Disaster Medicine and Public Health Preparedness

www.cambridge.org/dmp

Assessing the Public Health Consequences of Terrorist Attacks on Telecommunications Infrastructure: A Global Analysis

Zakaria Mani[1] and Krzysztof Goniewicz[2]

[1]Nursing College, Jazan University, Jazan, Saudi Arabia and and [2]Department of Security Studies, Polish Air Force University, Dęblin, Poland

Original Research

Cite this article: Mani Z and Goniewicz K (2024). Assessing the Public Health Consequences of Terrorist Attacks on Telecommunications Infrastructure: A Global Analysis. *Disaster Medicine and Public Health Preparedness*, **18**, e312, 1–7
https://doi.org/10.1017/dmp.2024.311

Received: 01 May 2024
Revised: 24 September 2024
Accepted: 23 October 2024

Keywords:
terrorism; telecommunications; public health; emergency response; security measures; international cooperation; global terrorism database (GTD)

Corresponding authors:
Zakaria Mani and Krzysztof Goniewicz;
Emails: zakaria.mani@jazanu.edu.sa;
k.goniewicz@law.mil.pl

Abstract

Objectives: This study investigates the public health implications of terrorist attacks on telecommunications infrastructure globally, assessing the direct and indirect impacts on emergency response and medical services.

Methods: Utilizing retrospective analysis, this research delves into incidents recorded in the Global Terrorism Database (GTD) from 1970 to 2020. The study employs descriptive statistical methods to identify patterns and examine the regional distribution and frequency of these attacks, alongside the types of weaponry used and the direct casualties involved.

Results: The analysis underscores a significant focus on telecommunications by terrorist groups, revealing a frequent use of high-impact weapons like explosives and incendiary devices aimed at maximizing disruption. The study highlights considerable regional variations in the frequency and nature of attacks, emphasizing the strategic importance of these infrastructures to public safety and health systems.

Conclusions: The findings demonstrate the critical need for robust security enhancements tailored to regional threats and the integration of advanced technologies in public safety strategies. The research advocates for enhanced international cooperation and policymaking to mitigate the impacts of these attacks, ensuring telecommunications resilience in the face of global terrorism.

Terrorist attacks on telecommunication infrastructure pose profound public health challenges globally.[1] As critical components of national security and public safety frameworks, telecommunication systems are integral to emergency communications, coordinating rescue operations, and disseminating public health alerts.[2] The deliberate targeting of these systems can cripple immediate response capabilities of health services and emergency responders, potentially leading to increased casualties and chaos.[3]

In recent years, the evolution of terrorist strategies has seen a marked shift towards targeting infrastructures that have wide-reaching impacts on public health and safety.[4] This shift underscores a tactical adaptation by terrorist groups to exploit vulnerabilities in critical systems, where the disruption can have cascading effects beyond the immediate area of attack. The strategic targeting of telecommunications, a sector that binds the fabric of modern society, represents a deliberate effort to undermine governmental operations and instill panic amongst the civilian population.[5] The impact of such attacks is not only immediate but poses long-term challenges to public confidence in national security measures.

The interconnected nature of modern infrastructures means that the impact of attacks on telecommunications extends well beyond the immediate loss of communication capabilities. Such disruptions can cripple financial services, hinder emergency and health care provision, and disrupt the everyday life of millions.[6] The dependency of various sectors on a robust telecommunications network highlights the potential for multi-sectoral crises stemming from a single point of failure. This vulnerability presents a complex challenge for national and international security frameworks, emphasizing the need for comprehensive strategies that enhance resilience across all critical infrastructures.

The rapid dissemination of information is crucial in managing emergencies effectively. Telecommunication networks ensure that the flow of critical information remains uninterrupted during crises.[7] When these networks are disrupted by terrorist activities, significant delays in emergency responses and medical services can exacerbate public health crises, affecting both the efficiency of immediate medical responses and long-term recovery efforts in the impacted regions.[8]

Moreover, disruptions to telecommunication infrastructure hinder the public's ability to reach emergency services, delaying treatment of injuries and potentially increasing mortality rates. The absence of functional communication networks complicates the tasks of locating victims, dispatching ambulances, and providing timely medical interventions, which underscores the dependency of modern emergency responses on robust telecommunication systems.[9]

This research has systematically analyzed the impact of terrorist attacks on telecommunication systems, focusing on subsequent public health repercussions across different geopolitical environments. By examining incidents where telecommunication systems were targeted, it identifies patterns in the aftermath and evaluates the effectiveness of current emergency response strategies.

