Journal of Criminology and Forensic Studies
ISSN: 2640-6578

Academic Strive
Researcher's perception is our reality

*Research Article* *Volume 5 Issue 1*

# Cyber-Terrorism A Wicked Problem

**Ajay C***

Chawla & Co., Delhi High Court, India

***Corresponding author:** Ajay Chawla, Chawla & Co., Delhi High Court, India, Tel: +91-9711777033; Email ID: advajaychawla@gmail.com

**Received Date:** September 03, 2023; **Published Date:** September 21, 2023

## Abstract

This research was undertaken to elucidate the legal framework governing cyber terrorism from the perspective of organized transnational crime, alongside an analysis of the varied modus operandi employed by cyber terrorists. The research adopts a normative legal approach, employing qualitative methodologies to gather data through an exhaustive examination of pertinent laws and regulations concerning cyber terrorism. As a normative legal study, secondary data sources serve as the foundation for the research. The research findings unveiled several international conventions capable of serving as legal instruments to address cyber terrorism. Additionally, the study identified diverse methods employed by terrorists to perpetrate cyber terrorism, including hacking, propaganda dissemination, fraudulent activities, Distributed Denial of Service (DDoS) attacks, and the distribution of viruses, worms, and malware. The research outcomes underscore that although a dedicated legal instrument specifically governing cyber terrorism is absent, several existing international conventions hold relevance and potential utility as resources for cyber terrorism law. It is noteworthy that a spectrum of modus operandi is utilized by cyber terrorists in their activities. Combating cyber terrorism and cyber-crime requires understanding how cyber terrorists act, what motivates them, and how to prevent their attacks. This guide looks at the evolution of cyber terrorism, highlights examples of cyber terrorism and cyberattacks, and offers tips for thwarting cyberattacks.

**Keywords:** Cyber Security; Cyber Crime; Cyber Terrorism; Terrorist; Hacking; Offense; Crime; Unethical; Guidelines

## Introduction

In recent times, the realm of cyber warfare has experienced an exponential surge, orchestrated by a diverse array of actors including hacktivists, governmental and non-governmental entities, non-state groups, and even terrorists. In today's technologically driven world, our reliance on computers and technology has reached unprecedented levels. The swift evolution of technology and information in the new era has not only granted convenient accessibility to the masses but has also brought forth novel threats.

Amid its advantages, the cyber landscape also harbors adverse effects and opportunities for malicious individuals to perpetrate cybercrimes. These cybercrimes bear a transnational nature, transcending geographical and temporal boundaries. Consequently, their impact extends beyond individuals to encompass organizations, nations, and legal interests safeguarded across multiple jurisdictions.

In today's era of globalization, profound transformations unfold, yielding both favorable and unfavorable outcomes. This global integration yields advancements in communication and transportation technologies while simultaneously reshaping political, social, and economic systems across the globe. Yet, this tide of globalization brings not only positive impacts but also negative consequences, one of which involves the surge of transnational crimes, notably terrorism [1].

Terrorism, in all its forms, constitutes a grave offense imperiling human values, disrupting public safety for both individuals and assets. It often targets state institutions, military/security establishments, and key figures within governance, such as heads of state or governments, strategic installations, and densely populated areas.

In today's context, terrorist groups have harnessed the virtual realm, transforming it into a new theater of operation. No longer reliant solely on traditional weapons like firearms and explosives, these groups have adopted a more sophisticated approach, centering on technology-driven strategies and tactics. Their activities have evolved beyond mere propaganda, training, fundraising, and physical attacks. They have expanded their scope to include cyber operations aimed at sabotaging online infrastructure, often executed from remote locations and cloaked in layers of technological concealment. This modern manifestation of their actions is commonly referred to as "cyber-terrorism."

The landscape has witnessed a shift, where formerly crime-free digital domains have now become host to cybercrimes. Traditional crimes have transitioned into cybercrimes, bringing about a transformative shift. The existing legal framework, such as Indonesia's Information and Electronic Transactions Law, falls short in explicitly addressing the intricacies of cyber-terrorism. The evolution is evident; tasks that once consumed significant time, like propaganda, recruitment, and training, now occur in mere seconds through easily accessible internet-integrated tools.

