CTED TRENDS REPORT

March 2017

PHYSICAL PROTECTION OF CRITICAL INFRASTRUCTURE AGAINST TERRORIST ATTACKS

CTED

UNITED NATIONS SECURITY COUNCIL
COUNTER-TERRORISM COMMITTEE
EXECUTIVE DIRECTORATE

1. INTRODUCTION

The present report is intended to bring to the attention of policymakers analytical perspectives on the above topic from academia and international and regional organizations. It was prepared in accordance with **Security Council resolutions 2341 (2017) and 2129 (2013). Security Council resolution 2129 (2013) requests CTED to identify emerging issues, trends and developments** relating to Council resolutions 1373 (2001) and 1624 (2005); to enhance its partnership with international, regional and subregional organizations, civil society, academia, and other entities in conducting research and information-gathering and in identifying good practices; and to support the Committee's efforts to promote implementation of resolutions 1373 (2001) and 1624 (2005).

CTED enhances its analytical capacity by **engaging with the global research community** and with research units of international, regional and subregional organizations on their assessment of current trends and challenges in terrorism and counter-terrorism, including developments on the ground, with the aim of supporting the Counter-Terrorism Committee's efforts to promote the implementation of the relevant Council resolutions. The present report is based on information gathered from partners in the **Committee's Global Counter-Terrorism Research Network** (see Research Network factsheet **here**[1]), as well as from other relevant academic sources, and does not constitute the Committee's or CTED's own assessment on protection of critical infrastructure. **The report is for informational purposes only and does not necessarily represent the views of the Committee or any of its members.**

2. BACKGROUND

Security Council Resolution 2341 (2017) directs the Committee, with the support of CTED, [...] to examine Member States' efforts to protect critical infrastructure from terrorist attacks as relevant to the implementation of resolution 1373 (2001) with the aim of identifying good practices, gaps and vulnerabilities in this field. The resolution also invites Member States to consider possible preventive measures in developing national strategies and policies.

In addition, paragraph 2 (b) of resolution 1373 (2001) calls on Member States to "[t]ake the necessary steps to **prevent the commission of terrorist acts,** including by provision of early warning to other States by exchange of information". Security Council Resolution 1566 (2004) calls on States to **prevent criminal acts, including against civilians, committed with the purpose of provoking a state of terror** in the general public or in a group of persons, intimidating a population, or compelling a Government or an international to do commit, or abstain from committing any act. The physical protection of critical infrastructure can prevent the commission of high-impact terrorist attacks. Moreover, the **immediate response to a terrorist attack against critical infrastructure** can prevent the "cascading" effects frequently associated with such attacks.

The Committee has held **two open briefings** on these matters: (i) an open briefing on **"Protection of Critical Infrastructure in Tourism",** held on 12 June 2014,[2] and (ii) an open briefing on **"Strengthening Emergency Responses in the Aftermath of Terrorist Incidents",** held on 16 June 2015.[3] On 21 November 2016, the Security Council held an **"Arria Formula" meeting on the "Protection of Critical Infrastructure against Terrorist Attacks",** initiated by the delegation of Ukraine, at which Member States presented their concerns and views on key aspects of this topic. The Counter-Terrorism Implementation Task Force (CTITF) has established a thematic Working Group on "Protection of Critical Infrastructure including Vulnerable Targets, Internet and Tourism Security".[4]

[1] https://www.un.org/sc/ctc/wp-content/uploads/2016/10/PARCFacts1.pdf

[2] UN Webcast of Committee Open Briefing "Protection of Critical Infrastructure in Tourism" https://s3.amazonaws.com/downloads2.unmultimedia.org/public/video/ondemand/1802658_Special%20CTC%20Mtg%20with%20Reps%20of%20Intl%20RegionalSubregional%20CTC-CTITF%20Joint%20Open%20Briefing%2011%20Jun%2014.mp4

[3] UN Webcast of CTC Open Briefing "Strengthening Emergency responses in the aftermath of terrorist incidents. 16 June 2015" http://webtv.un.org/watch/strengthening-emergency-responses-in-the-aftermath-of-terrorist-incidents-security-council-counter-terrorism-committee-ctc-open-briefing/4300495889001

[4] https://www.un.org/counterterrorism/ctitf/en/working-groups

3. WHAT IS CRITICAL INFRASTRUCTURE?

There is a need to strengthen efforts to improve security and protection of particularly vulnerable targets, such as infrastructure and public places, against terrorist attacks. Even though each State determines that which constitutes its critical infrastructure, Member States and academic experts have begun to identify a common understanding. Some authors (Schulman and Roe, 2006) define critical infrastructure as the "basic capabilities, technical systems and organizations which are responsible for the provision of assets". The European Commission defines critical infrastructure as an "asset or system which is essential for the maintenance of vital societal functions".[5] Critical infrastructure may include communications; emergency services; energy; dams; finance; food; public services; industry; health; transport; gas; public communications, radio and television; information technology; commercial facilities; chemical and nuclear sectors; and water. Many States increasingly depend on **infrastructure and assets that are partially or completely located outside their jurisdiction** and over which they have little or no control.[6]

Most critical infrastructure is owned by the private sector. IHS Janes (Srimoolanathan, 2014)[7] estimates that more than 80 per cent of the critical infrastructure of Western States is owned and operated by the private sector. Consequently - wherever the infrastructure is located - the State itself may no longer be able to ensure comprehensive security of critical infrastructure and may be largely dependent on the private sector for this purpose. A well-defined **public/private partnership is essential** for a policy on protection of critical infrastructure.[8]

Figure 1: Transmission towers.

