Scientific Research Publishing

Journal of Information Security, 2023, 14, 472-489
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Domestic Cyberterrorism & Strategic Communications: Literature Review

Robb Shawe, Ian R. McAndrew

Department of Cyber Leadership, Capitol Technology University, Laurel, MD, USA
Email: rshawe@captechu.edu, irmcandrew@captechu.edu

How to cite this paper: Shawe, R. and McAndrew, I.R. (2023) Domestic Cyberterrorism & Strategic Communications: Literature Review. *Journal of Information Security*, **14**, 472-489.
https://doi.org/10.4236/jis.2023.144027

Received: August 31, 2023
Accepted: October 24, 2023
Published: October 27, 2023

Abstract

Cyberterrorism poses a significant threat to the national security of the United States of America (USA), with critical infrastructure, such as commercial facilities, dams, emergency services, food and agriculture, healthcare and public health, and transportation systems virtually at risk. Consequently, this is due primarily to the country's heavy dependence on computer networks. With both domestic and international terrorists increasingly targeting any vulnerabilities in computer systems and networks, information sharing among security agencies has become critical. Cyberterrorism can be regarded as the purest form of information warfare. This literature review examines cyberterrorism and strategic communications, focusing on domestic cyberterrorism. Notable themes include the meaning of cyberterrorism, how cyberterrorism differs from cybercrime, and the threat posed by cyberterrorism to the USA. Prevention and deterrence of cyberterrorism through information sharing and legislation are also key themes. Finally, gaps in knowledge are identified, and questions warranting additional research are outlined.

Keywords

Cyberterrorism, Cybersecurity Information Sharing Act, Mal-Information, Misinformation, Disinformation, Fake News, Propaganda, Strategic Communications

1. Domestic Cyberterrorism

Background

In defining cyberterrorism, the focus is usually not just on the people carrying out the attacks (terrorists) and their motivation but also on the location, infrastructure target, and the medium used (see **Appendix A**). Unlike conventional terrorist attacks, where terrorists use or target well-known targets, cyberterror-

ism involves targeting one or more aspects of cyberspace or using cyberspace to facilitate the attack [1]. Therefore, information and communication technologies (ICT) can be and have been used for the dual purposes of committing terrorist-related offenses and being the target of such attacks. In the former case, terrorist-related offenses are a form of cyber-enabled terrorism [2].

2. Introduction

Domestic cyberterrorism refers to acts of cybercrime committed within a country's borders by individuals or groups who aim to disrupt or damage critical infrastructure, government systems, businesses, or individuals for ideological, political, or financial reasons (see **Appendix A**). These attacks can range from hacking into computer networks to steal sensitive information or launch disruptive attacks to spreading disinformation or propaganda online.

On the other hand, strategic communications involve deliberately using communication strategies and tactics to shape public opinion, influence decision-making processes, and achieve specific objectives. In domestic cyberterrorism, strategic communications can be employed to counter and mitigate cyber-attack effects and inform and educate the public about potential threats and necessary precautions.

Strategic communications can include efforts such as:

1) Crisis Communication: In a cyber-attack, government agencies, businesses, and organizations need effective crisis communication plans, which may involve timely and accurate messaging to stakeholders, reassuring the public, and providing guidance on responding to the incident.

2) Public Awareness Campaigns: Governments and cybersecurity organizations can run campaigns to educate the public about cyber threats, the importance of using strong passwords, regularly updating software, and avoiding suspicious links and attachments. These campaigns can also raise awareness about the potential consequences of domestic cyberterrorism and the importance of reporting any suspicious activities.

3) Collaboration with the Media: Collaborating with the media can help disseminate accurate and timely information to the public during and after a cyber-attack. Data can be shared through press releases, interviews, and social media platforms to ensure accurate reporting and prevent the spread of false information.

4) Social Media Monitoring and Response: Effective strategic communications should include monitoring social media platforms for any discussions or activities related to domestic cyberterrorism. Prompt responses to misinformation, rumors, or propaganda can help debunk false narratives and prevent further escalation.

5) Stakeholder Engagement: Engaging with key stakeholders, such as businesses, critical infrastructure operators, and community leaders, is crucial in developing a collaborative and coordinated response to domestic cyberterrorism. Sharing information and best practices and conducting joint exercises can en-

hance cybersecurity resilience.

6) Governments, law enforcement agencies, businesses, and individuals need to recognize the evolving nature of domestic cyberterrorism and the importance of strategic communications in addressing this threat. By implementing effective strategies and tactics, we can mitigate the impact of cyber-attacks, educate the public, and maintain public trust in the face of these challenges.

3. Domestic Cyberterrorism

Cyberterrorism is widely used and reasonably well understood, owing mainly to the tendency of terrorist groups to use the Internet and the ever-increasing level of sophistication with which these terrorists use the Internet [3]. The convergence of increased permeation and use of the Internet and the emergence and proliferation of both domestic and international terrorism has shifted the focus of 21st-century counterterrorism efforts and measures from the more conventional forms of terrorism to less conventional ones such as cyberterrorism [4]. Terrorists no longer use conventional means, whereas many organizations remain committed to using traditional methods such as hijackings, bombings, and kidnappings. However, the reasonably high level of secrecy and sophistication afforded by cyberspace makes cyberspace a more attractive avenue for use by terrorists [5]. With limited chances of getting detected while still maintaining the same capabilities, terrorists are using the Internet and cyberspace to carry out their activities. Today, [3] states that terrorists utilize cyberspace to target critical infrastructure and destruction or denial of service (among other goals).

