Pakistan Journal of Criminology
Vol. 16, No. 03, July—September 2024 (609-618)

The Role of Digital Technology in Countering Terrorism

Amer Fakhoury[1]

Abstract

Digital technology has an undeniable impact on many aspects of society in an era where it is global. This study explores the vital field of counterterrorism by examining the complex role that digital technology plays in both reducing and averting terrorist acts. To give a thorough grasp of how digital tools, platforms, and methodologies support ongoing efforts to combat terrorism on a national and international level, the study examines the relationship between technology and security. This study examines the ethical and privacy ramifications of using cutting-edge technologies in counterterrorism tactics, recognizing the fine line that must be drawn between personal liberties and security requirements. The purpose of the research is to provide policymakers, and security professionals with information regarding the new trends and possible advancements in the use of digital tools to protect societies from the ongoing threat of terrorism.

Keywords: Terrorism, countering terrorism, digital technology, international law, cybersecurity

Introduction:

Important developments in digital technology have acquired a significant role in the development of the international community. This development included several technological trends such as Artificial Intelligence, Cybersecurity and encryption, 5G mobile networks, and Blockchain. Despite the importance of these developments, the possibility that they will be used by criminal and terrorist gangs cannot be denied, as it has already been used by criminal organizations that have appeared on the international scene since the September 11 attacks. I want to recall the suicide attack that was carried out in 2017 known as "Manchester Arena terror attack" in Britain by a terrorist who decided to blow himself up by making a bomb himself. The report says that it turns out that the terrorist succeeded in making the bomb himself due to the fact he had "access to extremist material online (Glazzard, 2019). For many specialists in the field, terrorist recruitment, and the spread of violent extremist content across the world have all been made possible through the global reach of the internet. Thanks to the Internet, many terrorist organizations have become more famous in the world.

[1] Professor of Public International Law and Human Rights, College of Law, American University in the Emirates, United Arab Emirates (UAE). amer.fakhoury@aue.ae

This study is divided into three parts. The first study is Countering Terrorism Through Information Technology by Brian A. Jackson, et al. - This book gives a investigation of how data innovation can be utilized to counter psychological warfare, counting talks on computerized observation, information analytics, and cybersecurity measures. The second study is Digital Counterinsurgency: A Guide for Policymakers and Practitioners, by David Kilcullen - This book offers experiences into the utilize of advanced advances in counterinsurgency endeavors, which regularly meet with counterterrorism techniques, giving profitable points of view on advanced counterterrorism strategies. The third study is Cybersecurity and Cyberwar: What Everyone Needs to Know, by P.W. Artist and Allan Friedman - This asset investigates the part of cybersecurity in combating different dangers, counting fear-mongering, shedding light on the crossing point of computerized innovation and national security.

Research Questions:

1. Can tools like digital technology including surveillance systems assist in preventing and detecting terrorist activities worldwide?
2. What factors determine whether or not the use of digital technology, as supported by United Nations resolutions, is successful or not in combating terrorism?
3. Terrorists operate globally, so fighting them requires international coordination with digital tools. However, integrating new technologies worldwide faces many difficulties. So what challenges arise and how can countries overcome them?

Research Objectives:

1. To ascertain the efficacy of digital technology, including surveillance systems and big data analysis, in global attempts to prevent and uncover terrorist activities.
2. To examine the reasons for success or failure of international efforts on counter terrorism, as implied by UN resolutions, in using electronic devices.
3. To identify the challenges related to combining computer technologies into international frameworks aimed at combating terrorism.
4. To develop recommendations for policy makers on how to use digital technology effectively in fighting terrorism without compromising privacy and fundamental rights.

The Research Methodology:

The research methodology rams on quantitative analysis and evaluation of decisions made by the United Nations as well as global collaboration. The digital technology effectiveness will be assessed quantitatively to counter terrorism, whereas UN resolution and world initiative in fighting against terror through applying technology change will also be reviewed. Our approach that is mixed seeks to give an understanding of how digital technologies fit into the framework of global partnership for countering terrorism.