In this evolving milieu, novel crimes such as cyber hoaxes, cyberbullying, and cyber jihad have emerged. Given the intricacy and contemporary nature of these offenses, the legal framework demands revitalization to effectively combat cyber-terrorism and its multifaceted components.

## What is Cyberterrorism?

Cyberterrorism can be defined as the use of the internet and other forms of technology to disrupt, destroy, or threaten critical infrastructure and/or spread fear and panic, with the ultimate goal of causing physical or economic harm to a society or its people or Cyberterrorism is often defined as any premeditated, politically motivated attack against information systems, programs and data that threatens violence or results in violence. The definition is sometimes expanded to include any cyber-attack that intimidates or generates fear in the target population. Attackers often do this by damaging or disrupting critical infrastructure [2].

Emerging as a novel form of terrorism, this phenomenon capitalizes on the intricate interlinking and fragility of contemporary society's digital frameworks and networks, utilizing them to fulfill its malevolent goals. Over the past ten years, the specter of cyberterrorism has morphed into a progressively urgent focal point for both governmental bodies and enterprises. With technological progress persisting unabated and an expanding array of vital infrastructures joining the online realm, the capacity for cyber assaults to inflict substantial damage and turmoil has surged to unprecedented heights.

Various security organizations view cyberterrorism and the parties involved differently. The U.S. Federal Bureau of Investigation (FBI) defines cyberterrorism as any *"premeditated, politically motivated attack against information, computer systems, computer programs and data, which results in violence against noncombatant targets by subnational groups or clandestine agents."*The FBI views a cyberterrorist attack as different from a common virus or denial of service (DoS) attack. According to the FBI, a cyberterrorist attack is a type of cybercrime explicitly designed to cause physical harm. However, there is no consensus among governments and the information security community on what qualifies as an act of cyberterrorism.

Other organizations and experts have said that less harmful attacks can be considered acts of cyberterrorism. When attacks are intended to be disruptive or to further the attackers' political agenda, they can qualify as cyberterrorism, according to these other groups. In some cases, the differentiation between cyberterrorism attacks and ordinary cybercrime lies in the intention: The primary motivation for cyberterrorism attacks is to disrupt or harm the victims, even if the attacks do not result in physical harm or cause extreme financial harm.

In other cases, the differentiation is tied to the outcome of a cyber-attack. Many cybersecurity experts believe an incident should be considered cyberterrorism if it results in physical harm or loss of life. This can be either direct or indirect harm through damage to or disruption of critical infrastructure.

Physical harm is not always considered a prerequisite for classifying a cyber-attack as a terrorist event. The North Atlantic Treaty Organization, known as NATO, has defined cyberterrorism as a cyber-attack that uses or exploits computer or communication networks to cause "*sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal*."

According to the U.S. Commission on Critical Infrastructure Protection, possible cyberterrorist targets include the banking industry, military installations, power plants, air traffic control centers and water systems.

### Some Alternative Names for Cyberterrorism Include

- **Digital Terrorism**: This term emphasizes the use of digital technologies and the internet for terrorist activities.
- **Virtual Terrorism**: Highlighting the virtual or online nature of the attacks conducted for terroristic purposes.
- **Electronic Jihad**: Particularly associated with extremist groups using online platforms to spread propaganda and conduct attacks.
- **Cyber Jihad**: Similar to electronic jihad, it refers to the use of cyber means for ideological and political motives.
- **Techno-Terrorism**: This term underscores the use of technology to create fear and disruption in society.
- **InfoWar**: Referring to the use of information and communication technologies as tools of warfare, including terrorist activities.
- **Hacktivism**: While not exclusively related to terrorism, this term describes using hacking for political or social causes, which can include terrorist objectives.
- **Digital Warfare**: Highlighting the cyber aspect of modern warfare, which may involve terrorist actors as well.
- **Netwar**: Referring to conflict waged in the virtual domain, often involving non-state actors, which can encompass cyberterrorism.
- **Online Extremism**: Focusing on the spread of extremist ideologies and activities through online platforms, sometimes leading to cyberterrorism.

It's important to note that while these terms might highlight different aspects of cyberterrorism, they are often used interchangeably and can sometimes have varying interpretations depending on the context and perspective.

