

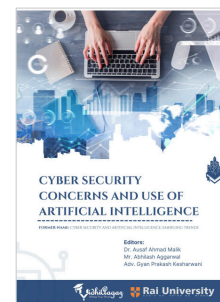
CHAPTER 13

Behind the Screen: Understanding and Countering Cyber-Terrorism in Modern Warfare

Nivedita Mahesh

in *Cyber Security Concerns and Use of Artificial Intelligence*, edited by Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani (VidhiAagaz 2024), pp. 114–119

ISBN 978-81-947620-5-8



CITATIONS

BLUEBOOK (21ST ED.)

Nivedita Mahesh, *Behind the Screen: Understanding and Countering Cyber-Terrorism in Modern Warfare*, in *CYBER SECURITY CONCERNS AND USE OF ARTIFICIAL INTELLIGENCE* 114 (Ausaf Ahmad Malik, Abhilash Aggarwal & Gyan Prakash Kesharwani eds., VidhiAagaz 2024).

OSCOLA (4TH ED.)

Nivedita Mahesh, 'Behind the Screen: Understanding and Countering Cyber-Terrorism in Modern Warfare' in Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani (eds), *Cyber Security Concerns and Use of Artificial Intelligence* (VidhiAagaz 2024) 114.

CHICAGO (17TH ED.)

Mahesh, Nivedita. "Behind the Screen: Understanding and Countering Cyber-Terrorism in Modern Warfare." In *Cyber Security Concerns and Use of Artificial Intelligence*, edited by Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani, 114–119. Maihar: VidhiAagaz, 2024. <https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-13/>.

APA (7TH ED.)

Mahesh, N. (2024). Behind the screen: Understanding and countering cyber-terrorism in modern warfare. In A. A. Malik & A. Aggarwal & G. P. Kesharwani (Eds.), *Cyber security concerns and use of artificial intelligence* (pp. 114–119). VidhiAagaz. <https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-13/>

SOURCE

<https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-13/>

RIGHTS

Free to read online. © VidhiAagaz 2024. All rights reserved: no part of this publication may be copied, reproduced, adapted or transmitted in any form or by any means without the prior written permission of the publisher.

Citations are given as a guide; check them against the style manual you follow. This page was added by VidhiAagaz to the downloaded file. The chapter follows, with the page numbers of the printed book.

BEHIND THE SCREEN: UNDERSTANDING AND COUNTERING CYBER-TERRORISM IN MODERN WARFARE

Nivedita Mahesh¹⁶

ABSTRACT

In today's digital age, the battlefield has expanded beyond borders and physical space, with Cyber-Terrorism becoming one of the most used weapons in modern warfare. Cyber Attacks such as the August 2022 DDoS attack on the Finnish Parliament and Russia's continued use of cyber attacks on Ukrainian infrastructure despite the existence of 18 conventions dealing with these issues have highlighted the need for active international cooperation to combat this new form of warfare. Defined as deliberate attacks by recognised terrorist organisations against computer systems, Cyber-Terrorism is designed to incite panic and destruction. In these circumstances, Leon Panetta's words "The potential for the next Pearl Harbor could very well be a cyber-attack", might as well be a real concern. The devastating consequences of cyber attacks were made clear in a 2023 study from the University of Minnesota, which revealed that between 42-67 US Medicare patients died due to ransomware incidents between 2016 to 2021. Thus, the destructive potential of Cyber-Terrorism ranges from blackouts to systematic collapse. The threat to civilian life and infrastructure is immense, as these attacks may eventually pave the way for larger terrorist operations. This paper is divided into key sections addressing the following: an analysis of real instances of the use of Cyber-Terrorism in warfare, understanding the motivations behind these attacks and their impact, and considering recent developments in AI that could help detect and neutralise cyber threats. The research methodology employed in this paper is qualitative, primarily relying on secondary data, drawing from reports, and official records from real incidents. Ultimately, this paper discusses measures, not just by preparing states in this battle against computers, but also against the individuals hiding behind the screen, destroying countless lives.