The interconnectedness of modern infrastructure means that disruptions to telecommunications impact more than just communication. Such attacks can cripple emergency health care, financial services, and essential daily operations, highlighting the critical role of telecommunications in crisis management. When networks are compromised, the flow of vital information halts, delaying emergency responses and increasing casualties. Moreover, the public's ability to access emergency services is hindered, potentially leading to higher mortality rates due to delayed medical interventions. This study examines the impact of these attacks on public health, focusing on how disruptions in telecommunications affect emergency response capabilities globally. The findings underscore the importance of enhancing resilience in telecommunication systems to mitigate public health crises resulting from such terrorist attacks.

Materials and Methods

Study Design and Overview

This study conducted a comprehensive retrospective analysis to assess the public health consequences of terrorist attacks on telecommunications globally. Our objective was to understand the patterns, frequencies, and impacts of these attacks, specifically focusing on their repercussions on emergency response services and medical infrastructure. By examining incidents from the Global Terrorism Database (GTD),[10] we aimed to elucidate the broader public health implications stemming from the disruption of critical communication infrastructures.

Data Sources and Selection

The primary data source for our analysis was the GTD, renowned for its comprehensive recording of terrorist incidents worldwide. The GTD classifies incidents based on various criteria, including the nature of the target, the weapons used, and the outcomes of the attack. For this study, we specifically extracted data related to attacks on telecommunications infrastructure. Our selection criteria included incidents that resulted in direct disruptions to telecommunications, documented from 1970–2020.

Data Preparation and Cleaning

Upon data extraction, a rigorous data cleaning process was undertaken to ensure the accuracy and consistency of the information. This included verifying the details of each incident, correcting any discrepancies, and removing incomplete records. The cleaned dataset was then organized into different categories based on the type of attack, the weapons used, and the geographic location of the incidents. This preparation was critical for conducting a reliable and valid analysis.

Analytical Framework

Quantitative analysis

Our study employed a quantitative research methodology using descriptive statistical techniques. This approach allowed us to calculate frequencies, percentages, and distributions of terrorist attacks on telecommunications across various dimensions, such as geographical regions and time periods. The intent was to identify and illustrate patterns and trends that could inform public health preparedness and policymaking.

Impact assessment

We also assessed the direct impacts of these attacks on public health systems, focusing on emergency response delays and disruptions in medical service provision. This involved analyzing the extent of the damage caused by different types of attacks and evaluating the subsequent effects on public health infrastructure.

Ethical considerations

Given the nature of the data, all analyses were performed with a commitment to ethical standards, ensuring that the study did not involve any direct interaction with human subjects or affect their privacy and confidentiality.

Results

Data from the Global Terrorism Database shows that terrorist attacks on telecommunications infrastructure disrupt emergency and medical communication systems, causing delays in medical responses and reducing the effectiveness of assistance. These disruptions also interfere with the dissemination of critical safety information and situational updates.

Weapon Types and Usage

Analysis of terrorist attacks on telecommunications infrastructure shows that explosives were the most used weapon, involved in 554 cases (Table 1). Incendiary devices were the second most frequently used, appearing in 419 cases. Firearms were involved in 78 incidents. Less common weapon combinations, such as "Explosives and Firearms" and "Firearms and Incendiary," highlight the diversity in terrorist tactics. Additionally, 43 cases were categorized as involving "Unknown" weapon types, indicating challenges in attribution.

Regional Distribution of Attacks

The geographical distribution of terrorist attacks on telecommunications infrastructure shows significant regional differences (Table 2). South Asia recorded the highest number of incidents (381), with a predominant use of incendiary devices and explosives. In contrast, North America experienced only 17 incidents, mostly involving incendiary devices. These variations in weapon use and frequency reflect regional security challenges and tactical preferences of terrorist groups.