### What Internet Offer to Terrorists

The internet offers the following advantages to the terrorist:

- Easy Access
- Minimum Regulation, Censorship, or any type of Govt. control
- Potentially high audience spread throughout the world
- Anonymity
- Fast circulation of information
- Low-cost maintenance of web page
- A multimedia effect- ability to combine text, graphics, audio-visual and to allow user to download movies, songs, books, posters very fast

### The Modus Operandi of Cyber Terrorism

The modus operandi of cyber terrorism finds a noteworthy exponent in the activities of ISIS. This assertion stems from the distinctiveness of extremist organizations such as ISIS in their intensive and methodical utilization of cyberspace. Emerged in 2013 under *Abu Bakr al-Baghdadi's* leadership, ISIS exemplifies a paradigm of "*New Terrorism*" wherein computers and the internet serve pivotal roles in their terroristic pursuits. This novel dimension of terrorism extends their reach into cyberspace, aligning with ISIS's objective to evoke terror and uncertainty within society, distinct from merely causing loss of life.

Indeed, ISIS poses a palpable threat within the realm of cyberspace, with a notable factor being their adept recruitment of skilled hackers proficient in infiltrating systems and compromising target computers. The recruitment of experienced hackers bolsters their capability to execute cyber-attacks effectively, amplifying the menace they pose to virtual domains.

Moreover, ISIS has ingeniously adapted its jihad efforts to capitalize on the virtual sphere. Utilizing cyberspace as a tool, they target potential jihadists, propagating their beliefs and ideologies of jihad while recruiting new adherents. Concurrently, they leverage social media platforms to propagate their doctrine, actively encouraging "lone wolf" attacks among their supporters.

As part of their arsenal, ISIS employs *Hybrid Cyber terrorism*, merging diverse tactics like hacking, propaganda dissemination, and fraudulent activities under the veneer of charitable initiatives. This multifaceted approach underscores the evolving sophistication of their operations, marking them as a distinct and formidable presence within the landscape of cyber terrorism.

### Types of Cyber-Terror Capability

In 1999 the Center for the Study of Terrorism and Irregular Warfare at the Naval Postgraduate School in Monterey, California, defined three levels of cyber-terror capability:

- **Simple-Unstructured**: the capability to conduct basic hacks against individual systems using tools created by someone else. The organization possesses little target-analysis, command-and- control, or learning capability.
- **Advanced-Structured**: the capability to conduct more sophisticated attacks against multiple systems or networks and possibly, to modify or create basic hacking-tools. The organization possesses an elementary target-analysis, command-and-control, and learning capability.
- **Complex-Coordinated**: the capability for a coordinated attack capable of causing mass- disruption against integrated, heterogeneous defenses (including cryptography). Ability to create sophisticated hacking tools. Highly capable target-analysis, command-and-control, and organization learning-capability [3,4].

### Examples of Cyber Terrorism

- Introduction of viruses to vulnerable data networks.
- Hacking of servers to disrupt communication and steal sensitive information.
- Defacing websites and making them inaccessible to the public thereby causing inconvenience and financial losses.
- Hacking communication platforms to intercept or stop communications and make terror threats using the internet.
- Attacks on financial institutions to transfer money and cause terror.

### Terrorist Exploitation of Cyberspace: Motivations and Mechanisms

Cyberspace has emerged as a compelling arena for terrorist activities due to its potential to cause widespread and far-reaching impacts. In contrast to conventional physical violence, cyber-attacks can inflict substantial damage on a nation's infrastructure and systems. The effects of traditional terrorism, such as bombings, are localized to specific physical areas, affecting limited communities. Cyber terrorism, however, possesses the capability to reach a broader segment of the population, potentially granting terrorist groups greater influence in achieving their political and social objectives.

The driving force behind cyber terrorists is rooted in their political agendas. Their attacks are strategically aimed at critical systems and infrastructures, uniting the hackers within terrorist organizations towards a shared goal. This collaborative approach can amplify the impact beyond the efforts of individual hackers.

