداث عنف جسدي أو الخوف بدافع من أيديولوجيات الإرهاب التقليدية». (Hua and Bapna, 2012). ويتبع كونواي (Conway) كل من متطلبات دينينج للتمييز بين الإرهاب السيبراني والاستخدام الإرهابي لأجهزة الكمبيوتر، ومن خلال تقديم مطلب التسبب في حدوث ضرر دون اتصال بالإنترنت (Conway, 2002)، أضافت مساهمة مبكرة من بوليت (Pollitt) شروطًا خاصة بالفاعل السيبراني، وهي أن الإرهاب السيبراني هو الهجوم المتعمد ذو الدوافع السياسية ضد المعلومات وأنظمة الكمبيوتر وبرامج الكمبيوتر والبيانات التي تؤدي إلى العنف ضد أهداف غير مقاتلة من قبل مجموعات وطنية فرعية أو عملاء سريين، «لكي يكون للإرهاب السيبراني أي معنى، يجب أن نكون قادرين على التمييز بينه وبين أنواع أخرى من إساءة استخدام الكمبيوتر؛ مثل جرائم الكمبيوتر، والتجسس الاقتصادي، وحرب المعلومات». (Pol-litt, 1998)

قدم تاهيهارم (Taliharm) تمييزًا مشابهًا يميز بين فهم الإرهاب السيبراني الموجه نحو الهدف (الضيق) (target-oriented (narrow) والموجه نحو الأدوات (الواسع) (tool-orient-ed (broad): يعرّف الأول بأنه هجمات مدفوعة بدوافع سياسية أو اجتماعية على أجهزة الكمبيوتر والشبكات والمعلومات، سواء تم تنفيذها من خلال أجهزة الكمبيوتر الأخرى أو ماديًا، وتسببت في إصابات، وإراقة الدماء أو ضرر جسيم، أو الخوف (يشار إليه بِـ «الإرهاب السيبراني الموجه نحو الهدف»). ويقوم الثاني بتسمية جميع الإجراءات التي يتم تنظيمها باستخدام الإنترنت أو أجهزة الكمبيوتر واستكمال الأعمال الإرهابية مثل الإرهاب السيبراني (يشار إليه بِـ « الإرهاب السيبراني الموجه نحو الأدوات». (Taliharm, 2010)

المناقشات حول فائدة الفهم الأوسع للإرهاب السيبراني من ناحية أخرى (Gordon & Ford, 2002). إن التركيز المهيمن على «الإرهاب السيبراني الخالص» (يتم تنفيذ الأنشطة الإرهابية بالكامل أو في المقام الأول في العالم الافتراضي) من المحتمل أن يكون مكلفًا نظرًا لإمكانيات ذلك لإخفاء الأنشطة الأخرى المتعلقة بالإرهاب على الإنترنت. (Jarvis &. Mac-donald, 2014, p. 3)

ويعرّف جوردان بلوتنيك وجيل سلاي (Jordan Plotnek and Jill Slay) الإرهاب السيبراني بأنه هجوم متعمد أو التهديد بمثل هذا الهجوم من قبل جهات فاعلة غير حكومية تعتزم استخدام الفضاء السيبراني لإحداث أضرار مادية أو نفسية اجتماعية أو سياسية أو اقتصادية أو بيئية أو غيرها. فالهدف هو إثارة الخوف أو إجبار الهيئات الحكومية أو غير الحكومية على التصرف بطريقة تعزز الأهداف الاجتماعية أو المالية أو الأيديولوجية للإرهابين (Maryville, 2023). كما يعرف بروس هوفمان (Hoffman) الإرهاب بأنه: «خلق واستغلال الخوف من خلال العنف أو التهديد بالعنف في السعي وراء التغيير السياسي». ينتج عن هذا المصطلح تعريف بسيط وإن كان دائريًا: الإرهاب السيبراني هو استخدام الإنترنت لارتكاب الإرهاب.

بالنظر إلى مجموعة أنشطة الإرهاب السيبراني الموصوفة في الأدبيات، يمكن توسيع هذا التعريف البسيط ليشمل التالي: الإرهاب السيبراني هو استخدام القدرات السيبرانية لإجراء عمليات التمكين والتخريب والتدمير في الفضاء السيبراني؛ لإنشاء واستغلال الخوف من خلال العنف أو التهديد بالعنف سعيًا وراء التغيير السياسي. (Brickey, 2012, p. 6). أما ستارك، فعرف الإرهاب السيبراني بأنه: «الاستخدام العمد أو التهديد بالاستخدام للحرب السيبرانية أو العنف السيبراني بأهداف سياسية أو اجتماعية أو اقتصادية أو دينية من قبل جماعات أو جماعات مدعومة من الدولة أو جماعات غير حكومية، وذلك لإثارة الخوف والقلق والمعاناة لدى مجتمع مستهدف، وذلك لعرقلة الأصول (الموجودات) العسكرية والمدنية» (Stark, 1999: 8–9). ويعرفه بولييت بأنه: «هجوم معد سابقًا بدوافع سياسية ضد المعلومات ونظم الحاسب والبيانات، والذي ينجم عنه عنف ضد أهداف غير قتالية من قبل مجموعات فرعية وعملاء سريين (clandestine) (Pollitt, 2001). ويعرفه فليمنج وستوهاي (Flemming & Stohi) بأنه: «أي فعل إرهاب يستخدم نظم المعلومات أو التقنية الرقمية (الحاسبات أو الشبكات) كوسيلة أو هدف» (Flemming & Stohi, 2001:31). ويقدم مارك بوليت (Mark Pollitt)، الوكيل الخاص لمكتب التحقيقات الفيدرالي، تعريفًا عمليًا مضمونه: «الإرهاب السيبراني هو هجوم مع سبق الإصرار بدوافع سياسية ضد المعلومات وأنظمة الكمبيوتر وبرامج الكمبيوتر والبيانات التي تؤدي إلى عنف ضد أهداف غير مقاتلة من قبل مجموعات دون الوطنية أو عملاء سريين»، ويلاحظ أن الإرهاب السيبراني هو نقطة التقاء علم التحكم الآلي والإرهاب. أمَّا جيمس لويس (James Lewis) من مركز الدراسات الاستراتيجية والدولية فقد عرف الإرهاب السيبراني بأنه: «استخدام أدوات شبكة الكمبيوتر لإغلاق البنية التحتية الوطنية الحيوية (مثل الطاقة والنقل والعمليات الحكومية) أو الإكراه أو التخويف للحكومة أو السكان المدنيين».

إن المناقشات حول الإرهاب السيبراني مناسبة وغالبًا ما تستدعي الإشارة والتمييز بين المفاهيم الضيقة والواسعة لهذا المصطلح (narrow and broad conceptions)؛ حيث تركز المفاهيم الضيقة على العمليات الإرهابية التي تتم عن طريق أو ضد البنية التحتية للمعلومات، وتركز المفاهيم الواسعة على الرغبة في دمج مجموعة أكثر تنوعًا من الأنشطة عبر الإنترنت والمرتبطة بالإرهاب بموجب هذا العنوان. وهكذا، كما يلاحظ برونست (Brunst): «غالبًا ما تتم صياغة وجهة نظر أكثر ضيقًا قريبة من مفهوم الإرهاب المشترك بين التعريفات، وقد تشمل فقط الهجمات ذات الدوافع السياسية ضد المعلومات وفقط إذا أدت إلى عنف ضد مستهدفين غير المقاتلين . . .. غالبًا ما تتضمن الاتجاهات الأوسع أشكالًا أخرى للاستخدام الإرهابي للإنترنت، وبالتالي قد يعرّف الإرهاب السيبراني بأنه أي استخدام تقريبًا لتكنولوجيا المعلومات من قبل الإرهابيين». (Brunst, 2010) (. (Jarvis &. Macdonald, 2014, p. 3

أصدر مركز دراسة الإرهاب والحرب غير النظامية (the Center for the Study of Terrorism and Irregular Warfare) في كلية الدراسات العليا البحرية في مونتيري بكاليفورنيا تقريرًا بعنوان الإرهاب السيبراني: التوقعات والآثار. وكان الهدف توضيح جانب الطلب للإرهاب. على وجه التحديد، تم تقييم احتمالات قيام المنظمات الإرهابية بمتابعة الإرهاب السيبراني، وخلصوا إلى أن حاجز الدخول لأي شيء يتجاوز الاختراق المزعج مرتفع للغاية، لقد جادلوا بأن الإرهاب السيبراني هو شيء من المستقبل، على الرغم من أنه يمكن متابعته كأداة ثانوية.

تعريف مكاتب التحقيقات الجنائية (الأمريكي) (FBI):

«الاستخدام غير القانوني للقوة (force) أو العنف ضد الأشخاص أو الشركات لتخويف أو إجبار الحكومة أو السكان المدنية أو أي جهة من أجل أهداف اجتماعية أو سياسية». وهو «هجوم بدافع سياسي مسبق ضد المعلومات، نظم الحاسب، أو برامج الحاسب، أو البيانات. والذي نتج عنه عنف ضد أهداف من قبل مجموعات فرعية وطنية أو عملاء سريين».

تعريف مركز حماية البنية التحتية الأمريكي (USA NIPC) :

«سلوك إجرامي من أجل استخدام الحاسبات والإمكانيات والاتصالات ونتج عنه عنف، أو تدمير وتخريب، أو تقطع في الخدمات؛ لخلق خوف من خلال خلق فوضى وتشويش وعدم تيقن لدى السكان بهدف التأثير على الحكومة أو السكان للتوافق مع أجندة سياسية أو إخبارية أو أيديولوجية معينة».

تعريف مركز خدمات الأمن الاستخباري الكندي (CSIS):

«درجة استخدام الأساليب السيبرانية (cyber-techniques) في التجسس (espionage) والتخريب (sabotage)، أو الإرهاب (terrorism)» (Bronskill, 2001p. A3). ويمكن تعريف الإرهاب السيبراني بأنه: «أي فعل إرهابي يستخدم نظم المعلومات أو التقنية الرقمية ومعداتها وبرمجياتها وناقلاتها وحاوياتها وشبكاتها كأداة أو كهدف بدوافع سياسية أو اجتماعية أو عقائدية».

وعرّف مكتب التحقيقات الفدرالي (The FBI) الإرهاب السيبراني بأنه: «الهجوم المتعمد بدوافع سياسية ضد المعلومات وأنظمة الكمبيوتر وبرامج الكمبيوتر والبيانات التي تؤدي إلى العنف ضد أهداف غير قتالية من قبل مجموعات دون وطنية (sub national) أو وكلاء سريين».

يمكن أن يكون هناك طريقتان مختلفتان إلى الإرهاب السيبراني:

- عندما تستخدم تقنية المعلومات كأداة لتنظيم الهجمات وتنفيذها.
- عندما يهدف إلى تدمير شبكات تقنية المعلومات. (Kaźmierczak, 2017)

إن الإرهاب السيبراني هو: «استخدام أدوات شبكات الكمبيوتر لإغلاقها وتعطل البنى التحتية الوطنية الحيوية (مثل الطاقة والنقل والعمليات الحكومية) أو إكراه أو ترهيب حكومة أو سكان مدنيين». وفرضية الإنترنت الإرهاب هو أن الدول والبنية التحتية الحيوية أصبحت أكثر اعتمادًا على الكمبيوتر شبكات لعملياتهم، يتم إنشاء انكشافات جديدة - «انكشاف سيبراني ضخم" (massive electronic Achilles heel') . (Kaźmierczak, 2017) تتضمن إحدى طرق فهم الإرهاب السيبراني فكرة أن الإرهابيين يمكن أن يتسببوا في خسائر فادحة في الأرواح، وفوضى اقتصادية عالمية وأضرار بيئية من خلال اختراق أنظمة البنية التحتية الحيوية. [Hardy & William, 2014]

وتشمل طبيعة الإرهاب السيبراني السلوك الذي يشمل تكنولوجيا الكمبيوتر أو الإنترنت، والتي هي: [Kelly, 2009]

- بدافع سياسي أو ديني أو أيديولوجي
- يهدف إلى تخويف الحكومة أو قسم من الجمهور بدرجات متفاوتة
- يتدخل بشكل خطير في البنية التحتية

ويبين الشكل التالي تلخيصًا للنتائج فيما يتعلق بتعريف الإرهاب السيبراني

(Jarvis & Macdonald, 2014)

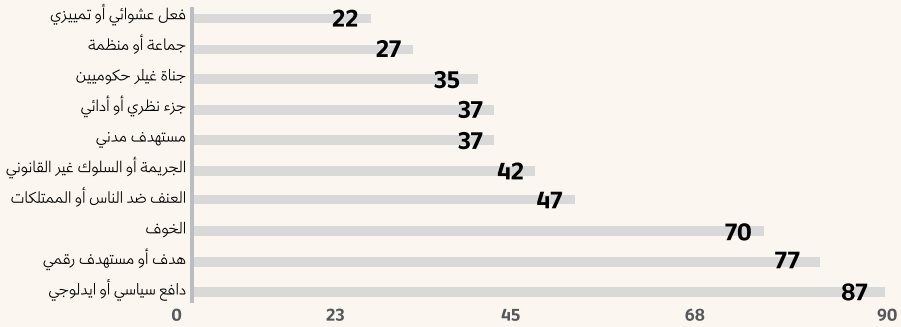


Figure 3. Important elements of cyberterrorism source: Jarvis & Macdonald, 2014 p.15 (الشكل: الباحث)

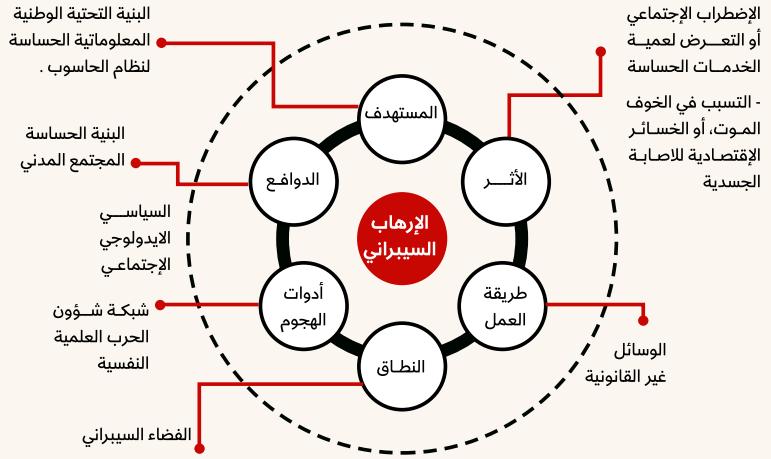
أجريت دراسة مسحية من قبل 118 باحثًا يعملون في 24 دولة عبر ست قارات؛ لتحديدثلاث قضايا في التعريف: (أ) الحاجة إلى تعريف محدد للإرهاب السيبراني لأي من صناع السياسات أو الباحثين؛ (ب) الخصائص الأساسية أو الأجزاء المكونة لذلك المفهوم، (ج) قيمة تطبيق مصطلح «الإرهاب السيبراني» على مجموعة من سيناريوهات فعلية أو محتملة. في حين أن الأغلبية من الباحثين يعتقدون بأن تعريفًا محددًا للإرهاب السيبراني ضروري للأكاديميين وصانعي السياسات، فالخلاف حول الشكل الذي قد يبدو عليه الأمر في إمكانية إضافية لتحفيز إعادة التفكير في الإرهاب على نطاق أوسع.

يتضمن تصنيف الإرهاب السيبراني ستة عناصر:

1. فاعل أو فاعلين (An actor or actors)، ويتمتع بثلاث سمات فريدة: غير حكومية، وإرهابية، وسرية.
2. دافع (A motive) قد يكون أيديولوجيًا، أو اجتماعيًا، أو اقتصاديًا، أو سياسيًا.
3. النية (An intent) أو الحث على إجراء ما أو الإكراه عليه، أو إحداث تغيير، أو تحقيق أهداف أخرى، أو التسبب في التدخل.
4. الوسائل (The means) في ارتكاب الفعل، والتي تتضمن استخدام جهاز كمبيوتر وشبكة للوصول إلى الفضاء السيبراني وعبور الحدود لارتكاب أعمال الحرب السيبرانية أو الجرائم، بما في ذلك الهجمات السيبرانية والتهديدات بالهجمات.

5. التأثير (An effect)، وهو في أغلب الأحيان العنف، أو انقطاع الخدمة، أو الأضرار الجسدية، أو التأثيرات النفسية الاجتماعية، أو الأضرار الاقتصادية، أو خروقات البيانات.
6. المستهدف (A target)، في أغلب الأحيان هم المدنيون، أو تكنولوجيا المعلومات والاتصالات (ICT)، أو مصادر البيانات، أو الوكالات الحكومية، أو المنظمات غير الحكومية، أو البنية التحتية المادية. (Maryville, 2023).

الشكل 2: مكونات الإرهاب السيبراني



/https://www.insightsonindia.com/security-issues/cyber-security/various-c ber-threats

الذئب المنفرد السيبراني (Cyber Lone Wolve):

انتشر مصطلح «الذئب المنفرد» في أواخر التسعينيات من قبل اثنين من العنصريين البيض، توم ميتزجر وأليكس كيرتس (Tom Metzger & Alex Curtis)، كجزء من الجهود المبذولة لتشجيع زملائهم العنصريين على التصرف بمفردهم في ارتكاب أعمال جرائم العنف. الذئب المنفرد هو الشخص الذي يرتكب أعمال عنف لدعم جماعة أو حركة أو أيديولوجية ما، لكنه يفعل ذلك بمفرده، خارج أي هيكل أو قيادة. ويتم تعريف إرهاب الذئاب المنفردة على النحو التالي:

«الهجمات الإرهابية التي ينفذها أشخاص (أ) يعملون بشكل فردي، (ب) لا ينتمون إلى جماعة أو شبكة إرهابية منظمة، (ج) أسلوب جرمي منفرد (modi operandi) دون أي قيادة خارجية مباشرة أو تسلسل هرمي». ويغطي هذا التعريف الذئاب المنفردة مثل الأمريكي نضال مالك حسن، قاتل فورت هود، وعبد الحكيم مجاهد محمد، الذي فتح النار على مكتب تجنيد عسكري أمريكي في ليتل روك، أركنساس، يشترك الإرهابي المنفرد في هويته الأيديولوجية أو الفلسفية مع جماعة إرهابية جماعة متطرفة، لكنه لا يتواصل مع تلك الجماعة، بينما تكون تصرفات الذئب المنفرد بدافع تحقيق هدف مجموعة معينة، يتم تصور وتوجيه التكتيكات والأساليب من قبل الفرد فقط، دون أي أمر أو توجيه خارجي.. بسبب هذا النقص في الاتصال الشخصي مع مجموعة أكبر، يشكل إرهاب الذئاب المنفردة مشكلة خاصة لمكافحة الإرهاب، لأن جمع المعلومات الاستخبارية عن الذئاب المنفردة أصعب بكثير من جمعها عن الإرهابيين التقليديين. وفي بحثهم بعنوان «الذئاب المنفردة؛ كيفية منع هذا على ما يبدو ظاهرة جديدة»، قام باكر ودي جراف (Bakker and de Graaf) بدراسة تزايد إرهاب الذئاب المنفردة وخصائصه، وتوصل إلى هذا الاستنتاج: «لا يوجد سجل تعريف (profile) موحد واحد للذئب المنفرد، ومع ذلك فإنه من الممكن التمييز بين الفئات المختلفة من الإرهابيين المنفردين بناءً على انتمائهم والخلفية الأيديولوجية أو الدينية (Buch, 2014, Kessler, 2016, 2021). لقد عطلت قراصنة الذئاب المنفردة أنظمة الكمبيوتر في الماضي وتستمر في إظهار وجودها في الفضاء السيبراني. فمن الممكن في المستقبل غير البعيد، لكي يصبح الفرد متحفزًا بدرجة كافية تجاه الصراع المتصور، النجاح في أول هجوم إلكتروني كبير على البنية التحتية للمقاطعة (Buch, 2014).