There are a number of difficulties in determining which assets should be considered "critical". Because of the dense interconnections, networks, nodes, links and interdependencies between sectors — facilitated by cyberspace — it is often difficult to prioritize. Moreover, that which should be considered "critical" changes over time.[9] Decision-makers are often unwilling to assume the **political risk of removing items from a "critical list",** resulting in the waste of resources. Often, "critical lists" and priorities **mirror popular fears and political priorities** and do not accurately reflect risks and probabilities. This ambiguity hampers the development of security measures. Moreover, it is not always taken into consideration that **some major infrastructures are "self-healing"** (e.g., roads may continue to be functional even if the traffic lights go out). Determining which assets are critical often requires detailed judgement and calculation.[10]

States must therefore consider:

(i) the **relationship between the public and private sector,** on the one hand, and

(ii) **the importance of a particular area of critical infrastructure,** on the other.

[5] https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en

[6] "Cyber Security and Global Interdependence: What is Critical? Chatham House. February 2013. https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/0213pr_cyber.pdf

[7] IHS Janes "Adopting a holistic approach to Protecting Critical Infrastructure (ES14E3). June 2014. http://www.janes.com/article/39495/adopting-a-holistic-approach-to-protecting-critical-infrastructure-es14e3

[8] "Counter-Terrorism challenges regarding the process of critical infrastructure protection" Editors D Caleta, P Shemella, September 2011.

[9] "Cyber Security and Global Interdependence: What is Critical? Chatham House. February 2013. https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/0213pr_cyber.pdf

[10] Ibid.

Integrating these considerations into national and international security frameworks is a difficult task, which requires the **engagement of all participants concerned.**[11]

4. VULNERABILITY OF CRITICAL INFRASTRUCTURE TO TERRORISM

On 16 January 2013, heavily armed terrorists stormed the isolated Tiguentourine gas facility at In Amenas, Algeria, which lies deep in the Sahara desert. Thirty-eight hostages were killed during the four-day siege and ensuing rescue operation.[12]

Figure 2: Gas facility, Amenas, Algeria, 16 January 2013.

In general terms, physical protection of critical infrastructure usually leads to **target-hardening,** which is intended to make it harder for terrorists to strike against selected targets. A fundamental problem in this context is that **terrorists adapt their behaviour to changes in the security landscape.** In this respect, terrorist threats are fundamentally different from safety issues and there is a limit to the extent to which experience with safety policies can help make better security policies.[13] Target-hardening against terrorist attacks ideally should be **flexible and dynamic,** rather than attempt to build walls around selected targets. One way to increase policy flexibility is for regulations to **focus on security outcomes, leaving the process flexible.** According to the OECD Transportation Research Centre[14], however, current practices tend to be too descriptive: the authorities decide on the measures to be taken and the implementing agencies (which have the security expertise) are not given the flexibility to adapt. This leads to **rigidities in operational practices.**[15]

Critical infrastructure represents a vast, global sector. It is therefore not possible to ensure its full protection at all times and in all places. Unfortunately, **it is likely that some terrorist attacks against critical infrastructure will succeed.** A useful component of a comprehensive strategy to protect critical infrastructure is the capacity to minimize the impact of terrorist attacks thorough adaptation - **impact reduction, responses to emergencies, and recovery.** The physical protection of the target also involves **reduction of the impact in the event that the attack takes place.**[16]

[11] Ibid.

[12] http://www.middle-east-online.com/english/?id=63622

[13] Ibid.

[14] OECD Transportation Research Center, "Terrorism and International Transport: Towards risk-based security Policy" Round Table 144.

[15] Ibid.

[16] Ibid.

Terrorists aim to spread fear, anxiety and panic, creating the perception that every citizen and critical node in a country's infrastructure is vulnerable to attack. This was the case on 22 March 2016, when two teams of ISIL operatives conducted simultaneous attacks in Brussels, at Zaventem airport (killing 11 people) and at Maelbeek metro (killing 20 people), respectively. Around 300 people were injured.[17]

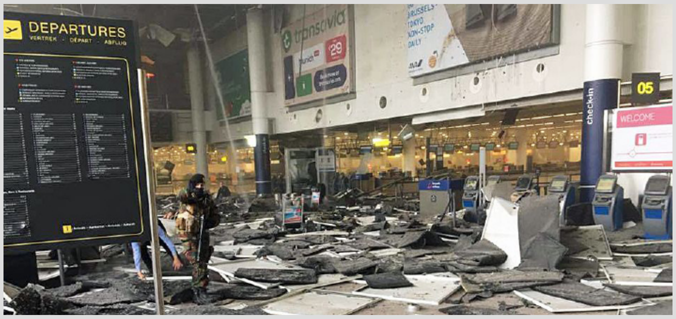


Figure 3: Zaventem airport, Brussels, Belgium, 22 March 2016.

In the following paragraphs, we shall consider the vulnerability of three types of critical infrastructure: (i) energy, (ii) transportation and (iii) water-supply, as well as the vulnerability of critical infrastructure to attacks committed by terrorists via the Internet.