Several factors contribute to the attractiveness of cyber-attacks for terrorist groups:

- **Cost-effectiveness**: Given their resource constraints, terrorists find cyber-attacks appealing due to their cost-efficient nature. These attacks require fewer individuals and resources while concurrently affecting a significant number of people. The cost-to-benefit ratio is notably high.
- **Anonymity**: Cyber-attacks enable terrorists to operate remotely and maintain anonymity. They can establish operations in regions with weak governance, ensuring their concealment from authorities.
- **Ease of Execution**: Many potential targets remain inadequately protected, rendering attacks relatively straightforward to execute. Attackers have a wide array of vulnerable targets to choose from.
- **Swift Deployment**: Once set up, cyber-attacks can be launched rapidly without extensive preparation, allowing for quick implementation.
- **Absence of Physical Barriers**: Unlike conventional terrorism, cyber terrorists are not impeded by physical barriers or checkpoints.
- **Connection Speed Independence**: Attack speed and form are not reliant on the attacker's connection speed, enabling them to exploit the full potential of victim computers.
- **Combination with Physical Terrorism**: The synergy between physical and cyber terrorism is considered highly effective in achieving terrorists' objectives.

In tandem with these motivations, terrorist organizations leverage their websites to incite and facilitate attacks. These groups exploit modern information technology and the internet for various purposes:

- **Planning**: Formulating plans and strategies.
- **Funding**: Raising and laundering funds.
- **Propaganda**: Disseminating extremist ideologies.
- **Secure Communication**: Facilitating internal communication.
- **Information Exchange**: Sharing knowledge and insights with similar groups.
- **Command and Control**: Directing operations.
- **Recruitment**: Attracting new members.
- **International Support**: Garnering global backing.
- **Intelligence Gathering**: Collecting valuable intelligence.
- **Information Warfare**: Engaging in digital warfare on behalf of nations.

The internet provides an environment marked by limited regulation, vast audiences, anonymity, and rapid information dissemination, rendering it a potent tool for terrorist organizations.

A pertinent example is evident in the *PKK/KONGRA-GEL* terrorist organization's utilization of websites. These platforms disseminate organizational history, biographies, and political aims. Notably, websites like "pajkonline.com" target women, previously involved in suicide bombings, while others encourage hacking expertise and reveal system vulnerabilities. This multifaceted illustration underscores the pervasive disruptive potential of such activities [5].

### The Most Notable Cyberterrorism Attacks of Recent Years

- **SolarWinds Attack**: This massive cyber-attack was carried out in 2020 and affected several government agencies and large corporations, including the Department of Homeland Security, the Treasury Department, and the Commerce Department. The attackers used a sophisticated supply- chain attack to breach Solar Winds, a software company and then used access to their clients' systems to carry out their malicious activities. The attack was discovered to be the work of Russian state-sponsored hackers.

- **WannaCry Ransomware Attack**: This global attack took place in May 2017 and affected more than 200,000 computers in over 150 countries. The attackers used a ransomware virus that encrypted computer systems and demanded a ransom payment in exchange for the decryption key. The Wanna Cry ransomware was spread through vulnerability in Microsoft Windows, and many organizations were affected due to the widespread use of the operating system.
- **NotPetya Attack**: This cyber-attack took place in June 2017 and targeted Ukrainian businesses and government organizations. The attack was disguised as a ransomware attack but was actually aimed at causing widespread destruction to the targeted organizations' IT systems. The attack was carried out using malware that spread rapidly through a vulnerable software update mechanism. The attack was believed to be the work of Russian state-sponsored hackers.
- **Operation Cloud Hopper**: This was a widespread cyber espionage campaign carried out by the Chinese state-sponsored hacking group APT10. The group targeted multiple organizations across several countries and stole sensitive data from managed IT service providers. The group was known for its advanced tactics, techniques, and procedures (TTPs) and its ability to compromise and steal data from high-value targets.

These are just a few examples of the many high-profile cyber-terrorism attacks that have taken place in recent years. It's important for organizations to stay vigilant and implement robust security measures to protect against these threats [4].

### Cyber Terrorism Attacks Have Become More Sophisticated

A significant security trend in recent years is the escalation of the threats posed by cyber terrorism to governments, businesses, and individuals as new technologies are developed. Government Technology reports that the surge in cyberattacks that began in 2020 is continuing in 2021 as attacks become more frequent and more damaging.