Keywords: Cyber-Terrorism, Cyber-Espionage, Modern Warfare, AI in Cyber Security.

INTRODUCTION

"Tomorrow's Terrorist may be able to do more damage with a keyboard than with a bomb"

- National Research Council

The concept of Cyber-Terrorism is not one that evolved overnight, rather it has been perfected over decades as the internet evolved into a crucial part of human life, almost as important as one's limb. As the information age began between the late 1980s to early 90s, there came the realisation that the technology that we depend on today could be maliciously used against us. This potential was first apparent when in 1988, a University student accidentally unleashed the Morris Worm infecting 6,000 systems. This fear was later intensified when in 1997, an NSA experiment revealed that hackers could access critical Pentagon systems, tamper with evidence, access classified information and shut down networks, all without stepping inside the building with the most basic phishing techniques.

By the early 2000s, Cyber-Terrorism became a weapon for ideological conflict as terror inflictors realised its potential. One such instance originated in Iraq where a network of over 100 websites known as "Iraq Net" was supposedly set up to launch DoS (Denial of Service) attacks on U.S corporations,

¹⁶ Student at Ramaiah University of Applied Sciences, Bengaluru, India.

being able to render useless, the most important computer systems across corporations. Based on this context, Yonah Alexander, a terrorism researcher remarked that “Sadam Hussein would not hesitate to use the cyber tool” Similarly, Jihadist groups have also explored the potential of an “Electronic Jihad” undermining Western infrastructure. The Handbook by Mohammad Bin Ahmad As-Sālim, “39 Ways to Serve and Participate in Jihad” is one such call for cyberattacks that may destroy American websites and other such entities that may seem hostile to the Jihadist cause. Non-state actors like the Islamic State’s “Cyber Caliphate Army” signal a broader use of cyber warfare for military, political or ideological goals.

From its conception, Cyberterrorism aimed to not only dismantle critical systems that humans rely heavily on but also instil panic across society. The fact that this type of terrorism is so remote that a hacker working in the Northern Hemisphere may upend entire societies in the Southern Hemisphere is certainly nerve-wracking. It became evident that without firing a single missile, a whole war could be declared through advanced hacking tactics. The fear of the unseen disrupting lives deeply impacts the public psyche. In 2016, India ranked among the top 5 countries that are most vulnerable to cyberattacks. Hacking groups like Transparent Tribe based in Pakistan which are notorious for targeting Indian Defence sectors, pose an increasing threat in South Asia in terms of Cyber espionage and disruption. Such attacks are reflective of the increasing scope and sophistication of Cyber- Terrorism, that too, so close to home.

The 21st century saw a significant evolution like cyberattacks, for instance, the proliferation of suspicious apps and targeted cyberattacks during the COVID-19 pandemic in 2020 and 2021 demonstrated how cybercriminals can take advantage of global emergencies and crises. According to Trend Micro, in the first quarter of 2021 alone, over 164 malicious apps were found, taking advantage of our reliance on digital connectivity during lockdown. Thus, the convergence of technology and terrorism has now become a formidable tool for both state and non-state actors to use as part of Cyber Warfare or even to further an ideological or political cause, which shall be further examined in the upcoming sections.

REAL-TIME CONSEQUENCES OF CYBER-TERRORISM

India with the second-largest online market in the world has, as previously mentioned, been especially susceptible to Cyber-Terrorism. Incidents such as the URI attack, Pulwama and the 26/11 Mumbai attacks stand as glaring examples of how technology in the wrong hands can have devastating effects. Especially during the 26/11 attacks, the terrorists used Google Earth, social media and mobile networks, as do common people. This is very similar to how the 9/11 terrorists operated, using hacking mechanisms to procure fake IDs, steal Social Security numbers, etc. Such attacks not only result in loss of lives but also instil fear about future attacks and undermine cybersecurity frameworks. Those who feared future attacks in 26/11 were probably right in doing so, as evidenced by the report from CERT-In revealing that in 2022 alone there were over 1.39 million cybersecurity attacks. When such are the numbers, ordinary civilians such as ourselves cannot even feel secure in our own homes, working on our systems. How are we to feel safe when Pakistani Cyber Criminals deface nearly 60 Indian websites every day? This fear was especially highlighted in a study by the Pew Internet and American Project

which found in 2003 that nearly half the Americans surveyed were concerned about Cyber- Terrorist attacks. The study revealed that while 38% of the participants were somewhat worried about such attacks, 11% had some serious concerns.