لماذا الإرهاب السيبراني؟

حددت الأبحاث الإرهاب السيبراني بأنه استخدام التكنولوجيا كوسيلة لخلق سياسي أو تغيير ديني أو أيديولوجي من خلال تخويف المؤسسات المدنية؛ عن طريق تعطيل أو تدمير البنى التحتية الحيوية في الفضاء السيبراني. الإرهاب السيبراني ليس من الضروري أن يسبب الموت أو الضرر الجسدي أو الدمار الاقتصادي الذي يمكن وصفه بأنه عمل إرهابي، طالما أنه يتداخل بشكل كبير مع شكل من أشكال البنية التحتية (Hardy, 2011). وقد وجد الباحثون أن الهجمات الإرهابية السيبرانية لديها القدرة على تعطيل السوق المالية، والتدخل في الخدمات، وتدمير ملفات وشبكات الكمبيوتر، وإثارة الذعر على نطاق واسع بين

المواطنين والأعمال (قاسم، 2012؛ هاردي، 2011؛ تافويا، 2011) (Cassim, 2012; Hardy, 2011; Tafoya, 2011). وتتركز خطورة الذئب المنفرد السيبراني في أن الذئب المنفرد يمكن أن يقوم بهجمات سيبرانية من أي مكان وضد مستهدفين متعددين محليًّا ودوليًّا، مما يشكل انتهاكًا للسيادة الوطنية والقانون الوطني والدولي.

إنَّ الإرهاب السيبراني يعد خيارًا جذابًا للإرهابيين المعاصرين لعدة أسباب:

1. أقل تكلفة من الأساليب الإرهابية التقليدية، فكل ما يحتاجه الإرهابي هو جهاز كمبيوتر شخصي واتصال بالإنترنت. ولا يحتاج الإرهابيون إلى شراء الأسلحة مثل البنادق والمتفجرات، وبدلًا من ذلك يمكنهم إنشاء فيروسات الكمبيوتر وإرسالها من خلال خط هاتف أو كابل أو اتصال لا سلكي.

2. الإرهاب السيبراني مجهول الهوية أكثر من الأساليب الإرهابية التقليدية، يستخدم العديد من متصفحي الإنترنت من الإرهابيين ألقابًا على الإنترنت «أسماء الشاشة»، أو يقومون بتسجيل الدخول إلى موقع ويب باعتباره «مستخدم ضيف» مجهول الهوية، مما يجعل الأمر صعبًا للغاية على الأجهزة الأمنية وقوات الشرطة لتعقب الهوية الحقيقية للإرهابيين، وفي الفضاء السيبراني هناك لا توجد حواجز مادية مثل نقاط التفتيش للتنقل، ولا حدود لعبورها، ولا وكلاء الجمارك.

3. تنوع هائل في الأهداف وعددها، يمكن للإرهابي السيبراني أن يستهدف أجهزة الكمبيوتر وشبكات الكمبيوتر الخاصة بالحكومات والأفراد والمرافق العامة، وشركات الطيران الخاصة، وما إلى ذلك. العدد الهائل والتعقيد للأهداف المحتملة يضمن أن يتمكن الإرهابيون من العثور على نقاط ضعف لاستغلالها، وقد أظهرت دراسات عديدة أن البنى التحتية الحيوية، مثل شبكات الطاقة الكهربائية وخدمات الطوارئ، معرضة لهجوم إرهابي عبر الإنترنت لأن البنى التحتية وأنظمة الكمبيوتر التي تقوم بتشغيلها معقدة للغاية، مما يجعلها فعالة من المستحيل القضاء على جميع نقاط الضعف فيها.

4. تنفيذ الإرهاب السيبراني عن بعد، وهي سمة جذابة بشكل خاص للإرهابيين؛ حيث يتطلب الإرهاب السيبراني تدريبًا بدنيًّا واستثمارًا نفسيًّا، ومخاطر الوفاة والسفر أقل من الأشكال التقليدية للإرهاب، فمن السهل على المنظمات الإرهابية تجنيد أتباعها والاحتفاظ بهم.

5. القدرة على التأثير على مستهدفين أكثر، كما أظهر فيروس «أحبك»، فإن الإرهاب السيبراني لديه القدرة على التأثير بشكل مباشر على عدد أكبر من الناس مقارنة بالطرق الإرهابية التقليدية، وبالتالي توليد تغطية إعلامية أكبر، وهو ما يريده الإرهابيون في نهاية المطاف (Weimann, 2004, p. 6).

خصائص الهجوم السيبراني (Cyber Attack Attributes):

بعد تحديد مفاهيم الفضاء السيبراني، من الممكن توصيف آثار الهجمات السيبرانية وقياس الهجمات السيبرانية، وبالتالي قياس القوة السيبرانية. ويقاس الهجوم السيبراني باستخدام مقياس التمرس (Sophistication) بناءً على الطبقات الموجودة في أنموذج الفضاء السيبراني، والذي يقترن بالأنشطة المستهدفة، ويوفر مقياسًا شاملًا للهجمات، ومقارنة توسيع نطاق الهجمات. ويقاس التمرس من حيث ست خصائص هي: المثابرة (persistence) والانتشار(propagation) والجدة (novelty) والدقة والانضباط (precision and accuracy) والتأثير(impact) والإسناد(attribution):

المثابرة (Persistence): يتم قياس هذا البعد من حيث الإجراءات أو الجهد المبذول من قبل المهاجم. على سبيل المثال، يتطلب هجوم رفض الخدمة (DOS) الإجراء المتواصل من المهاجم سيسجل أقل من الفيروس الذي لا يتطلب عملًا بشريًا للدعاية لنشرها. وفقا لذلك، سوف يسجل الفيروس أقل من تكاثر دودة ذاتية لا تتطلب تفاعل المنشئ بعد التسليم الأولي.

الانتشار (Propagation): يتم قياس هذا من حيث الجهد المطلوب لتسليم الحمولة. على سبيل المثال، هجوم ناجح على نظام غير متصل بالإنترنت سيحرز نقاطًا أعلى من أي نظام الوصول إليه بسهولة أكبر.

الجدة (Novelty): يقاس هذا من حيث تفرد التقنية المستخدمة بواسطة حمولة الهجوم ومقدار الجهد المبذول فيه تطوره. إن استخدام الثغرات غير المعروفة سابقًا سيحصل على درجة عالية.

الدقة والانضباط (Precision and Accuracy): يتم قياسها من حيث مدى تكتم الهجوم (discreet) في تحقيق تأثير معين. هذا يتضمن مستوى الأضرار الجانبية للأنظمة الأخرى أو الأشخاص ومدى تحديد توقيت الحدث. هجوم يركز على الهدف الفريد في وقت معين من شأنه أن يسجل درجات أعلى من الهدف العام بدون توقيت معين؛ لأنه يشير إلى تعقيد الهدف أو الرغبة في تقليل الأضرار الجانبية.

التأثير (Impact): يتم قياس هذا من حيث فعالية الهجوم، والذي يعتمد على قيمته النفسية وكذلك التأثير الفعلي على الهدف. يمكن أيضًا قياس التأثير من حيث التأثير الزمني، ويتأثر التسجيل بالدعاية وتقييم باحثي الأمن السيبراني الذين حددوا تفاصيل الهجوم الدقيقة، والتي لم يتم الإفصاح عنها للعامة. كلما كان التأثير أكثر شدة، زادت النتيجة.

الإسناد (Attribution): يتم قياسه من حيث قدرة هدف حملة القوة السيبرانية لتحديد المنشئ بدقة. وقد يسعى المنشئ إلى إخفاء هويته تمامًا أو قد يشير ضمنًا إلى أن مجموعة أخرى أو أن الدولة نفذت الهجوم من أجل عرقلة التحقيق. يعتمد مؤشر الإسناد على مهمة الهجوم السيبراني بشكل عام، وكلما زاد إخفاء الهوية، زادت النتيجة. (Venables, Shaikh, & Shuttleworth, 2015)

في عام 1999، حدد مركز دراسة الإرهاب والحرب غير النظامية في كلية الدراسات العليا البحرية (the Study of Terrorism and Irregular Warfare at the Naval Postgraduate School) في مونتيري، كاليفورنيا، ثلاثة مستويات لقدرة الإرهاب السيبراني:

بسيطة وغير منظمة (Simple–Unstructured): القدرة على إجراء اختراقات أساسية ضد الأنظمة الفردية باستخدام أدوات أنشأها شخص آخر، تمتلك المنظمة القليل من القدرة على تحليل الأهداف أو القيادة والسيطرة أو التعلم.

متقدمة التنظيم (Advanced–Structured): القدرة على تنفيذ هجمات أكثر تعقيدًا ضد أنظمة أو شبكات متعددة، وربما تعديل أو إنشاء أدوات القرصنة الأساسية، تمتلك المنظمة قدرة أولية على تحليل الأهداف والقيادة والسيطرة والتعلم.

معقدة منسقة (Complex–Coordinated): القدرة على شن هجوم منسق قادر على إحداث اضطراب شامل ضد الدفاعات المتكاملة وغير المتجانسة (بما في ذلك التشفير)، القدرة على إنشاء أدوات القرصنة المتطورة، قدرة عالية على تحليل الأهداف والقيادة والسيطرة والقدرة على التعلم التنظيمي. (Denning, 2000)

أهداف الإرهاب السيبراني ودوافعه:

وفقًا لتقييم التهديدات السنوية لمجتمع الاستخبارات الأمريكي (Annual Threat Assessment of the U.S. Intelligence Community) الصادر في 9 أبريل 2021 فإن التهديدات السيبرانية ضد المصالح الأمريكية؛ هجمات الإرهاب السيبراني الذي يستهدف تكنولوجيا

المعلومات والاتصالات والبنية التحتية المادية، ومقدمي الخدمات المدارة وبرامج الأعمال الشائعة. والهدف من هذه الهجمات هو سرقة المعلومات أو تخريب الأنظمة التي تصيبها. وتسرد شركة IBM الأهداف الأكثر شيوعًا للهجمات السيبرانية:

- معلومات سرية من الوكالات الحكومية (الأمريكية).
- البيانات الشخصية الحساسة.
- الوصول إلى البنية التحتية لتكنولوجيا المعلومات.
- أنظمة الدفع المالية.
- الأسرار التجارية والملكية الفكرية الأخرى.
- عناوين البريد الإلكتروني ومعرفات المستخدمين وكلمات المرور.
- قواعد بيانات العملاء والبيانات المالية.
- قوائم العملاء (Maryville, 2023).

يتمثل أحد الاتجاهات الأمنية المهمة في تصاعد التهديدات التي يشكلها الإرهاب السيبراني على الحكومات والشركات والأفراد مع تطور التقنيات الجديدة. وتشير تقارير التكنولوجيا الحكومية إلى أن الزيادة في الهجمات السيبرانية بدأت في عام 2020 واستمرت في عام 2021؛ حيث أصبحت الهجمات أكثر تكرارًا وأكثر ضررًا.

- في 5 فبراير 2021، استخدم المتسللون ثقبًا في إصدار قديم من Windows لاقتحام شبكة محطة معالجة المياه في فلوريدا ورفع مستويات هيدروكسيد الصوديوم (الغسول) إلى مستويات مميتة، لكن تم إحباط الهجوم قبل أن يحدث أي ضرر من قبل المشغل الذي لاحظ التغيير وقام بتصحيح المستويات. ومع ذلك، فإن الهجوم يسلط الضوء على مدى ضعف أنظمة المياه والبنية التحتية الحيوية الأخرى في الولايات المتحدة.
- يعد مكتب التحقيقات الفيدرالي الآن أن برامج الفدية (ransomware) تشكل خطرًا جسيمًا على المصالح الأمريكية مثل الإرهاب في أعقاب هجمات 11 سبتمبر 2001، حسبما ذكرت صحيفة نيويورك تايمز. وتقوم الوكالة حاليًا بتحليل 100 نوع مختلف من البرامج المستخدمة في هجمات برامج الفدية من قبل العصابات الإجرامية والمجموعات العاملة داخل الصين وروسيا. ويتوقع المحللون أن تستهدف المزيد من الهجمات الضارة البنية التحتية الحيوية في الولايات المتحدة.

- في أكتوبر 2021، حذرت وكالة الأمن القومي الأمريكية (NSA) الشركات من استخدام شهادات التشفير الرقمي لـ Transport Layer Security (TLS) للحماية من نوع جديد من البرامج الضارة يسمى ALPACA (بروتوكولات طبقة التطبيقات التي تسمح بالهجوم عبر البروتوكولات). تتسلل ALPACA إلى تطبيقات الويب المحصنة عبر خدمات غير تابعة لـ HTTP والتي تستخدم شهادة مطابقة لشهادة TLS أو مشابهة لها. تخدع هذه التقنية خوادم الويب للاستجابة لطلبات HTTP المشفرة باستخدام بروتوكولات غير مشفرة (Maryville, 2023).

تاريخ الإرهاب السيبراني (History of Cybersecurity):

بدأ الاهتمام العام بالإرهاب السيبراني في أواخر التسعينيات، عندما صاغ هذا المصطلح باري سي كولين (Barry C. Collin) (Tafoya, 2011)؛ حيث عرّف كولين الإرهاب السيبراني بأنه: «تقارب علم التحكم الآلي والإرهاب» (the convergence of cybernetics and terrorism). إن هدفه إثارة الخوف والذعر على نطاق واسع كان دائمًا في قلب الهجمات الإرهابية السيبرانية. وكانت أول دودة كمبيوتر تم نقلها عبر الإنترنت دودة موريس، التي أنشأها روبرت تابان موريس عام 1988، وهو طالب في جامعة كورنيل، كما يوضح موقع التكنولوجيا ARN. لم يكن المقصود من الدودة أن تكون ضارة، لكن خطأ في شفرتها تسبب في أن تصبح فيروسًا يتكاثر بسرعة ويصيب في النهاية حوالي 6000 جهاز كمبيوتر. تشير التقديرات إلى أن دودة موريس تسببت في أضرار تصل إلى 100 مليون دولار.

ومع اقتراب عام 2000، تزايدت المخاوف وعدم اليقين بشأن خلل الألفية (millennium bug)، كما تزايدت احتمالات وقوع هجمات من قبل الإرهابيين السيبرانيين، على الرغم من أن خطأ الألفية لم يكن بأي حال من الأحوال هجومًا إرهابيًا أو مؤامرة ضد العالم أو الولايات المتحدة، إلا أنه كان بمثابة حافز في إثارة المخاوف من احتمال وقوع هجوم إلكتروني مدمر واسع النطاق. وأشار المعلقون إلى أن العديد من حقائق مثل هذه الحوادث تبدو وكأنها تتغير، وغالبًا ما يكون ذلك من خلال تقارير إعلامية مبالغ فيها. وقد أدت الهجمات الإرهابية البارزة في الولايات المتحدة في 11 سبتمبر 2001، والحرب التي تلت ذلك على الإرهاب (War on Terror) من قبل الولايات المتحدة، إلى مزيد من التغطية الإعلامية للتهديدات المحتملة للإرهاب السيبراني في السنوات التالية. وغالبًا ما تناقش التغطية الإعلامية الرئيسية إمكانية وقوع هجوم كبير يستخدم شبكات الكمبيوتر لتخريب البنى

التحتية الحيوية؛ بهدف تعريض حياة البشر للخطر أو التسبب في اضطراب على نطاق وطني إما بشكل مباشر أو عن طريق تعطيل الاقتصاد الوطني .[White House shifts, 1999]

يقال إن مؤلفين مثل وين شوارتو وجون أركويلا (Winn Schwartau and John Arquilla) حققوا نجاحًا ماليًا كبيرًا في بيع الكتب التي تصف ما يزعم أنها سيناريوهات معقولة للفوضى الناجمة عن الإرهاب السيبراني (plausible scenarios of mayhem caused by cyberterrorism). ويزعم العديد من النقاد أن هذه الكتب كانت غير واقعية في تقييماتها حول ما إذا كانت الهجمات الموصوفة (مثل الانهيارات النووية وتفجيرات المصانع الكيميائية) ممكنة أم لا. إن القاسم المشترك بين ما يعده النقاد دعاية للإرهاب السيبراني هو عدم القابلية للتزييف؛ أي أنه عندما تفشل الكوارث المتوقعة في الحدوث، فإن ذلك لا يؤدي إلا إلى إظهار مدى حظنا حتى الآن، بدلًا من دحض النظرية. في عام 2016، ولأول مرة على الإطلاق، اتهمت وزارة العدل أرديت فريزي (Ardit Ferizi) بالإرهاب السيبراني، وهو متهم باختراق موقع عسكري وسرقة الأسماء والعناوين وغيرها من المعلومات الشخصية للموظفين الحكوميين والعسكريين وبيعها إلى داعش. [Andrew, 2017]

ومن ناحية أخرى، يقال أيضًا إنه على الرغم من الدراسات الكبيرة حول الإرهاب السيبراني، فإن مجموعة الأدبيات لا تزال غير قادرة على تقديم تقدير واقعي للتهديد الفعلي؛ على سبيل المثال: في حالة وقوع هجوم إرهابي عبر الإنترنت على البنية التحتية العامة مثل محطة توليد الكهرباء أو مراقبة الحركة الجوية من خلال القرصنة، هناك عدم يقين بشأن نجاحه لأن البيانات المتعلقة بهذه الظواهر محدودة (Pauline, 2012).