- On February 5, 2021, hackers used a hole in an old version of Windows to break into the network of a Florida water treatment plant and boost the levels of sodium hydroxide (lye) to lethal levels. The attack was thwarted before any damage could be done by an operator who noticed the change and corrected the levels. However, the attack highlights the vulnerability of water systems and other vital infrastructure in the U.S.
- The FBI now considers ransomware as grave a danger to U.S. interests as terrorism in the aftermath of the attacks of Sept. 11, 2001, as the *New York Times* reports. The agency is currently analyzing 100 different software variants used in ransomware attacks by criminal gangs and by groups operating within China and Russia. Analysts expect more damaging attacks to target critical infrastructure in the U.S.
- In October 2021, the U.S. National Security Agency (NSA) warned businesses against using wildcard Transport Layer Security (TLS) digital encryption certificates to guard against a new type of malware called ALPACA (Application Layer Protocols Allowing Cross-Protocol Attack). ALPACA infiltrates hardened web applications via non-HTTP services that use a certificate identical to or similar to a TLS certificate. The technique tricks web servers into responding to encrypted HTTP requests using unencrypted protocols [5].

The threat posed by cyber terrorism looms substantial, even though it doesn't rely on direct physical violence to cause harm. This subtlety often leads to a lack of awareness about its potential peril. As society progressively transitions toward digital platforms to enhance efficiency and economize costs, the avenues for compromising IT systems multiply incessantly. The ongoing advancements in cyberspace further magnify this susceptibility.

### Current Threats

Presently, cyberterrorism stands as one of the most formidable security threats on a global scale, surpassing even the development of nuclear weaponry and ongoing international conflicts. This heightened significance is attributed to the omnipresence of the internet and the profound responsibilities entrusted to this technological landscape. Digital weapons wield the potential to disrupt entire economic and societal frameworks, making them uniquely menacing. Key international security apprehensions encompass the following:

- **DDoS Attacks**: Denial of Service (DDoS) attacks, which number in the millions annually, pose a substantial concern. The resulting service interruptions can inflict substantial financial losses, costing hundreds of thousands of dollars per hour. Countermeasures are imperative, involving both robust security protocols and redundancy strategies to ensure the continued online presence during such assaults.
- **Social Engineering**: A stark illustration of vulnerabilities surfaced in 1997 when an NSA experiment demonstrated that 35 hackers could breach crucial Pentagon computer systems with ease. This group could manipulate accounts, reformat data, and even bring entire systems

to a halt. Often, hackers employed phishing tactics, disguising themselves as technicians and even engaging in telephone conversations to illicitly obtain passwords.

- **Third-Party Software**: Prominent retailers are intricately linked to a multitude of third-party resources, with a staggering 23% of these resources revealing at least one critical vulnerability. These companies bear the responsibility of diligently managing and consistently reassessing their network security strategies to ensure the safeguarding of sensitive personal data.

In light of these threats, proactive measures are indispensable for safeguarding critical systems, enhancing user awareness against social engineering tactics, and bolstering security protocols to mitigate the risks associated with third-party software vulnerabilities.

### Future Threats

Anticipating the future, as technology becomes deeply intertwined with society, it brings forth a new array of vulnerabilities and security threats within the intricate web of our established networks. Intrusion into these networks carries the potential to imperil entire communities and economic systems. The fluidity of future events underscores the necessity for adaptable systems capable of evolving in response to the shifting landscape.

Among the foreseeable cyberterrorism threats, a pressing concern revolves around the remote work scenario induced by the COVID-19 pandemic. The assumption that every home office maintains up-to- date and secure configurations is unrealistic. Consequently, adopting a zero-trust policy for home devices becomes pivotal for companies. This policy hinges on treating corporate resources and potentially unsecured devices within the same context, thereby necessitating appropriate measures to protect sensitive information.

The ascent of cryptocurrency has introduced fresh security threats into the landscape. Cyber criminals now exploit home computers and corporate networks to mine cryptocurrencies like bitcoin. This mining process demands extensive computational power, thereby jeopardizing business networks and triggering significant downtime if unaddressed.

As the cyber landscape continuously evolves, proactive measures are indispensable, spanning the implementation of robust security protocols for remote work environments, the cultivation of vigilant practices regarding home devices, and strategies to thwart the exploitation of computing power for illicit cryptocurrency mining.

### Collaborating to Confront the Escalating Menace of Cyber Terrorism

The crusade against cyber terrorism commences with raising awareness among governments, businesses, and individuals about the expanding specter of cyberattacks and equipping them with counteractive knowledge. Essential to this effort are computer security experts who assume a pivotal role in preempting and alleviating the hazards presented by cyber terrorists to governmental bodies, enterprises, and societies. A blend of user enlightenment and cutting-edge security methodologies will effectively repel cyber terrorists and their digital felonies.