Strategically, the meaning of cyberterrorism encompasses both a motivation (terrorism) and a domain (cyber or cyberspace) [6]. In practice, however, the cause and environment may not always be immediately known whenever a law enforcement officer responds to a terrorist attack at the tactical level. Moreover, cyberterrorism may not resemble anything like it due to the lack of apparent motivation and domain (at least in the short term).

In the medium-term to long-term, however, it may become clear that the attack is an act of cyberterrorism. Similarly, an attack may initially appear to have a clear domain and motivation only to be motivated by something other than terrorism or to have used or targeted something else, not just cyberspace. More often than not, attacks targeting cyber as the domain have been relatively easily recognized as such. However, many tend not to be linked to terrorism as the motivation until much later [7].

In the 21st century, terrorists more frequently and commonly use the Internet to carry out different attacks against different targets [8]. In an era where cyberterrorism has become prevalent and rampant, the expectation would be that there would be a universal definition of cyberterrorism and one universally accepted, at least within counterterrorism circles. However, there are still different (albeit broadly similar) reports of cyberterrorism based mainly on country, jurisdiction, and the purpose for which the term is being used [9]. Just as there is

no universally agreed-upon definition of cybercrime, the definition of cyberterrorism can vary markedly. There is no widely accepted definition of terrorism, with different countries, agencies, organizations, and legal jurisdictions adopting various means for the same concept for other reasons [1]. Similarly, a cyberterrorism act in one country or legal jurisdiction may not be viewed as a cyberattack in another territory. The implication is that contextual issues must be considered in defining cyberterrorism (including domestic cyberterrorism).

Some definitions could be considered expansive conceptions of cyberterrorism, while others could be regarded as narrow conceptions. For example, a comprehensive description of cyberterrorism widely used and adopted is "any form of online terrorist activity" [10]. The more biased understanding of the concept includes defining the term in terms of how it is committed and who is responsible for saving it. In this regard, cyberterrorism is defined as a crime that is not only dependent on cyber and carried out or executed for purposes of achieving some political objectives but also one that is for purposes of provoking fear, coercing, or intimidating the targeted population or government, and either causing or threatening to cause harm (including sabotaging) [6]. Specific definitions examples of cyberterrorism in this regard include "Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss", "Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact," and "Attacks that disrupt nonessential services or that are a costly nuisance would not" [9] [10].

According to one commonly used definition, cyberterrorism is using the Internet to carry out, support, engage in, or advance terrorism and related activities [10]. Cyberterrorism is also defined as using computer network tools to shut down critical national infrastructure or coerce or intimidate a civilian population or government [7]. Considering these definitions, domestic cyberterrorism occurs when an attack against computer networks is carried out by terrorists or people resident within the targeted country. A common feature of all these definitions of cyberterrorism is the political nature, which is the main distinction between cyberterrorism and cybercrime. Cyberterrorism is political, while cybercrime is personal [9].

4. Methods of Preventing Domestic Cyberterrorism

Cyberterrorism is premised on the view that new vulnerabilities are created as more critical infrastructure and nations have become increasingly dependent on computer networks (see **Appendix A**). Subsequently, it becomes more likely that a hostile individual, group of people, or even nation may want to exploit these vulnerabilities and penetrate computer networks that are poorly secured to either shut down or disrupt critical functions [11]. In the same vein, one commonly held assumption among scholars and practitioners is that the vulnerability of critical infrastructure and the vulnerability of computer networks are the same and that both significantly increase the risk posed to national security [2]

[5] [9]. While the assumption may not necessarily be valid, it is a fact that cyberterrorism poses a significant threat and needs to be addressed. Therefore, one strategy for addressing cyberterrorism is preventing cyberterrorist attacks before they occur.

To a large extent, there are no marked differences between preventing domestic and international cyberterrorism since both threats occur or are transmitted via computer networks [8], given the interconnected nature of computer networks that effectively blurs the distinction between what is considered a local or domestic cyber threat and an international one, cyberterrorism prevention strategies tend to focus more not on the geographical location of the source of the threat but rather the vulnerability of local or domestic computer networks [12]. Still, acts of domestic cyberterrorism tend to be easier to uncover than international ones under the ease with which sources or origins of such threats can be tracked and traced. It explains why sharing intelligence on vulnerabilities and threats is one of the most influential and preferred ways of preventing domestic cyberterrorism [9]. Put differently, sharing information plays an increasingly important role in the fight against domestic and cyberterrorism [11].