Understanding these regional patterns is critical for shaping effective counterterrorism strategies, enabling governments and international bodies to allocate resources more efficiently and develop region-specific responses.

Impact on Public Health: Fatalities

Data from Table 3 quantifies fatalities resulting from terrorist attacks on telecommunications, categorized by weapon type. Firearms accounted for the highest number of fatalities (100), despite being used less frequently than explosives, which resulted in 59

https://doi.org/10.1017/dmp.2024.311 Published online by Cambridge University Press

Table 1. Types and frequency of weapons used in attacks on telecommunications

Weapon type	Count of weapon type
Explosives	554
Incendiary	419
Firearms	78
Unknown	43
Firearms, Incendiary	27
Explosives, Firearms	23
Firearms, Explosives	18
Explosives, Incendiary	13
Explosives, Explosives	8
Sabotage Equipment	6
Incendiary, Melee	4
Incendiary, Firearms	4
Melee	3
Incendiary, Unknown	3
Explosives,Firearms, Firearms	2
Explosives, Unknown	2
Firearms, Firearms	2
Firearms, Explosives, Firearms	1
Melee, Sabotage Equipment	1
Melee, Melee, Explosives	1
Firearms, Unknown, Explosives, Explosives	1
Explosives, Incendiary, Unknown	1
Explosives, Explosives, Firearms	1
Explosives, Firearms, Explosives, Firearms	1
Explosives, Firearms, Incendiary	1
Melee, Melee, Firearms	1
Incendiary, Incendiary, Melee	1
Other	1
Explosives, Firearms, Melee	1
Explosives, Melee, Melee	1
Incendiary, Sabotage Equipment	1
Firearms, Firearms, Incendiary	1
Grand Total	**1224**

deaths. The combined use of firearms and incendiary devices led to 26 fatalities, further emphasizing the lethal potential of multiple weapon types used in coordinated attacks.

The data reveals that complex weapon configurations, such as "Explosives, Firearms, Explosives, Firearms," caused fewer fatalities,[8] but still posed significant disruption. Zero-fatality incidents were also reported, indicating that while not all attacks result in deaths, they can still strain public health resources and emergency responses. Overall, the total of 244 fatalities highlights the need for enhanced public health preparedness, efficient response systems, and improved surveillance to mitigate the effects of future incidents.

Table 2. Summary of regional distribution of weapon types in terrorist attacks on telecommunications

Region	Total incidents
South Asia	381
Sub-Saharan Africa	95
Southeast Asia	156
South America	153
North America	17
Middle East & North Africa	72
Western Europe	157
Central America & Caribbean	149
Australasia & Oceania	14
Eastern Europe	19
East Asia	6
Central Asia	5

Table 3. Fatalities by weapon type in terrorist attacks targeting telecommunications

Weapon type	Sum of fatalities
Firearms	100
Explosives	59
Firearms, Incendiary	26
Incendiary	20
Firearms, Explosives	11
Explosives, Explosives	9
Explosives, Firearms, Explosives, Firearms	8
Explosives, Firearms	6
Unknown	2
Explosives,Firearms, Incendiary	2
Firearms, Explosives, Firearms	1
Grand Total	**244**

Target Analysis

Analysis of terrorist attacks reveals that telecommunications infrastructure was the primary target in 1145 incidents, indicating its strategic importance in causing widespread disruption (Table 4). Other targets, often combined with telecommunications, include private properties, police, government facilities, and utilities, further amplifying the impact of these attacks.

Less frequent but significant incidents involved telecommunications being targeted alongside other critical infrastructure such as police, government, and utility services. This indicates a broader strategy aimed at amplifying the effects of attacks across multiple sectors, stressing the importance of bolstering security and resilience across interconnected systems.

