Reviewing the Health Care Impacts of Attacks on Critical Infrastructure

Cara Taubman, MD, MPH;[1] Alexander Hart, MD;[2] Attila Hertelendy, PhD;[3] Derrick Tin, MBBS;[4] Ryan Hata, MD;[1] Gregory R. Ciottone, MD[5]

1. Fellow, BIDMC Disaster Medicine Fellowship; Department of Emergency Medicine, Beth Israel Deaconess Medical Center and Harvard Medical School, Boston, Massachusetts, USA
2. Director of Research, BIDMC Disaster Medicine Fellowship; Department of Emergency Medicine, Hartford Hospital; University of Connecticut School of Medicine, Farmington, Connecticut, USA
3. Director of Research/Director of Innovation and Technology, BIDMC Disaster Medicine Fellowship; Department of Emergency Medicine, Beth Israel Deaconess Medical Center, Boston, Massachusetts, USA
4. Director of Counter-Terrorism Medicine, BIDMC Disaster Medicine Fellowship; Department of Emergency Medicine, Beth Israel Deaconess Medical Center and Harvard Medical School, Boston, Massachusetts, USA
5. Director, BIDMC Disaster Medicine Fellowship; Department of Emergency Medicine, Beth Israel Deaconess Medical Center; Associate Professor, Harvard Medical School, Boston, Massachusetts, USA

Correspondence:
Cara Taubman, MD, MPH
Fellow, BIDMC Disaster Medicine
   Fellowship
Department of Emergency Medicine
Beth Israel Deaconess Medical Center and
Harvard Medical School
Boston, Massachusetts, USA
E-mail: Ctaubman@bidmc.harvard.edu

Abstract

Introduction: Health care provision depends on reliable critical infrastructure (CI) to power equipment and to provide water for medication and sanitation. Attacks on CI limiting such functions can have a profound and prolonged influence on delivery of care.

Methods: A retrospective analysis of the Global Terrorism Database (GTD) was performed of all attacks occurring from 1970-2020. Data were filtered using the internal database search function for all events where the primary target was "Utilities," "Food or Water Supply," and "Telecommunications." For the purposes of this study, the subtype "Food Supply" was excluded. Events were collated based on year, country, region, and numbers killed and wounded.

Results: The GTD listed 7,813 attacks on CI, with 6,280 of those attacks targeting utilities, leading to 1,917 persons directly killed and 1,377 persons wounded. In total, there were 1,265 attacks targeting telecommunications causing 205 direct deaths and 510 wounded. Lastly, 268 attacks targeted the water supply with 318 directly killed and 261 wounded. Regionally, South America had the most attacks with 2,236, followed by Central America and the Caribbean with 1,390. Based on infrastructure type, the most attacks on utilities occurred in El Salvador (1,061), and the most attacks on telecommunications were in India (140). Peru (46) had the most attacks on its water supply.

Conclusion: The regions with the highest number of total attacks targeting CI have historically been in South America, with more attacks against power and utilities than other infrastructure. Although the numbers of persons directly killed and wounded in these attacks were lower than with other target types, the true impacts on lack of health care delivery are not accounted for in these numbers. By understanding the pattern and scope of these attacks, Counter-Terrorism Medicine (CTM) initiatives can be created to target-harden health care-related infrastructure.

Introduction

Critical infrastructure (CI) is a universal term used to describe assets and facilities essential to the functioning of a society. The systems and interconnecting networks that enable day-to-day operations are often taken for granted, yet a disruption to any one of those systems can have dire consequences across other sectors. The dangers of CI interdependencies and the downstream societal impacts were starkly demonstrated by a number of recent events, including the 2020 bombing of an AT&T facility in Nashville, Tennessee (USA). Interruption of telecommunications caused disruption in Emergency Medical Services, police, and fire response when the 9-1-1 emergency call system went down, as well as loss of

Abbreviations:
CI: critical infrastructure
CTM: Counter-Terrorism Medicine
EMR: electronic medical record
GTD: Global Terrorism Database
NHS: National Health Service
START: National Consortium for the Study of
   Terrorism and Responses to Terrorism
UNICEF: United Nations Children's Fund

	Number of Attacks	Total Persons Killed	Total Persons Wounded
Utilities	6,280	1,917	1,377
Water	268	318	261
Telecommunications	1,265	205	510

Table 1. Total Number of Attacks by Target

function of electronic medical records (EMRs) in multiple hospitals which further impeded health care services.[1]

Health systems have specific vulnerabilities with both direct and indirect consequences on patient outcomes. In 2021, the United Nations Children's Fund (UNICEF; New York, New York USA) warned that the deliberate attacks on the Libyan Man-Made River, which provides a significant part of the country's water supply, could lead to an increase in communicable diseases, particularly in children.[2] A 2017 report looking at the effects of explosive weapons on health care in Ukraine illustrated how the destruction of CI such as water and power lines has had a prolonged effect on the quality and availability of medical services.[3]

Health care delivery is dependent on resources provided by surrounding CI, which increasingly includes telecommunications. The 2017 WannaCry ransomware epidemic, which disabled Britain's National Health Service (NHS; London, United Kingdom) for several days, led to the cancellation of 19,000 appointments.[4] The NHS identified at least 139 of these appointments as being for patients who potentially had cancer, possibly delaying diagnosis and treatment.[5]

While several national and regional directives such as the United States Cybersecurity and Infrastructure Security Agency (CISA; Arlington, Virginia USA) exist to protect CI from intentional damage and mitigate the risk of failure of such assets, they remain vulnerable and at risk of intentional attacks. This paper explores historic terrorist attacks on CI, specifically energy, telecommunication, and water infrastructure, and aims to better understand the frequency and patterns of such disruptions on the health care sector.