بعض الأحداث المبكرة في تاريخ الإرهاب السيبراني:

- في مارس 1999، بدأ فيروس ميليسا (Melissa virus) ينتشر كالنار في الهشيم عبر الإنترنت، فوفقًا لمكتب التحقيقات الفيدرالي استهدفت ميليسا برنامج معالجة النصوص Word من Microsoft وبرنامج البريد السيبراني Outlook لإرسال رسائل تلقائيًا إلى أول 50 شخصًا في قائمة جهات اتصال الضحية. تم إنشاء الفيروس بواسطة ديفيد لي سميث ولم يكن المقصود منه تحقيق مكاسب مالية بل لإحداث الفوضى. دمرت ميليسا خوادم البريد الإلكتروني في مئات الشركات حول العالم، مما أدى مؤقتًا إلى منع الوصول إلى حوالي مليون حساب بريد إلكتروني.

- في مايو 2007، كانت الوكالات الحكومية والشركات الخاصة في إستونيا هدفًا لهجمات إلكترونية ضخمة استمرت لأسابيع بعد أن قامت الحكومة بإزالة بعض تذكارات الحرب العالمية الثانية الروسية من مدينة تالين. تسببت هجمات حجب الخدمة الموزعة (DDOS) في إغلاق أكبر بنك في إستونيا، مما أدى إلى خسائر تقدر بنحو مليون دولار.
- في أغسطس 2013، قامت مجموعة قراصنة تدعى الجيش الإلكتروني السوري (Syrian Electronic Army) بالاستيلاء على مواقع نيويورك تايمز، وهافينغتون بوست، وتويتر (New York Times, Huffington Post, and Twitter) من خلال اختراق شبكة ملبورن آي تي ()، وهي مزود خدمة الإنترنت الأسترالي الذي يدير أسماء نطاقات الشركات. وكانت المجموعة قد استهدفت في السابق مواقع واشنطن بوست وسي إن إن وتايم، وكان الدافع وراء الهجوم هو الانتقام من انتقادات الرئيس السوري بشار الأسد.
- في مايو 2017، ضرب هجوم برنامج الفدية WannaCry أنظمة Microsoft Windows، وطالب الضحايا بمبلغ 300 دولار من عملة البيتكوين (زادت لاحقًا إلى 600 دولار) لاستعادة الوصول إلى ملفات الكمبيوتر الخاصة بهم. وقبل أشهر من الهجوم، أصدرت مايكروسوفت تصحيحًا للثغرة الأمنية التي استغلها فيروس WannaCry، لكن العديد من المستخدمين لم يقوموا بتحديث نظامهم للحماية من الهجوم. وتسبب خطأ في كود الفيروس في منع الضحايا من استعادة ملفاتهم حتى لو دفعوا الفدية (Maryville, 2023).

حوادث سيبرانية مهمة:

يسرد هذا الجدول الزمني الحوادث السيبرانية المهمة، ونحن نركز على إجراءات الدولة، والتجسس، والهجمات السيبرانية التي تزيد خسائرها على مليون دولار، هذا هو وثيقة حية.

الجدول (3): حوادث سيبرانية كبيرة

السنة	الفاعل	الحادث	المستهدف
2003	نشطاء القرصنة الهنود	- هجمات DDoS التي أدت إلى إبطاء عمليات النظام لعدة ساعات. - أشار المتسللون إلى الكنديين. - اتهام رئيس الوزراء جاستن ترودو العلني للهند بقتل Hardeep Singh Nijjar كدافع للهجوم.	- المواقع العسكرية والبرلمانية الكندية
2023	قراصنة إيرانيون	- حملة تصيد احتيالي لاستهداف البنية التحتية الكهربائية للشبكة الإسرائيلية.	- شبكة السكك الحديدية الإسرائيلية (وتم استهداف شركات إماراتية في الهجوم نفسه)
2023	قراصنة برعاية الصين	- عمليات زرع البرامج الثابتة للبقاء مخفيين والتحرك في أهدافهم في الشبكات.	- الصناعات والشركات الحكومية الموجودة في أمريكا واليابان
2023	هجوم سيبراني ضخم	- مجهول	- وزارة التخطيط في برمودا. - تعطيل للخدمات.

2023	هجوم سيبراني مجهول	- عملية تصيد احتيالي. - هجوم الفدية.	- وزارة المالية الكويتية
2023	روسيا	- هجمات سيبرانية	- سلطات الوحدات التي تقوم بجمع وتحليل الأدلة على جرائم الحرب الروسية للمسؤولين الأوكرانيين وإنفاذ القانون الأوكراني. - البنية التحتية الأوكرانية.
2023	مجرمو الإنترنت الروس	- اختراق. - التحقيق المستمر في جرائم الحرب الروسية المرتكبة في أوكرانيا.	- تكنولوجيا المعلومات الخاصة بالمحكمة الجنائية الدولية. - مركز الدراسات الاستراتيجية والدولية (CSIS) واشنطن العاصمة.
2023	الصين	- العمليات السيبرانية الصينية في بحر الصين الجنوبي.	- القاعدة الصناعية الدفاعية الأمريكية والبنية التحتية الحيوية للولايات المتحدة.
2023	روسيا	- برامج الفدية بتسريب تفاصيل ضباط الشرطة الفيدرالية الأسترالية على شبكة الإنترنت المظلمة.	- شركة محاماة أسترالية تقدم خدماتها للعديد من الوكالات الحكومية الأسترالية.
2023	روسيا	- اقتحام مطور سياج بريطاني واستعادته.	- وزارة الخارجية البريطانية؛ حيث سرق قراصنة روس آلاف الوثائق منها، وقاموا بتحميلها على شبكة الإنترنت المظلمة. (تحتوي المستندات على تفاصيل إمكانية الوصول لقاعدة نووية في اسكتلندا، وسجون شديدة الحراسة، وتفاصيل أمنية وطنية أخرى)

المصدر: CSIS, 2023p 1-2 الجدول: الباحث

أساطير الإرهاب المادي والسيبراني Myths & Realties:

يلخص الجدول التالي عددًا من الأساطير المتعلقة بواقع الإرهاب التقليدي والبيئة السيبرانية الخاصة بالإرهاب السيبراني.

الجدول (4): الأساطير والواقع التقليدي والواقع السيبراني

الأسطورة	الواقع التقليدي	الواقع السيبراني
الأسطورة 1: الإرهاب عشوائي وليس محدد الاتجاه.	- الإرهاب ليس عشوائيًا وهو محدد الأهداف، ومدفوع بأهداف محددة جيدًا. - الطبيعة الرمزية للإرهاب تنزع لمفاقمة نظرة السمعة غير المنطقية للإرهاب.	- سيستمر الإرهاب السيبراني في غزوات هادفة وتهديدات إرهابية وعنف في البيئة السيبرانية. - إن زيادة الجمهور المعتمد على هذه البيئة يضيف أهمية لتكوين نسل جديد من وحوش الإرهاب.
الأسطورة 2: الإرهاب لا يعرف حدودًا ولا يحترمها.	- إن تاريخ الإرهاب قد امتاز بالحملات المخططة للإرهاب الدولي. - الجماعات الإرهابية الناجحة تفهم أهمية خدمة المؤسسات الداعمة وتتجنب عزلها بأفعال غير ضرورية من العنف.	- في عالم الإرهاب السيبراني، سيستمر الإرهابيون في اختيار أعدائهم ومستهدفيهم. - المواطن العادي يصبح أكثر وعيًا لها ويشعر بالتهديد. - رغم أن الجماعات الإرهابية تبقى على اتصال بدوائرها فإن جماعات ناشئة ستجد لها مكانًا في البيئة السيبرانية وستوسع حدود الإرهاب.
الأسطورة 3: الإرهاب مرادف لمصطلح الموت والدمار الشامل.	- العمليات الإرهابية التي تؤدي إلى دمار شامل هي حالات خاصة. - الحكومات والجماعات الإرهابية استغلت هذه الأسطورة؛ كُلٌّ لصالحه.	- إن طبيعة الإرهاب السيبراني يعمل في بيئة جديدة تتطور فيها وسائل العمليات الإرهابية. - كان دائمًا لدى الإرهابيين المقدرة على التدمير الشامل ولكن لم يختاروا ذلك.

الأسطورة 4: الإرهاب نشاط محصور في الفاعلين غير الحكوميين وهدفه خلق فوضى.	- إن الاعتقاد بأن الجماعات غير الحكومية المتمردة هي الوحيدة التي تلجأ للإرهاب قد أدى إلى سياسات غير مناسبة في مكافحة الإرهاب. - الإرهاب نوع من العنف يستخدم فاعلين متمردين حكوميين وغير حكوميين. - تبقى طبيعة الإرهاب كما هي، الأهداف فقط هي المختلفة بغض النظر عن مصادرها. - يهدف العنف من قبل الدولة إلى إحلال النظام.	- كل من الفاعلين الحكوميين والمتمردين سينقشون محرابهم الخاص في حقبة الإرهاب السيبراني. - إن هدف الإرهاب يختلف عن طبيعته. - الإرهاب يخدم عدة أهداف. - الإرهابيون سيستغلون الأنماط الجديدة من التقنيات ضمن البيئة السيبرانية لتحقيق أي هدف لديهم.
الأسطورة 5: جميع الإرهابيين مجرمون أو مجانين.	- يأتي الإرهابيون من خلفيات اقتصادية وتاريخية وسياسية واجتماعية واسعة. - يمكن أن يكون الإرهابي شخصًا مجنونًا أو مجرمًا، ولكن الإرهاب يمكن أن ينبعث من مجموعة من الظروف المعقدة.	- في عالم الإرهاب السيبراني فإن الجماعات الإرهابية ذات الأجندة السياسية المحددة ستستمر في السيطرة.
الأسطورة 6: الحكومات دائمًا تعارض الإرهاب غير الحكومي.	- تجد الحكومات أن من المفيد دعم الإرهابيين غير الحكوميين. - يأخذ الدعم أشكالًا متنوعة، وقد يكون الإرهاب محليًا أو دوليًا. - وعلى الرغم من أنه ينظر للإرهاب بأنه سلاح الضعيف، إلا أن العديد من اللاعبين الرئيسين يدعمونه وينخرطون فيه.	- الإرهاب السيبراني يُدعَم من الحكومات بالطريقة ذاتها التي يُدعَم فيها الإرهاب التقليدي طالما أن الحكومات بقيت تعتقد بأن نتائج الإرهاب لصالحها.
الأسطورة 7: إن مصدر الإرهاب السياسي الحديث يمكن أن يوجد في شر شخص واحد أو اثنين من الفاعلين.	- إن تكرار أن شيطانًا معينًا أو مجموعات شيطانية معينة هي مصدر الإرهاب ما هو إلا ممارسة سياسية ليس لها وجود في الواقع. - الإرهابيون ليسوا عربًا أو غربيين فقط، ولا يساريين أو يمينيين فقط، بل إن التركيز يكون على المجموعة غير المرغوب فيها. - الإرهاب ليس عملية وصم، ولكنه عمليات عنف مرتبطة بالمشكلات الاقتصادية والسياسية والاجتماعية.	- إن الإرهاب السيبراني سيعامل كأسوأ نوع من الإرهاب طالما أنه غير معلوم الطبيعة، وسيستخدم لربطه بمجموعات مثل الإسلام أو الأصوليين، مما يجعله أكثر رعبًا. - الفاعلون الشياطين سيصورون على أنهم إرهابيون فضائيون، والعكس بالعكس.

المصدر: الأساطير والواقع التقليدي والواقع السيبراني للإرهاب ص 29-26 (بتصرف)
Flemming and Stohl, 2001. available at: http://www.comm.ucsb.edu/Research/Myths%20and%20Realities%20of%20Cyberterrorism.pdf

الحرب السيبرانية (Cyberwarfare) والإرهاب السيبراني (cyberterrorism):

يحذر العديد من خبراء الأمن السيبراني من أن الحرب السيبرانية تشكل تهديدًا وشيكًا، وأنها مسألة وقت فقط قبل أن يحدث هجوم إلكتروني ضخم، ويصر آخرون على أن التهديد مبالغ فيه (Parks, 2013). تمثل الحرب السيبرانية والإرهاب السيبراني تهديدًا متزايدًا في هذا العالم، وقد أصبحت مجموعات كثيرة تدرك إمكانية الحرب السيبرانية والإرهاب السيبراني، ومع تقدم الوقت وازدياد عدد الدول التي أصبحت أكثر حوسبة، وزيادة عدد الناس الذين يعتمدون على التقنيات والإنترنت في حياتهم، ومع انتقال المال والأعمال والتفاعلات إلى الفضاء السيبراني، فمن المتوقع المزيد والمزيد من الهجمات السيبرانية عبر الفضاء السيبراني.

إن الحرب السيبرانية تستخدم أجهزة الكمبيوتر عبر الإنترنت للقيام بأعمال حربية (الحرمان من الخدمة) ضد البنية المعلوماتية الحساسة، وخاصة في القطاعات الحيوية والمهمة (قطاع المواصلات والاتصالات والبنوك والكهرباء والماء ..... إلخ)، ويمكن أن يشمل ذلك تشويه مواقع الويب، وتوزيع هجمات رفض الخدمة، وتوزيع الدعاية، وجمع البيانات السرية عبر الإنترنت.

إن الإرهاب السيبراني يختلف عن الحرب السيبرانية، فهو ينطلق من أهداف سياسية وأيديولوجية واجتماعية، (وقد يكون فرديًا «الذئب المنفرد السيبراني Cuber lone wolf»)، وينقل رسالة سياسية إلى الحكومة أو الأمة التي يعارضها، كما يسعى إلى اختراق المواقع الحكومية وسرقة معلومات سرية للغاية يمكن للإرهابيين استخدامها ضد تلك الحكومة، ويسعى الإرهاب السيبراني أيضًا إلى إحداث رعب وخوف كبير لدى شرائح سيبرانية واسعة؛ من خلال استهداف خدمة ما أو أحد مكونات البنية التحتية الكونية الحساسة.

أما الحرب السيبرانية فهي تستخدم وسائل الهجوم في الإرهاب السيبراني، ولكن المستهدف يكون العدو (دولة ما وأحيانًا حلفاءها وداعميها)، وهما متشابهان من حيث أن كليهما يتضمنان استخدام أنظمة الكمبيوتر ضد أنظمة الكمبيوتر الأخرى، كما لا تتوقف النتائج في كليهما على التخريب السيبراني، بل تتعداه إلى التخريب والدمار المادي أحيانًا (Surabhi, 2012). ويصف تقرير بعنوان «سباق التسلح السيبراني الجديد» ما يلي: «في المستقبل، لن تقع حروب فقط يقاتل فيها جنود مسلحون أو بطائرات تلقي قنابل، سيتم قتالهم أيضًا بنقرة واحدة على نصف العالم بعيدًا، ويطلق العنان لبرامج الكمبيوتر المسلحة بعناية لتعطيل أو تدمير الصناعات الحيوية مثل المرافق والنقل والاتصالات والطاقة. مثل هذه الهجمات

يمكن أن تؤدي أيضًا إلى تعطيل الجيش والشبكات التي تتحكم في حركة القوات ومسار الطائرات والمقاتلين، وقيادة السفن الحربية والسيطرة عليها». (Siber & Friedman, 2015).

القصة التالية تلخص القادحة التي أشعلت الاهتمام بالحرب السيبرانية:

في يوم السبت 4 يونيو من العام 1983، كان Ronald Reagan الرئيس رونالد ريغان في كامب ديفيد يقضي يومه في مطالعة بعض الأوراق، ثم تناول طعام العشاء، وكما كان يفعل في كثير من الأحيان، جلس لمشاهدة أحد الأفلام. كان عرض تلك الليلة هو فيلم (ألعاب الحرب)، (War Games) المناورات الحربية بطولة ماثيو برودريك (Matthew Broderick)، لعب فيه دور فتى مراهق بارع في أمور التكنولوجيا، يخترق من دون قصد الحاسوب الرئيسي في قيادة دفاع الفضاء الجوي لأمريكا الشمالية، وظنًّا منه أنه يلعب لعبة حاسوبية جديدة أوشك على إشعال حرب عالمية ثالثة. في صباح اليوم التالي، عاد ريغان إلى البيت الأبيض، وعقد اجتماعًا حضره وزراء الخارجية والدفاع والخزانة، إلى جانب فريقه لشؤون الأمن القومي، ورئيس الهيئة المشتركة لرؤساء الأركان، وستة عشر من أعضاء الكونغرس البارزين. كان الاجتماع لمناقشة نوع جديد من الصواريخ النووية وأرجحيّة محادثات الأسلحة مع الروس، لكن ريغان لم يستطع إبعاد ذلك الفيلم عن ذهنه، وفجأة في لحظة ما، نحّى أوراقه جانبًا، وسأل ما إذا كان أي شخص آخر قد شاهد ذلك الفيلم. لم يكن أحد قد شاهد الفيلم؛ إذ إنه كان قد عرض من فوره في دور السينما في يوم الجمعة الأخير. ثم انطلق ريغان في عرض ملخص تفصيلي عن حبكة الفيلم الروائية. أجال بعض البرلمانيين النّظر في الغرفة بابتسامات مكبوتة، أو بحواجب مقوّسة تعبيرًا عن دهشتهم، فقبل ذلك بأقل من ثلاثة أشهر، كان ريغان قد ألقى خطاب (حرب النجوم) داعيًا فيه العلماء إلى استحداث أسلحة ليزرية يمكنها – في حالة الحرب- أن تسقط الصواريخ النووية السوفييتية حينما تندفع نحو أمريكا، ولم تلقَ الفكرة أي قبول؛ إذ إنها بدت فكرة غريبة ومجنونة. الآن، ما الذي كان الرجل العجوز بصدده؟ بعد أن انتهى ريغان من عرضه لملخص الفيلم، توجه إلى الجنرال جون فيسي (John Vessey) رئيس الهيئة المشتركة لرؤساء الأركان، الضابط الأعلى في جيش الولايات المتحدة وسأله: هل يمكن حدوث مثل هذا الأمر في الواقع؟ هل يمكن لأحد اقتحام حواسيبنا المهمة شديدة الحساسية؟ قال فيسي – الذي نشأ متمرسًا على مثل هذه الاستفسارات- إنه سوف ينظر في الأمر. بعد ذلك بأسبوع عاد الجنرال بإجابته إلى البيت الأبيض، فقد اتضح أن فيلم ألعاب الحرب (المناورات الحربية) لم يكن قط مستبعدًا وغير معقول. قال فيسي: السيد الرئيس، المسألة أسوأ كثيرًا مما تظن. فجّر سؤال ريغان سلسلة من المذكرات، ومجموعات العمل، والدراسات، والاجتماعات، اشترك فيها الكثير من

