International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Techno Terrorism

Irfan Hamid [a], *Samar Ansh* [b]

[a] *M. Tech Scholar, Department of Computer Science and Technology, Central University Punjab, Bathinda, India- 151001*

[b] *Cyber Security Research, Department of research, Cyber Security Council, Ontario, Canada- M5B 2L7*

ABSTRACT

"Term to use technology as tools to harm or destruct". Artificial intelligence is heavily utilized by social media firms in their efforts to prevent and remove terrorist information from their platforms. Beginning with the claim that such initiatives amount to an effort to control human behavior, this article argues that they should be viewed as a type of regulation that is subject to rule of law principles. The following three sets of rule-of-law concerns are covered in the paper. The first group has to do with enforceability. The paper argues that consideration must be given to the entire social-media ecology, as well as to white supremacists other than the so-called Islamic State and other types of violent extremism, and highlights the displacement effects that have come about as a result of the automated removal and blocking of terrorist content. The article then turns its attention to two additional sets of problems, including how precisely social media firms define terrorist content and whether the processes by which a user may challenge the suspension of their account or the banning or deletion of information are appropriate. Rule by law is merely a necessary, not sufficient, precondition for abiding by the principles of the rule of law. The study agenda identified in the paper's conclusion includes a variety of problems that have emerged from the conversation and are both topical and promising, and they may be greatly aided by legal studies.

Keywords: artificial intelligence, cyber toolkits, cyber warfare, machine learning, techno-weapon.

1. Introduction

The information technology (IT) business, the security community, and the media are all paying close attention to the threat posed by techno-terrorism. Journalists, legislators, and specialists from a range of areas have popularized the idea of adept cyberterrorists causing chaos by hacking into computers that operate dams or air traffic control systems, putting millions of lives at risk as well as the nation's security. And yet, not a single incidence of actual Techno terrorism has been documented, despite all the apocalyptic scenarios predicted by the dark internet. How serious is the threat posed by technological terrorism? The potential danger from technological terrorism is undoubtedly quite concerning because the majority of essential infrastructure in Western society is networked through computers. Hackers have shown that anyone may access sensitive information and the functioning of essential services, despite their motivations not being the same as those that drive terrorists. Theoretically, terrorists may so imitate hackers and after hacking into public and private computer networks, cripple or at the very least take down the military, financial, and service sectors of developed nations. As our societies become more dependent on information technology, a new type of vulnerability has emerged, allowing terrorists to approach heretofore completely unattainable targets like air traffic control and national security systems. A nation is more susceptible to cyberattacks on its infrastructure the more technologically advanced it is.

Thus, there is good reason to be concerned about the threat that technological terrorism may pose. However, this does not imply that all of the worries that have been expressed in the press, during congressional debates, and in other public forums are valid and justified. While some worries are wildly overblown, others are simply unfounded. Additionally, it has been too frequently overlooked to distinguish between the potential and actual harm caused by cyber terrorism, and the generally innocuous actions of most hackers have been mistaken for the threat of pure techno terrorism.

This research looks at the past, present, and potential of technological terrorism. It starts by explaining why there is so much anxiety about "Techno terrorism," outlines what constitutes "Techno terrorism" and what does not, and analyses the attractiveness of "Techno terrorism" to terrorists. After that, the paper examines the evidence for and against Western society's susceptibility to cyberattacks, drawing on a number of recent research and publications to highlight the concerns raised and determine if we should be so worried. Future-focused, the conclusion makes the case that we should keep a sharp eye out for potential threats without succumbing to exaggerated anxieties.

2. Literature Review

Techno-terrorism is an attractive option for modern terrorists for several reasons

- Although we would not disclose them in detail for reasons of national security, the MoD takes the safety of our networks very seriously and has a variety of contingency strategies in place to mitigate against increasingly sophisticated intrusions. [1]
- It started by evaluating the terms already used to describe cyberwar and cyberwarfare and identified two issues that needed to be fixed. First,

it was discovered that neither cyberwarfare nor cyberwarfare has a generally agreed meaning. This is problematic because it is impossible to debate the more complicated concerns or even identify when cyberwarfare is taking place without a common definition. Second, we discovered that the phrases "cyber conflict" and "cyber warfare" are regularly used synonymously. We contended that this was equally problematic since war and warfare have different meanings. [2]