Global Patterns and Temporal Trends

The geographic distribution of terrorist attacks on telecommunications, shown in Table 5, indicates that India (133 incidents) and

https://doi.org/10.1017/dmp.2024.311 Published online by Cambridge University Press

Table 4. Types of targets involved in terrorist attacks on telecommunications

Target type	Count of target type
Telecommunication	1145
Telecommunication, Private Citizens & Property	15
Police, Telecommunication	9
Telecommunication, Telecommunication	8
Telecommunication, Telecommunication, Telecommunication	7
Business, Telecommunication	6
Government (General), Telecommunication	5
Telecommunication, Government (General), Private Citizens & Property	4
Private Citizens & Property, Telecommunication	4
Utilities, Telecommunication	2
Telecommunication, Utilities	2
Educational Institution, Telecommunication	1
Government (General), Telecommunication, Telecommunication	1
Telecommunication, Journalists & Media	1
Police,Telecommunication, Private Citizens & Property	1
Journalists & Media, Telecommunication	1
Police, Telecommunication, Utilities	1
Business, Telecommunication, Utilities	1
Business, Government (General), Telecommunication	1
Telecommunication, Police	1
Private Citizens & Property, Telecommunication, Telecommunication	1
Telecommunication, Private Citizens & Property, Police	1
Private Citizens & Property, Telecommunication, Utilities	1
Military, Educational Institution, Telecommunication	1
Telecommunication, Terrorists/Non-state Militia	1
Military, Telecommunication, Private Citizens & Property	1
Government (General), Private Citizens & Property, Telecommunication	1
Military, Telecommunication	1
Telecommunication, Government (General)	1
Grand Total	**1225**

El Salvador (119 incidents) are the most affected countries. This highlights regional vulnerabilities that may be influenced by geopolitical and socio-economic factors. Countries with fewer than 3 incidents are grouped under "Other" to simplify the table.

The chronological analysis of attacks from 1970–2020 shows a significant rise in incidents, peaking in 2020 with 138 attacks (Figure 1). This trend reflects the growing capabilities of terrorist organizations and the increasing strategic importance of telecommunications in modern society. The escalation in attack frequency emphasizes the need for dynamic, proactive global security measures to mitigate these evolving threats.

Table 5. Geographic distribution of terrorist attacks on telecommunications

Country	Count of Incidents
India	133
El Salvador	119
Nepal	93
Afghanistan	88
Thailand	78
Philippines	73
Peru	59
Pakistan	55
Colombia	54
Nigeria	38
United Kingdom	36
Spain	34
Kenya	32
Netherlands	31
France	28
Iraq	23
Chile	21
Algeria	19
Other (countries with fewer than 3 incidents)	125
Total	**1225**

Country-Specific Fatalities from Terrorist Attacks on Telecommunications

This analysis highlights the number of fatalities caused by terrorist attacks on telecommunications infrastructure, segmented by country. El Salvador and Nigeria, with the highest fatality counts, demonstrate the severe public health impacts of disrupted communication networks (Figure 2).

The data illustrates both the severity of these attacks and the vulnerability of telecommunications systems in specific geopolitical contexts. Countries with the highest fatalities, such as El Salvador and Nigeria, underscore the critical role telecommunications play in national security and emergency response. Conversely, countries with fewer or no fatalities still experience significant disruptions, pointing to varying levels of preparedness and resilience.

The differences in fatality rates across countries emphasize the need for region-specific counterterrorism strategies. Tailored protective measures, enhanced emergency response systems, and international cooperation are essential to mitigate the impacts of such attacks and safeguard public safety and health against threats targeting critical infrastructure.

Discussion

The findings from this study not only confirm the strategic targeting of telecommunications by terrorist groups but also illuminate the critical vulnerabilities within our global and regional security frameworks. The frequent targeting of telecommunications not only reflects its importance in emergency communications and

https://doi.org/10.1017/dmp.2024.311 Published online by Cambridge University Press