الدوائر والمؤسسات المعنية. بعد مضي خمسة عشر شهرًا، أسفرت تلك الجهود عن صياغة التوجيه الرئاسي السري المتعلّق بالأمن القومي (إن إس دي دي – 145) (NSDD-145)، وكان بعنوان السياسة القومية بشأن الاتصالات وأمن نظم المعلومات المؤللة (National Policy in Telecommunications and Automated Information Systems Security)، وقع عليه ريغان في 17 ديسمبر من العام 1984. ..... وجهه ريغان إلى الجنرال فيسي، متبوعًا بوثيقة سياسات رائدة مبتكرة، وكانت المرة الأولى التي يتطرق فيها رئيس أمريكي، أو يصدر فيها توجيه من البيت الأبيض، لما سيصطلح على تسميته لاحقًا بِـ «وسائل الحرب السيبرانية». (كابلان/ عبد المجيد 2019/2016 ص ص11-13)

بحلول منتصف فترة رئاسة أوباما، كانت أكثر من عشرين دولة قد شكلت وحدات متخصصة في وسائل الحرب السيبرانية ضمن جيوشها، كان كل يوم يجلب معه تقارير بشأن هجمات سيبرانية جديدة ليس فقط ضد الشبكات الحاسوبية الخاصة بالبنتاغون أو بمقاولي ومتعهدي وزارة الدفاع، ولكن أيضًا ضد الشبكات الحاسوبية التي لدى البنوك، وتجار التجزئة، والمصانع، وشبكات الطاقة الكهربائية، والمنشآت المائية؛ أي كل الأشياء المتصلة بشبكة حاسوبية. وبحلول أوائل القرن الحادي والعشرين، شمل ذلك كل شيء تقريبًا، وعلى الرغم من قلة المعلن في هذا الخصوص، كانت الولايات المتحدة - وبضع قوى غربية أخرى- هي أيضًا تشن هجمات سيبرانية على الشبكات الحاسوبية الخاصة بدول أخرى. (كابلان/عبد المجيد 2016/2019)

وقع أوباما أمرًا تنفيذيًّا لتمكين الولايات المتحدة من فرض عقوبات على الأفراد أو الكيانات التي يشتبه في مشاركتها في أعمال ذات صلة بالإنترنت، وتم تقييم هذه الأفعال على أنها تهديدات محتملة للأمن القومي الأمريكي أو القضايا المالية أو قضايا السياسة الخارجية.[FACT SHEET, 2015] وقد اتهمت السلطات الأمريكية رجلًا بارتكاب 92 هجومًا إلكترونيًّا على أجهزة الكمبيوتر التي تستخدمها وزارة الدفاع. [Patrick, 2003]، كما قام اتحاد شركات مقره نبراسكا بإلقاء القبض على أربعة ملايين محاولة قرصنة خلال ثمانية أسابيع. [Kevin, 2016]، وفي عام 2011 زادت هجمات الإرهاب السيبراني بنسبة 20%. [Roland, 2013] وفي مايو 2021، أعلن الرئيس جو بايدن عن أمر تنفيذي يهدف إلى تحسين الأمن السيبراني في أمريكا، وجاء ذلك بعد زيادة هجمات الأمن السيبراني التي استهدفت القطاعين العام والخاص في البلاد، وتهدف الخطة إلى تحسين الدفاع السيبراني للحكومة من خلال زيادة قدرتها على تحديد الهجمات وردعها والحماية منها واكتشافها والرد عليها. وتحتوي الخطة على 10 أقسام مكتوبة في الوثيقة، تشمل - على سبيل المثال

لا الحصر- تحسين تبادل معلومات التهديد، وتحديث الأمن السيبراني للحكومة، وإنشاء مجلس مراجعة الأمن السيبراني (Executive Order on Improving the Nation's Cybersecurity, 2021)

ويشير مصطلح «الحرب السيبرانية» إلى الحرب التي تجري في الفضاء السيبراني من خلال الوسائل والأساليب السيبرانية، في حين أن كلمة «الحرب» مفهومة بشكل شائع على أنها تشير إلى سير الأعمال العدائية العسكرية في حالات النزاع المسلح، ويمكن وصف «الفضاء السيبراني» بأنه شبكة عالمية مترابطة من المعلومات الرقمية والبنية التحتية للاتصالات، بما في ذلك الإنترنت وشبكات الاتصالات، وأنظمة الكمبيوتر والمعلومات المقيمة فيها. وهكذا على سبيل المثال العدوى من شبكة كمبيوتر الخصم المحارب التي تحتوي على فيروس خبيث، فإنها تشكل عملاً من أعمال الحرب السيبرانية، في حين أن القصف الجوي لقيادة إلكترونية عسكرية لا يعد كذلك. (Melzer, 2011).

الأسلحة المستخدمة في الحرب السيبرانية:

تتضمن الحرب السيبرانية (Cyberwarfare) هجمات إلكترونية متعمدة من قبل دولة واحدة أو أكثر ضد أخرى، وأبعد من ذلك غالبًا ما يختلف خبراء الأمن والمسؤولون الحكوميون والقادة العسكريون حول أنواع الجرائم السيبرانية التي ينبغي أن تعد أعمال حرب سيبرانية (Parks, 2013).

كانت دولة إستونيا في منطقة البلطيق هدفًا لهجوم واسع النطاق لحجب الخدمة أدى في نهاية المطاف إلى جعل البلاد غير متصلة بالإنترنت، ومنعت من الخدمات المعتمدة على الاتصال بالإنترنت في أبريل 2007، وتشمل البنية التحتية لإستونيا كل شيء، بدءًا من الخدمات المصرفية عبر الإنترنت وشبكات الهاتف المحمول إلى تعطيل الخدمات الحكومية والوصول إلى معلومات الرعاية الصحية لبعض الوقت. وقد شهدت الدولة المعتمدة على التكنولوجيا اضطرابات شديدة، وكان هناك قدر كبير من القلق بشأن طبيعة الهجوم والقصد منه، كما جاء الهجوم السيبراني نتيجة الخلاف الإستوني الروسي حول إزالة تمثال برونزي يصور جنديًا سوفييتيًا من حقبة الحرب العالمية الثانية من وسط العاصمة تالين. [3] وفي خضم الصراع المسلح مع روسيا، تعرضت جورجيا على نحو مماثل لهجمات متواصلة ومنسقة على بنيتها التحتية السيبرانية في أغسطس/آب 2008. وفي كل من هاتين الحالتين، تشير الأدلة الظرفية إلى هجمات روسية منسقة، ولكن إسناد الهجمات أمر بالغ الصعوبة، وعلى الرغم من أن كلا البلدين يتهمان موسكو بالمساهمة في الهجمات السيبرانية،

إلا أنه لا يوجد دليل يثبت المسؤولية القانونية. وقد تم إيقاف الخدمات عبر الإنترنت للبنوك والخدمات الحكومية الإستونية بسبب المستوى العالي الذي لا يمكن السيطرة عليه من حركة المرور على الإنترنت، كما تعطلت وسائل الإعلام، وبالتالي لم تتمكن محطات البث من نقل أخبار الهجمات السيبرانية، وتعرضت بعض الخدمات للهجوم لمدة 22 يومًا، بينما تم إيقاف الخدمات الأخرى عبر الإنترنت بالكامل، واستمرت أعمال الشغب والنهب لمدة 48 ساعة في تالين- إستونيا، كان الهجوم السيبراني بمثابة دعوة للاستيقاظ لإستونيا والعالم بأسره بشأن أهمية الدفاع السيبراني.

مع استمرار تزايد الهجمات السيبرانية حول العالم، لا تزال الدول تنظر إلى الهجمات على إستونيا في عام 2007 كمثال على كيفية مكافحة الهجمات السيبرانية والإرهاب في المستقبل، ونتيجةً لهذه الهجمات، أصبحت إستونيا الآن واحدة من أفضل الدول في مجال الدفاع السيبراني والسلامة عبر الإنترنت، وتعد عاصمتها تالين موطنًا لمركز الدفاع السيبراني التابع لحلف شمال الأطلسي. وتواصل حكومة إستونيا تحديث بروتوكولات الدفاع السيبراني واستراتيجيات الأمن السيبراني الوطنية، كما يقوم مركز الدفاع السيبراني التعاوني التابع لحلف شمال الأطلسي في تالين بإجراء أبحاث وتدريبات حول الأمن السيبراني، ليس فقط لمساعدة إستونيا، ولكن أيضًا الدول الأخرى الأعضاء في الحلف (((Johnson and Post (1998) .

أهم أنواع هجمات الحرب السيبرانية (Types of Cyber Warfare Attacks):

1. **التخريب (Sabotage):**

يجب على المنظمات الحكومية تحديد المعلومات الحساسة والمخاطر إذا تم اختراقها. قد تقوم الحكومات المعادية أو الإرهابيون بسرقة المعلومات أو تدميرها أو الاستفادة من التهديدات الداخلية؛ مثل الموظفين غير الراضين أو المهملين أو الموظفين الحكوميين المنتمين إلى الدولة المهاجمة.

2. **هجمات رفض الخدمة (DoS):**

تمنع هجمات DoS المستخدمين الشرعيين من الوصول إلى موقع الويب عن طريق إغراقه بالطلبات المزيفة وإجبار موقع الويب على التعامل مع هذه الطلبات. يمكن استخدام هذا النوع من الهجمات لتعطيل العمليات والأنظمة الحيوية ومنع الوصول إلى المواقع الحساسة من قبل المدنيين أو الأفراد العسكريين والأمنيين أو هيئات البحث.

3. **شبكة الطاقة الكهربائية (Electrical Power Grid):**

تسمح مهاجمة شبكة الطاقة للمهاجمين بتعطيل الأنظمة الحيوية وتعطيل البنية التحتية، وربما تؤدي إلى أضرار جسدية. يمكن أن تؤدي الهجمات على شبكة الطاقة أيضًا إلى تعطيل الاتصالات وجعل الخدمات؛ مثل الرسائل النصية والاتصالات، غير قابلة للاستخدام.

4. **الهجمات الدعائية (Propaganda Attacks):**

محاولات السيطرة على عقول وأفكار الأشخاص الذين يعيشون في بلد مستهدف أو يقاتلون من أجله. يمكن استخدام الدعاية لكشف حقائق محرجة، أو نشر الأكاذيب لجعل الناس يفقدون الثقة في بلدهم، أو الوقوف إلى جانب أعدائهم.

5. **الاضطراب الاقتصادي (Economic Disruption):**

تعمل معظم الأنظمة الاقتصادية الحديثة باستخدام أجهزة الكمبيوتر. يمكن للمهاجمين استهداف شبكات الكمبيوتر الخاصة بالمؤسسات الاقتصادية؛ مثل أسواق الأوراق المالية، وأنظمة الدفع، والبنوك لسرقة الأموال أو منع الأشخاص من الوصول إلى الأموال التي يحتاجون إليها.

6. **الهجمات المفاجئة (Surprise Attacks):**

وهذه هي المعادل السيبراني لهجمات مثل بيرل هاربور و11 سبتمبر. الهدف هو تنفيذ هجوم واسع النطاق لا يتوقعه العدو، مما يمكن المهاجم من إضعاف دفاعاته. ويمكن القيام بذلك لتمهيد الطريق لهجوم جسدي في سياق الحرب الهجين (hybrid warfare).

أمثلة على عمليات الحرب السيبرانية (Examples of Cyber Warfare Operations):

1. **فيروس ستكسنت (Stuxnet Virus):**

كان فيروس ستكسنت هو الدودة التي هاجمت البرنامج النووي الإيراني. إنها واحدة من أكثر الهجمات السيبرانية تعقيدًا في التاريخ. انتشرت البرامج الضارة عبر أجهزة Universal Serial Bus المصابة وأنظمة الحصول على البيانات المستهدفة والتحكم الإشرافي.

2. **سوني بيكتشرز هاك (Sony Pictures Hack):**

وجاء الهجوم على شركة سوني (Sony Pictures) عقب صدور فيلم «المقابلة» الذي قدم صورة سلبية لكيم جونغ أون. وينسب الهجوم إلى قراصنة الحكومة الكورية الشمالية، وقد وجد مكتب التحقيقات الفيدرالي أوجه تشابه مع هجمات البرامج الضارة السابقة التي شنها الكوريون الشماليون، بما في ذلك التعليمات البرمجية وخوارزميات التشفير وآليات حذف البيانات.

3. **الجندي البرونزي (Bronze Soldier):**

في عام 2007 نقلت إستونيا تمثالًا مرتبطًا بالاتحاد السوفيتي، وهو الجندي البرونزي، من وسط عاصمتها تالين إلى مقبرة عسكرية بالقرب من المدينة. عانت إستونيا من عدد من الهجمات السيبرانية الكبيرة في الأشهر التالية، وكانت مواقع الحكومة الإستونية ووسائل الإعلام والبنوك مثقلة بهجمات حجب الخدمة (DoS) الضخمة، وبالتالي تم قطع اتصالها بالإنترنت.

4. **الدب الباهظ (Fancy Bear):**

تدعي Crowd Strike أن مجموعة الجرائم السيبرانية الروسية المنظمة Fancy Bear استهدفت قوات الصواريخ والمدفعية الأوكرانية بين عامي 2014 و2016. وقد انتشرت البرامج الضارة عبر تطبيق Android مصاب تستخدمه وحدة المدفعية D–30 Howitzer لإدارة بيانات الاستهداف.

التقنيات الناشئة والإرهاب السيبراني (msirorretrebyC & seigolonhcet gnigremE):

هناك اهتمام كبير ومتزايد بظهور تقنيات ناشئة جديدة على وجه الخصوص من منظور صنع السياسات. ومع ذلك، تفتقر التقنيات الناشئة العناصر التأسيسية الرئيسية؛ أي الإجماع على ما يصنف على أنها تكنولوجيا "ناشئة» (emerging). وقد طور روتولو وزملاؤه (Rotolo and Hicks, & Martin) تعريفًا من خلال الجمع بين الفهم الأساسي للمصطلح على وجه الخصوص مفهوم «النشوء» يحدد التعريف خمس سمات تظهر في التقنيات الجديدة، هي: (1) الحداثة الجذرية (radical novelty)، (2) النمو السريع نسبيًا (relatively fast growth)، (3) التماسك (coherence)، (4) التأثير البارز (prominent impact,)، (5) عدم اليقين والغموض (uncertainty and ambiguity). (Rotolo and Hicks, & Martin, 2015, p. 1).

ونستعرض فيما يلي أهم التقنيات الناشئة وإمكانية توظيفها في الإرهاب السيبراني، وما ينجم عنها من تحديات للأمن الوطني والسيادة الوطنية.

الذكاء الاصطناعي والإرهاب السيبراني (msirorretrebyC & IA) :

الذكاء هو القدرة على اكتساب المعرفة وتطبيقها لتحقيق نتيجة. إن الحصول على آلة تعمل بهذه الطريقة هو المقصود عمومًا بالذكاء الاصطناعي (Burns, 2022)؛ حيث يتيح الذكاء الاصطناعي (AI) للآلات إمكانية التعلم من التجربة والتكيف مع المدخلات الجديدة وأداء

مهام شبيهة بالبشر، وتعتمد معظم أمثلة الذكاء الاصطناعي اليوم – من أجهزة الكمبيوتر التي تلعب الشطرنج إلى السيارات ذاتية القيادة– بشكل كبير على التعلم العميق ومعالجة اللغة الطبيعية (Goodnight, 2022).

الذكاء الاصطناعي هو محاكاة عمليات الذكاء البشري بواسطة الآلات، وخاصة أنظمة الكمبيوتر، وتشمل التطبيقات المحددة للذكاء الاصطناعي الأنظمة الخبيرة، ومعالجة اللغة الطبيعية، والتعرف على الكلام، ورؤية الآلة. ويفهم «الذكاء الاصطناعي» على أنه يصف مجالًا يهتم بتطوير الأدوات التكنولوجية التي تمارس الصفات الإنسانية، كما يهتم الذكاء الاصطناعي بتطوير أنظمة الكمبيوتر التي تحاكي التفكير البشري، وعندما تكون كذلك فإنها تطبق في مجال المعرفة العقلانية. وقد تطور هذا الأمر وأدى إلى وجود صلة بين علوم الكمبيوتر والعلوم الفيزيائية، وخاصة السيبرانية، مما جعل من الممكن إدخال السلوكيات العقلانية في الأنظمة الفيزيائية التي أصبح سلوكها مستقلًا، هذه هي الطريقة التي تطورت بها الروبوتات وواصلت التقدم. يعد الإنسان نفسه على أنه منشئ ومشرف ومستخدم بارز في صنع القرار في الأنظمة. (Cardon, 2018).

للذكاء الاصطناعي (AI) تأثير عميق على مجتمعنا؛ في الرعاية الصحية والزراعة والصناعة والخدمات المالية والتعليم، ولكن كما قال الأمين العام للأمم المتحدة أنطونيو وذكر غوتيريس في استراتيجيته لعام 2018 بشأن التكنولوجيات الجديدة، إنه: «على الرغم من أن هذه التكنولوجيات تحمل وعودًا كبيرة، إلا أنها ليست خالية من المخاطر، وبعضها يثير القلق وحتى الخوف، فيمكن استخدامها لأغراض ضارة كما لها نتائج سلبية غير مقصودة العواقب». ربما يجسد الذكاء الاصطناعي هذه الازدواجية أكثر من أي تكنولوجيا ناشئة أخرى اليوم، في حين أنها يمكن أن تجلب إدخال تحسينات على العديد من القطاعات، كما أن لديها القدرة على عرقلة التمتع بحقوق الإنسان الأساسية والحريات، وخاصة الحق في الخصوصية، وحرية الفكر والتعبير، وعدم التمييز. إن أي استكشاف لاستخدام التقنيات التي تدعم الذكاء الاصطناعي يجب أن يسير دائمًا جنبًا إلى جنب مع الجهود المبذولة لمنع انتهاك حقوق الإنسان. وفي هذا السياق، أنشأت العديد من المنظمات الدولية والإقليمية والسلطات الوطنية ومنظمات المجتمع المدني العاملة، مبادرات تهدف إلى وضع مبادئ توجيهية أخلاقية فيما يتعلق باستخدام الذكاء الاصطناعي، فضلًا عن ظهور الأطر القانونية الأولية. (UNICRI & UNCCT, 2021).