Methods

Data collection was performed using a retrospective database search through the Global Terrorism Database (GTD).[6] This database is open access, with publicly available data collection methodology utilizing artificial intelligence that identifies events from news media around the world daily, as confirmed by human evaluation of the events by the National Consortium for the Study of Terrorism and Responses to Terrorism (START; College Park, Maryland USA). The GTD defines terrorist attacks as: "The threatened or actual use of illegal force and violence by a non-state actor to attain a political, economic, religious, or social goal through fear, coercion, or intimidation." The GTD database does not include acts of state terrorism. The GTD contains no personal identifiers for victims and links specific events to open-source news articles.

The GTD database was downloaded and searched using the internal database search functions for all events that occurred from January 1, 1970 - December 31, 2020. Years 2021 and 2022 were not yet available at the time of the study. "Utilities," "Food or Water Supply," and "Telecommunications" as primary target types were selected for the purpose of this study. Events were analyzed based on country, region, and numbers killed and wounded. All classifications were pre-determined by the GTD. The GTD codes "Utilities" as "Facilities for the transmission or generation of energy. For example, power lines, oil pipelines, electrical transformers, high tension lines, gas, and electric substations are all included in this value. This value also includes lampposts or streetlights." The GTD further breaks this target type into subtypes of "Electricity, Gas, and Oil." The GTD codes "Food or Water Supply" as "Attacks on food or water supplies or reserves are included in this value. This generally includes attacks aimed at the infrastructure related to food and water for human consumption." The GTD subtypes of this target type are "Food Supply" and "Water Supply." For the purposes of this study, only the subtype "Water Supply" was analyzed. Lastly, "Telecommunications" in the GTD includes "Attacks on facilities and infrastructure for the transmission of information. More specifically, this value includes things like cell phone towers, telephone booths, television transmitters, radio, and microwave towers."

Results were exported into an Excel spreadsheet (Microsoft Corp.; Redmond, Washington USA) for analysis. Double data entry and analysis were performed to ensure validity. Attacks met inclusion criteria if they fulfilled the three terrorism-related criteria below, as set by the GTD. Ambiguous events were excluded when there was uncertainty as to whether the incident met any of the criteria for GTD inclusion as a terrorist incident. The three criteria were determined within the database and not by the authors. First criterion states that "The act must be aimed at attaining a political, economic, religious, or social goal." Second criterion is that "There must be evidence of an intention to coerce, intimidate, or convey some other message to a larger audience (or audiences) than the immediate victims." Last criterion is that "The action must be outside the context of legitimate warfare activities, ie, the act must be outside the parameters permitted by international humanitarian law, particularly the admonition against deliberately targeting civilians or non-combatants."

Results

The GTD listed a total of 7,813 attacks on CI (Table 1). Most attacks were against utilities with 6,280 attacks leading to 1,917 persons killed and 1,377 persons wounded. There were 1,265 attacks on telecommunications causing 205 deaths and 510 wounded. A total of 268 attacks on water supply were documented. These accounted for 318 killed and 261 wounded (Table 1).

South America had the highest number of attacks on CI with 2,236, followed by the Central America and Caribbean region with 1,390. The regions with the lowest number of attacks were East Asia and Central Asia with 10 and 15, respectively (Figure 1).

Utilities made up the highest percentage of attacks in all regions except Australia and Oceania where attacks on telecommunications accounted for 74% (Figure 2).

The individual countries with the highest number of attacks on utilities were El Salvador (1,061), Columbia (821), and Peru (653); Figure 3. The GTD further breaks down utilities to

Total Attcks on Infrastructure by Region
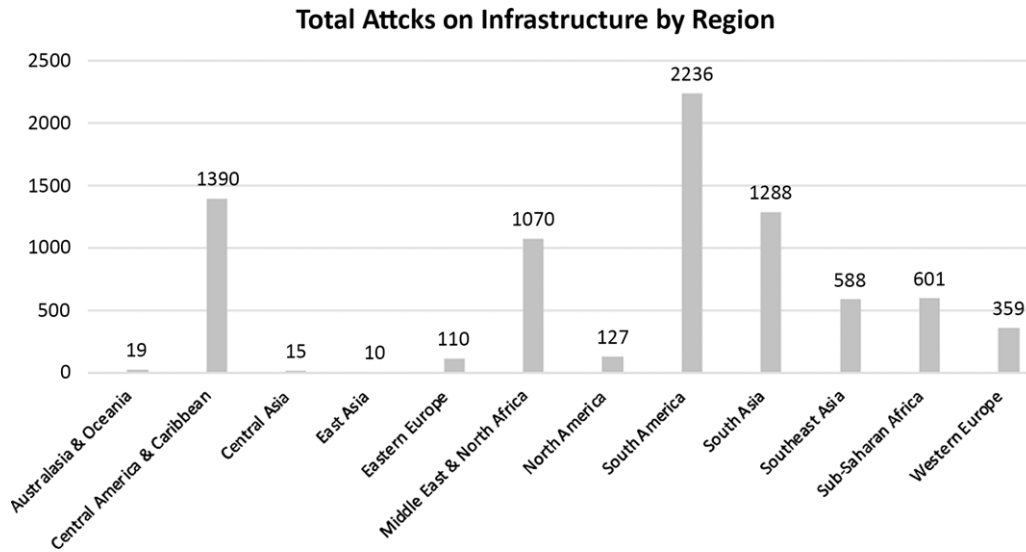
Taubman © 2023 Prehospital and Disaster Medicine

Figure 1. Total Attacks on Infrastructure by Region.