As noted, any method to prevent cyberterrorism includes defining the infrastructure targeted and the people involved. At least considering and understanding the targeted infrastructure and the people involved has been determined to be a more effective way of preventing or responding to an attack. The people in this regard include analysts, investigators, and subject matters. On the other hand, the appropriate infrastructure has to be in place to allow responders to share information with other stakeholders [2]. Two of the most well-known and widely used domestic cyberterrorism prevention methods are the use of legislation and the sharing of data [13]. Since deterring cyberterrorism depends on perpetrators' perceptions of the expected punishment and ease of getting caught, legislation and information sharing are critical. While the predicted punishment depends mainly on the legal national framework, the probability of getting caught largely relies on the ability of perpetrators to be identified and cooperation for information sharing among a nation's counterterrorism or other security agencies [3].

4.1. Role of Legislation in Preventing Cyberterrorism

Legislation is essential in preventing cyberterrorism, but it should be considered alongside other techniques for a comprehensive approach. Here are some different techniques commonly used in preventing cyberterrorism:

1) Technical Measures: This includes firewalls, intrusion detection systems, encryption, and other security technologies to protect networks and systems from cyberattacks.

2) Information Sharing: Collaboration and threat intelligence sharing between government agencies, cybersecurity organizations, and private sector entities can help identify and mitigate cyber threats more effectively.

3) International Cooperation: Since cyberterrorism is a global issue, international cooperation through agreements and partnerships is crucial for combating it effectively, which involves sharing information, coordinating responses, and jointly taking action against cybercriminals.

4) Awareness and Education: Educating individuals, organizations, and governments about cybersecurity risks and best practices is essential for prevention, which includes training employees to identify and respond to cyber threats and increasing public awareness about online safety.

5) Public-Private Partnerships: Collaboration between government agencies and private sector organizations can enhance cybersecurity efforts. Sharing expertise, resources, and information can strengthen defenses against cyberterrorism.

When comparing legislation to these techniques, it is crucial to consider that legislation provides legal frameworks and enforcement mechanisms to address cyberterrorism. It can define crimes, establish penalties, and empower authorities to investigate and prosecute cybercriminals. Legislation can also compel organizations to implement cybersecurity measures and report incidents. However, more than legislation is required to prevent cyberterrorism. Technical measures, information sharing, international cooperation, awareness, and public-private partnerships are also necessary for a comprehensive approach to cybersecurity. These techniques complement legislation by focusing on proactive measures, building defenses, enhancing collaboration, and raising awareness.

Additionally, it has to be noted that international law does not explicitly prohibit cyberterrorism. However, several countries, including the U.S., have enacted and implemented national cyberterrorism laws, most of which have provisions that make it an offense to carry out malicious acts aimed at interfering with the functioning or destroying critical infrastructure [13]. These national laws are motivated mainly or inspired by several provisions of some United Nations (U.N.) international conventions and protocols that explicitly prohibit acts of terrorism against critical infrastructure sectors like transportation, nuclear, and government. Notable examples of such conventions include the 1980 Convention on the Physical Protection of Nuclear Material and the 1963 Convention on Offences and Certain Other Acts Committed on Board Aircraft (and its supplementary Protocol of 2014) [14].

However, the use of national legislation to prevent or fight cyberterrorism is often associated with the risk of such laws being misused by governments to undermine the fundamental freedoms and rights of the people [15], primarily due to the subjective nature of cyberterrorism, whose definition is country-specific. Cyber-attacks increase the risk of certain acts being mislabeled as constituting cyberterrorism with detrimental consequences. Further, this could explain why critics of specific cyberterrorism laws contend that legislation tends to be overly broad and designed to be used by governments to prosecute dissidents and activists [13].

4.2. Cybersecurity Information Sharing Act

The Cybersecurity Information Sharing Act (CISA) is a U.S. federal law that encourages sharing cybersecurity threat information between government and private sector entities (see Appendix A). It is just one of many techniques used to prevent cyberterrorism. Here are some other standard techniques and how they compare to CISA:

1) Network Monitoring and Intrusion Detection Systems (IDS): These systems monitor network traffic and detect any suspicious activities that may indicate a cyberattack or intrusion. CISA, on the other hand, focuses more on information sharing and collaboration to identify and respond to cyber threats rather than detecting them.

2) Encryption: Encryption is a technique used to protect sensitive data by encoding it, making it unreadable to unauthorized parties. While CISA does not directly address encryption, it can play a role in cybersecurity efforts to protect information that is being shared and transmitted.

3) Vulnerability Management: This technique involves identifying and addressing software, systems, and network vulnerabilities to prevent cyberterrorist exploitation. CISA complements vulnerability management by providing a framework for sharing information about emerging threats and vulnerabilities, enabling organizations to protect their systems better.

4) Incident Response Planning: Organizations develop incident response plans to outline the steps and procedures to be followed during a cyberattack. CISA helps improve incident response planning by facilitating the exchange of threat intelligence and best practices among public and private entities.

5) Employee Training and Awareness: Human error is often a weak point that cyberterrorists exploit. Organizations can reduce the risk of successful attacks by providing cybersecurity training and promoting employee awareness. While CISA does not directly involve employee training, it indirectly increases cybersecurity awareness through information sharing.

It is important to note that CISA is just one of many techniques and strategies to prevent cyberterrorism. The effectiveness of these techniques may vary depending on the specific organization, threat landscape, and cybersecurity goals. Adopting a holistic approach by combining multiple techniques and staying updated on industry best practices is recommended.