وتتجلى هذه الازدواجية بشكل واضح على شبكة الإنترنت؛ حيث يشكل النشاط الإرهابي السيبراني المتزايد تحديًا متزايدًا، وقد أشار فيسبوك إلى أنه قام على مدار عامين بإزالة أكثر من 26 مليون قطعة من المحتوى؛ من مجموعات مثل الدولة الإسلامية في العراق والشام (داعش)، وتنظيم القاعدة. وقد أثبتت وسائل التواصل الاجتماعي أنها أدوات قوية في أيدي هذه المجموعات؛ حيث تمكنها من التواصل ونشر الرسائل بين أفرادها، وجمع الأموال، وتجنيد المؤيدين، وإلهام وتنسيق الهجمات، واستهداف الأشخاص الضعفاء. وفي استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب (A/RES/60/288)، قررت الدول الأعضاء العمل مع الأمم المتحدة، مع إيلاء الاعتبار الواجب للسرية واحترام حقوق الإنسان، والامتثال للالتزامات الأخرى بموجب القانون الدولي؛ لاستكشاف سبل تنسيق الجهود على المستويين الدولي والإقليمي لمكافحة الإرهاب السيبراني على شبكة الإنترنت، واستخدام الإنترنت كأداة لمواجهة انتشار إرهاب. وفي الوقت نفسه، تعترف الاستراتيجية بأن الدول الأعضاء قد تحتاج إلى المساعدة للوفاء بهذه الالتزامات، وتسعى لاستكشاف كيفية استخدام الذكاء الاصطناعي لمكافحة التهديد بالإرهاب على الإنترنت. (UNICRI & UNCCT, 2021).

لقد جاء في تقرير مواجهة الإرهاب على الشبكة بالذكاء الاصطناعي: مراجعة عامة لوكالات إنفاذ القانون في جنوب آسيا وجنوب شرق آسيا، and Countering Terrorism On-line With Artificial Intelligence: An Overview For Law Enforcement Counter-Terror-ism Agencies In South Asia And South-East Asia(2021)، أنه يمكن توظيف تطبيقات الخرائط في الذكاء الاصطناعي في سياق مكافحة الاستخدام الإرهابي للإنترنت ووسائل التواصل الاجتماعي، مع التركيز على ستة مجالات تم تحديدها لحالات الاستخدام، وهي: 1) التحليلات التنبئية للأنشطة الإرهابية، 2) تحديد المناطق الساخنة للتطرف، 3) الكشف عن المعلومات الخاطئة والمضللة التي ينشرها الإرهابيون لأغراض استراتيجية، 4) الإشراف الآلي على المحتوى وإزالته، ومكافحة الخطاب الإرهابي والمتطرف العنيف، 5) إدارة متطلبات تحليل البيانات الثقيلة. ويجب أن تكون وكالات إنفاذ القانون ومكافحة الإرهاب مستعدة للتصدي لها في استكشافهم للتكنولوجيا، ولا سيما التحديات السياسية والقانونية المحددة، بالإضافة إلى القضايا التقنية. كما جاء في التقرير أنه ينبغي لوكالات إنفاذ القانون ومكافحة الإرهاب أن تعترف بما يلي:

- الـذكاء الاصطناعـي ليـس مثاليًـا، وقـد لا يكـون كذلـك أبـدًا. لا تـزال هنـاك العديـد مـن التحديـات التقنيـة، بينمـا الـذكاء الاصطناعـي أصبـح أكثـر فعاليـة ودقـة، وقـد يسـتغرق الوصـول إليـه قـدرًا كبيـرًا مـن الوقـت علـى المسـتويات المطلوبـة مـن قبـل كل مـن المسـتخدمين النهائيـين والمجتمـع المدنـي، إذا كان مـن الممكـن تحقيـق ذلـك علـى الإطـلاق.

- لا يوجـد حـل «مقـاس واحـد يناسـب الجميـع». يجـب أن تكـون أدوات الـذكاء الاصطناعـي مصممـة خصيصًـا لسـياقات ومتطلبـات محـددة.

- قدم الذكاء الاصطناعي النتائج كحسابات احتمالية وليست تنبؤات معصومة من الخطأ.

- لا يسـتطيع الـذكاء الاصطناعـي القضـاء علـى الإرهـاب والتطـرف العنيـف علـى الإنترنـت مـن جانـب واحـد. الاسـتثمارات في الـذكاء الاصطناعـي ينبغـي أن تكـون محاطـة بالجهـود الراميـة إلـى منـع التطـرف والتطـرف العنيـف مـن جذوره.

وجاء في مجال احترام حقوق الإنسان وحماية المجتمع المدني ما يلي:

- ينبغـي الاعتـراف بالتأثيـر المحتمـل علـى حقـوق الإنسـان لاسـتخدام الـذكاء الاصطناعـي لمكافحـة الإرهـاب عبـر الإنترنـت.

- ينبغـي وضـع قوانـين وسياسـات وطنيـة تحـدد وتنظـم اسـتخدام أدوات الـذكاء الاصطناعـي في مكافحـة الإرهـاب عبـر الإنترنـت (UNICRI & UNCCT, 2021).

ذكاء التهديد السيبراني والإرهاب السيبراني (Cyber Threat Intelligence & Cyberterrorism):

معلومـات التهديـد، أو ذكاء التهديـد السـيبراني (Cyber Threat Intelligence)، هـي معلومـات تسـتخدمها المنظمـة لفهـم التهديـدات التـي تسـتهدفها أو ستسـتهدفها حاليًـا. تسـتخدم هـذه المعلومـات لإعـداد ومنـع وتحديـد التهديـدات السـيبرانية التـي تتطلـع إلـى الاسـتفادة مـن المـوارد القيمـة، وتعـد معلومـات التهديـد السـيبراني (CTI) السـياق الكامـل للتهديـد السـيبراني للإبـلاغ عـن تصميـم الإجـراءات الدفاعيـة عاليـة الاسـتهداف. وتجمـع عوامـل التهديـد السـيبراني المتعـددة، بمـا في ذلـك دوافـع مجرمـي الإنترنـت ومؤشـرات التسـوية، لمسـاعدة فـرق الأمـن علـى فهـم تحديـات التهديـد السـيبراني المتوقـع والاسـتعداد لهـا. (ULIslam, 2022)؛ مـن خـلال منـح فـرق الأمـن وعيًـا متقدمًـا بالتهديـدات السـيبرانية الوشـيكة، كمـا يمكـن لـذكاء التهديـد

السيبراني اتباع نهج استباقي للأمن السيبراني، وهو أكثر أنواع الدفاع السيبراني فعالية، فذكاء التهديدات السيبرانية يعد أمرًا بالغ الأهمية؛ لأنه أحد أفضل الطرق للدفاع ضد التهديدات المستمرة المتقدمة (Advanced Persistent Threats (APTs)، والتهديد المستمر المتقدم عبارة عن حملة هجوم سيبراني طويلة المدى؛ حيث يختبئ المجرمون السيبرانيون داخل شبكة تم اختراقها لمراقبة البيانات الحساسة وسرقتها باستمرار، وتعد البرامج الضارة أكثر تعقيدًا من سلالات البرامج الضارة الأخرى؛ مثل برامج الفدية الضارة، وعلى عكس حملات التصيد الاحتيالي أيضًا، فإن الهجمات ليست آلية في الأساس، بل تتم إدارتها من قبل مجموعات مجرمي الإنترنت المنظمة والمتطورة.

وللتعامل مع هذه التهديدات السيبرانية وحل المشكلات ووضع استراتيجيات الدفاع، عليك أن تكون متقدمًا عليها بخطوة؛ إذ يمكن لمتخصصي الأمن:

- اتخاذ قرارات مستنيرة للاستجابة للحوادث.
- فهم عملية اتخاذ القرار الذي يقوم به الهاكر.
- إثبات فعالية العمليات الأمنية لرؤساء أمن المعلومات وأصحاب المصلحة وصناع القرار من خلال تقارير الذكاء.
- فهم التكتيكات والتقنيات والإجراءات ((tactics, techniques, and procedures (TTPs للهجمات السيبرانية الوشيكة (ULIslam, 2022).

إنترنت الأشياء والإرهاب السيبراني Internet of Things (IoT) & Cyberterrorism)) :

يتيح إنترنت الأشياء تواصل الأجهزة المرتبطة عبر الإنترنت، وإرسال الأوامر والمهام دون تدخل بشري، ويحدث ذلك بشكل تلقائي إذا تواجدت تلك الأجهزة في نطاق جغرافي تغطيه شبكة الإنترنت، يمكن – مثلًا– التحكم في تدفئة مبنى سكني أو الإضاءة بالتشغيل والإغلاق من خلال تلك التقنية، وكذلك إذا استخدمت في مصنع يمكن تشغيل الآلات ومتابعتها، وإمكانية الإبلاغ المسبق عن وجود خلل. بإمكان تلك التقنية الناشئة أن تصبح جزءًا من حياتنا اليومية وجعلها أكثر كفاءة، عبر الأجهزة القابلة للارتداء، وإطلاق صافرات الإنذار عند استشعار دخان أو حريق، وترتيب الأجندة اليومية لمواعيد المسؤولين تلقائيًا، وإرشادنا إلى أماكن مواقف السيارات، ومتابعة الظروف الطبيعية لمنطقة ما من تربة وطقس. ومن المتوقع أن تصبح مجالات معينة هي الأقرب لدمجها مع تقنية إنترنت الأشياء؛ مثل الاتصالات

وتوجيه الأجهزة الذكية المختلفة من حواسب شخصية وهواتف ذكية، والرعاية الصحية، عبر مراقبة المرضى وتسجيل حالاتهم إلكترونيًا، والإبلاغ عن الحالة الصحية للمريض قبل وقوع خطر. وكذلك بيع التجزئة؛ حيث يوفر للتجار معلومات عن المخزون لديهم، وعمليات البيع والشراء، بينما يزود المستهلكين بما يمكن أن يثير اهتمامهم في المتاجر من منتجات. ويمكن أيضًا الاستفادة من تطبيق إنترنت الأشياء في القطاع الصناعي؛ لمراقبة الجودة والمخزون والآلات، وتوفير التكاليف المنفقة على المخاطر، ومساعدة المسؤولين على اتخاذ القرار وفقًا للمعلومات المتوفرة لديهم، ورفع الإنتاجية. إنترنت الأشياء (IoT) هو شبكة من المعدات (الأشياء) المادية التي تحتوي على تقنية مدمجة للتواصل والاستشعار أو التفاعل مع حالاتها الداخلية أو البيئة الخارجية. ومن أمثلة أجهزة إنترنت الأشياء في السوق: الهواتف الذكية، والثلاجات الذكية، والساعات الذكية، وأجهزة إنذار الحريق الذكية، وأقفال الأبواب الذكية، والدراجات الذكية، وأجهزة الاستشعار الطبية، وأجهزة تتبع اللياقة البدنية، ونظام الأمان الذكي، وما إلى ذلك، هي أمثلة قليلة على منتجات إنترنت الأشياء (Software Testing Help, 2023).

هناك خمس ميزات مركزية لإنترنت الأشياء، والتي تمكن الإرهاب السيبراني، هذه الميزات هي أن إنترنت الأشياء غير آمن جذريًا، وأن مكونات إنترنت الأشياء موجودة في العالم، وأن مشاركة الأعداد الهائلة من أجهزة إنترنت الأشياء يعني أن الهجمات المحتملة مكثفة، ومن المرجح أن يتم تشغيل إنترنت الأشياء من خلال مجموعة من جوانب الذكاء الاصطناعي، مما يجعلها غامضة، وأن إنترنت الأشياء غير مرئي إلى حد كبير. ومن خلال الجمع بين هذه العوامل الخمسة معًا، يبرز إنترنت الأشياء كتهديد ناقل للإرهاب السيبراني.

إن إنترنت الأشياء هو شيء موجود في العالم وبالتالي يمكنه تمكين التأثيرات المادية الناجمة عن الهجمات السيبرانية. أنه مع نمو إنترنت الأشياء في نطاقه وتغلغله في مجتمعنا العوالم المادية والسلوكيات، فهذا يعني أن الإرهاب السيبراني ليس مسألة ما إذا كان، لكن متى (Henschke, 2021).

إنترنت كل شيء والإرهاب السيبراني (Internet of everything & Cyberterrorism):

إنترنت كل شيء (IoE) هو مفهوم يوسع من تركيز إنترنت الأشياء (IoT) على الاتصالات من آلة إلى آلة (M2M)؛ لوصف نظام أكثر تعقيدًا يشمل أيضًا الأشخاص وعمليات إنترنت كل شيء (IoE). نشأ مفهوم إنترنت كل شيء في شركة Cisco، التي تعرف إنترنت كل شيء على أنه: «الاتصال الذكي بين الأشخاص والمعالجة والبيانات والأشياء». نظرًا لأنه في إنترنت الأشياء، تتم جميع الاتصالات بين الأجهزة، ويتضمن مفهوم إنترنت كل شيء أي نوع من

الكائنات أو الكيانات المادية أو الافتراضية التي يمكن جعلها قابلة للتوجيه وإعطاء القدرة على نقل البيانات دون تدخل من إنسان إلى آلة، تلك هي الأشياء الموجودة في إنترنت كل شيء أيضًا تشتمل على الاتصالات والتفاعلات التي ينشئها المستخدم والمرتبطة بكل الأجهزة المتصلة بالشبكة على مستوى العالم. (TechTarget Contributor, 2015).

ومن هنا فإنَّ الأشياء الموجودة في إنترنت الأشياء غالبًا ما تكون عناصر لم يكن من الممكن ربطها بالشبكة في الماضي، لذلك تعد أتمتة اتصالات الأشياء أيضًا أمرًا أساسيًّا لمفهوم إنترنت الأشياء. (TechTarget Contributor, 2015)

وتكمن الخطورة في توظيف الإرهاب السيبراني – وخاصة الذئب المنفرد السيبراني– لهذه التقنيات في تنفيذ هجمات سيبرانية كارثية تلحق الأذى والدمار السيبراني والمادي بقطاعات حيوية كثيرة وبمستهدفين كثر. وقد تأخذ هذه الهجمات شكل حرب سيبرانية عابرة للحدود ومتعددة المستهدفين والدول والجماعات، ويصعب كشفها في الوقت المناسب.

الطائرات دون طيار والإرهاب السيبراني (Drones & Cyberterrorism):

ارتبط مصطلح طائرات بدون طيار «الدرون» بالاستخدامات العسكرية والتجسس، لكن بالإمكان استخدام تلك التقنية أيضًا في القطاع المدني؛ لمراقبة خطوط أنابيب الغاز والبترول، وإطفاء الحرائق الصعبة في حالات الكوارث الطبيعية، وكذلك بالإمكان استخدامها في مجال الأرصاد، ودراسة أحوال الطقس، في قادرة على التحليق لفترات طويلة وبارتفاع يصل إلى 15 ألف متر، دون أن تكون مرئية أو مسموعة. وفرضت تلك التقنية نفسها بسرعة لانخفاض تكلفتها مقارنة بالطائرات العادية، فهي ليست بحاجة لمقصورة أو معدات، ويمكن التحكم فيها دون تعريض العنصر البشري للخطر، كما يمكن شراؤها عبر الإنترنت. وفي 2006، بدأ استخدام الطائرات دون طيار في مجالات الإغاثة من الكوارث، ومراقبة الحدود، وإطفاء حرائق الغابات ورش المبيدات، وتطورت استخداماتها بمرور الوقت، حتى أصبحت تستخدم في السينما ومجالات التصوير الفوتوغرافي في حفلات الزفاف (رؤيا، 2019) (البداينة، قيد النشر).

وتستخدم هذه المعدات في تهريب المخدرات؛ حيث تم إسقاط عدد منها على الحدود الأردنية السورية، لأن عصابات تهريب المخدرات تستخدم هذه الطائرات في تهريب المخدرات ومخاطر نشر المخدرات في المنطقة، وخاصة الخليج العربي. كما يمكن استخدامها في الإرهاب التقليدي والسيبراني في التدمير للبنى التحتية الحساسة، أو زرع معدات التجسس أو أي نوع من التخريب السيبراني أو المادي، بما في ذلك الاغتيالات.

إنترنت الأجسام (Internet of bodies (IoB)& Cyberterrorism):

تمت صياغة مصطلح إنترنت الأجسام (IoB) في عام 2016، وهو يصف الأجهزة المتصلة التي تراقب جسم الإنسان، وتجمع البيانات الفسيولوجية، أو القياسات الحيوية، أو السلوكية، وتتبادل المعلومات عبر شبكة لاسلكية أو مختلطة، ويمكن أيضًا اعتبار تطبيقات الأجهزة المحمولة المستقلة من إنترنت الأشياء، والتي تحلل النشاط البدني والبيانات المتعلقة بالصحة؛ مثل ضربات القلب وضغط الدم ودورات النوم. ويندرج إنترنت الأجسام تحت مظلة حلول إنترنت الأشياء الأوسع، ولكن كما يوحي الاسم، تضمن أجهزة إنترنت الأجسام تآزرًا أوثق بين البشر والأدوات أكثر من منظمات الحرارة والثلاجات والستائر المتصلة، وتأتي منتجات إنترنت الأجسام في أشكال مختلفة؛ حيث تتراوح في التعقيد من الساعات الذكية وأجهزة تتبع اللياقة البدنية، التي يستخدمها ما يقرب من 21٪ من الأمريكيين، إلى أنظمة توصيل الأنسولين القابلة للزرع، وأجهزة الاستشعار القابلة للابتلاع، وأدوات تحفيز الدماغ، كما تشمل فوائد تنفيذ حلول إنترنت الأجسام على نطاق واسع التشخيص والعلاج الأفضل للحالات الصحية، وخطط التأمين الشخصية، وزيادة الإنتاجية، وتحسين السلامة العامة – على سبيل المثال لا الحصر–، لكن التبني المتزايد لإنترنت الأجسام يمكن أن يؤدي أيضًا إلى الوصول غير المصرح به إلى المعلومات الحساسة من قبل أطراف ثالثة، والتفاوتات الصحية القائمة على الدخل، وإقامة دولة مراقبة عالمية. (Klubnikin, 2022). يقال إن ديك تشيني نائب الرئيس الأميركي السابق قد ألغى المراقبة الإلكترونية لبطارية تنظيم ضربات القلب؛ خوفًا من هجمات سيبرانية تستهدف حياته، وكذلك انتشرت أخبار أن جيش الاحتلال الإسرائيلي يزرع شرائح تتبع لدى جنوده؛ لتتبع أمكنة وجودهم في حالة الأسر، وإنَّ هذه الشرائح تستخدم في مجالات بدائل عن البطاقات الائتمانية والذكية وفي المؤسسات الحساسة بدلًا من البطاقات التقليدية، وهنا يأتي دور التدخل السيبراني في نسخها أو تعطيلها وإلحاق الأذى بالمستخدمين والمؤسسات.