Breakdown of Attacks on Infrastructure by Region

■ Telecommunications ■ Utilities ■ Water
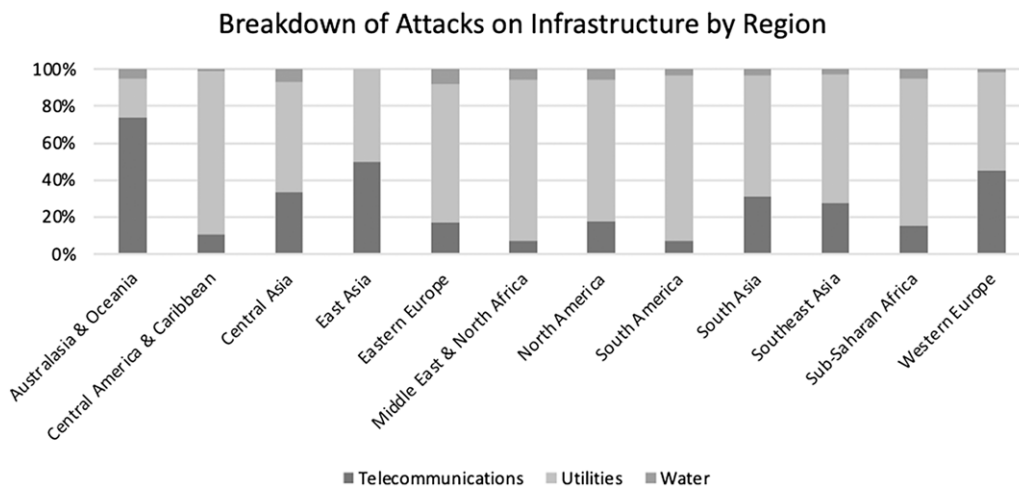
Taubman © 2023 Prehospital and Disaster Medicine

Figure 2. Breakdown of Attacks on Infrastructure by Region.

Top 20 Countries with Attacks on Utilities
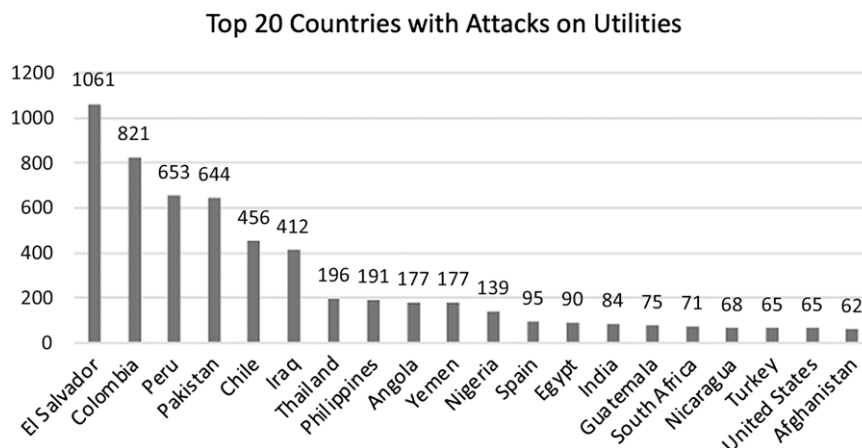
Taubman © 2023 Prehospital and Disaster Medicine

Figure 3. Top 20 Countries with Attacks on All Utilities.

	Total	Electricity	Gas	Oil
1	El Salvador (1,061)	El Salvador (1,058)	Pakistan (339)	Colombia (553)
2	Colombia (821)	Peru (637)	Egypt (38)	Iraq (128)
3	Peru (653)	Chile (449)	Russia (22)	Yemen (128)
4	Pakistan (644)	Pakistan (275)	Yemen (22)	Nigeria (122)
5	Chile (456)	Iraq (270)	Colombia (20)	Turkey (33)
6	Iraq (412)	Colombia (248)	Algeria (20)	Pakistan (30)
7	Thailand (196)	Thailand (194)	Syria (16)	India (28)
8	Philippines (191)	Philippines (185)	Nigeria (16)	Iran (26)
9	Angola (177)	Angola (164)	Ukraine (14)	Libya (21)
10	Yemen (177)	Spain (82)	Iraq (14)	Peru (14)

<div align="right">Taubman © 2023 Prehospital and Disaster Medicine</div>

Table 2. Top 10 Countries with Attacks on Utilities Broken Down by Utility Subtype
Note: Total Number in Parenthesis.

electricity, gas, and oil. The country with the most total attacks was El Salvador, which also had the highest number of attacks on electricity. Pakistan had the highest number of attacks on gas, and Colombia had the most on oil (Table 2). Of the attacks on utilities, the number per year ranged from a low of five in 1973 and 1974 to a high of 388 in 1991. While there was a dip in the 1990s-early 2000s, attacks on utilities had another peak in the 2010s (Figure 4).

Attacks on telecommunications saw a major increase in 2008, which has been sustained with the highest number ever recorded in 2020 (137); Figure 5. India had experienced the highest number of attacks on telecommunications with 140 total attacks, followed by El Salvador (118), Nepal (98), and Afghanistan (88); Figure 6.

In recent years, there have been far fewer attacks on water systems than on utilities and telecommunications (Figure 7). The countries with the most attacks were Peru (46), Iraq (25), and Pakistan (20); Figure 8.

Discussion
Over the last several decades, increased energy usage has been seen globally, with increases in both access and consumption.[7] Lee pointed out that although attacks on energy infrastructure are a small percentage of total attacks at this time, they are of interest to some terrorists based on their motivation. For terrorists whose motivation is related to economics or climate, infrastructure targets such as energy facilities are attractive as destruction of these targets may have economic impacts. They also point out that energy facilities are vulnerable due to their low mobility and high concentration based on resources needed; for example, oil facilities are often concentrated around locations where oil is naturally found. Nigeria, a country with some of the highest number of attacks on oil infrastructure, has many groups with these motivations. Groups point to oil production causing environmental devastation and poor compensation for communities effected in the Niger Delta as motivations for attack.[8,9] Facilities in remote locations may be more difficult to protect.[10] This was pertinent in 2019 when drones were used to target Saudi Arabia's Aramco Facility causing the largest disruption of oil production on record.[11]