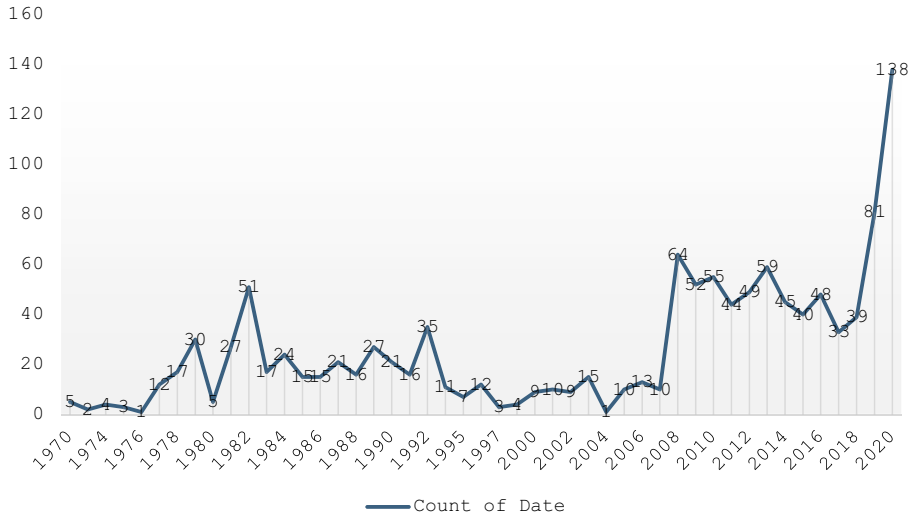

Figure 1. Chronological trends of terrorist attacks on telecommunications (1970–2020).

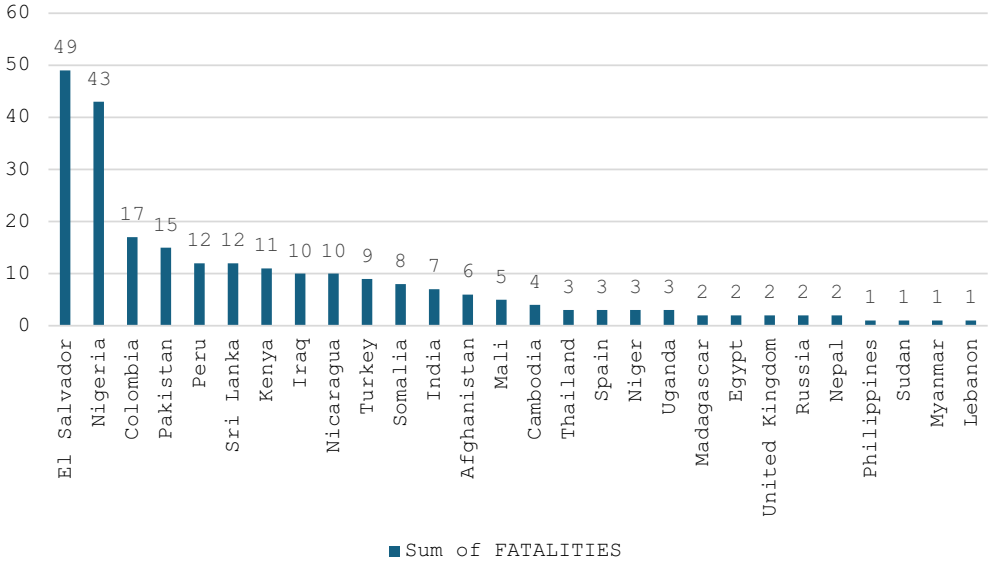

Figure 2. Fatalities resulting from terrorist attacks on telecommunications by country.

public safety but also demonstrates the high impact such disruptions can have on public health and crisis management.

Telecommunications systems have emerged as prime targets due to their ability to amplify the effects of terrorist acts far beyond the immediate physical damage.[11–12] The disruption of these systems cripples emergency response efforts at critical moments, exacerbates crises, and prolongs recovery times, thereby magnifying the terrorists' intended impact of instilling fear and chaos.[13] This aligns with findings from Mahmood et al., who notes the psychological and societal impacts of targeting critical infrastructure.[14]

The prevalent use of explosives and incendiary devices reveals a tactical sophistication and adaptability among terrorist groups.[15] These findings suggest that terrorists are selecting weapons based not only on their availability but also on their ability to cause maximum disruption to communication networks. The sophistication of attacks, including the use of combined weapon types, points to a calculated approach to overcome security defenses and exploit vulnerabilities within public health response frameworks.

The strategic selection of telecommunications as targets by terrorists is further corroborated by the overwhelming evidence of their preference for high-impact weapons, such as explosives.[16] The systematic use of these weapons, as revealed in our study, highlights their intent to cause maximum disruption. This not only incapacitates the communication infrastructure but also has a direct bearing on the ability of emergency services to manage crises effectively. These findings underscore the need for enhanced protective measures specifically designed to withstand such high-impact threats to maintain operational continuity in telecommunication services during critical times.