4.1 Energy sector

The energy sector is extremely vulnerable because it has a significant impact on several other sectors of critical infrastructure within an economy. The global nature of the energy industry – and its impact on the global economy – demands that serious consideration be given to addressing its vulnerabilities.[18] The production and supply of energy resources relies on a complex system of infrastructures that are among the most critical in the world. They include pipelines, rigs, refineries, flow stations, manifolds, terminals, fuel cisterns, electrical energy pylons, pump stations, processing plants, vessels and tankers.[19]

Al-Qaida and its affiliates have attacked facilities and personnel of oil companies in Algeria, Iraq, Kuwait, Pakistan, Saudi Arabia and Yemen, and have also captured numerous oil fields. The UN estimates that the income generated by ISIL from oil and oil products in 2015 was between $400 million and $500 million.[20]

Even though some authors note that energy attracts only a small share of terrorist attacks, trends suggest a sharp rise terrorists' interest in oil and gas[21] (see figure 4).

As with terrorist attacks in general, attacks on energy (and mining-related) targets are geographically concentrated. According to START[22], from 2010-2014, Pakistan experienced almost as many attacks (439) as the next three States, Yemen (170), Colombia (161), and Iraq (146), combined. The Philippines, with 73 attacks, rounds out the top five.

[17] " New Trends in Terrorism's Targeting of the Business Sector" - Mackenzie Institute, September 2016 http://mackenzieinstitute.com/new-trends-in-terrorisms-targeting-of-the-business-sector/

[18] IHS Janes "Adopting a holistic approach to Protecting Critical Infrastructure (ES14E3). June 2014. http://www.janes.com/article/39495/adopting-a-holistic-approach-to-protecting-critical-infrastructure-es14e3

[19] UNISA. African Security Review, September 2015 "Terrorism, insurgency, kidnapping, and security in Africa's energy sector" http://www.tandfonline.com/doi/pdf/10.1080/10246029.2015.1072967?needAccess=true

[20] S/2016/92 Report of the SG on the threat posed by ISIL, January 2016 http://www.un.org/en/ga/search/view_doc.asp?symbol=S/2016/92

[21] "Risky Routes: Energy Transit in the Middle East" Brookings Doha Center Analysis, April 2016 https://www.brookings.edu/wp-content/uploads/2016/07/en-energy-transit-security-mills-2.pdf

[22] START Terrorism Trends with a Focus on Energy and Mining, June 2015 https://www.start.umd.edu/pubs/START_TerrorismEnergyAttacks_ResearchBrief_June2015.pdf

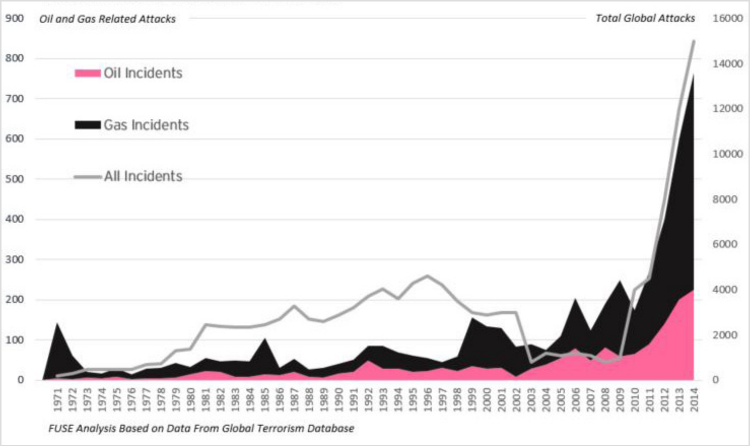


Figure 4: Global attacks on oil and gas infrastructure (source: Brookings).

The overwhelming majority of attacks on energy (and mining-related) targets during this time period (74 per cent) were bombings. Even though bombings were also the most common attack type for terrorist incidents during this time period, they accounted for a lower percentage (54 per cent) as compared with attacks on energy (and mining-related) targets. Facility and infrastructure attacks, which include arson and sabotage tactics, are the second most common type of attack against energy (and mining-related) targets. They are also more than twice as prevalent, accounting for 11 per cent of attacks, as compared with terrorist incidents in general (4.5 per cent).[23]

Country	# of attacks
Pakistan	439
Yemen	170
Colombia	161
Iraq	146
Philippines	73
India	42
Nigeria	38
Thailand	37
Turkey	28

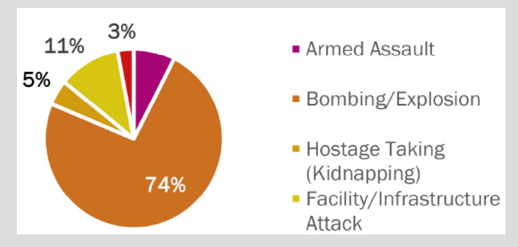


Figure 5: Types of attacks on energy and mining sectors worldwide 2010-2014 (source: START)

4.2 Vulnerability of critical water-supply infrastructure

On 22 November 2016, the Secretary-General informed the Security Council[24] that control of dams had often been a strategic terrorist goal, as in the case of operations carried out by ISIL. Stratfor (A Vishwanath, 2015),[25] noted that ISIL had used water as both a target and a weapon. ISIL has not only destroyed water-related infrastructure such as pipes, sanitation plants and bridges, it has also used water as an instrument of violence by deliberately flooding towns, polluting bodies of water, and ruining local economies by disrupting electricity generation and agriculture. According to Stratfor, between 2013 and 2015, ISIL launched around 20 major attacks (and countless smaller attacks) against Syrian and Iraqi water infrastructure – including flooding villages, threatening to flood Baghdad, closing the dam gates in Fallujah and Ramadi, cutting off water to Mosul, and allegedly poisoning water in small Syrian towns.