الإرهاب السيبراني والتقنيات الناشئة: تحديات الأمن الوطني السيبراني والسيادة الوطنية:

يعمل الأمن السيبراني على منع التهديدات التي تتعرض لها أنظمة الأمن القومي والقضاء عليها، مع التركيز على القاعدة الصناعية الدفاعية، وتحسين أمن الأسلحة السيبرانية، كما أنها تسعى جاهدة لتعزيز التعليم والبحث في مجال الأمن السيبراني وبناء الحياة المهنية. وفي قطر تم إنشاء الوكالة الوطنية للأمن السيبراني بموجب القرار الأميري رقم 1 لسنة 2021 الصادر بتاريخ 25 مارس 2021، وترتبط الوكالة مباشرة بمجلس الوزراء؛ ليدمج جهود الجهات الحكومية الفاعلة في مجال المحافظة على الأمن السيبراني في الدولة تحت

مظلة واحدة، ويعزز إمكاناتها لحماية الدولة ودعم صمودها في مواجهة تهديدات الفضاء السيبراني؛ من خلال دعم وتمكين مبادرات الأمن السيبراني، وتكثيف التعاون مع كيانات القطاعين الحكومي والخاص بالدولة؛ بهدف التصدي لجميع التهديدات السيبرانية المحتملة التي قد تؤثر على البنية التحتية المعلوماتية، والتي باتت تشكل الشريان الحيوي لاقتصاد الدولة، ومن مهامها إعداد الاستراتيجية الوطنية للأمن السيبراني وتحديثها بالتنسيق مع الجهات المعنية، والإشراف على تنفيذها بعد اعتمادها من مجلس الوزراء، ووضع وتحديث السياسات وآليات الحوكمة والمعايير والضوابط والإرشادات اللازمة لتعزيز الأمن السيبراني بالتنسيق مع الجهات المعنية، وتعميمها على الجهات ذات العلاقة ومتابعة الالتزام بها، ووضع وتحديث أطر إدارة المخاطر السيبرانية، ومتابعة الالتزام بها (الوكالة الوطنية للأمن السيبراني، 2023).

صرح الرئيس باراك أوباما (Obama) أن الأمن السيبراني هو أحد أهم التحديات التي تواجه الولايات المتحدة، وقد أشار إلى المفارقة المتمثلة في أن التقنيات نفسها التي تستخدمها الولايات المتحدة والتي تمكن من تحقيق إنجازات عظيمة يمكن أيضًا أن تستخدم لزعزعة أمنها وإلحاق الأذى بمواطنيها، وعلى سبيل المثال: فإنَّ تقنيات المعلومات وأنظمة الدفاع نفسها التي تجعل الجيش الأمريكي متقدمًا جدًّا، يتم استهدافها، مما قد يؤدي إلى زيادة نقاط الضعف، وبالتالي تعد الهجمات السيبرانية المستمرة تهديدًا للأمن القومي الأمريكي (Klein, 2015).

يتطور الأمن السيبراني باعتباره تقنية ناشئة مهمة، ولا يزال التهديد من المتسللين الذين يحاولون الوصول إلى البيانات بشكل غير قانوني يمثل تحديًا للإجراءات الأمنية، كما يتم استخدام التكنولوجيا الناشئة لتعزيز الأمن. وسيظل الأمن السيبراني تقنية رائجة للدفاع ضد التهديدات السيبرانية، ويمنع أمان الشبكة الوصول غير المرغوب فيه إلى شبكة الكمبيوتر وإساءة استخدامها. إنها تساعد في المهاجمة للهجمات والدفاع عنها، فضلًا عن الأخطار الداخلية، ويمكن أن تمنع جدران الحماية والشبكات الافتراضية الخاصة بعض الهجمات السيبرانية، كما يمكن أن تكون ناجحة للغاية؛ مثال: توفر إمكانية تلقي البيانات من الأجهزة الذكية (مثل Apple Watch وFitbit وما إلى ذلك) للمهنيين الطبيين القدرة على التنبؤ بالمشكلات الصحية المحتملة وعلاجها قبل ظهور أي أعراض على المريض. (Gadgil, 2022)

السيادة القومية السيبرانية والإرهاب السيبراني (Cyber National Sovereignty & Cyberterrorism):

تعد الهجمات السيبرانية على السيادة الوطنية انتهاكًا لها، وخاصة إذا اتصلت بمعدات في الفضاء المادي للدولة، فالسيادة (Sovereignty)عنصر أساسي في القانون الدولي والعلاقات الدولية، ومن البديهي أن ينطبق مبدأ السيادة في الفضاء السيبراني، تمامًا كما هو الحال في أي مكان آخر. إنه ينشط عددًا من الالتزامات لجميع الدول، السيادة تعني الاستقلال في العلاقات بين الدول، وتمنح كل دولة الحق الحصري في ممارسة وظائفها داخل أراضيها، فعند تقييم الانتهاك المحتمل للسيادة الإقليمية لدولة ما، يجب تقييم نطاق أو حجم أو تأثير أو شدة الاضطراب الناجم، بما في ذلك تعطيل الأنشطة الاقتصادية والاجتماعية أو الخدمات الأساسية أو الوظائف الحكومية بطبيعتها أو النظام العام أو السلامة العامة؛ لتحديد ما إذا كان انتهاك السيادة الإقليمية للدولة المتضررة مكانًا محجوزًا. بشكل عام، تقييم تأثير أو شدة التأثيرات السيبرانية بالطريقة نفسها ووفقًا لمعايير الأنشطة المادية نفسها، والأنشطة السيبرانية التي تتعدى مستوى من الآثار الضئيلة، وتتسبب في آثار ضارة كبيرة داخل إقليم دولة أخرى دون موافقة تلك الدولة، يمكن أن ترقى إلى حد انتهاك قاعدة السيادة الإقليمية فيما يتعلق بالدولة المتضررة. من المهم أيضًا ملاحظة أن الأنشطة السيبرانية التي لها آثار في دولة أخرى لا تشكل وجودًا ماديًا في أراضي تلك الدولة. على هذا النحو، لا تنتهك السيادة الإقليمية لمجرد ممارسة الأنشطة البعيدة في أو من خلال البنية التحتية السيبرانية الموجودة داخل أراضي دولة أخرى. (von Heinegg, 2012)

قد تشكل الأنشطة السيبرانية التي تتسبب في فقدان الوظائف فيما يتعلق بالبنية التحتية السيبرانية الموجودة داخل أراضي الدولة المتأثرة أيضًا انتهاكًا للسيادة الإقليمية، إذا تسببت الخسارة الناتجة في الوظيفة في آثار ضارة كبيرة مماثلة لتلك التي تسببها الأضرار المادية للأشخاص أو الممتلكات. على سبيل المثال، سيحدث انتهاك للسيادة الإقليمية عندما يؤدي النشاط السيبراني إلى إحداث تأثير ضار كبير يستلزم إصلاح أو استبدال المكونات المادية للبنية التحتية السيبرانية في الدولة المتضررة. ويمكن أن يشكل فقدان وظائف المعدات المادية التي تعتمد على البنية التحتية المتأثرة من أجل العمل جزءًا من الانتهاك، ويشمل تقييم الآثار كلًا من العواقب المقصودة وغير المقصودة التي تصل إلى الحد الأدنى المطلوب لتحريك الانتهاك.

لا تتطلب قاعدة السيادة الإقليمية الموافقة على كل نشاط سيبراني له آثار، بما في ذلك فقدان بعض الوظائف، وفي دولة أخرى لن تشكل الأنشطة التي تسبب آثارًا ضئيلة انتهاكًا للسيادة الإقليمية، بغض النظر عما إذا كانت تتم في السياق السيبراني أو غير السيبراني،

كما لا تمنع الدول – بموجب قاعدة السيادة الإقليمية– من اتخاذ تدابير ذات آثار ضئيلة للدفاع ضد النشاط الضار للجهات الفاعلة السيبرانية الخبيثة أو لحماية مصالحها الأمنية الوطنية.

وينطبق مبدأ السيادة الإقليمية على الفضاء السيبراني، فهو يحمي البنية التحتية الموجودة داخل أراضي الدولة، ويحظر على الدول التدخل في البنية التحتية السيبرانية الموجودة في أراضي دولة أخرى، وهذا بالتأكيد صحيح إذا كان السلوك يمكن عزوه (يمكن عزوه إلى ماذا؟؟)، وإذا ألحق ضررًا (شديدًا) بسلامة أو وظائف البنية التحتية السيبرانية للدولة الأجنبية، إضافةً إلى ذلك فإن الدول ملزمة بعدم السماح باستخدام أراضيها عن علم في أعمال تنتهك السيادة الإقليمية لدولة أخرى، ومع ذلك فهناك صعوبة في معرفة إذا انطلقت الهجمات السيبرانية من البنية التحتية السيبرانية الحكومية لدولة المنشأ. وللدول الحق في ممارسة ولايتها القضائية الإقليمية (territorial jurisdiction) على الأنشطة السيبرانية داخل أراضيها، إلا أن خصائص الفضاء السيبراني وضرورة الحفاظ على وظائف الإنترنت تتطلب فرض قيود توافقية على ممارسة الحقوق الإقليمية القضائية (von Heinegg, 2012)

وفقًا لإعلان جون بارلو (John Barlow) إعلان استقلال الفضاء السيبراني (A Declaration of the Independence of Cyberspace): "فالمفاهيم القانونية لا تنطبق على الفضاء السيبراني" (Barlow, 1996). يرتكز النظر إلى الفضاء السيبراني باعتباره مجالًا غير قانوني على عدد من الافتراضات؛ الافتراض الأول هو أن الفضاء السيبراني يختلف عن الفضاء الواقعي، فهو فضاء بلا حدود والشخصية الموجودة في كل مكان تتميز عن المساحات المادية والمحدودة التي تخضع للتنظيم القانوني. والافتراض الثاني هو أن الفضاء السيبراني مطابق لأصله ويجب أن يظل التصور والتصميم وإشراك العديد من أصحاب المصلحة، ويجب أن يبقى أمرًا أساسيًا ومساحة مفتوحة ولامركزية وتشاركية لا يعيقها التنظيم القانوني، أو على الأقل لا تخضع حصرًا للتنظيم الذي تقوده الدولة. (Tsagourias, 2021) في تقريرين متتاليين، أكد فريق الخبراء الحكوميين التابع للأمم المتحدة المعني بالأمن السيبراني ('UN GGE')(Gov-ernmental Experts on Cyber Security أن السيادة والمعايير الدولية التي تنبع من السيادة تنطبق على الأنشطة السيبرانية. وبالمثل، اتفق خبراء دليل تالين 2.0 بالإجماع على أن القانون الدولي الحالي ينطبق على العمليات السيبرانية، وقد تبين أن جوهر حجة ريد (Rid) صحيح في العالم: «إن معظم الهجمات السيبرانية ليست عنيفة ولا يمكن فهمها بشكل معقول على أنها شكل من أشكال أعمال العنف (Rid, 2013)، يحمل «دليل تالين» (Tallinn Manual) الأصلي وجهة النظر هذه، والتي تجسده القاعدة 11: (تشكل العملية السيبرانية استخدامًا

للقوة من حيث حجمها وآثارها إذا كان يمكن مقارنتها بالعمليات غير السيبرانية التي تصل إلى مستوى استخدام القوة) (Schmitt, 2013)".

إن الهجمات السيبرانية ببساطة لم يكن لها التأثيرات المادية التي يمكن اعتبارها حربًا أو إرهابًا، وتماشيًا مع التعريف أعلاه، فإن الإرهاب السيبراني شيء مثل استخدام أو استغلال الإنترنت لإحداث فعل جسدي العنف الموجه ضد غير المقاتلين أو الأبرياء؛ لتحقيق بعض الأهداف الثانوية الأيديولوجية أو الدينية أو السياسية. والأهم من ذلك، يجب أن تكون هذه الأفعال بارزة، إنهم بحاجة إلى تغطية واسعة أو دعاية لاعتبارها ناجحة في نهاية المطاف. (Rid, 2013)

الحياد السيبراني والحرب السيبرانية (Neutrals, Cyber Neutrality & Cyberwarfare):

وردت المسؤولية الأساسية للمحايدين (responsibility of neutrals) في المادة 5 (1) لاهاي الخامس، وتطبق كذلك في الصراع السيبراني، لذلك يجب على الدولة المحايدة ألا تسمح عمدًا بحدوث أعمال حرب سيبرانية (cyber warfare) يتم إطلاقها من البنية التحتية السيبرانية الموجودة في أراضيها أو تحت سيطرتها الحصرية. هذا الحظر لا ينطبق فقط على الحالات التي يكون فيها لدى أجهزة الدولة معرفة فعلية بعمل عدائي من أعمال الحرب السيبرانية، ولكن أيضًا في حالات المعرفة الظنية؛ على سبيل المثال: إذا كانت الدولة المحايدة ليست لديها بنية تحتية سيبرانية متطورة خاصة بها، ولذلك تم التعاقد مع مزود تجاري، يفترض أن الدولة المحايدة لديها المعرفة التي تملك المزود التجاري؛ من أجل الحفاظ على الحياد بشكل فعال، فمن واجب الدولة المحايدة أن تراقب بشكل فعال – قدر استطاعتها– الأراضي والبنية التحتية الخاصة بها من أجل منع إطلاق عمل من أعمال الحرب السيبرانية من أراضيها أو من البنية التحتية السيبرانية التي تسيطر عليها بشكل فعال، وإنَّ هذا الواجب هو واجب مراقبة يعتمد بالضرورة على الوسائل والأفراد المتاحين للدولة المحايدة وعلى المستوى التقني للدولة المحايدة، ولكن يجب على الدولة المحايدة أن تفعل كل ما في وسعها في الحفاظ على حيادها من خلال مراقبة شبكاتها السيبرانية ومنع استخدامها في أعمال عدائية (Johnson & Post, 1998).

القانون الدولي والحرب السيبرانية (International Law & Cyberterrorism):

عند تفسير القانون الدولي الحالي وتطبيقه على الحرب السيبرانية، فمن الواجب إيلاء الاعتبار للخصائص المحددة للفضاء السيبراني. والجدير بالذكر هنا، أن الفضاء السيبراني هو المجال الوحيد الذي هو من صنع الإنسان بالكامل، فهو الذي أنشأه ويحافظ عليه، كما

أنه يملكه ويديره بشكل جماعي من قبل أصحاب المصلحة من القطاعين العام والخاص في جميع أنحاء العالم، ويتغير باستمرار استجابةً للابتكار التكنولوجي. وفي الفضاء السيبراني لا تخضع المعلومات والحمولات السيبرانية للحدود الجيوسياسية أو الطبيعية التي يتم نشرها على الفور بين أي نقطة أصل وأي وجهة متصلة من خلال الطيف الكهرومغناطيسي. هذه السفر في شكل رقمي متعدد الأجزاء من خلال مسارات غير متوقعة قبل إعادة تشكيلها في وجهتها. في حين أن الفضاء السيبراني متاح بسهولة للحكومات والمنظمات غير الحكومية والمؤسسات الخاصة والأفراد على حد سواء، فانتحال عنوان IP واستخدام شبكات الروبوت – على سبيل المثال– يجعل من السهولة إخفاء أصل العملية، وبالتالي يجعل تحديد الأنشطة السيبرانية وإسنادها بشكل موثوق أمرًا صعبًا بشكل خاص (Melzer, 2011)

المتحاربون والحياد السيبراني (Belligerents and Cyber Neutrality):

نقطة البداية لتحليل الالتزامات الحربية مع احترام الأنشطة السيبرانية بموجب قانون الحياد هو الافتراض الأساسي لأن تكون الأطراف المتحاربة محظورة من إجراء العمليات السيبرانية ضد العدو من داخل الأراضي المحايدة. وينطبق الحظر نفسه على استخدام الإنترنت على البنية التحتية المحايدة التي تقع خارج المنطقة المحايدة في حالتين؛ الأولى إذا كان يتمتع بمزايا الحياد بسبب الحصانة السيادية، والثاني هو إذا كانت البنية التحتية أو الأنظمة للحاسوب الخاص أو نظام لكينونة خاصة أو شخص من دولة محايدة لا تقع ضمن أراضي المحارب (Jensen, 2012). إنَّ قانون الحياد (law of neutrality) يحمي البنية التحتية السيبرانية الموجودة على أراضي دولة محايدة أو الموجودة في منصات الحصانة السيادية وغيرها من الأشياء التي تستخدمها الدولة المحايدة لأغراض حكومية غير تجارية، ويجب على الدول المحايدة (The neutral States) أن تظل محايدة، ولا يجوز لها المشاركة في أنشطة إلكترونية تدعم الأعمال العسكرية التي يقوم بها أحد الأطراف المتحاربة على حساب الطرف المتحارب الآخر. إضافةً إلى ذلك، فهي ملزمة باتخاذ جميع التدابير الممكنة لإنهاء إساءة استخدام البنية التحتية السيبرانية الموجودة داخل أراضيها أو على منصاتها المناعية السيادية من قبل المتحاربين (Belligerents). ويحظر على المتحاربين استخدام بنية تحتية إلكترونية محايدة بغرض ممارسة حقوق قتالية ضد العدو أو ضد الآخرين. ومن المهم الإشارة إلى أن مصطلح «حقوق المتحارب» لا يقتصر على الهجمات السيبرانية، بل يشير إلى جميع التدابير التي يحق للطرف المتحارب اتخاذها بموجب قانون النزاع المسلح ضد العدو المتحارب أو مواطني العدو أو مواطني الدول المحايدة.