Region-specific trends in the choice of weaponry and targets underscore the need for localized security protocols and preparedness measures. Just as the motivations and resources of terrorist groups vary across different regions, so too must the countermeasures be

https://doi.org/10.1017/dmp.2024.311 Published online by Cambridge University Press

adapted to these regional specifics. This echoes Boyle who discusses the adaptation of security strategies to regional terrorist capabilities and objectives.[17]

Furthermore, our analysis highlights significant regional variations in the types of attacks and the frequency with which they occur. This regional specificity in terrorist strategies suggests that counter-terrorism measures cannot be one-size-fits-all but must be tailored to address specific regional threats and vulnerabilities. It also points to the potential benefits of a decentralized approach to telecommunication security, where regional authorities are empowered with the knowledge and resources to defend against the specific types of threats most likely to occur in their areas.

The temporal trends identified in our study, showing an increase in the frequency of attacks over recent decades, signal an escalating threat to global telecommunications infrastructure. This trend underscores the urgency for continuous evolution in security technologies and strategies to outpace the increasing sophistication and capabilities of terrorist groups. Part of this spike in attacks, especially in 2020, may be attributed to conspiracy theories linking 5G technology to the spread of COVID-19. As documented by De Cauwer et al.,[18] a significant number of these incidents involved arson attacks on 5G masts, fueled by misinformation about the health risks associated with 5G. This trend highlights the growing influence of conspiracy theories on terrorist activities and emphasizes the importance of addressing disinformation as part of broader counterterrorism and public safety strategies.

The integration of advanced predictive analytics and artificial intelligence could play a critical role in foreseeing and mitigating potential attacks before they occur.

The discussion raises critical considerations for future counter-terrorism strategies and the enhancement of telecommunications resilience. Building on the insights provided by this study, there is a clear imperative for developing more sophisticated threat detection and response strategies. These strategies should leverage advanced technologies to fortify telecommunications against such attacks, as suggested by Zhu & Li, who advocate for the integration of newer technologies to bolster critical infrastructure.[19]

Additionally, the stark differences in fatality rates across countries as identified in our results not only reflect the direct human cost of these attacks but also highlight disparities in national preparedness and emergency response capabilities. Countries with higher fatalities might benefit from international support and cooperation to build more resilient public health and emergency response systems. This collaboration could extend beyond intelligence sharing to include joint exercises and training programs, fostering a more unified and effective global response to such threats.[20]

These insights necessitate a proactive stance in international policymaking, where the protection of telecommunications infrastructure is integrated as a core component of national and international security strategies. Policymakers must consider both preventive and reactive measures in their strategic planning to ensure that telecommunication networks can resist and recover from terrorist attacks without substantial loss of functionality.

Lastly, the implications of our findings extend beyond the realm of security and emergency management to influence policy decisions related to the development and deployment of telecommunication infrastructure globally. Ensuring that new technologies not only enhance connectivity but are also resilient to attacks should be a priority in the planning and implementation stages of infrastructure projects.

In weaving these aspects together, the study highlights a critical nexus between terrorism, technology, and public health that demands a concerted, multidisciplinary approach to security and emergency preparedness. By aligning counter-terrorism efforts more closely with technological advancements and operational realities, we can forge a path towards a safer, more resilient global society.

Furthermore, the findings advocate for a reinforced collaborative approach in international security efforts. As underscored by Choudhary et al.[21] and Shortland and Forest,[22] the complexity and transnational nature of modern terrorist threats necessitate a unified response that spans borders and sectors. Enhancing international cooperation and intelligence sharing is crucial not only for pre-empting attacks but also for ensuring a robust defense against the dynamically evolving threats to global telecommunications infrastructure.[23] This collaborative stance must integrate cutting-edge technological solutions and strategic policymaking to bolster our collective security frameworks effectively.[24]

In sum, the study not only deepens the understanding of how telecommunications are targeted in terrorist attacks but also enhances the discourse on global and regional responses to these threats. By aligning counter-terrorism efforts more closely with the technological and operational realities of modern telecommunications, policymakers and security experts can better protect these vital systems and ensure that public health infrastructures are not unduly compromised in future attacks.