[23] Ibid.

[24] https://www.un.org/press/en/2016/sc12598.doc.htm

[25] "The Water Wars Waged by the Islamic State" November 2015. https://www.stratfor.com/weekly/water-wars-waged-islamic-state

The Istituto Affari Internazionali (Lossow, 2016) notes that, in this specific hydrological context, in which water is an immensely scarce resource, control over water infrastructure has been a central pillar of ISIL's expansion strategy. Lossow provides some concrete examples:

- In June 2014, ISIL blocked water pipes in the predominantly Christian town of Qaraqosh in Iraq, took over farms and agricultural land, and expelled most of the 50,000 residents.
- In the Shiite areas of Diyala province, water has been cut off a number of times.
- After seizing the large Iraqi dams at Falluja, Mosul, Samarra and Ramadi, ISIL interrupted local water supplies and also deliberately deprived distant Shiite areas in the lower reaches of the Euphrates and Tigris of water.
- Following the capture of the Ramadi Dam in May 2015, ISIL drastically reduced the water for the irrigation systems and treatment plants in the predominantly Shiite downstream provinces of Babil, Karbala, Najaf and Qadisiya, which are among Iraq's most important agricultural centres, thereby putting the food security of the entire country at risk.
- In April 2014, ISIL closed the Falluja Dam floodgates and diverted the water over an irrigation channel into a side valley, thereby inundating land up to 100 km away and placing the city of Abu Ghraib under up to four metres of water. Between Falluja and Abu Ghraib more than 10,000 houses, 200 square kilometres of fertile farmland, and almost the entire harvest were destroyed and the livestock killed. Up to 60,000 residents in the area lost their livelihood and were displaced by the flood. According to FATF,[26] by releasing water held by the Fallujah Dam, ISIL destroyed cropland 160 kilometres downstream, leaving millions of people without water in the cities of Karbala, Najaf and Babil.

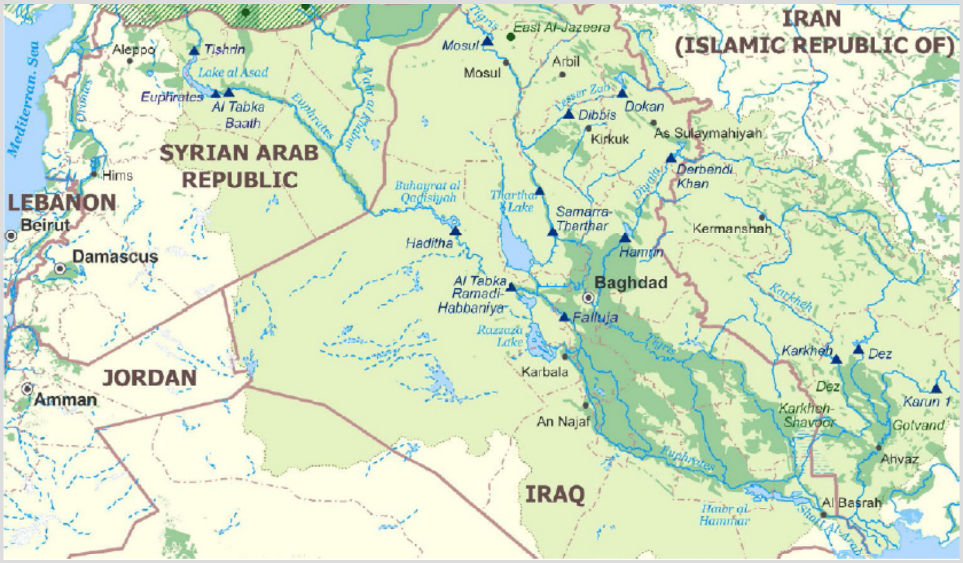


Figure 6: Dams on the Tigris and Euphrates in Syria and Iraq (source: Istituto Affari Internazionali).

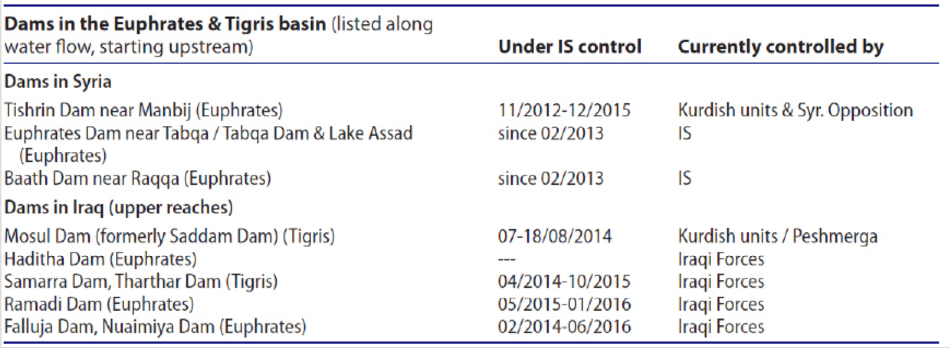
Contaminated water: Water can be used as a weapon to expel populations by soiling or poisoning water resources through the introduction of chemical or biological agents. However, this practice has not played a central role in Syria and Iraq and has mostly been applied at the local level. Lossow provides the following examples:

[26] http://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organisation-ISIL.pdf

- ISIL deliberately contaminated drinking water with crude oil in the Balad district of the Salahaddin Governorate in December 2014.
- Poisoned water supplies have also been reported from Aleppo, Deir ez Zor, Raqqa and Baghdad,
- A planned attack on the water supply in Pristina, Kosovo, which intended to contaminate the largest water reservoir uphill of the city – Gracanica Lake, also known as Badovac Lake – was prevented just before its execution.
- In one of its video messages, ISIL called on its followers to deploy the water weapon and poison the drinking water of its enemies wherever possible.