Health care systems can look to previous incidents of large-scale "blackouts" to understand potential impacts. In 2003, a tree branch fell onto high-voltage power lines leading to the largest power outage in North American history, affecting an estimated 50 million people.[12] This wide-spread power failure led to an increased number of patients presenting to New York City hospitals due to medical device failure,[13,14] respiratory disease,[15] and injuries that were attributed to the blackout.[16] The New York City Department of Health and Mental Hygiene reported multiple hospital generator failures, issues with equipment sterilization, the release of 500 million gallons of untreated sewage into local waterways, and the loss of mechanization of syndrome surveillance mechanisms.[16] The power outage itself affected the population's health when compared to data from comparable weather.[17] For example, syndromic surveillance demonstrated an increase in diarrheal illness in the days that followed.[18]

The impacts of power failure due to natural disaster or equipment failure could be seen with power failure due to intentional attack. Regarding attacks on power infrastructure, four of the top ten affected countries are in South and Central America. All are in the top five, with El Salvador having the highest number of attacks at 1,061, followed by Colombia with 821, Peru with 653, and Chile with 456. Pakistan is the only country in the top of the list outside of this region. In all four South and Central America countries, attacks on electricity infrastructure are the most common.

The United States has seen an increase of attacks on the power grid in 2022 and 2023.[19] The Program on Extremism from George Washington University (Washington, DC USA) has noted that the energy infrastructure is of interest to violent extremist groups in the United States.[20]

Water is a crucial resource, from drinking water to power and industrial functions, making it a target with a long history of attempted and successful attacks. These attacks can be to impede the system of delivery or to contaminate the contents.[21] There are a number of points where contaminants, including bioweapons, can be introduced, starting upstream from collection points.[22] Water systems increasingly rely on complex systems and smart technology making them vulnerable to cyber threats as well as disruptions in power.[23,24] One group looked at attacks on water infrastructure, particularly dam projects in Afghanistan, India, and Pakistan. They found in all three countries, there are water infrastructure projects that have faced scrutiny by local groups due to mistrust in the government or concern that the project is used to further domestic or foreign policy agenda.[25] These three countries are all in the top ten for attacks on water infrastructure. Pakistan was recorded to have 20 events. Afghanistan and India were found to have 11 events each. Groups reviewing naturally occurring and accidental waterborne outbreaks have highlighted this area of vulnerability for terrorists.[26] Clean water is a cornerstone of sanitation, hydration, and the mixing of medications, as
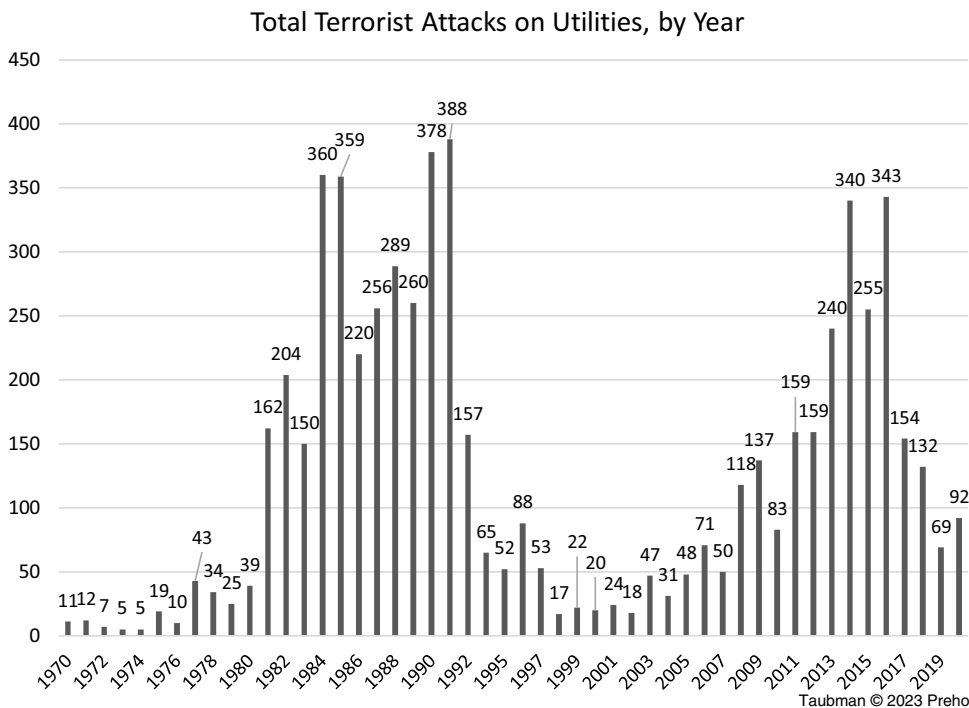
**Figure 4.** Attacks on All Utilities, by Year.
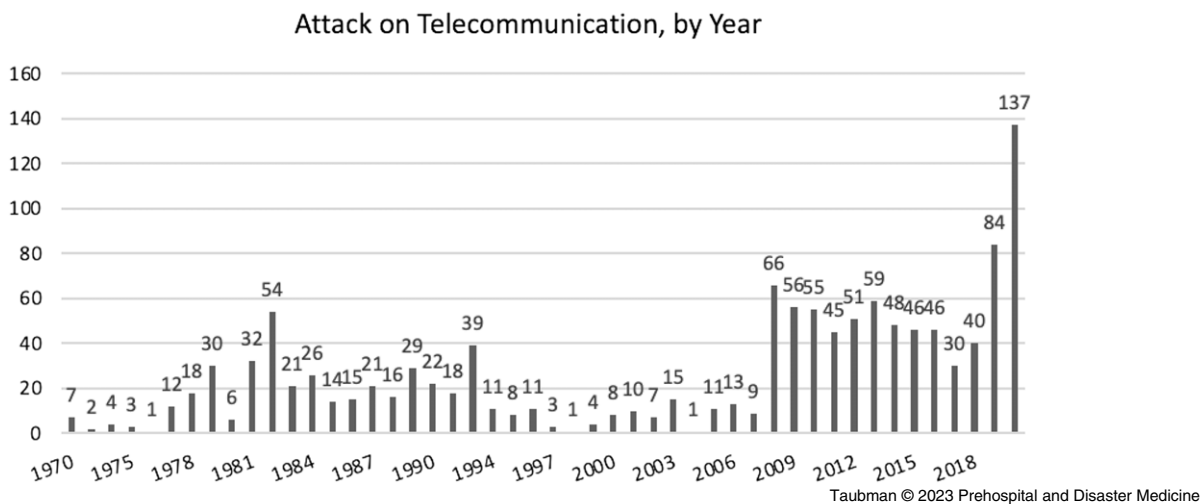
Figure 5. Attacks on Telecommunications, by Year.