Understanding Terrorism: Defining the Phenomenon

According to paragraph 3 of resolution 1566 in 2004, the United Nations Security Council describes terrorist acts as criminal acts where people try to make someone die or suffer intensely, or they take people away in order to frighten the rest of society, one particular collection of citizens, or some certain individuals. This kind of crime can involve threatening large populations in order to force rulers to act in particular ways or not to act at all; in terms of international instruments on terrorism, they would be found to be in breach of these provisions. I believe that the description declared by the UN Security Council has powerful implications, understanding its motive and method makes us to understand completely what it is all about. This stresses the seriousness of terrorism and the necessity for worldwide cooperation in handling it effectively.

When this resolution was adopted, it was not expected in the minds of the international legislator that international terrorism would exploit modern technology to spread the ideas of extremism in all its forms in this way that we see in 2022. The same technology that is used to combat extremism can be an important tool in the hands of extremists.

From other side, let me recall a very important and well-known resolution adopted one year back from the aforementioned resolution, on 2003 by United Nations Security Council which is resolution 1456 who says in para 6 […] States must ensure that any measure taken to combat terrorism comply with all their obligations under international law, and should adopt such measures in accordance with international law, in particular international human rights, refugee, and humanitarian law. I recall those two decisions for the simple reason that countries resort to digital technology to monitor the movements of terrorist organizations of different degrees, types, danger, and loyalties, stems from the general interest of the international community, which realized, albeit late, that the Internet has become a safe refuge for those organizations that were and are spreading their extremism, intellectual and ideological, among young people who are more vulnerable to manipulate.

Addressing the Negative Impacts of Information and Communications Technologies: Preventing Misuse and Promoting Responsible Usage

Although digital technology has the potential to enhance human living standards, it might alternatively become a critical tool for terrorist gangs. A lot of wary parasitic diplomatic divisions and the United Nations Office of Counter-Terrorism (UNOCT) have registered considerable concerns regarding the misuse of information and communication technologies by terrorist gangs especially through the internet and new digital technologies to execute, encourage, recruit, fund, or scheme terrorist activities or as asserted by some academicians like (Behr, Reding, Edwards, & Gribbon, 2013) "online platforms provide more chances for radicalization and speed up the mobilization process of radicalized individuals".

Because technology has advanced, and some apps have been discovered that make it hard for the police to follow certain internet users, who use virtual private networks (VPNs), as a result, terrorist factions can move easily across national borders (Harrison, 2022) says, Malaysia is an important example of the rising risk of terrorism inspired by other countries because it has lots of internet access, many encrypted messaging services are popular there, VPN's are significant and a group of experienced foreign fighters who may encourage others from Syria to become radicalized and carry out attacks in Malaysia.

Multi-stakeholder cooperation and the role of digital technology in countering terrorism

While there are various Security Council resolutions addressing terrorism, Nevertheless UNSC Resolution 2341 is considered one of the most important decisions that stress the significance of cooperation between all local and regional sectors to confront the modern threats of terrorist acts and terrorists alike. UNSC Resolution 2341 from 2017 strongly advises countries to create solid partnerships with stakeholders in the public and private sectors so that they can share information and expertise. The main goal of this cooperation is to stop, shield from, and react to terrorist attacks on vital infrastructures which can be achieved through mutual training and setting up communication networks.

Bridging the Gap between Local and International Pillars: Enhancing Collaboration and Cooperation.