- A classified list of cyber weapons and cyber tools, including viruses with the ability to damage an adversary's crucial networks, has been produced by the Pentagon. Regardless of whether a consensus can be achieved on what constitutes a cyberweapon. [3]
- The space domain was also added fifty years ago. In the last 25 years, ubiquitous networking and widespread digitalization have combined to create cyberspace, the newest member of the expanding family of domains. We are informed that cyberspace permeates the other domains because it would substantially hinder warfighters in each of the previous domains if an attempt was made to block their access to cyberspace. This article will argue that this understanding of cyberspace and what militaries may do by operating "inside" is the incorrect way to see cyberspace and what it has become as the new high ground of warfare, the one domain to governs them all and the ether that binds them. [4]
- Because there was no access to it, early combat did not consider the air to be a sphere of battle. A similar case may be made when considering cyberspace. Although electrostatic space has almost always existed, we have only lately developed boats that are adequate for conducting operations there. In opposition to Libicki, the US Department of Defense claims that there are five distinct areas of conflict, including cyberspace. [5]

3. Techno terrorism for Terrorists/ criminals

Techno-terrorism is an attractive option for modern terrorists for several reasons:

- First, it is less expensive than conventional terrorist techniques. The terrorist only needs a computer and an internet connection. Instead of purchasing weapons like firearms and bombs, terrorists may construct and distribute computer viruses via a phone line, cable, or wireless link.
- Second, compared to more conventional terrorist tactics, cyberterrorism is more anonymous. Terrorists utilize online aliases, or "screen names," like many Internet users do, or access websites as anonymous "guest users," making it difficult for security organizations and law enforcement to determine the terrorists' true identities. Additionally, there are no actual obstacles in cyberspace, such as checkpoints, borders, or customs officers that must be avoided.
- Third, there are a huge variety and quantity of objectives. Computers and computer networks used by governments, people, public utilities, commercial airlines, and other organizations might be the target of technological terrorism. Terrorists will be able to locate weak points and openings due to the sheer amount and complexity of potential targets. Key infrastructures including electric power grids and emergency services are vulnerable to a cyberattack due to computer systems, according to various studies and infrastructures are so sophisticated that it is almost difficult to find and fix all vulnerabilities.
- Fourth, technological terrorism may be carried out remotely, which is a quality that terrorists find very alluring. Techno-terrorism makes it simpler for terrorist organizations to enlist and keep supporters since it needs less physical training, psychological commitment, risk of death, and travel than traditional forms of terrorism.
- Fifth, as the “I LOVE YOU” virus demonstrated, technological terrorism has the ability to directly harm more people than conventional terrorist tactics, resulting in more media attention, which is ultimately what terrorists desire.

3.1 Nuclear power plant attack

Cyber terrorists trying to get access to nuclear power plants around the world. In 2011 first time the US detect Orion software as been major vector of the attack. Again in 2021 US reported attackers trying to gain access and clear 3rd level of security to control the plant. That was dangerous if however, they access more than one level. In December 2019 NPCIL (India) confirm a cyber-attack against kudankulam Nuclear Power Plant.

3.2 Iran’s nuclear Scientist killed using AI

Now Artificial Intelligence is acting to harm or plan for man-made disasters. Years ago, Iran’s nuclear scientists were murdered (by Israel Government) from a distance of 3500 KM using IA to monitor weather, wind, etc. Another side Israel launches “The International Cyber Terrorism Regulation Project”. Without shooting range, a sniper is hit the target from just 3.5 km away.

3.3.Father Stan Swamy Email Forensic

Social activist arrested by NIA (India) in 2021 for charges of conspiracy against Gov. of India. NIA confirmed they recovered email enough to convict a suspect. Another side tech expert claimed that these emails are planted by NIA in the same way and couldn’t authenticate for further investigation. Before the execution of the case, the suspect is dead in jail and the truth is out there.

3.4 Howard university- Journalist email Forgery

Indian Journalist Nidhi Razdan (NDTV) received a mail from Howard University offering a job to appoint a lecturer at the university. After this mail, she resigned from her current service. After a couple of months, she communicates with the authorities to join the university. Then she was surprised to know that they never send such mail. That mail was a spoof by cyber criminals. Still, these tools are used to trap /scam people.

3.5 Brainwash- Conviction

Social media become a weapon to harm and motivate people to act in unlawful activity. Cyber Criminals and anti-social elements use social media platforms to brainwash innocent users. Low and enforcement agencies' surveillance of social media platforms to detect actors using keystrokes and similar techniques. Actors (cyber-criminals) target innocent people and brainwash them to commit crimes and terror activity over society.

3.6 NASA satellite hacking by (LTTE)

A banned terrorist organization LTTE (Liberation Tigers of Tamil Eelam) hacked NASA satellite in 2007 to establish communication for the organization. They used this communication link till NASA found a security breach in 2009. It's a surprise that NASA missed security breaches for 2 years and LTTE used these security holes.