In July 2022, Chinese Advanced Persistent Threat actors launched an attack on Belgium's government and military, to gather intelligence and steal trade secrets. What is surprising to note is that this attack was sponsored by the Chinese government itself, demonstrating how Cyber-Terrorism is also used in State-sponsored espionage activities. On a similar line was the 2014 Sony cyberattack, which was linked to North Korea. The attack was deemed to be in response to the controversial Sony film "The Interview", satirising North Korean leader Kim Jong Un. Threats of physical terrorist attacks on theatres playing the movie were also made through this cyberattack.

Another such instance is the use of cyber-warfare tactics such as the 2010 Stuxnet worm, allegedly developed by the U.S. in conjunction with Israel which severely disabled Iran's nuclear infrastructure. Such attacks include China's breach of the U.S. Office of Personnel Management in 2015 and Russia's interference in the 2015 U.S. presidential election. These examples prove the impact of cyberattacks on the day-to-day functioning of a government or the capability to undermine a nation's democratic process.

Russia and Ukraine

Throughout the conflict, cyberattacks have been used alongside conventional warfare to disrupt civilian life and infrastructure using techniques such as wiper malware that permanently alters data and the attack on the Viasat satellite network that cut off the internet across parts of Ukraine and Europe, affecting wind turbines in Germany and around 9,000 subscribers in France. A malware attack also breached the process of allowing refugees into Romania. Such attacks have mainly targeted water, power and communication infrastructure, leaving many Ukrainians devoid of essential resources. This was accompanied by infiltration of media with false information. At one point the mass was falsely led to believe that President Zelensky was incapacitated, causing chaos. As mentioned previously, even some of Europe has been victim to the effects of these cyberattacks. Unlike physical war, cyber warfare tends to cause direct effects in areas outside the conflict zones as well.

The case of Hamas and Israel

While the world has been focused on missiles and rockets, a parallel war is taking space in cyberspace. Hamas has been known for employing cyberattacks ranging from phishing schemes to DoS attacks on news outlets, banks and hospitals. For instance, on the dreadful day of October 7th, 2023, Hamas hackers infiltrated the 'RedAlert' app used to warn civilians about impending strikes and threats, making the attack completely unprecedented. Meanwhile, Israel has used internet blackouts in Gaza as part of its attempt to cripple communication channels among militants, garnering international criticism over this response. These instances just to name a few of the many that may be involved in the Israel-Hamas war demonstrate a poignant example of how Cyber-Terrorism is used in modern warfare, in hampering alerts sent to civilians thereby causing a breakdown of digital as well as physical infrastructure.

One may notice that in all these instances, the one common impact has been on civilian lives. Any act ranging from the hacking of Jerusalem Post's website to the disabling of Indian Defence Systems by cyber espionage sends a message to the civilians: "When it comes to cyberattacks, even your country cannot protect you". In some unfortunate instances, it is nations themselves that are engaging in attacks of such nature. Nevertheless, the individuals operating behind these screens know one thing for sure, that people fear the unknown or the invisible and that is exactly what gives these individuals the confidence to thrive on our anxiety.

CYBER-TERRORISM OR AFFORDABLE TERRORISM?