Figure 7: ISIL's propaganda regarding Mosul's dam.

Control of major water resources and dams gave ISIL control over the supplies used to support agriculture and electricity generation. According to Stratfor (A Vishwanath, 2015),[27]Mosul Dam, for example, gave ISIL control over 75 per cent of Iraq's electricity generation while it was in the group's possession.



Dams in the Euphrates & Tigris basin (listed along water flow, starting upstream)	**Under IS control**	**Currently controlled by**
Dams in Syria		
Tishrin Dam near Manbij (Euphrates)	11/2012-12/2015	Kurdish units & Syr. Opposition
Euphrates Dam near Tabqa / Tabqa Dam & Lake Assad (Euphrates)	since 02/2013	IS
Baath Dam near Raqqa (Euphrates)	since 02/2013	IS
Dams in Iraq (upper reaches)		
Mosul Dam (formerly Saddam Dam) (Tigris)	07-18/08/2014	Kurdish units / Peshmerga
Haditha Dam (Euphrates)	---	Iraqi Forces
Samarra Dam, Tharthar Dam (Tigris)	04/2014-10/2015	Iraqi Forces
Ramadi Dam (Euphrates)	05/2015-01/2016	Iraqi Forces
Falluja Dam, Nuaimiya Dam (Euphrates)	02/2014-06/2016	Iraqi Forces

Figure 8: Important dams under ISIL's control as of July 2016 (source: Istituto Affari Internazionali).

[27] "The Water Wars Waged by the Islamic State" November 2015. https://www.stratfor.com/weekly/water-wars-waged-islamic-state

ISIL's replication of the same strategy in North Africa. ISIL has established a similar strategy in North Africa to control key resources and use them as weapons against the populations and Governments that it seeks to coerce or destroy.

IHS Janes (country report December 2016)[28] provides some recent examples of attacks against critical water-supply infrastructure in Libya and a forecast of ISIL's future plans in this regard: in a December 2016 attack, around 60 ISIL militants raided the Great Man-made River (GMR) Project station in Ash Shawayrif, southwest of Sirte, which is a network of pipes and pumping stations that will supply water to the Libyan Sahara and the northern cities of Benghazi, Sirte, and Tripoli. This was the second attack against the GMR network in just one week.

According to IHS Janes, such attacks reflect the strategy that ISIL is likely to follow in the coming months: to target critical and strategic infrastructure located in scarcely populated areas, such as water and power stations, where the security presence is thin, while attempting to regroup, resupply, and continue to recruit.

4.3 Transportation sector

Transportation facilities and vehicles are attractive targets for terrorist attacks because of the high concentration of potential victims. They also offer the possibility of turning vehicles into weapons, with a potentially significant increase in victims (e.g., aeroplanes). The difficulty of protecting the many potential targets while maintaining smooth transport operations and the difficulty of determining the probability of attack also increase their appeal to terrorists.[29] In addition, open access to public transportation limits the scope of potential security improvements.

Not every attack on public transportation will amount to a threat to critical infrastructure. However, the table below provides a snapshot of the types of transportation most frequently targeted in terrorist attacks worldwide. The most frequent targets were buses and trains, which comprised 61.6 per cent of all transportation targets worldwide between 1970 and 2014.

According to START[30], airports represented 6.4 per cent of all transportation targets and subway systems made up 1.9 per cent of all transportation targets.

Critical transportation infrastructure is characterized by a strong linkage between public and private organizations. The transportation sector is especially complex because public/private partnerships are not just bilateral in nature, but rather a complex system of partnerships between a number of public and private institutions.

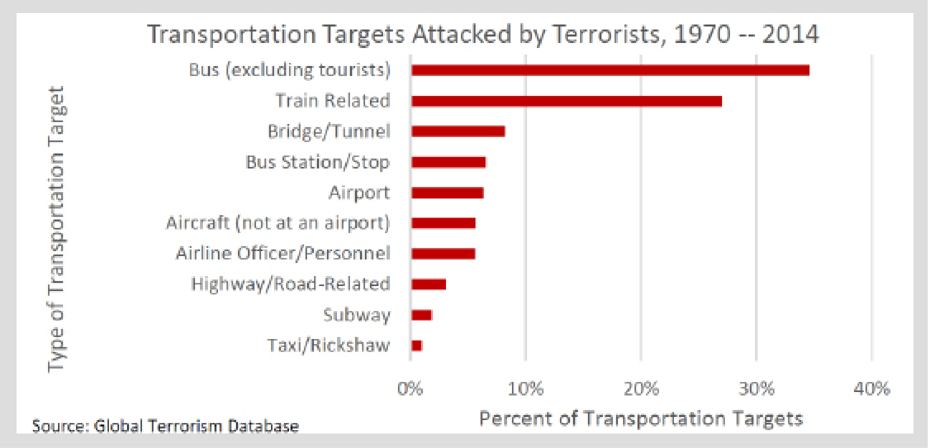


Figure 9: Transport infrastructure attacked by terrorists between 1970-2014.