As information sharing in the context of domestic cyberterrorism is discussed, the Cybersecurity Information Sharing Act (CISA) comes to the fore. As one of the most important yet controversial federal cyber security laws of the U.S., CISA was explicitly designed to help improve cybersecurity within the U.S. by, among other ways, facilitating and encouraging the sharing of information on and about cybersecurity threats. Specifically, CISA has provisions that permit sharing of Internet traffic information between government agencies and manufacturing and technology companies within the U.S., especially during a cybersecurity threat [15]. However, the available research on CISA focuses on its con-

troversial provisions. Additionally, CISA's value has been questioned, with those opposed to it contending that it shifts responsibility from businesses to the government and, in doing so, increases the vulnerability of private data and information. Furthermore, CISA has been opposed to or criticized for leading to the dispersion of confidential information across the different government agencies [14].

Proponents argue that CISA does not necessarily require companies to share such personal information, but that receipt of such information from private companies is achieved through a particular system [15]. Regardless of the specific approach used, CISA has been primarily portrayed as making confidential information vulnerable by sharing it with law enforcement agencies with possible far-reaching implications for personal data security. As mentioned earlier, CISA is perceived as a tool the government uses to target and punish dissenters by mislabeling them as cyberterrorists and, therefore, punishing them [2]. While CISA has provisions that supposedly prevent sharing personal data deemed irrelevant to cybersecurity [15], it is easier for government agencies and private companies to determine which data or information is relevant or irrelevant after first accessing it. Ultimately, CISA effectively means that all confidential data will likely be accessed by the seven security agencies, including the police and the NSA. The implication is that while information shared can be used to prosecute cyberterrorism offenses, it can also be used to prosecute other crimes [11].

Moreover, some researchers agree that for cyber terrorists, the likelihood of launching a cyberattack depends on the perceived ease of getting caught [4] [5] [16]. As rational actors, cyberterrorists weigh their actions' costs and benefits before deciding whether to launch an attack. An attack is only likely to be undertaken if expected rewards exceed costs [5]. The implication is that cyberterrorism attacks are likely to be prevented if terrorists are made to believe that they are being tracked down, which is where sharing of information is critical.

Among other purposes, enhanced and coordinated sharing of important information regarding suspected terrorist activities, such as propaganda, messaging, disinformation, misinformation, and fake news, can go a long way in helping detect and even apprehend suspects [3]. Interagency cooperation in information sharing is crucial, especially where several security agencies are responsible and involved in the fight against cyberterrorism. Everyone shares cyberspace; by extension, any attack will likely affect everyone. Moreover, cyberterrorism is hard to detect, and perpetrators are challenging to identify. Therefore, only interagency cooperation can help make such identification and detection possible and more accessible [10].

Prior to the 9/11 terrorist attacks, it is alleged that there was a poor or total lack of cooperation and coordination among the different agencies responsible for U.S. internal (homeland) security. Information lapses were particularly notable, with some agencies having had practical intelligence but either failed to share it or delayed sharing it [13]. Such mistakes could become particularly costly in

cyberterrorism, where information sharing is especially critical. Through enhanced interagency cooperation in information sharing, security agencies stand better chances of preventing and deterring attacks by domestic cyberterrorists [13], which is where CISA comes into play.

Furthermore, CISA makes it possible and more manageable for suspected or known cyberterrorists to be identified, tracked down, and prosecuted [16]. As such, the mere existence of the legislation increases the cost for cyber terrorists. CISA also reduces the rewards associated with engagement in cyberterrorism as it effectively makes it harder for cyber terrorists to generate, share, and disseminate misinformation, fake news, disinformation, and misinformation, all craved by cyber terrorists. Given that cyberterrorists thrive on publicity [12], any legislation that diminishes or eliminates such publicity effectively reduces these cyberterrorists' expected rewards from engaging in cyberterrorism.

5. Information Sharing: Benefits and Enablers

Some researchers have described terrorism as the purest form of information warfare since acts of terrorism impact many people and utilize information [17]. Indeed, giving messages is essential for terrorists; this messaging is usually done by creating an environment of tension and fear among the masses. In essence, terrorism-related actions' main objective and effect are to convey particular messages, ensure the masses are horrified, and terrorize the people through influence (often done through communications) [20]. Terrorists will, therefore, use the media and mass communication tools as the stage for carrying out their activities [18].

Preventing domestic cyberterrorism entails stopping people from either supporting violent extremism or becoming terrorists by, among other possible actions, ensuring that any material, information, or communication that encourages radicalization by glorifying violent extremists is acted against [1] [19]. This measure entails targeting sources of information and how the data is generated and shared. Since the generation of information is in itself complex to police or monitor, more focus has been placed on the sharing or dissemination of extremist details [13]. While virtually all communication channels can be used to encourage radicalization, the Internet is particularly notable. Therefore, the main focus is usually on suspicious information posted on and disseminated over the Internet [18].