The COVID-19 pandemic as discussed, has been a vulnerable period for the rest of the world and a thriving period for cyberattacks. With most of the world shifting towards digital platforms for school or work, the time to carry out cyberattacks could not have been better, it was as if all the targets had gathered in one place, like sheep in a pen awaiting their slaughter. A Statista survey of IT security professionals worldwide revealed that between the first quarter of 2020 and July of 2022, cyberattacks such as data leakage saw a 55% increase and other attacks like phishing emails, ransomware and account takeovers increased by 51%.

Unlike conventional terrorism which requires financial aid, considerate planning and other resources, Cyber- Terrorism can be carried out at a fraction of their costs, thus emerging as a form of "Affordable Terrorism", making it easier for infiltrators to cause a whole lot more damage than incurred by them. Carrying out conventional forms of terrorism can generally cost a lot for the terrorists themselves. For this purpose, ISIS has an estimated war chest of around \$2 billion financed by oil smuggling. Likewise, the 9/11 attacks seemed to have cost Al-Qaeda between \$400,000 to \$500,000 to train and transport the terrorists. Other instances including the 2004 Madrid train bombings and London car bomb attacks cost terrorists between \$10,000- \$14,000, regardless of whether their missions were a success or a failure. In stark contrast to this, cyberattacks are relatively "affordable" for terrorists. Carrying out a cyber attack is cheaper than committing to cybersecurity itself, this proportion is simply unfair. Armor's Black Market report finds that Personally Identifiable Information is available for less than \$200 per record while credit card information can cost as little as \$10. Entire accounts containing up to \$15,000 can be bought for around \$1000. Hacking tutorials can be purchased for around \$5 and basic malware can be obtained for \$45 as per Top10VPN's Hacking Tools Price Index. While these attacks may be cheap for the perpetrators, they are anything but that for victims. The expenses incurred come not only in the form of money lost but also loss of crucial data, malfunctioning of essential services, damaged reputations and even loss of lives.

Another factor is that while traditional terrorism is localised to one area at a time, Cyber- Terrorism can cause widespread damage. For example, the infamous "ILOVEYOU" virus in 2000, through careful social engineering impacted users across the globe within hours. This proved that cyberattacks may not only be of a large scale but may be immediate as well. Thus, the ability to conduct Cyber- Terrorism remotely furthers its appeal. When you work remotely, leave a lesser impression than you do in person. This may be the logic behind why there is lesser accountability for those operating anonymously behind screens. This gives them a sense of impunity and lessens the likelihood of their capture or death. But

we must make no mistake, hiding behind a screen does not make Cyber- Terrorism any less devastating. The anonymity that those behind the screens hold does not wash the blood on their hands. The keyboard has become today's weapon of terror and it has the potential to reach beyond the other end of the screen.

MEASURES

India, realising the gravity of the threat imposed in cyberspace, has been proactive in taking up measures to strengthen its cybersecurity framework. New encryption and privacy policies are in place. The National Cyber Policy of 2013 laid the base for a national strategy alongside recent initiatives for digital empowerment. However, Section 66F of the Information Technology Act (Amendment), 2008 is currently the only provision in the nation directly addressing Cyber-Terrorism. The evolving nature of cyber threats calls for a stronger framework in this arena. To meet the fast-growing complexities and sophistication of Cyber- Terrorism, India and other nations alike must evolve in tandem with emerging technologies. International cooperation and robust public-private partnership models are needed in the wake of cyberattacks on both states and corporations and even on other entities.

Along with these measures, understanding the motivations behind Cyber- Terrorism may yield an even more robust framework of response. Knowing underlying factors can help us better understand what crucial sectors of society may require more security or what demography of netizens are being targeted, allowing the prioritisation of security in certain areas. There may be a myriad of motivations driving cyberattacks, money, politics and ideology being the heart of such causes. In certain dire situations, the motivation may even be the mere sense of accomplishment that comes with dismantling huge systems. Some treat it as a sport, the bigger the bragger. While Cyber- Terrorism increases anxiety and militancy regardless of the motivations behind it, the context of its operation matters. The identity of the perpetrator or their cause helps explain their attitude towards the cyberattack. For instance, knowing that the LTTE is behind a cyberattack may mean something different to a Sri Lankan or Indian as it may to, say, a Canadian national.