The process of confronting terrorism via the Internet requires the cooperation of four main parties, distributed internally and externally. Confrontation with terrorists cannot take place without close cooperation between them. These parties are: States, regional organizations, the private sector and civil society. For that reason on of the main principles that have been adopted by UNSC on 23 December 2015, (S/2015/939, p. 10) known as (Madrid guiding

principles) where the decision confirms that all the four aforementioned parties: 'Parties should form strong partnerships to create better ways to monitor and study terrorist content sent via the Internet and other communication technologies and combat incitement to terrorism by using it for intelligence and passing on relevant law-enforcement agencies. Countermessaging could also be an effective measure to prevent such occurrences. It is therefore important that all stakeholders come together for a discussion on how best to deal with this type of material on the web and other forms of modern communication channels. Regardless of the threats that may occur via the Internet, it must be said that digital technology must face four categories of terrorist challenges, which are:

Kinetic cyber-attacks on critical infrastructure[2]: If cyber-attacks happen in critical infrastructures, the results would be catastrophic. Shut down the power of a hospital, alter the temperatures in nuclear cooling towers, and exploit features in smart cars while they are in motion are some destructive scenarios (Das, 2019). Spread of terrorist content online; online terrorist communications and Digital terrorist financing. For sure, countries should invest in a new discipline such as digital forensic investigator, or forensic analyst. In this point, three main points will be examined, namely the role of Interpol, Criminal Courts In The Era of Digital Technology, the Virtual private network (VPN), and how to Tackle The Dark Web

Understanding the Role of Interpol in Digital Forensics Investigations: Exploring the Responsibilities of a Digital Forensic Investigator.

I concur with the assertion made by (Kohn, Mariki, & Eloff, 2013) regarding their definition of digital forensics where they says that the combination of validated and established scientific methods that are used for the sake of securing, complete, thorough and objective evidence towards both preservation, collection, validation, identification, analysis, interpretation as well as full presentation of digital evidence from digital sources for the purpose of facilitating or enhancing the reconstruction of events regarded as criminal or even helping to predict the unauthorized actions that can be disruptive to planned operations

So, computer forensic investigators help recover information from computers and other digital storage devices. The saved data can then be used in criminal investigations or as evidence in cases of cybercrimes. I concur with Sulthana's perspective that digital forensics involves gathering and examining digital evidence from various devices like mobile phones, laptops, desktops, routers, and

[2] Critical Infrastructure Sectors such as Chemical Sector, Commercial Facilities Sector, Communications Sector, Dams Sector, Defense Industrial Base Sector, Emergency Services Sector, Energy Sector, Tram Hacking, Water Distribution System Hacking,

similar gadgets used to perpetrate crimes. Interpol has prioritized digital forensics since it offers technical aid on electronic technology to all its members. Its duties can be divided into various main categories: Operational support involves highly skilled forensic help at both the Interpol Digital Forensics Laboratory as well as in carrying out Incident Response missions. Another point refers to advising member nations, with Interpol aiding them to establish and keep current laboratories appropriate international standards that would enhance their capability assisting criminal inquiries and prosecution processes. Interpol also organizes training programs for its member states, teaching standard methods and solutions in digital forensics. Additionally, it brings together experts globally to share knowledge and enhance their daily practices.

Criminal Courts in The Era of Digital Technology

Is it possible to determine the identity and place of residence of the cybercriminal on social networks, what tools are used to confirm conviction, and how effective are the penal measures for foreign websites? The issue of identifying a particular user on a social network is one of the most complex issues, especially about judicial systems facing terrorist operations. It is necessary in terms of identifying the perpetrators of some crimes that may be committed on the web. Fortunately, due to the great development in digital technology, we now have what is known as the Internet Protocol or IP address which is a long string of numbers assigned to every device connected to a network that uses Internet Protocol as the medium for communication. Digital forensics which holds that "objects and surfaces that come into contact will transfer material from one to another (Marasa & Michelle , 2014)

Digital traces are left behind as the result of individuals' use of information and communication technology in the field of digital forensics. (Albert & Venter, 2017) argue that a person utilizing information and communication technology can leave a "digital footprint," which refers to the data left behind by ICT users that can reveal information about them, including but not limited to age, gender, race, ethnicity, nationality, sexual orientation, thoughts, preferences, habits, hobbies, medical history, and concerns about medicine, psychological disorders, employment status, affiliations, relationships, geolocations, routines and other activities.