In this regard, two kinds of information can be singled out as important and worth sharing (see **Appendix A**). The first is information about a cyberterrorism threat, which can help prevent the threat from becoming an actual attack. This information is shared with intelligence agencies for appropriate action [20]. The second type of information is designed to radicalize. Terrorists usually use such information to recruit or solicit support for their cause and activities, and it should be identified, labeled, and shared among security and intelligence agencies for appropriate action [10]. Members of the public also need to be involved in the

sharing of information. Specifically, they need to constantly look for suspicious info, including information deemed misleading, deceptive, or fake news. Such information should be reported to relevant authorities for appropriate action. Either way, sharing information is critical in the prevention of domestic cyber-terrorism.

An important issue in preventing domestic cyberterrorism is deterrence. Regarding terrorism, the priority of actions taken is usually symbolic and not result-oriented, as in conventional warfare [17]. These symbolic actions restrain terrorists or potential terrorists from acting at a time and place they consider undesirable. For terrorists, an act of destruction or violence that is not newsworthy, locally or internationally, is not worth their time and effort. Ultimately, terrorists tend to refrain from carrying out attacks if these attacks are less likely to generate a lot of media attention [18]. As a result, counterterrorism efforts must focus on limiting or preventing all kinds of publicity surrounding terrorism and terrorist-related activities. Moreover, the focus has to be defeating terrorists in their information game, whereby this approach neutralizes not only those likely to perpetuate the act of terrorism but also those who support terrorism and terrorists [21]. In essence, the prevention of domestic cyberterrorism has to focus not just on the violence caused or likely to be caused but also on the beliefs and opinions responsible for driving some people into using, tolerating, or supporting violence.

As was rightly argued before, ICTS plays a crucial role in promoting and supporting terrorism but also engagement in acts of terrorism [20]. Notable terrorist acts that are committed or executed using (or through) various ICTs include but are not limited to the spreading of propaganda (that includes incitement, radicalization, and recruitment to terrorism), financing of terrorist or terror-related activities, planning off terrorist attacks, and carrying out terrorist attacks [12]. The one feature common to all these acts is the centrality of (or reliance on) information. While all forms of terrorist attacks require careful coordination and planning that, in turn, depend on accurate conveyance and sharing of information among terrorists, cyberterrorism is mainly dependent on information [18]. Ironically, in turn, this explains why preventing cyberterrorism depends, to a large extent, on the ability and capacity of counterterrorism agencies to quickly and deliberately share information about known and suspected threats. Like is the case with most (if not all) terrorist attacks, domestic cyberterrorism and cyberterrorism as a whole rely on open-source information and secret communications. Intercepting this information and communications is critical to disrupting cyber-attacks [20].

Information sharing is also vital whereby, more often than not, it is usually difficult or even impossible to determine the exact nature of a cyberattack (whether it is an act of terrorism or a mere criminal act), the origin of the attack (local versus international), and the people responsible for the attack [11]. Most of the time, the only valid and reliable information is the knowledge that an attack has

occurred. With such confusion and lack of clarity, multiple agencies or organizations are likely to respond to an attack. These responders could include those concerned with cybercrime, those dealing with cyberterrorism, and those involved with overall external security. Only once the attack gets properly defined and classified (as an act of cyberterrorism) can it be assigned to the relevant agency [17]. The gist of the argument refers to the sharing of information, especially intelligence, is critical in preventing cyberterrorism since there is usually no telling which security agency is likely to identify a threat first. The earlier and faster a threat is identified and relevant agencies notified, the higher the chances that a planned or impeding act of cyberterrorism can be prevented or thwarted [21].

The value of information sharing in countering domestic cyberterrorism illustrates how terrorists and other extremist groups usually target individuals for recruitment and radicalization by using social media platforms, traditional media, networking sites, and online propaganda [20]. Since these channels rely heavily (if not exclusively) on information sharing, good and effective strategic communications are on the part of counterterrorism players; however, there are good and not-so-good practices in using strategic communications. Therefore, the focus has to be on identifying the sound patterns to use in preventing the appeal of not just terrorism but violent extremism as well. Of particular importance is the need to address threats posed by narratives often employed by domestic terrorists by, among other measures, engaging nongovernmental organizations and local communities in developing tailored strategies for countering violent extremist narratives [12].

It has to be reiterated that violent extremist narratives should be prioritized since the focus has to be on preventing as opposed to fighting terrorism. Such prevention tends to be more effective if the violent extremist narrative that often encourages or leads to the commission of acts of terrorism is identified and prevented [18]. Additionally, this includes monitoring the communication, as mentioned earlier, channels for misinformation, disinformation, fake news, and propaganda. While misinformation is used to describe false information that is spread regardless of whether there is intent to mislead, disinformation describes information that is biased or deliberately misleading [8]. Therefore, disinformation is synonymous with propaganda and is also used to refer to manipulated facts or narratives. Propaganda, on its part, specifically refers to information utilized to promote a given point of view or political cause (especially if it is misleading or biased) [17].