إجراءات تحقق المتطلبات (Due diligence):

ينبغي على أي دولة ألا تسمح - عن علم- باستخدام أراضيها في أعمال تتعارض مع حقوق الدول الأخرى. ويتوقع من الدولة التي لديها معرفة بنشاط سيبراني ضار أن تتخذ جميع الخطوات المناسبة والمتاحة بشكل معقول والممكنة؛ لوقف الأنشطة السيبرانية المستمرة أو الوشيكة مؤقتًا التي تؤدي أو ستؤدي إلى آثار ضارة كبيرة تؤثر على الحقوق القانونية لدولة أخرى. وستعتمد العتبة الدقيقة التي تؤدي إلى هذا التوقع على مجمل الظروف في تلك الحالة، وهذا يشمل ما إذا كانت الدولة على علم بالأفعال غير المشروعة، وقدراتها التقنية وغيرها من قدراتها لاكتشاف هذه الأفعال ووقفها، وما هو معقول في هذه الحالة؛ على سبيل المثال: لن يتوقع على الأرجح من دولة ذات قدرات تقنية محدودة أن تستجيب إذا فشلت في اكتشاف نشاط إلكتروني ضار ينبع من أو من خلال البنية التحتية السيبرانية على أراضيها، ومع ذلك فبمجرد أن تدرك هذا الأمر، فمن المتوقع أن تستجيب الدولة. (Jensen, 2012)

التدابير المضادة (Countermeasures):

يحق للدول استخدام التدابير المضادة للرد على الأفعال غير المشروعة دوليًا، بما في ذلك في الفضاء السيبراني. ويحدد القانون الدولي العرفي لمسؤولية الدول الحدود في ممارسة الحق في اتخاذ التدابير المضادة، وهي الإجراءات التي قد تكون غير قانونية لولا ذلك. فعل غير مشروع دوليًا. قد لا تشكل تهديدًا أو استخدامًا للقوة، ويجب أن تكون متسقة مع القواعد القطعية الأخرى للقانون الدولي، ويجب أن تكون متناسبة. يمكن أن تكون الإجراءات المضادة القانونية للرد على الأفعال السيبرانية غير المشروعة دوليًا غير سيبرانية بطبيعتها، ويمكن أن تشمل العمليات السيبرانية ردًا على الأفعال غير المشروعة دوليًا غير السيبرانية. والدولة التي تتخذ تدابير مضادة ليست ملزمة بتقديم معلومات مفصلة تعادل مستوى الأدلة المطلوبة في عملية قضائية لتبرير إجراءاتها المضادة على الإنترنت، والفعل غير المشروع دوليًا في السياق السيبراني هو فعل أو إغفال مرتبط بالإنترنت: يشكل خرقًا لالتزام قانوني دولي، سواء تجاه دولة أخرى أو المجتمع الدولي بأكمله، وينسب إلى دولة بموجب القانون الدولي. ويعترف القانون الدولي بالاستثناءات لما يمكن أن يكون أفعالًا غير مشروعة دوليًا، كما تشمل الأمثلة حالات الدفاع عن النفس والإجراءات المضادة (البداينة، قيد النشر)

ويستنتج انه من المرجح ان يستغل الإرهاب السيبراني الوضع القانوني الدولي للدولة المحايدة ويستغل بنيتها التحتية كملذات آمنة للعمل الإرهابي السيبراني وللحرب السيبراني، ويستخدمها لشن أعمال وهجمات وعمليات سيبرانية على مستهدفين داخل الدولة المحايدة وخارجها. ويأتي هذه الاستغلال تجنبا لاستخدام التدابير المضادة للرد على الأفعال غير المشروعة دوليًا وخزفا من الانكشاف والملاحقة القانونية والسيبرانية للأفعال الإرهابية السيبرانية. كما انه يستغل الضبابية في تطبيق القانون الدولي على الأنشطة الضارة في كل دولة في الفضاء السيبراني.

المضامين الأمنية للتقنيات الناشئة والفضاء السيبراني:

كما أنَّ للتقنيات الناشئة العديد من الوظائف الإيجابية في مجالات الحياة البشرية كافة، فإنَّ الهجمات السيبرانية لها استخدام مزدوج ويمكن تطويعها في حماية وخدمة أعمال الإرهاب السيبراني، فللذكاء الاصطناعي تأثير عميق على الحياة الإنسانية؛ من الرعاية الصحية والزراعة والصناعة إلى الخدمات المالية والتعليم. ومع ذلك فإنَّه ليس خاليًا من المخاطر، وربما يجسد الذكاء الاصطناعي هذه الازدواجية أكثر من أي تكنولوجيا ناشئة أخرى، كما أن لديه القدرة على عرقلة التمتع بحقوق الإنسان الأساسية والحريات، وحرية الفكر والتعبير، وعدم التمييز. إن أي استخدام للتقنيات التي تدعم الذكاء الاصطناعي يجب أن تسير دائمًا جنبًا إلى جنب مع الجهود المبذولة لحماية حقوق الإنسان، ويمكن توظيف تقنيات الذكاء الاصطناعي في الهجمات السيبرانية، وإلحاق الخراب والتدمير للبنى التحتية الحساسة؛ من اتصالات ومواصلات وبنوك وغيرها.

إنترنت الأشياء يتيح تواصل الأجهزة المرتبطة عبر الإنترنت، وإرسال الأوامر والمهام دون تدخل بشري وبشكل تلقائي إذا تواجدت تلك الأجهزة في نطاق جغرافي تغطيه شبكة الإنترنت. ويمكن للإرهاب السيبراني توظيف هذه الميزات لإنترنت الأشياء في استخدام غير آمن، وإنَّ مكونات إنترنت الأشياء متوافرة، ويوجد عدد كبير من مستخدميه، ومن هنا يبرز إنترنت الأشياء كتهديد ناقل للإرهاب السيبراني، وهذا يعني أن الإرهاب السيبراني ليس مسألة ما إذا كان، لكن متى (Henschke, 2021).

ويوسع إنترنت الأشياء التركيز على الاتصالات من آلة إلى آلة، ويشمل أيضًا الأشخاص وعمليات إنترنت كل شيء. إنه «الاتصال الذكي بين الأشخاص والمعالجة والبيانات والأشياء»، ويتضمن مفهوم إنترنت كل شيء أي نوع من الكائنات أو الكيانات المادية أو الافتراضية التي يمكن جعلها قابلة للتوجيه وإعطاء القدرة على نقل البيانات دون تدخل من إنسان إلى آلة.

وتكمن الخطورة في توظيف الإرهاب السيبراني - وخاصة الذئب المنفرد السيبراني- لهذه التقنيات في تنفيذ هجمات سيبرانية كارثية تلحق الأذى والدمار السيبراني والمادي بقطاعات حيوية كثيرة وبمستهدفين كثر، وقد تأخذ هذه الهجمات شكل حرب سيبرانية عابرة للحدود ومتعددة المستهدفين والدول والجماعات، ويصعب كشفها في الوقت المناسب.

أمَّا إنترنت الأجسام فهو يصف الأجهزة المتصلة التي تراقب جسم الإنسان، وتجمع البيانات الفسيولوجية، أو القياسات الحيوية أو السلوكية، وتتبادل المعلومات عبر شبكة لا سلكية أو مختلطة. ويمكن أيضًا اعتبار تطبيقات الأجهزة المحمولة المستقلة التي تحلل النشاط البدني والبيانات المتعلقة بالصحة؛ مثل ضربات القلب وضغط الدم ودورات النوم، من إنترنت الأشياء. وتأتي منتجات إنترنت الأجسام في أشكال مختلفة؛ تتراوح في التعقيد من الساعات الذكية وأجهزة تتبع اللياقة البدنية إلى أنظمة توصيل الأنسولين القابلة للزرع، وأجهزة الاستشعار القابلة للابتلاع، وأدوات تحفيز الدماغ، والمضامين الأمنية لهذه التقنية كثيرة؛ منها ما هو فردي، ومنها ما هو مؤسسي، فقد استخدمت هذه التقنيات في الجيوش وفي الصحة، ممَّا يجعل من الممكن جدًّا استثمارها في هجمات سيبرانية فردية أو موجهة نحو مؤسسات معينة، وتعطيل الدخول إليها أو الخروج منها.

وقد ارتبطت تقنية طائرات بدون طيار «الدرون» بالاستخدامات العسكرية والتجسس، كما أنه بالإمكان استخدام هذه التقنية أيضًا في الاستخدامات المدنية والإنسانية الكثيرة؛ حيث استخدمت عصابات تهريب المخدرات هذه الطائرات في تهريب المخدرات، ومخاطر نشر المخدرات في المنطقة، وخاصة الخليج العربي. كما يمكن استخدامها في الإرهاب التقليدي والسيبراني في التدمير للبنى التحتية الحساسة، أو زرع معدات التجسس أو أي نوع من التخريب السيبراني أو المادي، بما في ذلك الاغتيالات.

وفي مجال الدفاع السيبراني فإنَّ تقنية ذكاء التهديد السيبراني مناسبة، وهي معلومات تستخدمها المنظمة لفهم التهديدات التي تستهدفها، كما تستخدم هذه المعلومات لإعداد ومنع وتحديد التهديدات السيبرانية التي تتطلع إلى الاستفادة من الموارد القيمة، ويمكن توظيف ذكاء التهديد السيبراني في الدفاع السيبراني والوقاية من الهجمات السيبرانية بوضع الخطط الاستباقية.

والخلاصة هنا أنه كما أنَّ للتقنيات الناشئة استخدامات كبيرة في مجال الحياة البشرية، إلا أنها يمكن أن تستخدم في تهديد الأمن البشري والإنساني الفردي والمجتمعي والدولي على شكل هجمات سيبرانية وإرهاب سيبراني وحروب سيبرانية. وإنَّ أهم التحديات الأمنية السيبرانية التي تواجه المجتمع الرقمي اليوم هي استخدام التقنيات الناشئة في الإرهاب والحرب السيبرانية (الهجوم والدفاع السيبراني)، فعندما يكون العدو السيبراني ذئب منفرد سيبراني أو مجموعة إرهاب سيبرانية، فمن الصعوبة بمكان للحكومات ملاحقة هذه القوى، ومن السهولة شل الحياة في مجتمع ما دون أن تتمكن الدولة من الرد على منفذ الهجوم، الذي قد يكون ذئبًا منفردًا سيبرانيًا جالسًا في أحد المقاهي.

الخلاصة والمناقشة والتوصيات:

تناولت هذه الدراسة موضوع الإرهاب السيبراني والتقنيات الناشئة وتحديات السيادة الوطنية السيبرانية والدولة المحايدة في الفضاء السيبراني، كما تناولت مكونات الفضاء السيبراني وتطوره وخصائصه كحاضنة للإرهاب السيبراني، وتركزت المراجعة على الإرهاب السيبراني؛ من حيث مفهوم الإرهاب السيبراني، وتطوره، وأشكاله، والطرق الشائعة في الهجمات الإرهابية السيبرانية، والحرب السيبرانية، والأساطير الشائعة حول الإرهاب التقليدي والسيبراني. وناقشت الدراسة بعض المضامين الأمنية للتقنيات الناشئة؛ كالذكاء الاصطناعي وإنترنت الأشياء، وإنترنت الاجسام، وإنترنت كل شيء، وذكاء التهديد السيبراني، والأمن السيبراني، كما استعرضت تحديات الإرهاب السيبراني لقضايا السيادة الوطنية والدولة المحايدة والقانون الدولي.

هل بات الفضاء السيبراني مهددًا للفضاء المادي؟

يتمتع الفضاء السيبراني بخصائص مميزة وفريدة تجعله حاضنة آمنة للإرهاب السيبراني، فيمكن من خلاله شن هجمات سيبرانية ضد مستهدف واحد أو عدد من المستهدفين داخل الدولة أو خارج الحدود الوطنية، كما أنَّ هناك تنوعًا هائلًا في الأهداف التي يمكن الوصول إليها بالإرهاب السيبراني وفي عددها، وفي الفضاء السيبراني لا توجد حواجز مادية؛ مثل نقاط التفتيش للتنقل، ولا حدود لعبورها، ولا وكلاء للجمارك، كما يمكن فيه استهداف أجهزة الكمبيوتر وشبكات الكمبيوتر الخاصة بالحكومات والأفراد والمرافق العامة، وشركات الطيران الخاصة، وفي نطاق دولي واسع.

لماذا الإرهاب السيبراني؟

الإرهاب السيبراني خيار جاذب للإرهابين والمجرمين بسبب سهولة التنفيذ، والخفاء، والكلفة المنخفضة، وعدم الحاجة لمواد ومعدات كما هو الحال في الإرهاب التقليدي (مثل البنادق والمتفجرات)، ويمكن إنشاء فيروسات الكمبيوتر وإرسالها؛ من خلال خط هاتف أو كابل أو اتصال لا سلكي، ويمكن استغلال كل التقنيات الناشئة في التخطيط والتنفيذ والحماية، كما أنَّ إخفاء الهوية أمر سهل في الإرهاب السيبراني، حتى اكتشاف الحادث الإرهابي السيبراني قد يحتاج إلى بعض الوقت، مما يمكن من انتشاره في قطاعات كبيرة ومستهدفين متعددين.

هل نشهد سباق تسلح سيبراني؟

هناك سباق تسلح سيبراني بين اللاعبين والجماعات السيبرانية ذات الأيدولوجيات السياسية، وأحيانًا الناشطين في مجالات مختلفة ممن يعتقدون بأنّ مناصرة طرف ما في صراع بين دولي قضية واجب، ومن ذلك نشاط الهجمات السيبرانية المنفردة والمستقلة والمدعومة من الحكومات في الحرب على أوكرانيا، وفي صراعات القوة والاقتصاد بين الولايات المتحدة وكل من الصين وروسيا وغيرهم. وقد سارعت الدول لبناء المؤسسات السيبرانية الدفاعية والهجومية، وسنَّت القوانين السيبرانية التي تنظم السلوك في الفضاء السيبراني الوطني، كما أنَّ الأمم المتحدة شرعت في وضع المدونات والأدلة للسلوك الأخلاقي للدولة في الفضاء السيبراني.

نحو أنموذج (Paradigm) جديد في الأمن السيبراني

يمثل الفضاء السيبراني بعدًا جديدًا هو البعد الخامس، وهذا الفضاء – بما يملكه من خصائص فريدة– قد ربط العالم ببعضه بعضًا، وجعل حركة الناس والأفكار والأعمال والثقافات ميسرة وسهلة. إلا أن ذلك قد وفر حاضنات للإرهاب السيبراني والجرائم والتهديدات السيبرانية، وأصبحت مهددات الأمن غير تقليدية، ليست جيوشًا ولا جماعات إرهابية تقليدية، بل أصبح الرصاص بايتات حاسوب ونبضات كهرومغناطيسية، كما أن الجندي السيبراني لم يعد بالضرورة أن يكون في جيش تقليدي، فالذئب المنفرد السيبراني يمثله عامل منفرد. كما يمكن للفرد والجماعات القيام بهجمات سيبرانية بدوافع شخصية أو سياسية أو أيديولوجية من أي مكان وضد مستهدفين متعددين، فهم كالأشباح، من الصعب كشفهم، وليس من السهولة حصرهم.

هل أنتج العصر الرقمي والفضاء السيبراني معاني جديدة للأمن بأشكاله كافة؟ وهل نحن أمام أشكال جديدة للحروب والصراعات، حروب ليس بالضرورة أن يخوضها جيوش بل هواة ومراهقون ولصوص حاسب؟ هل نحن في عصر استبدل فيه الرصاص ببايتات الحاسوب والموجات؟ وهل نحن أمام استخدام محتمل لما يعرف بالنبض الكهرومغناطيسي (Electromagnetic Pulse EMP)؟ وهي ظاهرة يمكنها إيقاف تشغيل جميع الأجهزة، وتدمير أي جهاز إلكتروني. هل تبدل مفهوم السيادة الوطنية والحياد؟ والسؤال المركزي هنا: هل نستطيع مواجهة التحديات الأمنية السيبرانية بالأدوات التقليدية؟ إذا كانت الإجابة لا، وهي لا، فإننا أمام ولادة أنموذج (Paradigm) جديد في الأمن السيبراني. والحاجة إلى أنموذج كهذا ضرورية لاستيعاب المستجدات الرقمية والسلوك الرقمي لدى الناس، وما يرتبط به من قضايا السيادة الوطنية، والدولة المحايدة، والقانون الدولي، والهجمات السيبرانية، وغيرها.

المراجع

أولًا: المراجع العربية

- البحر، عبد الرحمن (1999). معوقات التحقيق في جرائم الإنترنت. «رسالة ماجستير غير منشورة». الرياض: أكاديمية نايف العربية للعلوم الأمنية.
- البداينة، ذياب (1993). اتجاهات الطلبة نحو استخدام الحاسوب: دراسة مقارنة. مجلة رسالة الخليج، العدد 46، 162-133.
- البداينة، ذياب (1997). جرائم الحاسوب الدولية. بحث مقدم في الدورة العلمية «مكافحة جرائم الحاسب الآلي»، معهد التدريب بأكاديمية نايف العربية للعلوم الأمنية، الرياض، السعودية.1997.
- البداينة، ذياب (1998). استخدام الحاسب الآلي في البحث العلمي في دراسة السلوك الإجرامي. بحث مقدم في الدورة التدريبية «مناهج البحث العلمي في دراسة السلوك الإجرامي»، أكاديمية نايف العربية للعلوم الأمنية، الرياض – السعودية. 1998.
- البداينة، ذياب (1999 أ). جرائم الحاسب والإنترنت. في مركز الدراسات والبحوث، ص 93- 126، الظواهر الإجرامية المستحدثة وسبل مواجهتها. الرياض: المؤلف.
- البداينة، ذياب (1999 ب). التقنية والجريمة المنظمة، الفكر الشرطي، م 7، ع 4، ص 1818- 215.
- البداينة، ذياب (2000أ). استخدام التقنيات الحديثة في مكافحة الإرهاب. بحث مقدم في الحلقة العلمية: تبادل المعلومات في مكافحة الإرهاب في ظل الاتفاقيات العربية والدولية، أكاديمية نايف العربية للعلوم الأمنية، الرياض، السعودية. 2000.
- البداينة، ذياب (2000ب). استخدام تطبيقات الإنترنت في كشف المتفجرات. بحث مقدم في الدورة التدريبية «استخدام التقنيات في استخدام الأسلحة والمتفجرات في العمليات الإرهابية». معهد التدريب، أكاديمية نايف العربية للعلوم الأمنية، الرياض، السعودية. 2000.
- البداينة، ذياب (2001أ). استخدام الحاسب في مكافحة التزوير. ورقة مقدمة في الدورة المخبرية: مركز التدريب. أكاديمية نايف العربية للعلوم الأمنية. الرياض، السعودية. 2001.
- البداينة، ذياب (2001ب). مراجعة كتاب «الآثار الاجتماعية للحاسب». المجلة العربية للدراسات الأمنية، أكاديمية نايف العربية للعلوم الأمنية. الرياض، ع 16، ص 384-367.
- البداينة، ذياب (2002). الأمن وحرب المعلومات. عمان: دار الشروق.