No doubt that the digital transformation provides opportunities to transform the judicial work environment into a virtual reality. So that judicial institutions such as ICC are allowed to use the data of modern technology in managing their judicial work, such as writing records investigations, memoranda and judgments, managing sessions, formulating decisions, and implementing

judgments issued by those institutions. Judiciary bodies such as the ICC can use modern technology data to manage judicial operations such as recording, investigating, preparing memorandums and judgments, conducting meetings, making decisions, and enforcing judgments rendered by these bodies. Data can be obtained and used for intelligence objectives (UNODC, 2011, Criminal Intelligence Manual for Analysts) or can be tendered in a law court as digital proof. These digital proofs can be deployed in criminal courts to prosecute terrorists who leave their digital signatures on the Internet. It bears repeating that the IP Address helps to find out who an Internet subscriber is rather than who uses the network, and this makes it difficult to trace terrorists who use the Internet.

Identification of the Internet service subscriber is an essential element in determining the starting point in the judicial investigation, and the subscriber in the Internet service has to refer to the user who performed the terrorist act, but, in some cases, this is impossible, especially in cases where individuals access the network through Public computers, so it is very difficult to identify the users since the IP address, especially the public network, does not help in this case to reach the user responsible for the terrorist act. It is not about the ability of government authorities to arrest terrorists who use the Internet to spread their extremism in society, but also the need for judges to have knowledge in informatics and modern technology in order to be able to adjudicate the cases before them.

Virtual private network (VPN) vis-à-vis the digital technology.

Many people are familiar with the term VPN, and many people, telecom and networking professionals and non-professionals alike, use the technology to varying degrees. To clarify how these networks work, when a terrorist activates his VPN service on a particular device and visits a website that specializes in arms trafficking, the requests are routed through his VPN to this behavior is not considered normal mode because it is sent in encrypted form. exposed to law enforcement. This is due to the emergence of more dangerous programs.

But in time, (EUROPOL Public Information, Changes in Modus Operandi of Islamic State Terrorist Attacks)" VPNs are being used to carry out criminal activities over the Internet or hide the activity of a particular person or situations associated with extremism such as terrorism. For that reason, some specialists, (Barrett, 2017) invite the governments and ask "telecommunication companies to build backdoors into their products, which would give law enforcement a way to access encrypted data."

Collaborative Effort to Tackle the Dark Web

Far from legal control and responsibility and eluding the eyes of secret agencies and state controls, terrorist organizations may communicate in complete covertness via the "dark web." This makes information protected and makes tracking of electronic activity by, for example, the service provider or the Government almost impossible. On this network, there are sites not only for the sale of forged and stolen documents, credit card data, and personal accounts but also a black market for all illegal activities, a haven for criminals and terrorists. The terrorist shooting of two mosques in southern New Zealand, a few years back, which killed 49 people, revealed a new pattern of violence and extremism within Western societies, based heavily on dark Internet. These networks are characterized by the fact that they allow the launch of websites and the dissemination of information without disclosing the publisher's identity or location. The dark Internet is accessible through services provided by electronic programs such as (TOR). The TOR or The Onion Router which is a way to ensure that law enforcement authorities may not track communications or find out where they come from on the Internet by transferring data through a large number of points or Servers. This undoubtedly poses a serious threat to the security of all societies, and requires the need for concerted international efforts to confront it.