### Protecting Businesses from Cyber Terrorism Necessitates a Comprehensive Strategy Encompassing Various Measures

- **Implement Strong Passwords**: Recognize the potency of robust passwords. Software capable of swiftly cracking passwords underscores the necessity for complexity. You need to update passwords routinely, and never recycle them across various logins.
- **Stay Informed**: Maintain vigilance through staying current with cyber security updates and government advisories. Awareness of the latest threats empowers proactive preparation against potential acts of terrorism.
- **Foster Cyber Awareness**: Cultivate a workforce versed in cyber security. Engage all employees in comprehensive training and education, stressing the significance of sustained vigilance and prompt reporting of suspicious activities.
- **Vet Third-Party Vendors**: Acknowledge that a business's cyber defense extends to third-party vendors. Scrutinize potential vendors by demanding transparency about their cyber security practices prior to any agreements or transactions. This ensures the overall strength of the cyber security posture.

By combining these measures, businesses can substantially fortify their defenses against the evolving threat landscape posed by cyber terrorism.

## If You Find That One of Your Accounts has Been Compromised by Hacking, Follow these Step-By-Step Guidelines:

- **Update Your Devices**: Ensure that the operating systems and apps across your devices are up to date. These updates incorporate the latest security patches. If you use antivirus software, perform a scan using the most recent version, although this may not be necessary for mobile devices.

- **Contact Your Provider**: If you're locked out of your account, navigate to your account provider's homepage and locate the support or help section. This will outline the process for recovering your account.
- **Check Email Account**: If your email account was compromised, regain control and then inspect your email filters and forwarding rules. It's common for hackers to set up forwarding rules that send copies of your emails to their own accounts. Your provider's help pages should offer instructions on this.
- **Change Passwords**: Once you've ensured that no unauthorized forwarding rules are active, change passwords for all accounts linked to the compromised one. Additionally, modify passwords for accounts that send password reminders or resets to the hacked account.
- **Enable 2-Factor Authentication**: Implement 2-factor authentication (2FA) to add an extra layer of security against potential future breaches.
- **Notify Contacts**: Inform your contacts, friends, and followers about the hacking incident. This step not only updates them about your situation but also aids in preventing them from falling victim to similar attacks. Notify your contacts regardless of whether you've successfully regained control of your account.
- **Create a New Account**: If you're unable to recover your account, you might consider creating a new one. After doing so, inform your contacts about your new account. Remember to update your information on essential platforms like banks, utility services, and online shopping websites.

By adhering to these steps, you can navigate the aftermath of a hacking incident and bolster your defenses against cyber threats.

## Conclusion

Efforts are being actively pursued to enhance awareness among citizens, the judicial sector, and law enforcement agencies regarding the critical significance of averting computer-related crimes. Initiatives encompass the education of judges, officials, and law enforcement personnel on matters related to financial crimes and cyber offenses. Moreover, a comprehensive approach entails the expansion of codes of conduct governing computer usage, bolstering information technology curricula, and formulating policies to safeguard victims.

In line with these endeavors, member states are urged to reinforce international collaboration to counter the menace of cybercrime. A pivotal recommendation lies in encouraging the UN Committee on Crime Prevention and Control to disseminate guidelines and standards that empower member states to effectively combat cybercrime across national, regional, and international domains. This measure seeks to stimulate and advance research and analysis, thereby discovering novel strategies to tackle future challenges posed by cybercrime.

Additionally, the comprehensive approach extends to the realm of international legal cooperation. It underscores the integration of cybercrime considerations within the implementation of extradition agreements and collaborative assistance mechanisms aimed at crime prevention. It is increasingly apparent that addressing and mitigating cyber terrorism necessitates extensive collaboration with stakeholders at both national and international levels. This cooperative stance is vital for a unified and effective global response to the threat of cyber terrorism.

## References

1. Roger Spitz (2023) The Definitive Guide to Thriving on Disruption Quotes.
2. Sheldon R, Katie TH (2022) Cyberterrorism. Security.
3. Wikipedia Contributors (2023) Cyberterrorism.
4. Dogrul M, Aslan A, Celik E (2011) Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism.
5. Cyber-Laundering and Cyberterrorism – Sanction Scanner (2022) Sanction Scanner.