- البداينة، ذياب (2003). أمن المعلومات، مجلة مركز دراسات المستقبل، جامعة أسيوط، العدد 8، 36-9.
- البداينة، ذياب (2004). الإنترنت والمخدرات، الدراسات الأمنية، السنة 1ع 1 ص 17- 39.
- البداينة، ذياب (2006). دور الأجهزة الأمنية في مكافحة جرائم الإرهاب الإلكتروني. دورة تدريبية «مكافحة الجرائم الإرهابية المعلوماتية» - المعهد الملكي للشرطة- المملكة المغربية. 2006.
- البداينة، ذياب (2007). أمن المعلومات في العصر الرقمي. ملتقى عمان 13 الثقافة العربية في العصر الرقمي. 2007-4-19-17 عمان - الأردن.
- البداينة، ذياب (2008). الإرهاب التخيلي. في الجرائم المعلوماتية. جامعة نايف العربية للعلوم الأمنية. 2008.
- البداينة، ذياب (2010). دور الشباب في محاربة الإرهاب: الإرهاب وتكنولوجيا المعلومات. 2010 المجلس الأعلى للشباب، عمان.
- البداينة، ذياب (2011). الشباب والإنترنت والمخدرات، وزارة الثقافة، عمان.
- البداينة، ذياب (2013). الرصد والتحليل العلمي لمحتويات الشبكات في مجال الإرهاب. ورقة مقدمة في الندوة العلمية «توظيف شبكات التواصل الاجتماعي في مكافحة الإرهاب»، الرياض 23-27/2/2013.
- البداينة، ذياب (2020). الإشاعة السيبرانية في المجتمع الرقمي: أمثلة في الوقاية في التعامل مع جائحة فيروس الكورونا (COVID-19). مجلة دراسات قانونية وأمنية. المجلد 1 العدد 1ص 66-9.
- البداينة، ذياب (قيد النشر). المدخل إلى الأمن السيبراني: المفاهيم والتطبيقات والمخاطر الاجتماعية السيبرانية. دار الفكر. عمان.
- كابلان فرد، (2016) ترجمة لؤي عبد المجيد (2019). المنطقة المظلمة: التاريخ السري للحرب السيبرانية. عالم المعرفة 470. الكويت.
- كوهين، إيليوت (2001). إدارة الأمن القومي في عصر المعلومات. ص 140-111. في مركز الإمارات للدراسات والبحوث الاستراتيجية. القيادة والإدارة في عصر المعلومات. الإمارات: المؤلف.
- ميدان، (2023). الحرب على الجبهة السيبرانية.. 35 فريقًا من القراصنة يحاربون لأجل فلسطين.

ثانيًا: المراجع الأجنبية

- Al-badayneh, D. (2008). Social Causes of Terrorism in the Arab Society. PP 132-143 in Understanding Terrorism: Analysis of Sociological and Psychological Aspects. IOS press. NATO, OTAN. The NATO science for Peace and Security program. IOS press.
- Al-badayneh, D. (2011). University Under Risk: The University as Incubator for Radicalization. In Developing Prevention Strategies and Tactics in Countering Radicalization. NATO & Turkish Police Academy.
- Al-badayneh, D. (2013A). Human behavior: when and where virtual society meets physical society. European Journal of Science and Theology, February 2013, Vol. 9, No. 1, 3-17.
- Al-badayneh, D. (2013B) Human behavior: when and where virtual society meets physical society. European Journal of Science and Theology, February 2013, Vol. 9, No. 1, 3-17.
- Al-badayneh, D. (2016C). Religious behavior and radicalization Among Arab Youth: Implications for terrorism recruitment and de-radicalization pp 130-145 in Ekici, S., Akdogan H, Ekici A, and Warnes. Countering Terrorist Recruitment in the context of Armed Counter-Terrorism Operations. IOS press, NATO Science for Peace and Security Program.
- Al-badayneh, D. et al., (2012) Fearing Future Terrorism: Perceived Personal, National, Regional and International Threats of Terrorism in Counter Terrorism in Culturally and Linguistically Diverse Communities. NATO & Turkish Police Academy.
- Al-badayneh, D. et al., (2016B). The Impact of Political Affiliation, Political Participation and life Satisfaction on Radicalization Among University Students. British Journal of Arts and Social Sciences. ISSN: 2046-9578, Vol. 21 No. II British Journal Publishing, Inc. pp 140-150 http://www.bjournal.co.uk/volume/BJASS___21___2.aspx.

- Al-badayneh, D. et al., (2017). Determining factors of radicalizing Among Arab university students. Turkish Journal of Security Studies 19(2). Pp 85-114.
- Al-badayneh, D. et al., (2020). Radical Thoughts: Fears About and Supporting ISIS Among Jordanian College Students. NATO and Meson University. NATO Science for Peace and Security Series book, 'From Territorial Defeat to Global ISIS: Lessons Learned,' is set to be published by IOS Press.
- Al-badayneh, D. et al., (2023). Developing A Robust Legal System Through Scale for Youth Extremism Across Arab Cultures. International Journal of Criminal Justice Science Vol 18 Issue 1 January –June 2023pp 29-51 https://ijcjs.com/menu-script/index.php/ijcjs/article/view/589/400.
- Al-badayneh, D. et.al., (2022). Cyberbullying Victimization, Strains and Delinquency in Qatar. European Journal of Science and Theology, December 2022, Vol.18, No.6, 37-45.
- Al-badayneh, D., et al., (2016A). Radicalizing Arab University Students: A global Emerging Threat. Journalism and Mass Communication. Vol.2 pp 67-78.
- Andrew. B, (2017). "Ardit Ferizi, hacker who aided Islamic State, sentenced for helping terror group with 'kill list'". The Washington Times. Retrieved 1 March 2017.
- Barlow, J. P., (1996). 'A Declaration of the Independence of Cyberspace' (Davos 1996) https:// www.eff.org/ cyberspace -independence.
- Blake, Andrew. "Ardit Ferizi, hacker who aided Islamic State, sentenced for helping terror group with 'kill list'". The Washington Times. Retrieved 1 March 2017.
- Brickey, J. (2012). Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace. https://www.researchgate.net/publication/235782714.
- Bronskill, J. (2001). CSIS on alert for cyber saboteur's spy against monitors threats to computer network. Report, Ottawa Citizen. A3.
- Brunst, P. W. (2010). Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet," in Marianne Wade and Almir Maljevic´, eds., A War on Terror?: The European Stance on a New Threat, Changing Laws and Human Rights Implications (New York: Springer, 51–78, 51.

- Burns, E., Laskowski, N., & Tucci, L., (2022). What is artificial intelligence (AI)? https://www.techtarget.com/searchenterpriseai/definition/AI-Artificial-Intelligence
- Bussell, Jennifer. (2013). Cyberspace. Encyclopedia Britannica. https://www.britannica.com/topic/cyberspace
- Cardon, A., (2018) Beyond Artificial Intelligence: From Human Consciousness to Artificial Consciousness. ISTE Ltd. UK.
- Cassim, F. (2012). Addressing the spectre of cyber terrorism: A comparative perspective. Potchefstroom Electronic law Journal, 15 (2), 380-415.
- Center for Strategic and International Studies (CSIS). (2023). Significant Cyber Incidents. Washington, DC.
- Clark, D., & Csail, M., (2010) Characterizing cyberspace: past, present, and, future.
- Conway, M. (2002). Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet," First Monday 7, no. 11 http://firstmonday.org/ojs/index.php/fm/article/view/1001/922
- Cross, S. E. (2000). Cyber threats and US economy. Http//www.cert.org/congressional testimony/cross__testiony__Feb2000.html.
- Dan C. Marinescu, (2017). Complex Systems and Clouds. pp 1-32 in Complexity and Complex Thermo-Economic Systems, 2020 in Complexity and Complex Thermo-Economic Systems. Elsevier Inc. All.
- Denning, D. (2000). "Cyberterrorism," Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives, 23 May 2000, www.stealthiss.com/documents/pdf/cyberterrorism.pdf.
- Denning, D. E. (2000a). Cyberterrorism. Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services U.S. House of Representatives, May 23.
- Denning, D. E. (2000b). Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. http://www.nautilus.org/info-policy / workshop /papers/denning.html.

- Denning, D. E. (23 May 2000). "Cyberterrorism". cs.georgetown.edu. Archived from the original on 10 March 2014. Retrieved 19 June 2016.
- Denning, D. E. and Baugh, Jr. W.E. (1999). Hiding Crime in Cyberspace. http://www.cs.georgetown.edu/~denning/.
- Executive Order on Improving the Nation's Cybersecurity". The White House. 12 May 2021. Retrieved 6 December 2021.
- FACT SHEET: Executive Order Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities". whitehouse.gov. 1 April 2015. Retrieved 1 March 2017.
- Gadgil, S.(2022) 11 Top Emerging Technology Trends to Watch in 2020 https://www.clariontech.com/blog/11-top-emerging-technology-trends-to-watch-in-2022.
- Garibaldi, S. and Deane, F. (2023), "Cyberspace as a fifth dimension of national security: trade measure exceptions", Journal of International Trade Law and Policy, Vol. 22 No. 2, pp. 67-88. https://doi.org/10.1108/JITLP-01-2023-0004.
- Goodnight. J., (2022). Artificial Intelligence: What it is and why it mattershttps://www.sas.com/en__us/insights/analytics/what-is-artificial-intelligence.html.
- Gordon, S., and Ford, R., (2002). Cyberterrorism? Computers & Security 21, no. 7: 636–647.
- Hardy, K. (2011). WWWMDs: Cyber-attacks against infrastructure in domestic anti-terror laws. Computer Law & Security Review, 27 (2), p. 152-161.
- Hardy, K., Williams, G. (2014). What is 'Cyberterrorism'? Computer and Internet Technology in Legal Definitions of Terrorism. In: Chen, T., Jarvis, L., Macdonald, S. (eds) Cyberterrorism. Springer, New York, NY. https://doi.org/10.1007/978-1-4939-0962-9__1.
- Hardy, K., Williams, G. (2014). What is 'Cyberterrorism'? Computer and Internet Technology in Legal Definitions of Terrorism. In: Chen, T., Jarvis, L., Macdonald, S. (eds) Cyberterrorism. Springer, New York, NY. https://doi.org/10.1007/978-1-4939-0962-9__1.

- Henschke A., (2021). Terrorism and the Internet of Things: Cyber–Terrorism as an Emergent Threat. Pp 71–87.
- Hogeveen, B. (2022). The UN norms of responsible state behavior in cyberspace Guidance on implementation for Member States of ASEAN. The Australian Strategic Policy Institute.
- https://www.csis.org/programs/strategic–technologies–program/significant–cyber–incidents.
- Hua J. & Bapna, S. (2012). "How Can We Deter Cyberterrorism?" Information Security Journal: A Global Perspective 21, no. 2: 102–114, 104.
- Jarvis, L., & Macdonald, S. (2014). What Is Cyberterrorism? Findings From a Survey of Researchers, Terrorism and Political Violence, DOI: 10.1080/09546553.2013.847827.
- Johnson, D., and Post, D., (1998), 'Law and borders: The rise of law in cyberspace' Stanford Law Review 1367. Contra see Jack L Goldsmith, 'Against cyberanarchy' (1998) 65 Universityof Chicago Law Review 1199.
- Kaźmierczak, D.) (2017). Cyberterrorism, Cybercrime and Cybersecurity, [w:] red. J. Kuck, Współczesne zagrożenia w zarządzaniu i bezpieczeństwie, UKiP J&D Gębka Gliwice, 2014, ISBN 978–83–64590–00–9; str/p. 439–474.
- Kessler, G. C. (2016). Lone–Operator Cyberterrorism. Journal of Information Warfare Vol. 15, No. 1 (2016), pp. 15–28.
- Kessler, G. C. (2021) Lone Operator Cyberterrorism from the Perspective of a Hacker. Pp 45 – 50. Volume 123: Lone Actors – An Emerging Security Threat. NATO Science for Peace and Security Series – E: Human and Societal Dynamics. IOS Press. Amsterdam. The Netherlands.
- Klein, J. J., (2014). "Some Principles of Cyber Strategy," ISN Security Watch, 21 August 2014, http://www.isn.ethz.ch /DigitalLibrary/Articles/Detail/?id=182955.
- Klubnikin, A. (2022). What is the Internet of Bodies (IoB), and why should you care? https://itrexgroup.com/blog/internet–of–bodies–iob–definition–benefits–examples/.

- Krepinevich,A. F., (2012). Cyber Warfare: A 'Nuclear Option'? Washington, DC: Center for Strategic and Budgetary Assessments, 2012), 8, http://csbaonline.org/publications/2012/08/cyber-warfare-a-nuclear-option/.
- Maryville (2023). Cyber Terrorism: What It Is and How It's Evolved https://online.maryville.edu/blog/cyber-terrorism/.
- Melzer, N. (2011). Cyberwarfare and International Law. The United Nations Institute for Disarmament Research (UNIDIR. Geneva, Switzerland.
- Ministry of Transport and communications (Qatar). (2018) Ethical Responsibility In A Digital World. https://www.safespace.qa/sites/default/files/2019 12/ethical___responsibility___in___the___digital___world-en.pdf.
- Novikov D.A. Cybernetics: From Past to Future. – Heidelberg: Springer, 2016. – 107
- Parks, P. J. (2013). Cyberwarfare. ReferencePoint Press.
- Pauline,. R., (2012). Law, Policy, and Technology: Cyberterrorism, Information Warfare, and Internet Immobilization: Cyberterrorism, Information Warfare, and Internet Immobilization. Hershey, PA: Information Science Reference. p. 354. ISBN 9781615208319.
- Pollitt, M. M. (1998). Cyberterrorism: Fact or Fancy,'' Computer Fraud & Security 2: 8–10, 9.
- Pollitt, M. M. (2001). Cyber Terrorism. Fact or Fancy? www.cosc. Georgetown.edu/denning/insosec/pollitt.html
- Rid T (2013) Cyber war will not take place. Hurst & Company, London.
- Roland, F., (15 February 2013). "Improving cybersecurity". CQ Researcher.
- Rotolo, D., and Hicks, D., & Martin, B., R., (2015). What Is an Emerging Technology? Research Policy, 44(10): 1827–1843, Available at SSRN: https://ssrn.com/abstract=2564094 or http://dx.doi.org/10.2139/ssrn.2564094
- Schelling, T. (1966). Arms and Influence. New Haven: Yale University Press.
- Schmitt MN (ed.) (2013) Tallinn manual on the international law applicable to cyber warfare, Cambridge. Cambridge.

- Schmitt, M. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. United States Naval War College, Newport, Rhode Island. https://doi.org/10.1017/9781316822524
- Singer, P.W., & Friedman A. (2015). Cybersecurity and Cyberwar: What Everyone Needs to Know. Strategic Studies Quarterly, (Review by: Chris Bronk) Vol. 9, No. 1 (SPRING 2015), pp. 141–143.
- Software Testing Help (2023). 18 Most Popular IoT Devices In 2023 (Only Noteworthy IoT Products). https://www.softwaretestinghelp.com/iot-devices/.
- Standage, Tom (1999). The Victorian Internet. New York, N.Y.: Berkley Books.
- Stark, R. (1999). Cyber Terrorism: Rethinking New Technology, Department of Defense and Strategic Studies.
- Stech, F. J. (1994). Wining CNN Wars Parameters, (10–29).
- Surabhi, M. (2012). Cyber Warfare And Cyber Terrorism. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract__id=2122633
- Tafoya, W. I. (2011). Cyber terror. FBI Law Enforcement Bulletin, 80 (11), p. 1–7.
- Tafoya, W. L.(2011). "Cyber Terror", FBI Law Enforcement Bulletin (FBI.gov), November 2011.
- Taliharm, A–M. (2000). Cyberterrorism: In Theory or in Practice?" Defense Against Terrorism Review 3, no. 2 59–74, 63–64.
- Taylor, E., & Hakmeh, J. (2021) Editorial introduction vol 6.3 – cyberspace4all: towards an inclusive cyberspace governance, Journal of Cyber Policy, 6:3, 267–270, DOI: 10.1080/23738871.2021.2016880https://www.tandfonline.com/doi/full/10.1080/23738871.2021.2016880.
- Tsagourias, N., (2021). The legal status of cyberspace: sovereignty redux? Pp 9–31 in Michael N. Schmitt Research handbook on international law and cyberspace. Edward Elgar Publishing Limited. UK.
- Ul Islam, N., (2022). Reasons Why Cyber Threat Intelligence Is Important.
- UNICRI & UNCCT (2021) Countering Terrorism Online With Artificial Intelligence: An Overview for Law Enforcement and Counter–Terrorism Agencies in South Asia and South–East Asia. United Nations Office of Counter–Terrorism (UNOCT). New York, NY.

- Vedantu, (2023). Introduction to Cyberspace. https://www.vedantu.com/commerce/introduction-to-cyberspace
- Venables, A., Shaikh, S. A., & Shuttleworth, J. (2015). A Model for Characterizing Cyberpower. Conference: International Conference on Critical Infrastructure Protection. https://hal.inria.fr/hal-01431010/file/978-3-319-26567-4__1__Chapter.pdf
- von Heinegg, W., H., (2012). Legal Implications of Territorial Sovereignty in Cyberspace. 2012 4th International Conference on Cyber Confl ict. C. Czosseck, R. Ottis, K. Ziolkowski (Eds.) NATO CCD COE Publications, Tallinn.
- Weimann, G. (2005). Cyberterrorism: The Sum of all Fears?," Studies in Conflict & Terrorism 28, no. 2 129–149, 131.
- Weimann, G. (2012). Lone-wolf, Communication, Internet, Social media, Open-Source Jihad, al-Qaeda. JTR Volume 3, Issue 2 – Autumn 2012 pp 75–90.
- Weimann, G. (2012). Lone-wolf, Communication, Internet, Social media, Open-Source Jihad, al-Qaeda. JTR Volume 3, Issue 2 – Autumn 2012 pp 75–90 Lone Wolves in Cyberspace. Journal of terrorism research, 3. pp 75–90.
- Weimann, G., (2004). Cyberterrorism How Real Is the Threat? United States Institute of Peace. Special Report 119 December 2004. https://www.usip.org/sites/default/files/sr119.pdf
- Weimann, G., (2006). Terror on the Internet: The New Arena, the New Challenges (Washington, D.C.: U.S. Institute of Peace Press, 2006).
- White House shifts Y2K focus to states, CNN (February 23, 1999)". CNN. 23 February 1999. Retrieved 25 September 2011.
- White House shifts Y2K focus to states, CNN (February 23, 1999)". CNN. 23 February 1999. Retrieved 25 September 2011.
- White, C. & Kenneth C. (1998). Cyber-Terrorism: Modem Mayhem." Carlisle Barracks, Pennsylvania: U.S. Army War College.
- White, J. (1991). Terrorism: An introduction. Pacific Gover, CA: Books/Cole.
- Yunos, Z., & Sulaman, S. (2017). Understanding Cyber Terrorism from Motivational Perspectives. Journal of Information Warfare, 16(4), 1–13. https://www.jstor.org/stable/26504114