Recent Developments in AI that may help neutralise cyber threats

However, the fight against Cyber- Terrorism is not just a matter of international cooperation or policy, it is also a technological arms movement. As cyber threats are evolving into more sophisticated forms, we must employ the latest innovations and advances in Artificial Intelligence to neutralise these threats. Artificial Intelligence or AI, in particular, can be used in its full capacity to identify these threats before major damage is caused. As per a survey by The Economist Intelligence Unit, 48.9% of security experts and executives consider AI and machine learning as potential tools to combat modern security threats. Machine learning when backed by data science and relevant areas of technological study can prove to be a very useful tool in this war against Cyber- Terrorism. For instance, a global bank used Paladon's AI-based Managed Detection and Response Service to detect advanced attacks, data leakage, ransomware and malware attacks based on data science and machine learning capabilities.

AI can detect new as well as current attacks by analysing consistent patterns and training neural networks to recognise suspicious activities in the initial stage itself. This manner of predictive detection was in use by CompStat, an early form of AI which was also used by the NYPD in "predictive policing".

AI can also detect anomalies or entities out of the ordinary that may signal a polymorphic malware attack. Even before the advent of Cyber- Terrorism, AI-based tools like Armorway used AI to predict terrorist threats to port security in cities like New York and Boston. By using this predictive tool, coupled with an understanding of Cyber-Terrorist motivations, cybersecurity systems can anticipate and timely stop attacks before they may even be executed.

Another subset of AI known as “Deep Learning”, can identify patterns through its vast neural networks. It is especially useful in countering malware attacks that rewrite codes to slip past traditional detection methods. By recognising behavioural patterns, even if the code is altered by the attacking entities, Deep Learning models can reduce the time taken for detection. Additionally, Supervised Machine Learning with the help of known datasets of previous incidents, can block emerging threats. This model is used by Extended Detection and Response systems to improve threat identification and mitigation steps.

Certain new developments in AI also allow for what is known as “threat deception”. This advanced method allows AI to create artificial environments to trap or mislead cyber attackers, in a manner, borrowing a page from their book. These environments use decoys to interact with the cyber attackers while deterring their attacks at the same time. This type of technology helps cybersecurity frameworks stay ahead of their adversaries.

AI can thus rapidly detect potential threats in real-time, improve accuracy in detecting the said threats, identify vulnerabilities in a system before attackers may exploit them and automatically respond with security measures such as blocking attacks and isolating attacked systems to contain cyberattacks. However, cybersecurity systems must stay ahead of the game as AI is also being increasingly adopted in cyberattacks. While AI may be automated in its tasks, human involvement is essential in assessing threats and making informed decisions towards alleviating them. Fighting Cyber- Terrorism thus requires a multi-layered approach. From framing policies that secure the interests of our cyberspace to using AI against impending cyberattacks, this war on our digital space requires our full efforts to avert dire consequences. All these mechanisms alongside an understanding of what factors motivate such attacks can save the world a lot of loss, both in terms of material assets and human lives.

CONCLUSION

Bruce Schneier once remarked, “Only amateurs attack machines, professionals target people”. We are now ironically at a juncture where people are targeted through machines, by other persons hiding behind the safety of a screen. As nations and institutions struggle to brace their defences against unpredictable attacks, it is clear that Cyber- Terrorism has achieved its goal - being a continuing fear among the masses. The anonymity enjoyed by the attackers makes them more dangerous. The scariest is the unknown, something one cannot see, touch or feel but one is aware of. Such is the nature of Cyber-Terrorism. It is time the various nations, institutions and corporations around the world understand that modern warfare is not limited to land, air, or sea; we are now moving towards the realm of cyberspace where the threats can be equally devastating and far-reaching. The fight against Cyber- Terrorism is a race against technology and more importantly, against some of our own kind, willing to stop at nothing.