[28] http://janes.ihs.com/Janes/Display/1792151

[29] Ibid.

[30] START "Terrorism in Belgium and Western Europe; Attacks against Transportation targets; Coordinated Terrorist Attacks". March 2016. https://www.start.umd.edu/pubs/START_BelgiumTransportationCoordinatedAttacks_BackgroundReport_March2016.pdf

Moreover, it is expected that the complexity of critical transport infrastructure will increase over time, as new communications networks are included in the overall transportation network. **Mistrust, unaligned goals, diverging strategies, unfair risk accumulation on few partners or inefficient distributionof responsibilities** can result in failure of the public/private partnership.[31]

4.4. Vulnerability of critical infrastructure to terrorist attacks committed through the internet

Research indicates that terrorist organizations do see attacks against critical infrastructure through the Internet as a preferred modus operandi. The Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security" noted in a report of July 2015[32] that **the use of ICT for terrorist purposes, beyond recruitment, financing, training and incitement, including for terrorist attacks against ICTs or ICT-dependent infrastructure, is an increasing possibility which, if left unaddressed, may threaten international peace and security.**

The following are some key conclusions drawn by leading research institutions relating to the vulnerabilities of critical infrastructure to terrorist attacks committed through the Internet, as defined in section 2 of this report:

- Critical infrastructure is vulnerable to all type of attacks and increasingly to attacks committed through the Internet.[33]
- It is increasingly clear that nothing online is safe.[34]
- ISIL intentionally misrepresents its online capabilities in its propaganda and is probably not capable of carrying out spectacular attacks through the Internet, such as targeting critical infrastructure. However, ISIL actively seeks to recruit individuals capable of carrying out attacks through the Internet and is likely to be able to do so.[35]
- There is growing concern that terrorist groups may eventually develop the capacities to use the Internet and broader cyberspace to conduct disruptive and destructive attacks against critical infrastructure, with the potential to cause significant harm.[36]
- The capacity to carry out attacks through the Internet need not necessarily come from within ISIL. The availability of cybercrime tools and services on underground criminal markets is likely to allow ISIL and other terrorist organizations to further bolster their existing abilities.[37]

[31] "Critical Infrastructure: Making it Private or Public – An Institutional Economic Discussion on the Example of Transport Infrastructure". I Geis, W Schulz, April 2015.

[32] A/70/174 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. July 2015. http://www.un.org/en/ga/search/view_doc.asp?symbol=A/70/174

[33] World Economic Forum. White Paper. "Global Agenda Council on Cybersecurity" April 2016. http://www3.weforum.org/docs/GAC16_Cybersecurity_WhitePaper_.pdf

[34] Ibid.

[35] STRATFOR "The Coming Age of Cyberterrorism" October 2015. https://www.stratfor.com/weekly/coming-age-cyberterrorism

[36] ICT4PEACE Foundation "Private Sector Engagement in Responding to the Use of the Internet and ICT for Terrorist Purposes" http://ict4peace.org/wp-content/uploads/2016/12/Private-Sector-Engagement-in-Responding-to-the-Use-of-the-Internet-and-ICT-for-Terrorist-Purposes-2.pdf .

[37] STRATFOR "The Coming Age of Cyberterrorism" October 2015. https://www.stratfor.com/weekly/coming-age-cyberterrorism

- ISIL seeks to recruit skilled individuals capable of carrying out complex attacks through the Internet.[38]
- The growth of ICT black markets opens the space to “hackers-for-hire”.[39]
- The expected growth of billions of Internet-enabled devices (industrial “Internet of Things” (IoT)) will bring significant security challenges, including the use of IoT by terrorists to commit attacks against critical infrastructure.[40]
- Cloud computing and encryption enhance the complexity of the challenge.[41]

In this context, the protection of critical infrastructure against attacks through the Internet, in general —– which includes potential terrorist attacks — currently faces complex challenges, which are notably highlighted in the **World Economic Forum’s “White Paper – Global Agenda Council on Cybersecurity”[42]:**

1. **International fragmentation:** differences in approach to cybersecurity, data jurisdiction and legal enforcement (as well as culture, language and politics) across jurisdictional and territorial boundaries can make it difficult to effectively prevent, investigate and prosecute attacks committed through the Internet;
2. **International norm-setting:** international political differences and country-specific agendas can make it difficult to develop consensus norms regarding cybersecurity;
3. **Roles with respect to the private sector:** the varying and sometimes confrontational roles that the public sector must play can create tensions and trust deficits with the private sector;
4. **Misalignment of incentives for cybersecurity best practices:** Companies often fail to take basic steps to protect their systems and their users because they are placed in the difficult position of balancing the market pressures of rapid innovation against sustained investments in cybersecurity, which may raise costs or delay delivery of products to market;
5. **Ecosystem complexities:** Today’s software and hardware environments are increasingly complex ecosystems populated by a network of interacting devices, networks, people and organizations. This means that cybersecurity solutions often require the voluntary engagement, cooperation and investment of many independent entities, even though the incentives and mechanisms for taking such actions are distributed inconsistently across the ecosystem.