A less commonly used term is mal-information, which describes the information that is true but whose sharing or dissemination is done to cause harm [22]. Misinformation and disinformation are closely related to (but distinct from) fake news, which can be described as information that not only mimics mainstream news interns of form but is also totally fabricated, misleading, emotionally charged, sensational, and purposefully crafted [11]. Often, terrorists use misinformation, disinformation, and fake news to spread their narrative and, in doing so, achieve

one of their goals of causing fear and panic among members of the public. Therefore, preventing or curbing disinformation, misinformation, malformation, and fake news is critical in preventing domestic terrorism. Such behavior requires close monitoring of—even possibly control—all or most media (especially new media such as social media) [20].

Technological and Compliance Challenges of Information Sharing

Technology is a significant challenge associated with information sharing (see **Appendix A**). In the 21st century, new media such as social media, blogs, and networking sites have facilitated communication. Therefore, it is much easier for terrorists to spread disinformation, misinformation, and fake news, whereby, unlike traditional media, such new media tends to be difficult or even impossible to regulate. Today, unlike in the past, any information can spread worldwide in seconds, owing to the widespread reach and use of new forms of media. Terrorists use this to disseminate false or misleading information to advance their agenda [18].

Therefore, it is sometimes impossible for counterterrorism agencies to prevent misinformation, disinformation, and fake news from being generated and spread [21]. Suppose traditional media were the only channels through which information was shared. However, this is virtually impossible in the information age, where social media and other new media reign supreme and are the preferred mode of communication [17].

In a democracy like the U.S., where freedom of expression is highly esteemed, regulating or controlling information generation, use, and dissemination is even more challenging. While authorities can conceivably prosecute individuals and organizations for generating, sharing, or disseminating false or misleading information, this often occurs when it is too late to avert the damage [21]. Moreover, it can be challenging for security agencies, let alone members of the public, to distinguish between accurate information on the one hand and misinformation, disinformation, and fake news on the other [14].

Some technologies also make it impossible for those posting and spreading misinformation, disinformation, and fake news to be identified or for the recipients of such information not to trace their sources or points of origin [4]. Further, this has made sharing important information among law enforcement or counterterrorism agencies extremely difficult.

Ultimately, the responsibility for sharing information lies—or should lie—with the person or people who generate the information. At least, this should be the case in a democratic country such as the U.S., where data is supposed to be free from censorship. However, it is a fact that generators of information and those who disseminate it do not pay attention to its accuracy [10]. Therefore, it has been proposed that media companies or platforms should be held accountable for misinformation, especially disinformation (as well as fake news). Recently, especially after the advent of social media, the debate has shifted to the need to censor technology companies that own platforms where misleading, false, or in-

appropriate information is posted and subsequently shared or disseminated [1].

However, compliance with such measures remains a significant challenge even if they were to be implemented. Technology companies such as Facebook, Twitter, and YouTube cannot stop users from posting content on their platforms. After all, these platforms are designed to post and share content. Moreover, there is reason to believe these companies are negatively affected by disinformation, misinformation, and fake news. Furthermore, they want to prevent such information from being posted and shared on their platforms. However, they mostly cannot do so for logistical and legal reasons [12]. Legally, preventing specific people, even suspected terrorists or extremists, from using particular social media platforms is discriminatory and violates their constitutional rights [16]. Therefore, the requirement to share personal data and information about suspicious activity and people is challenging to implement as it violates or can potentially violate their privacy policies with e force.

Minimally, technology companies can erase misleading information once posted. Unfortunately, erasing already posted information comes with the risk that it has long been shared with many other people by the time it is done. Sometimes, companies flag information as misleading, fake news, or outright disinformation [4]. While this is no doubt applicable as it warns subsequent recipients or audiences of the true nature of the information, it does not stop the information from being acted upon by those targeted. Moreover, the data will most likely have been shared by others by the time it is flagged [16]. Ultimately, media companies and even users of social media platforms cannot comply with laws governing or prohibiting the generation or sharing of information considered false, fake, or misleading.

Then there is the issue of jurisdiction. Within cyberspace, there needs to be a clearer understanding of where one's jurisdiction starts and ends since cyberspace is not defined by geographical boundaries—no national or international laws [14]. Since cyber terrorists are difficult to detect, there is usually no telling whether they fall within a given national jurisdiction and are subject to a country's federal laws. A terrorist group responsible for an attack may be appropriately determined to be physically located in a given place. However, there may still be challenges and questions regarding whether such a group may be considered a subnational group. Defining a subnational group within cyberspace is challenging [21]. Ultimately, it is not immediately clear which government should have responsibility for which terrorist group (especially where and when the group operates locally but has an international cell). These jurisdictional challenges render compliance with and enforcement of national laws challenging.

Technological Challenges

- Data Format Incompatibility: If multiple parties share information, technical challenges may be involved in ensuring all systems can read and process the data that can be tackled by defining standardized data formats that everyone can use.

- Data Security and Privacy: With information sharing, there is always a risk that sensitive data could be exposed to unauthorized parties. Encryption and access controls can help mitigate these risks.
- Data Volume Management: Too much data can overload information, impeding decision-making. Data compression and prioritization tools can help manage this.