4. Financial Terror/scam

In the current scenario, no missile needs to destroy a nation, it can be destroyed by crashing the digital infrastructure of the country. And Terrorists / Criminals are directly using technology to commit a crime and now these days affect finance and the economy.

4.1 Cryna Malware Attack / Ransomware

Technology and tools enhance to rob people years back ago. In 2017 attackers start mass robbing and launching malware named cryna malware, where infected system data was encrypted attacker crackers collected billions of dollars in the form of Bitcoin. Bitcoin is invented as a secure digital currency, but now this is a symbol of terror activity. This year's (2021) world's biggest ransom collected from a firm offers a cryptocurrency deal. Attackers attacked and hacked the server of this firm.

4.2 KYC scam in India

Many financial transaction technologies introduced in past years in India for instant banking services ie.- Google pay, Pay TM, BHIM, UPI, etc. Cybercriminals target innocent and non-tech people to trap and scam them for KYC updates and sometimes in the name of promotional offers like phone pe bonus points.

4.3 Russia-Ukraine Cyber Attack

In the past, many individual groups and Government sponsored hackers trigger stock exchanges globally to crash down the economy and financial infrastructure, but recently in the war between Russia and Ukraine, the Servers of Ukraine Bank were targeted by Russia using viper malware to destroy financial infrastructure and collapse the economy. Viper malware erases data from the server which can't be recovered.

4.4 Canada Immigration Scam

Technology changed the race of mankind as well as terror and crime also. A Chinese businessman named Wang (Sunny) used a single visa to the entry of more than 260 people. With help of technology, he sends people to Canada, and with the same process agency detected this fraud. Later emerge new cases and discover more than 1600 plus clients checked off to arrive at Canadian airports.

5. Political Techno Terror- Pegasus

Gov. Regulate and process lawful activity like dark web and Pegasus. Government illegally spies on people to monitor and collect personal-sensitive information using this application without superior regulatory activity. This is a current example of Techno-Terrorism used by Gov. and enforcement agencies.

6. Dark -web

Dark Web /Black Web is run over TOR browser with a specific configuration with different encryption policy and used by cybercriminals, terrorists, and government-sponsored spies to achieve their illicit purposes.

Third, Human trafficking, Drugs, Arms, and all illegal activity are done by criminals, terrorists, Smugglers, etc.

Identity theft is a major issue for people where personal and sensitive information sale for just money.

Dark-web has widely used the platform to commit cybercrime/ terror-based activity, but in the past, this platform became a victim once- more than 7600 onion (domain) website is shut-down (Hacked) within a single night. This was the 2nd biggest crime committed over the dark web, of course, silk road was the 1st organized crime.

7. Conclusion

This essay begins by suggesting that social media firms' attempts to employ AI to track individual and government-sponsored terrorism are futile. The conversation that followed demonstrated the applicability of several rule-of-law tenets, such as maximal certainty, congruence, non-discrimination, and enforceability, and in the process prompted several queries that collectively make up a promising and urgent research topic. Which definitional technique should social media firms use when defining terrorism, for instance? Should they provide a specific exception for individuals with a good reason? If so, how should they go about identifying right and unfair causes? More details about the elements that lead the AI to prohibit material might and ought to be given to users. Could these elements be more clearly reflected in the terms of service language? How can the sense of prejudice be lessened if the AI is not equally good at recognizing content from various types of violent extremism? The solutions to some of these problems have been partially developed in this study, but much more work has to be done. Our main goal has been to emphasize the societal significance of these issues as part of global and national efforts to combat modern terrorism, as well as to establish that legal academics are uniquely qualified to address these issues. As a result, legal research has a lot to say on both these topics and the wider trend toward non-normative modes of regulation.

(***Techno-terrorism is more dangerous than a missile, it performs silently, and impacts 1000 times more on our world***.)

References

B. Schneier, (June 2013). Has u.s started an internet war?, CNN, accessed 27/05/14 URL http://edition.cnn.com/2013/06/18/opinion/schneier-cyberwar-policy

L. Alford, Cyber warfare: A new doctrine and taxonomy, US Air Force, 1640 accessed 25/05/14 (April 2001). https://www.researchgate.net/publication/276248097_Cyber_warfare_Issues_and_challenges

L. Arimatsu, (2012) A treaty for governing cyber-weapons: Potential benefits and practical limitations, in: Cyber Conflict (CYCON), 2012 4th International Conference on, 2012, pp. 1-19.

D. E. Denning, (2000) Reflections on cyberweapons controls, Computer Security Journal 16 (4) (2000) 43{53. URL http://www.rand.org/pubs/external_publications/EP51077.html

Michael Robinsona, (2015), De Montfort University. https://www.researchgate.net/publication/276248097