well as other functions within the health care setting. Lack of access to clean water in hospitals of low- and middle-income countries has been shown to negatively impact surgical care.[27]

Contamination of water can have long-term impacts on the health and well-being of a community. In 2014, the water system in Flint, Michigan (USA) switched sources. During this change, the system was not treated to prevent the corrosion of pipes, leading to increased levels of lead in water provided to the community.[28] In 2016, this was found to correlate with, and likely cause an increase in, the percentage of estimated blood lead levels in children.[29] The Flint Registry has enrolled potentially exposed members of the community and monitors health and childhood development.[28] In addition to the direct medical effects of wide-spread water contamination, there are potentially secondary effects. A survey of

Flint residents from 2019-2020 showed a high prevalence of presumptive depression and posttraumatic stress disorder (PTSD).[30] A clean, reliable source of water not only impacts the health of a population, it can potentially affect the operations of a health care system. In August of 2022, heavy rainfall flooded the aging water treatment plan in Jackson, Mississippi (USA). The damage caused by flooding caused pumps to fail and water to stop flowing into the city's pipes.[31] This lack of water impacted the ability of some hospitals' fire suppression systems, resulting in a fire watch.[32,33] Other facilities had their air conditioning systems affected or had to provide portable bathrooms for staff, visitors, and patients.[33,34] Some local facilities were unaffected, as they had created their own water resource by constructing wells in response to previous water supply cut offs.[35]
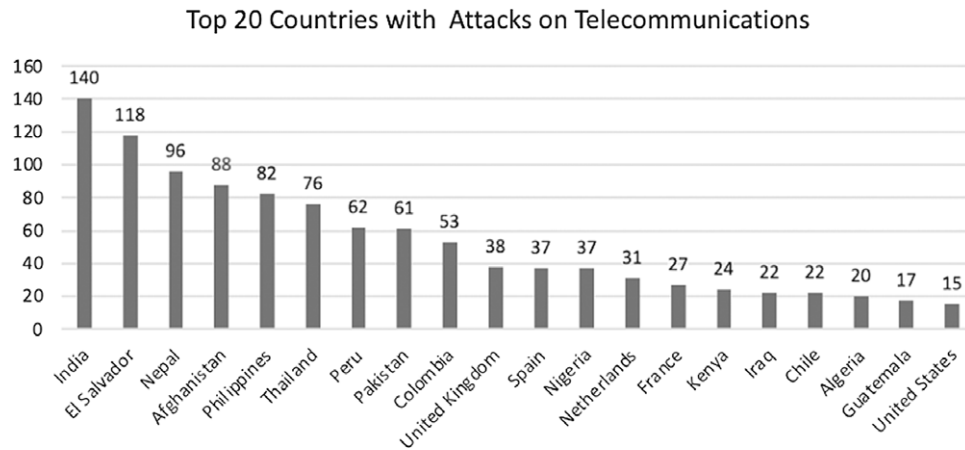
Top 20 Countries with Attacks on Telecommunications

Figure 6. Top 20 Countries with Attacks on Telecommunications.
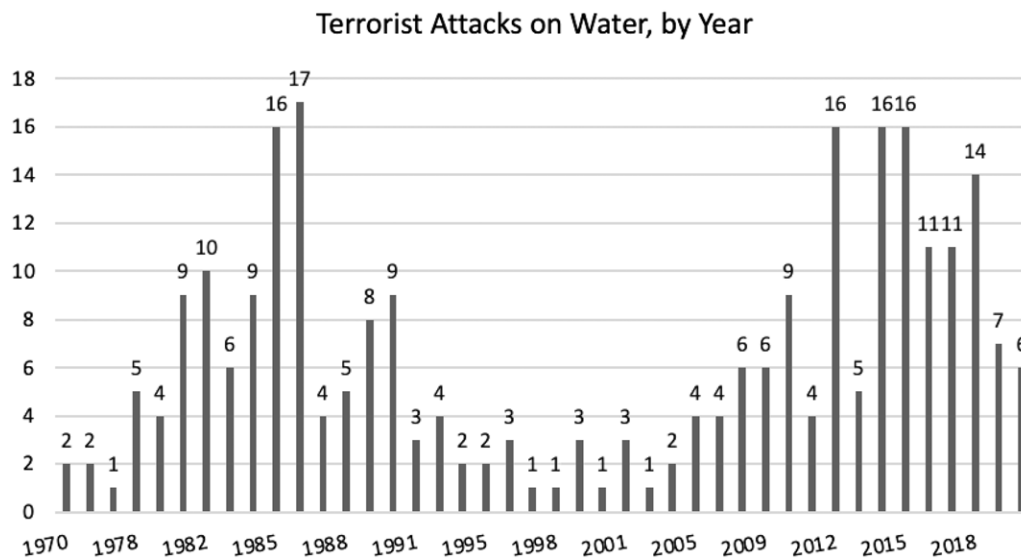
Terrorist Attacks on Water, by Year