Compliance Challenges

- Data Governance and Regulatory Compliance: Information sharing may need to comply with specific regulatory frameworks or industry standards, which can be addressed by establishing clear governance policies and workflows that ensure compliance.
- Data Retention and Destruction: There may be requirements to retain certain types of data for a certain period or to delete data after a specific time. Tools that automate retention and destruction can help manage this.
- Data Access and Auditing: Controlling who can access shared data and ensuring that all access is logged and monitored is crucial to maintaining compliance. Access controls and audit trails can help manage this.

Counter-Measures

- Establish Information Sharing Agreements: Clearly define the shared data, how, and by whom.
- Use Data Standards and Interoperability: Adopt standardized data formats and communication protocols to increase compatibility for information sharing.
- Secure Data Exchange: Use encryption, access controls, and other security measures to prevent unauthorized access and ensure data privacy.
- Automate Compliance: Use tools that automate data retention, destruction, access control, and audit trails to help comply with regulations.

The key to addressing technological and compliance challenges in information sharing is establishing clearly defined governance policies and workflows and using appropriate technical tools to facilitate sharing and ensure compliance.

6. Comments on the Methodology

As a multidisciplinary subject matter, cyberterrorism has been investigated using various methods, including primary and secondary research. Regarding secondary research, most research on the subject matter has utilized systematic literature reviews, document analysis, and Internet searches. Primary research methods include questionnaires, surveys, structured and unstructured interviews (direct and indirect over the telephone), and participant observation. Some researchers have investigated the topic using focus group discussions with selected experts or people with firsthand knowledge or experience on the subject (i.e., counterterrorism, cybercrime, and other security experts). At least one researcher utilized cyber-terrorism training exercises in different places and times. Therefore, available research on the subject matter can be reasonably reliable despite the

vast array of methods used by the researchers, and most of them reached a consensus on most of the issues investigated.

7. Gaps in Knowledge

Based on the initial literature review, it is evident that cyberterrorism and strategic communications have generated much interest among scholars, practitioners, and policymakers from various disciplines. Cyberterrorism is multidisciplinary, from politicians and legal practitioners to cybersecurity and technology experts, explaining why a large body of scholarly and non-scholarly research exists. Among the most widely researched issues in this respect include (but are not necessarily limited to) the meaning of cyberterrorism, how cyberterrorism differs from other cyber-related offenses such as cybercrime, and the threat (both real and perceived) posed by cyberterrorism to the U.S. In addition, the prevention or deterrence of cyberterrorism and the techniques that can be used to fight cyberterrorism have also been widely researched. Specifically, the role of information sharing in the fight against cyberterrorism has been widely investigated. When used in this manner and context, information sharing is portrayed mainly by researchers as forming part of strategic communications.

8. Conclusions

Notably, some significant gaps in knowledge remain, especially regarding the more specific theme of domestic cyberterrorism. To a large extent, researchers must still start distinguishing between domestic and non-domestic (international or global) cyberterrorism. As a result, this could be attributed to cyberspace being effective without geographical boundaries [13]. Therefore, it is an oxymoron to classify cyberterrorism based on either being international or domestic. Subsequently, researchers have deliberately or inadvertently avoided using this distinction and instead approach the issue of cyberterrorism holistically.

By extension, available research on the prevention or deterrence of cyberterrorism applies to cyberterrorism more generally and not specifically to domestic cyberterrorism. Similarly, the various aspects of information sharing concern cyberterrorism in general and not domestic cyberterrorism; If anything, the very meaning of domestic cyberterrorism is not precisely clear and is primarily derived from the importance of domestic terrorism.

Given the identified gaps in knowledge, future researchers may be interested in asking and possibly conducting research around the following questions:

1) How exactly does domestic cyberterrorism differ from non-domestic (international or global) cyberterrorism?

2) To what extent does domestic cyberterrorism threaten national security?

3) In which ways is information sharing sufficient (or inadequate) in preventing domestic cyberterrorism?

4) How effective has CISA been in preventing domestic cyberterrorism?

5) What extra measures, if any, are needed for the relevant security agencies to

effectively and sustainably mitigate the threat posed by domestic cyberterrorism?

Acknowledgements

I want to express my special appreciation to my committee member and Chair, Dr. Ian A. McAndrew, FRAeS, Dean of Doctoral Programs and Engineering Faculty. I am grateful for Dr. McAndrew's timeless support in encouraging my research and writing to continue developing as a scientist and pursuing a third doctorate. Dr. McAndrew's advice on research and academia remains priceless. I would also like to thank Carmit Levin for her enduring support-furthermore, thanks to my cousin, Ms. Maria Boston, whose academic inputs were invaluable.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Harrison Dinniss, H.A. (2018) The Threat of Cyber Terrorism and What International Law Should (Try to) Do about It. *Georgetown Journal of International Affairs*, **19**, 43-50. https://doi.org/10.1353/gia.2018.0006

[2] Janparvar, M., Salehabadi, R. and Ahmadi, S. (2019) Management of Strategic Cyberspace Boundaries to Control Cyberterrorism. *Soft Power Studies*, **8**, 99-126.