Results and Discussion

The results of the study show the different ways in which digital technology can be applied to counterterrorism. The research found that through numbers, it was able to establish how digital technologies including surveillance systems and data analytics are important in preventing and detecting global terrorist activities. Case studies and statistical examinations revealed successful implementations leading to thwarting terrorist threats. Additionally, an examination of UN-mandated international cooperation efforts unveiled complexities of nations working together in using digital tools for counterterrorism. Although there were some promising initiatives, information sharing and resource allocation posed a challenge. Furthermore, the paper studied how the subtle perceptions on privacy and civil liberties impacted on people’s acceptance and implementation of digital counter-terrorism strategies. A qualitative analysis brought out stakeholder perspectives and concerns, emphasizing the need to strike a balance between security imperatives as well as fundamental rights.

Conclusion and Recommendations

Technology has dramatically improved people's quality of life. However, it is a double-edged sword. The rapid development of the technology and its

widespread commercial use pose challenges to Member States' efforts to prevent abuse by terrorist organizations. The efficacy of digital technology, encompassing surveillance systems and big data analysis, in preventing and uncovering terrorist activities globally remains a topic of ongoing investigation and debate.

The global reach of the Internet has clearly enabled the recruitment of terrorists and the spread of violent extremist content around the world. Thanks to the Internet, many terrorist organizations have become well known around the world. Given the potential of the Internet for criminals to commit crimes, and the facilitation of communication and information exchange between criminals, the possibility of meeting in a virtual world to plan and prepare actions for criminals across multiple states. It will be considered. In some cases, even these organized crime groups target specific states or commercial and economic institutions. This could result in serious economic damage to those states and agencies. The international community is now demanding a shift from regular conflicts, in which terrorist organizations enjoy great success, to another type of online virtual conflict. Virtual conflicts online are considered to be the most dangerous and difficult, and perhaps the last, conflict. I believe that fighting terrorism is crucial, but protecting privacy is also important. Governments, or countries members in the United Nations can use digital tools against terrorism while keeping people's rights safe. They should have strong data protection rules and only watch specific targets instead of engaging in mass surveillance of everyone. Checking often how anti-terror actions impact privacy is wise. Working with othe-r countries on best practices while respecting human rights helps. Educating the public about digital tools used against terror, and their limits, and getting input from privacy groups makes policies better.

References

Antwi-Boasiako, A., & Hein, V. (2017). A Model for Digital Evidence Admissibility Assessment. In Advances in Digital Forensics.

Barrett, B. (2017). The Encryption Debate Should End Right Now. Wired. https://www.wired.com/story/encryption-backdoors-shadow-brokers-vault-7-wannacry/

Behr, V., Reding, A., Edwards, C., & Gribbon, L. (2013). Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism. RAND Corporation.

Das. (2019). Analysis of cyber-attacks in IoT-based critical infrastructures. *International Journal of Information Security Science*, 8(4):122-133

Glazzard, A. (2019). Shooting the Messenger: Do Not Blame the Internet for Terrorism. RUSI Newsbrief.

Kohn, M. D., Mariki, M., & Eloff, J. (2013). Integrated Digital Forensic Process Model. *Computers and Security*, 38, 103-115.

Marasa, M.-H., & Michelle, D. (2014). Forensic Science.

Seth Harrison, E. T. (2022). Evolving Terror. Center for Strategic and International Studies. Retrieved from https://www.csis.org/npfp/evolving-tech-evolvingterror

Sulthana, T., Pawar, D. (2021). Digital Forensic Investigator for Cloud Computing Environment. In: Bhateja, V., Satapathy, S.C., Travieso-Gonzalez, C.M., Flores-Fuentes, W. (eds) Computer Communication, Networking and IoT. Lecture Notes in Networks and Systems, vol 197. Springer, Singapore. https://doi.org/10.1007/978-981-16-0980-0_6

United Nations Security Council. (2004). Resolution 1566 (2004) on Threats to international peace and security caused by terrorist acts.

United Nations Security Council Counter-Terrorism Committee. (2015). Madrid Guiding Principles. (S/2015/939). Retrieved from http://undocs.org/S/2015/939

United Nations Security Council. (2017). Resolution 2341 (2017) on protection of critical infrastructure against terrorist acts.