Although there is no “quick fix”, the White Paper identifies steps that organizations can take to begin to address cybersecurity challenges: (i) adopting best practices and cyber hygiene; (ii) improving authentication systems; and (ii) preparing for attacks (e.g.: by enhancing forensic capabilities, developing business continuity plans).

[38] Ibid.

[39] STRATFOR "Examining the Islamic State’s Cyber Capabilities" November 2015. https://www.stratfor.com/analysis/examining-islamic-states-cyber-capabilities

[40] World Economic Forum. "Network Name ; "Industrial IoT." https://www.weforum.org/events/world-economic-forum-annual-meeting-2016/sessions/the-internet-of-things-is-here/

[41] Council of Europe. Octopus Conference 2016 "Cooperation against Cybercrime. Key messages". https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806be360

[42] http://www3.weforum.org/docs/GAC16_Cybersecurity_WhitePaper_.pdf

5. PREVENTION, PREPAREDNESS, MITIGATION, INVESTIGATION, RESPONSE AND RECOVERY

The physical protection of critical infrastructure is a complex process that needs to encompass the entire cycle of a possible terrorist attack. It requires cooperation domestically and across borders. The physical protection of critical infrastructure can **prevent** the commission of high-impact terrorist attacks. Inevitably, some terrorist plots will succeed. The **immediate response** may prevent the “cascading” effects that such attacks frequently entail, including further victims.[43]

5.1. Security Council resolution 2341 (2017), on the protection of critical infrastructure against terrorist attacks

On 13 February 2017, the Security Council adopted resolution 2341 (2017), which calls on Member States to explore ways to assess vulnerabilities, interdependencies and capabilities of, as well as the cascading effects of, the impacts of terrorist attacks on their critical infrastructure.

The resolution notably:

“**Encourages** all States to make concerted and coordinated efforts, including through international cooperation, to raise awareness, to expand knowledge and understanding of the challenges posed by terrorist attacks, in order to improve preparedness for such attacks against critical infrastructure;

Calls upon Member States to consider developing or further improving their strategies for reducing risks to critical infrastructure from terrorist attacks, which should include, inter alia, assessing and raising awareness of the relevant risks, taking preparedness measures, including effective responses to such attacks, as well as promoting better interoperability in security and consequence management, and facilitating effective interaction of all stakeholders involved;

Calls upon Member States to explore ways to exchange relevant information and to cooperate actively in the prevention, protection, mitigation, preparedness, investigation, response to or recovery from terrorist attacks planned or committed against critical infrastructure;

Further calls upon States to establish or strengthen national, regional and international partnerships with stakeholders, both public and private, as appropriate, to share information and experience in order to prevent, protect, mitigate, investigate, respond to and recover from damage from terrorist attacks on critical infrastructure facilities, including through joint training, and use or establishment of relevant communication or emergency warning networks;

Encourages the United Nations as well as those Member States and relevant regional and international organizations that have developed respective strategies to deal with protection of critical infrastructure to work with all States and relevant international, regional and subregional organizations and entities to identify and share good practices and measures to manage the risk of terrorist attacks on critical infrastructure;

The resolution also:

“**Directs** the CTC, with the support of the Counter-Terrorism Executive Directorate (CTED) to continue as appropriate, within their respective mandates, to examine Member States efforts to protect critical infrastructure from terrorist attacks as relevant to the implementation of resolution 1373 (2001) with the aim of identifying good practices, gaps and vulnerabilities in this field;

[43] OECD Transportation Research Center, “Terrorism and International Transport: Towards risk-based security Policy” Round Table 144.

Encourages in this regard the CTC, with the support of CTED, as well as the CTITF to continue working together to facilitate technical assistance and capacity building and to raise awareness in the field of protection of critical infrastructure from terrorist attacks, in particular by strengthening its dialogue with States and relevant international, regional and subregional organizations and working closely, including by sharing information, with relevant bilateral and multilateral technical assistance providers."

The following practices adopted by Member States describe the main areas and players that can be involved in the process of physically protecting critical infrastructure (PCI):

5.2. Prevention and preparedness

- Because a terrorist attack against critical infrastructure is likely to have implications beyond national borders, regional and international perspectives need to be integrated.
- In order to ensure better preparedness and response, an international network of "PCI focal points" can be appointed by Member States and relevant international, regional and subregional organizations. Policy guidance containing operational aspects, including early-warning systems and information-sharing, could also be developed.
- It can be beneficial for PCI focal points to partner with the private sector, as appropriate.
- Prevention elements. These elements can be considered in partnership by a "PCI focal points network" and in consultation with the private sector, civil society and academia, with the aim of facilitating effective interaction of all stakeholders:
  1. Cross-sectoral risk assessment, including vulnerabilities, interdependencies, capabilities, and cascading effects of impacts on critical infrastructure.
  2. Alert level and prioritizing.
  3. Emergency operation plans tailored to each critical infrastructure sector (e.g., public transportation, water supply, energy, banking and finance, telecommunications).
- Some States undertake stocktaking exercises to:
  1. Determine existing means and capabilities.
  2. Centrally compile and store this information.
  3. Compare existing capabilities against identified requirements.
  4. Outcome of comparison = areas for improvement.
- Some States appoint PCI specialized intelligence units within the police for:
  1. Collection and processing of information.
  2. Ongoing identification of vulnerable critical infrastructure (e.g. access control and identity verification screening search and detection; cyber security; supply chain integrity and security).
  3. Identifying and assessing terrorist threats to critical infrastructure; detecting terrorists' operational planning, including their financial, logistical, and training support networks.
  4. Proactively warning the appropriate national and international authorities of terrorist risks, threats, and actual plots.