[3] Kerttunen, M. (2020) Cyberterrorism: A Schrödinger's Cat. In: Tikk, E. and Kerttunen, M., Eds., *Routledge Handbook of International Cybersecurity*, Routledge, London, 161-173. https://doi.org/10.4324/9781351038904-15

[4] Veerasamy, N. (2020) Cyberterrorism—The Specter That Is the Convergence of the Physical and Virtual Worlds. In: Benson, V. and Mcalaney, J., Eds., *Emerging Cyber Threats and Cognitive Vulnerabilities*, Academic Press, Cambridge, 27-52. https://doi.org/10.1016/B978-0-12-816203-3.00002-2

[5] Droogan, J. and Waldek, L. (2018) Should We Be Afraid of Cyber-Terrorism? *International Journal of Electronic Security and Digital Forensics*, **10**, 242-254. https://doi.org/10.1504/IJESDF.2018.093017

[6] Jarvis, L. and Macdonald, S. (2015) What Is Cyberterrorism? Findings from a Survey of Researchers. *Terrorism and Political Violence*, **27**, 657-678. https://doi.org/10.1080/09546553.2013.847827

[7] Mayer Lux, L. (2018) Defining Cyberterrorism. *Revista chilena de derecho y tecnología*, **7**, 5-25. https://doi.org/10.5354/0719-2584.2018.51028

[8] Schoen, F. and Lamb, C.J. (2012) Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference. National Defense University Press, Washington DC.

[9] Broeders, D., Cristiano, F. and Weggemans, D. (2021) Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy. *Studies in Conflict & Terrorism*. https://doi.org/10.1080/1057610X.2021.1928887

[10] Jarvis, L., Macdonald, S. and Nouri, L. (2014) The Cyberterrorism Threat: Findings from a Survey of Researchers. *Studies in Conflict & Terrorism*, **37**, 68-90. https://doi.org/10.1080/1057610X.2014.853603

[11] Klein, J.J. (2015) Deterring and Dissuading Cyberterrorism. *Journal of Strategic Security*, **8**, 23-38. https://doi.org/10.5038/1944-0472.8.4.1460

[12] Denning, D.E. (2001) Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. In: Arquilla, J. and Ronfeldt, D., Eds., *Networks and Netwars*: *The Future of Terror*, *Crime*, *and Militancy*, RAND, Santa Monica, 239-288.

[13] Nechyporuk, M., Pavlikov, V., Filipenko, N., Spitsyna, H. and Shynkarenko, I. (2020) Cyberterrorism Attacks on Critical Infrastructure and Aviation: Criminal and Legal Policy of Countering. In: Nechyporuk, M., Pavlikov, V. and Kritskiy, D., Eds., *ICTM* 2020: *Integrated Computer Technologies in Mechanical Engineering*-2020, Springer, Cham, 206-217. https://doi.org/10.1007/978-3-030-66717-7_17

[14] Nweke, L.O. and Wolthusen, S. (2020) Legal Issues Related to Cyber Threat Information Sharing among Private Entities for Critical Infrastructure Protection. 2020 12*th International Conference on Cyber Conflict* (*CyCon*), Estonia, 26-29 May 2020, 63-78. https://doi.org/10.23919/CyCon49761.2020.9131721

[15] Yang, A., Kwon, Y.J. and Lee, S.Y.T. (2020) The Impact of Information Sharing Legislation on the Cybersecurity Industry. *Industrial Management & Data Systems*, **120**, 1777-1794. https://doi.org/10.1108/IMDS-10-2019-0536

[16] Vakilinia, I., Tosh, D.K. and Sengupta, S. (2017) Privacy-Preserving Cybersecurity Information Exchange Mechanism. 2017 *International Symposium on Performance Evaluation of Computer and Telecommunication Systems* (*SPECTS*), Seattle, 9-12 July 2017, 1-7. https://doi.org/10.23919/SPECTS.2017.8046783

[17] Korte, J. (2017) Mitigating Cyber Risks through Information Sharing. *Journal of Payments Strategy & Systems*, **11**, 203-214.

[18] Rantos, K., Spyros, A., Papanikolaou, A., Kritsas, A., Ilioudis, C. and Katos, V. (2020) Interoperability Challenges in the Cybersecurity Information Sharing Ecosystem. *Computers*, **9**, Article 18. https://doi.org/10.3390/computers9010018

[19] Jarvis, L. and Macdonald, S. (2014) Locating Cyberterrorism: How Terrorism Researchers Use and View the Cyber Lexicon. *Perspectives on Terrorism*, **8**, 52-65.

[20] Ramadhan, I. (2020) Cyber-Terrorism in The Context of Proselytizing, Coordination, Security, and Mobility. *Journal of Islamic World and Politics*, **4**, 179-197. https://doi.org/10.18196/jiwp.4252

[21] Abbasi Kalimani, A., Mahboubi, M. and Noori, F. (2020) New Strategies to Prevent Cyber Terrorism. *Crime Prevention Approach*, **3**, 145-172.

[22] Wardle, C. and Derakhshan, H. (2017) Information Disorder: Toward an Interdisciplinary Framework for Research and Policy-Making. Council of Europe, Eurométropole de Strasbourg. https://rm.coe.int/information-disorder-report-november-2017/1680764666

Appendix A: Mind Map