**Figure 7.** Terrorist Attacks on Water, by Year.

Armed conflict has shown how attacks on CI affect health care. Within the first 162 days of the war in Ukraine, 15 cities had disruptions of electricity and eight had disruption of their water supply.[36] In response, UNICEF delivered water and generators to hospitals in Karkheive, Ukraine to counteract interruption of services.[2] During the conflict in Syria, the Islamic State of Iraq and Syria (ISIS) deliberately contaminated water with crude oil.[37] In fact, in 2016, it was estimated that 50% of the country was damaged in the conflict, partly due to intentional attacks on water infrastructure as well as power supply needed.[38]

Loss of telephone service in a hospital can affect how staff are alerted to emergencies, how clinical teams formulate and carry out treatment plans, and how they reach out to patient families for important decisions. In much of the world where prehospital emergency care is available, help is summoned by telephone. Interruption of such service may delay the public's ability to access care. In 2019, CenturyLink (Monroe, Louisiana USA), which provides service to several United States emergency call centers, experienced an outage. This impacted the emergency services in a large geographic area where the public could not reach the 9-1-1 emergency system to call for help.[39] The use of internet-based technology in some emergency call systems may improve response, but this also creates a new vulnerability in the form of a cyberattack.[40]

Proliferation of EMRs, telehealth capabilities, and network-based equipment have increased efficiency and improved health care delivery.[41] However, increasing dependency on these tools makes the systems which rely upon them more vulnerable to disruption. The global connectedness via the internet has presented an entirely new target to those seeking to attack infrastructure. While kinetic attacks such as the 2022 targeting of land and subsea cables in and around France remain a serious threat,[42] the utilization of cyberattacks by violent non-state-based organizations has taken on a distinct similarity to hybrid-warfare.[43] While there is currently debate on whether ideologically motivated cybercrime rises to the level of cyberterrorism, the United States Department of Homeland Security (Washington, DC USA) has predicted the use of cyberattacks as a likely methodology of terrorist activity.[44]

Top 20 Countries with attacks on water
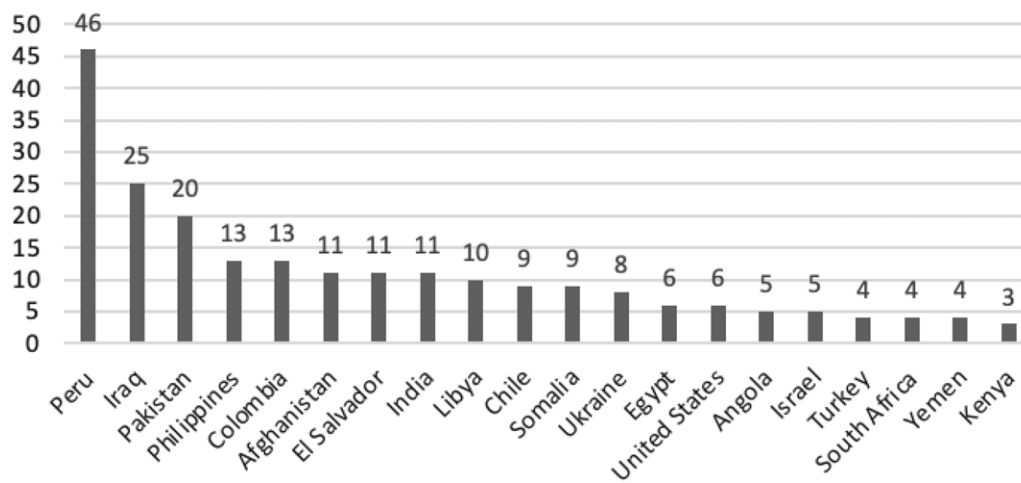
Taubman © 2023 Prehospital and Disaster Medicine

Figure 8. Top 20 Countries with Attacks on Water.

The attractiveness of targeting CI by nefarious actors via cyberattacks is of particular concern, and several recent accounts have highlighted the vulnerabilities of CI to cyberattacks.

Health care is particularly vulnerable to cyberattacks and is one of the most frequently targeted and costly entities, with an average total cost of US$10.1 million per breach in the United States.[45] The proliferation of EMRs, telehealth capabilities, and network-based equipment have increased efficiency and improved health care delivery.[41] However, increasing dependency on these systems makes them more vulnerable to disruption via cyberattacks. One study reported an increase in medication errors during EMR downtime.[46] After the 2010 Chilean earthquake, many hospitals were able to maintain electrical systems due to backup generators. However, they did not have a redundant communications system. Kirsh, et al reported that this breakdown in communications created "enormous difficulties in coordinating aid and for requesting outside help."[47]

Further research is needed to fully understand the potential impact of these events. Deeper evaluation of direct and indirect impacts to local health systems for attacks found in the GTD should be considered to fully understand impact these events have.

As health care systems and facilities conduct hazard vulnerability analysis, attention should be paid to understanding the interconnected complexities of the resources needed to support such systems. Facilities in locations where attacks on utilities are more prevalent need to look at how their institutions can continue to function when supply is cut, particularly in the case of a long-term interruption of service, and hospital systems should prophylactically engage with Disaster Medicine specialists who are specifically trained to understand and operate in complex crisis environments. Understanding the health care impacts of intentional attacks such as terrorism events is the subspecialty domain of Counter-Terrorism Medicine (CTM), a niche yet increasingly important area of study and discussion as the modern environment of threat rapidly evolves. Hospital systems should incorporate mitigation strategies to prevent the loss of services when CI is interrupted. Development of emergency operations and "downtime" plans should be prioritized, simulation drills of critical infrastructure failure drills should be performed, and multi-agency

discussions with other key stakeholders regarding potential failures should take place, especially if they are in a region of potential risk to such attacks.