5.3. Mitigation and emergency response plans

- Emergency response plans can include the actions necessary to address the short-term, direct effects of an attack against critical infrastructure.

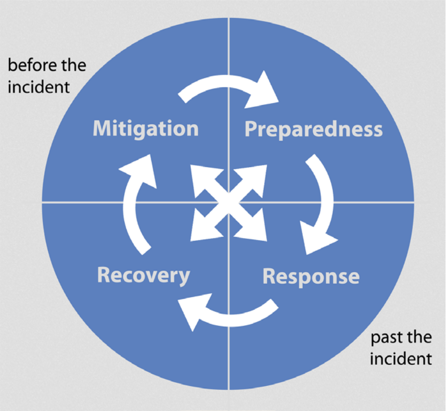
- The response plan can also include the execution of plans prepared in the prevention phase.
- A "crisis-management plan" can also be developed. If effectively designed, it can reduce the effects of an incident; assist in the rescuing of victims; prevent further casualties; restore public order; protect the crime scene; identify the cause of damage or the source of the attack; preserve evidence of an attack; and help bring perpetrators to justice. The response needs to be multidisciplinary, involve both public and private sectors, and be aimed at (i) protecting the civilian population; and (i) ensuring continuity of business.
- A PCI specialized law enforcement attack-response structure can include:
  1. International/regional crisis command.
  2. National crisis command centre.
  3. Intelligence and information-gathering.
  4. Unit for the verification of evidence, witness accounts, and intelligence.
  5. Forensic police investigation unit.
  6. Victims unit.
  7. Witnesses unit.
  8. Hearing, questioning and search unit.
  9. Immunization, isolation or quarantine unit.
- Policy arrangements for military assistance in crisis management can also be considered.
- National and international tests of response systems through real-life exercises can also increase the effectiveness of the response.

Preparing for an attack while including a recovery plan can mitigate its consequences; improve security and resilience of critical infrastructure; and minimize impacts and recovery time.

5.4. Recovery

The recovery phase can include the development, coordination, and execution of "service and site-restoration plans". These plans include the reconstitution of Government operations and services, as well as different assistance programmes to address targeted needs (e.g., to provide housing). Restoration can be effected through public assistance programmes, as well as through private-sector, non-governmental programmes.

Some key elements to consider in the "service and site restoration plans" include the long-term care and treatment of affected persons; additional measures for social, political, environmental, and economic restoration; evaluation of the incident to identify lessons learned; post incident reporting; and development of initiatives to mitigate the effects of future incidents.



6. INTERNATIONAL EFFORTS TO PROTECT CRITICAL INFRASTRUCTURE

The following are examples of current international efforts to protect critical infrastructure, including from terrorist threats:

- European Union. “European Programme for Critical Infrastructure Protection”[44]
- Inter-American Committee Against Terrorism of the Organization of American States (OAS/CICTE), “Protection of Critical Infrastructure against Emerging Threats”[45] and “Tourism Security Programme”.[46]
- NATO “Energy Security”[47] and “Civil Emergency Planning”[48]
- INTERPOL Major Event Support Teams (IMEST)[49]
- INTERPOL Incident Response Teams (IRT)[50]
- OSCE “Non-Nuclear Critical Energy Infrastructure Protection from Terrorist Attacks” [51]
- Regional Cooperation Council “Integrated Infrastructure Planning”[52]
- UN General Assembly Resolution A/RES/58/199 on “Creation of a global culture of cybersecurity and the protection of critical information infrastructures”.[53]
- UN Counter-Terrorism Implementation Task Force (CTITF) Working Group on PCI[54]
- Council of Europe, Budapest Convention and Related Standards[55]
- Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security[56]
- Information Sharing and Analysis Center (ISAC)[57]

[44] https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en

[45] https://www.sites.oas.org/cyber/Documents/CICTE%20DOC%201%20DECLARATION%20CICTE00955E04.pdf

[46] http://www.oas.org/en/sms/cicte/programs_tourism.asp

[47] http://www.nato.int/docu/review/2011/climate-action/energy_security/EN/index.htm

[48] http://www.nato.int/cps/en/natohq/topics_50093.htm

[49] https://www.interpol.int/INTERPOL-expertise/Response-teams/Major-Events-Support-Teams

[50] https://www.interpol.int/INTERPOL-expertise/Response-teams/Incident-Response-Teams

[51] http://www.osce.org/secretariat/103954?download=true

[52] http://www.rcc.int/articles/27/integrated-infrastructure-planning-by-miroslav-kukobat-head-of-infrastructure-and-energy-unit-regional-cooperation-council-secretariat#!prettyPhoto

[53] http://www.un.org/en/ga/search/view_doc.asp?symbol=a/res/58/199

[54] https://www.un.org/counterterrorism/ctitf/en/protection-critical-infrastructure-including-vulnerable-targets-internet-and-tourism-security

[55] https://www.coe.int/en/web/cybercrime/the-budapest-convention

[56] http://www.un.org/en/ga/search/view_doc.asp?symbol=A/70/174

[57] http://www.nationalisacs.org/