Limitations

The scope and impact of this research are subject to several limitations that are important to acknowledge. First, the reliance on data from the Global Terrorism Database presents challenges related to the accuracy and completeness of the reported information. While the GTD is a comprehensive repository of terrorist incidents, the variability in data collection methods across different regions and periods can introduce inconsistencies. These inconsistencies may influence the analysis of attack patterns and frequencies, potentially affecting the robustness of our conclusions.

Another significant limitation arises from the geographical coverage of the data. Although the study is global in scope, the distribution of data is not uniform across all regions. This uneven representation can lead to an overemphasis on regions with more complete data while underrepresenting areas where terrorism might be equally prevalent but less reported. Such disparities could skew our understanding of regional differences in terrorist tactics and the effectiveness of counterterrorism measures.

The study's focus on telecommunications-related incidents restricts its ability to explore the interconnectedness with other types of infrastructure attacks, which might also impact public health outcomes. Terrorist strategies often involve multiple target types, and the exclusion of these related attacks could limit a fuller understanding of the broader strategies employed by terrorist groups.

Additionally, while this research employs quantitative methods to assess the impact of terrorist attacks on public health, the complexity and depth of the consequences can be challenging to capture fully through statistical analysis alone. Qualitative data, such as detailed case studies or firsthand accounts, would complement and enhance the quantitative findings, offering deeper insights into the immediate and long-term effects of these disruptions on public health systems.

https://doi.org/10.1017/dmp.2024.311 Published online by Cambridge University Press

While this study provides valuable insights into the repercussions of terrorist attacks on telecommunications and public health, these limitations must be considered when interpreting the findings. Future research could address these gaps by incorporating a more diverse set of data sources, expanding geographical focus, and integrating qualitative methods to provide a more comprehensive analysis of the threats posed by terrorism to public health infrastructure.

Conclusions

This study has systematically examined the impact of terrorist attacks on telecommunications infrastructure, highlighting the vulnerabilities and public health consequences these attacks create. Telecommunications, vital for emergency responses, are a primary target due to their ability to amplify societal disruption. The use of high-impact weapons like explosives and incendiary devices reflects a tactical approach aimed at maximizing chaos, which cripples emergency responses and public health infrastructure. Our research demonstrates the need for region-specific counterterrorism strategies, as regional variations in attack frequency and methods necessitate localized security measures. Furthermore, the increasing trend in these attacks calls for advancements in security technologies, including the integration of predictive analytics and artificial intelligence, to better mitigate these threats. Finally, international collaboration is essential to enhance resilience in telecommunications, demanding a unified global response to protect critical infrastructure. These insights should guide policymakers in developing effective, technology-driven security strategies that ensure the functionality of telecommunications during crises and support efficient emergency responses.

Data availability statement. The datasets used and/or analyzed during the current study are available from the corresponding author on reasonable request.

Acknowledgments. The authors extend their appreciation to the Deputyship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research work through project number (ISP2398).

Funding statement. This research received no external funding.

Competing interest. The authors declare no conflict of interest.