Limitations

The GTD is a comprehensive record of documented global terrorist events. It is maintained by START and is the basis for other terrorism-related measures, such as the Global Terrorism Index. Reliance wholly on the GTD is partially mitigated by confirmation with other lay sources and searches for other online searches, but if there are incidents not reported in the GTD, this could limit the veracity of the findings. Using pre-existing databases such as the GTD as a data source also inherently introduces potential challenges, such as miscoding errors or data entry errors. Furthermore, the lack of a universally agreed-upon definition of the term "terrorism" can create inconsistencies between databases in the labelling of such events. Clear and detailed documentation of terrorist events is further hindered by restrictions on reporting, the lack of independent corroboration, and the lack of transparency within certain government sources. Infrastructure needed to report, detect, and investigate terrorism events is likely lacking in many parts of the world, leading to potential under-reporting of events.

Finally, this study does not directly measure the impact of attacks of health care but measures the frequency of pattern of attacks seen in the past. The discussion is based on existing literature of other similar events and their consequences.

Conclusion

The regions with the highest number of total attacks targeting CI have historically been in South America, with more attacks against power and utilities than other infrastructure. The numbers of persons directly killed and wounded in these attacks were lower than those with other target types. Each event is unique, and the impact on local health systems is an important area of research as the true impacts these attacks have on health care delivery may not be fully accounted for with these numbers. By understanding the pattern and scope of these attacks, CTM initiatives can be created to mitigate and respond to interruptions in CI, allowing health care facilities to continue care.

Author Contributions

CT participated in the conception and design of the research. CT acquired and analyzed the data and interpreted the results. RH performed a secondary analysis of data to ensure validity. CT, RH, AH, AH, and DT contributed to writing the manuscript and reviewed the results and discussion. GC provided oversight and final approval of manuscript. All authors have read the manuscript and approved its submission.

References

1. Rojas R, McGee J, Lee E, Cavendish S. When Nashville Bombing Hit a Telecom Hub, the Ripples Reached Far Beyond. *New York Times.* December 29, 2020. https://www.nytimes.com/2020/12/29/us/nashville-bombing-telecommunications.html. Accessed June 2023.
2. United Nations Children's Fund (UNICEF). UNICEF Libya Country Office Annual Report – 2021. https://www.unicef.org/reports/country-regional-divisional-annual-reports-2021/Libya. Accessed June 2023.
3. Harvard Law School International Human Rights Clinic and PAX. Operating Under Fire. The Effects of Explosive Weapons on Health CAre in the East of Ukraine. 2016. https://paxforpeace.nl/publications/operating-under-fire/. Accessed June 2023.
4. Field M. WannaCry cyber-attack cost the NHS £92m as 19,000 appointments cancelled. *The Telegraph.* October 11, 2018. https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/. Accessed June 2023.
5. Ghafur S, Kristensen S, Honeyford K, Martin G, Darzi A, Aylin P. A retrospective impact analysis of the WannaCry cyberattack on the NHS. *npj Digital Medicine.* 2019;2(1).
6. National Consortium for the Study of Terrorism and Responses to Terrorism (START). Global Terrorism Database 1970-2020. https://www.start.umd.edu/gtd. Accessed 2022.
7. Ritchie H, Roser M, Rosado P. Energy. *Our World in Data.* 2020. https://ourworldindata.org/energy. Accessed June 2023.
8. Tobor JO. Terrorism or clamor for resource control: an analysis of Nigeria's Niger Delta militants. *Journal of Terrorism Research.* 2016;7(3):23.
9. Ugwueze MI, Onuoha FC. Hard versus soft measures to security: explaining the failure of counter-terrorism strategy in Nigeria. *Journal of Applied Security Research.* 2020;15(4):547–567.
10. Lee C. Why do terrorists target the energy industry? A review of kidnapping, violence, and attacks against energy infrastructure. *Energy Research & Social Science.* 2022;87:102459.
11. Hubbard B, Karasz P, Reed S. Two Major Saudi Oil Installations Hit by Drone Strike, and U.S. Blames Iran. *New York Times.* September 14, 2019. https://www.nytimes.com/2019/09/14/world/middleeast/saudi-arabia-refineries-drone-attack.html. Accessed June 2023.
12. Minkel JR. The 2003 Northeast Blackout–Five Years Later. *Scientific American.* August 13, 2008. https://www.scientificamerican.com/article/2003-blackout-five-years-later/. Accessed June 2023.
13. Greenwald PW, Rutherford AF, Green RA, Giglio J. Emergency department visits for home medical device failure during the 2003 North America blackout. *Acad Emerg Med.* 2004;11(7):786–789.
14. Prezant DJ, Clair J, Belyaev S, et al. Effects of the August 2003 blackout on the New York City health care delivery system: a lesson for disaster preparedness. *Crit Care Med.* 2005;33(1 Suppl):S96–101.
15. Dominianni C, Lane K, Johnson S, Ito K, Matte T. Health impacts of citywide and localized power outages in New York City. *Environmental Health Perspectives.* 2018;126(6):067003.
16. Beatty ME, Phelps S, Rohner C, Weisfuse I. Blackout of 2003: public health effects and emergency response. Public Health Reports. 2006;121(1):36–44.
17. Lin CJ, Richardson DB, Hilborn ED, Weinberg H, Engel LS, Wade TJ. Emergency department visits for acute gastrointestinal illness after a major water pipe break in 2010. *Epidemiology.* 2019;30(6):893–900.
18. Marx MA, Rodriguez CV, Greenko J, et al. Diarrheal illness detected through syndromic surveillance after a massive power outage: New York City, August 2003. *Am J Public Health.* 2006;96(3):547–553.
19. Levenson M. Attacks on Electrical Substations Raise Alarm. *New York Times.* February 4, 2023. https://www.nytimes.com/2023/02/04/us/electrical-substation-attacks-nc-wa.html. Accessed March 15, 2023.
20. Krill I, Clifford B. Mayhem, Murder, and Misdirection: Violent Extremist Attack Plots Against Critical Infrastructure in the United States, 2016-2022. September 2022. https://extremism.gwu.edu/report-mayhem-murder-and-misdirection-violent-extremist-attack-plots-against-critical-infrastructure. Accessed June 2023.
21. Gleick PH. Water and terrorism. *Water Policy.* 2006;8:481–503.
22. Meinhardt PL. Water and bioterrorism: preparing for the potential threat to US water supplies and public health. *Annual Review of Public Health.* 2005;26(1):213–237.
23. Bello A, Jahan S, Farid F, Ahamed F. A systemic review of the cybersecurity challenges in Australian water infrastructure management. *Water.* 2022;15(1):168.
24. Thornton J. Managing Cascading Disasters in Texas Water Infrastructure Systems: A Qualitative Study. Dissertation. Colorado Technical University; 2020.
25. Ashraf T, Dinar S, Veilleux J. Dams, terrorism, and water nationalism's response to globalization and development: the case of South Asia. *Terrorism and Political Violence.* 2022;34(5):958–978.
26. Khan AS, Swerdlow DL, Juranek DD. Precautions against biological and chemical terrorism directed at food and water supplies. *Public Health Rep.* 2001;116(1):3–14.
27. Chawla SS, Gupta S, Onchiri FM, Habermann EB, Kushner AL, Stewart BT. Water availability at hospitals in low- and middle-income countries: implications for improving access to safe surgical care. *J Surg Res.* 2016;205(1):169–178.
28. Ruckart PZ, Ettinger AS, Hanna-Attisha M, Jones N, Davis SI, Breysse PN. The Flint water crisis: a coordinated public health emergency response and recovery initiative. *J Public Health Manag Pract.* 2019;25(1):S84–S90.
29. Hanna-Attisha M, Lachance J, Sadler RC, Champney Schnepp A. Elevated blood lead levels in children associated with the Flint drinking water crisis: a spatial analysis of risk and public health response. *Am J Public Health.* 2016;106(2):283–290.
30. Reuben A, Moreland A, Abdalla SM, et al. Prevalence of depression and posttraumatic stress disorder in Flint, Michigan 5 Years After the Onset of the Water Crisis. *JAMA Network Open.* 2022;5(9):e2232556.
31. Breslow J. The water crisis in Jackson follows years of failure to fix an aging system. *NPR.* August 31, 2022. https://www.npr.org/2022/08/31/1120166328/jackson-mississippi-water-crisis. Accessed June 2023.
32. Bean M. How hospitals are responding to the water crisis in Mississippi. *Becker's Hospital Review.* August 31, 2022. https://www.beckershospitalreview.com/care-coordination/how-hospitals-are-responding-to-the-water-crisis-in-mississippi.html. Accessed June 2023.
33. Public Statement - City of Jackson Water Impact on UMMC. 2022. https://www.umc.edu/news/News_Articles/2022/08/Jackson-Water-Imapct-UMMC.html. Accessed June 2023.
34. Vera A, Hanna J, Salahieh N. Jackson, Mississippi, mayor says he hopes water service can be restored this week, as residents endure lines for bottles. *CNN.* September 1, 2022. https://www.cbs58.com/news/jackson-mississippi-mayor-says-he-hopes-water-service-can-be-restored-this-week-as-residents-endure-lines-for-bottles. Accessed June 2023.
35. Reily R. 2010 water crisis sparked Jackson hospitals to take action. *Clarion Ledger.* https://www.clarionledger.com/story/news/2022/08/31/2010-water-crisis-sparked-jackson-hospitals-to-take-action/65466395007/. Accessed June 2023.
36. Haque U, Naeem A, Wang S, et al. The human toll and humanitarian crisis of the Russia-Ukraine war: the first 162 days. *BMJ Global Health.* 2022;7(9):e009550.
37. Abbara A, Zakieh O, Rayes D, et al. Weaponizing water as an instrument of war in Syria: impact on diarrheal disease in Idlib and Aleppo governorates, 2011–2019. *Int J Infect Dis.* 2021;108:202–208.
38. Vidal J. Water supplies in Syria deteriorating fast due to conflict, experts warn. *The Guardian.* September 7, 2016. https://www.theguardian.com/environment/2016/sep/07/water-supplies-in-syria-deteriorating-fast-due-to-conflict-experts-warn. Accessed June 2023.
39. Cimpanu C. CenturyLink outage takes down several 911 emergency services across the US. *ZDNET.* 2018. https://www.zdnet.com/article/centurylink-outage-takes-down-several-911-emergency-services-across-the-us/. Accessed March 18, 2023.
40. Goebel M, Dameff C, Tully J. Hacking 9-1-1: infrastructure vulnerabilities and attack vectors. *J Med Internet Res.* 2019;21(7):e14383.
41. Kelly JT, Campbell KL, Gong E, Scuffham P. The internet of things: impact and implications for health care delivery. *J Med Internet Res.* 2020;22(11):e20135.
42. Burgess M. The Unsolved Mystery Attack on Internet Cables in Paris. *Wired.* July 22, 2022. https://www.wired.com/story/france-paris-internet-cable-cuts-attack. Accessed June 2023.
43. Granholm F, Tin D, Ciottone GR. Not war, not terrorism, the impact of hybrid warfare on emergency medicine. *Am J Emerg Med.* 2022;62:96–100.
44. Holt TJ, Lee JR, Freilich JD, et al. An exploratory analysis of the characteristics of ideologically motivated cyberattacks. *Terrorism and Political Violence.* 2022;34(7):1305–1320.
45. Lis P, Mendel J. Cyberattacks on critical infrastructure: an economic perspective. *Econ Bus Rev.* 2019;5:24–47.
46. Hanuscak TL, Szeinbach SL, Seoane-Vazquez E, Reichert BJ, McCluskey CF. Evaluation of causes and frequency of medication errors during information technology downtime. *Am J Health Syst Pharm.* 2009;66(12):1119–1124.
47. Kirsch TD, Mitrani-Reiser J, Bissell R, et al. Impact on hospital functions following the 2010 Chilean earthquake. *Disaster Med Public Health Prep.* 2010;4(2):122–128.