References

1. **Lindert J**, **Bilsen J**, **McKee M.** Terrorist attacks: a public health issue. *Eur J Public Health.* 2018;**28**(6):986.
2. **Zhang Z**, **Tang J.** Analysis of news dissemination path and impact of big data technology in public health emergencies. *J Environ Public Health.* 2022; 2022.
3. **Alam MM**, **Le Moullec Y**, **Ahmad R**, et al. A primer on public safety communication in the context of terror attacks: the NATO sps "counter-terror" project. In: *Advanced Technologies for Security Applications: Proceedings of the NATO Science for Peace and Security'Cluster Workshop on Advanced Technologies', 17-18 September 2019*, Leuven, Belgium. Springer Netherlands; 2020:19–34.
4. **Stewart MG**, **Mueller J.** Terrorism risks, chasing ghosts and infrastructure resilience. *Sustain Resilient Infrastruct.* 2020;**5**(1–2):78–89.
5. **Cavaliere GA**, **Alfalasi R**, **Jasani GN**, et al. Terrorist attacks against healthcare facilities: a review. *Health Security.* 2021;**19**(5):546–550.
6. **Roshanaei M.** Resilience at the core: critical infrastructure protection challenges, priorities and cybersecurity assessment strategies. *J Comput Commun.* 2021;**9**(8):80–102.
7. **Khorram-Manesh A**, **Goniewicz K**, **Burkle Jr FM.** Unleashing the global potential of public health: a framework for future pandemic response. *J Infect Public Health.* 2024;**17**(1):82–95.
8. **Torpan S**, **Hansson S**, **Rhinard M**, et al. Handling false information in emergency management: a cross-national comparative study of European practices. *Int J Disaster Risk Reduct.* 2021;**57**:102151.
9. **Barten DG**, **Klokman VW**, **Cleef S**, et al. When disasters strike the emergency department: a case series and narrative review. *Int J Emerg Med.* 2021;**14**:1–9.
10. **Global Terrorism Database** (GTD). Information on Terrorist Events Around the World. 2023, START.umd.edu. Accessed Feb, 15, 2024.
11. **Veerasamy N.** Cyberterrorism–the spectre that is the convergence of the physical and virtual worlds. In: *Emerging Cyber Threats and Cognitive Vulnerabilities*. Academic Press; 2020:27–52.
12. **Adigwe CS**, **Mayeke NR**, **Olabanji SO**, et al. The evolution of terrorism in the digital age: investigating the adaptation of terrorist groups to cyber technologies for recruitment, propaganda, and cyberattacks. *Asian J Bus Account.* 2024;**24**(3):289–306.
13. **Gkeredakis M**, **Lifshitz-Assaf H**, **Barrett M.** Crisis as opportunity, disruption and exposure: exploring emergent responses to crisis through digital technology. *Inf Organ.* 2021;**31**(1):100344.
14. **Mahmood R**, Jetter M. *Communications technology and terrorism.* J Confl Resolut. 2020;**64**(1):127–166.
15. **Santaspirt M.** *Improvised explosive devices: assessing the global risk for use in terrorism*. Doctoral dissertation, Rutgers University Graduate School: Newark, NJ; 2020.
16. **Feltes J.** Weapons of Mass Destruction—Conceptual and Ethical Issues with Regard to terrorism. In: *Counter-Terrorism, Ethics and Technology: Emerging Challenges at the Frontiers of Counter-Terrorism*. Cham: Springer International Publishing; 2021:49–69.
17. **Boyle MJ**. Weapon of choice: terrorist bombings in armed conflict. *Stud Conflict Terrorism.* 2022;**45**(9):778–798.
18. **De Cauwer H**, **Barten DG**, **Tin D**, et al. Terrorist attacks against COVID-19-related targets during the pandemic year 2020: a review of 165 incidents in the Global Terrorism Database. *Prehosp Disaster Med.* 2023;**38**(1):41–47.
19. **Zhu Y**, **Li N.** Virtual and augmented reality technologies for emergency management in the built environments: a state-of-the-art review. *J Saf Sci Resil.* 2021;**2**(1):1–10.
20. **Khorram-Manesh A**, **Mortelmans LJ**, **Robinson Y**, et al. Civilian-military collaboration before and during Covid-19 pandemic—a systematic review and a pilot survey among practitioners. *Sustainability.* 2022;**14**(2):624.
21. **Choudhary SA**, **Khan MA**, **Sheikh AZ**, et al. Role of information and communication technologies on the war against terrorism and on the development of tourism: evidence from a panel of 28 countries. *Technol Soc.* 2020;**62**:101296.
22. **Shortland N**, **Forest JJ**. Tracking terrorism: the role of technology in risk assessment and monitoring of terrorist offenders. *Science Informed Policing.* 2020:57–76.
23. **Kotsias J**, **Ahmad A**, **Scheepers R.** Adopting and integrating cyber-threat intelligence in a commercial organisation. *Eur J Inf Syst.* 2023;**32**(1):35–51.
24. **Mani ZA**, **Goniewicz K.** Transforming healthcare in Saudi Arabia: a comprehensive evaluation of Vision 2030's impact. *Sustainability.* 2024; **16**(8):3277.