Chapter 28

Prevention of Terrorist Attacks on Critical Infrastructure

Anneli Botha

Targeting critical infrastructure is an attempt to destabilize the social and economic functioning of the state and, therefore, will remain an extremely important concern for those tasked with prevention of terrorist attacks. The number of incidents grew substantially as a comparison of attacks between the periods 2000-2009 and 2010-2017 shows. While the threat of cyber-attacks against critical infrastructure is gaining momentum, the use of firearms and explosives still remains the preferred *modus operandi*. As a result, the protection of critical infrastructure had been an important component of governments' counterterrorism strategies in focusing on both traditional tactics and, more critically, on new technological advances such as the growing threat presented by Unmanned Aerial Vehicles (UAVs). Developing successful counter- and preventative measures starts with understanding the "enemy," specifically the objectives, the political message, and capabilities of terrorist organizations. It also requires continuous risk, threat, and vulnerability assessments to plan and implement steps for anticipating and preventing infrastructure attacks.

Keywords: critical infrastructure protection, key resources, key assets, risk assessment, threat assessments, vulnerability assessments

Recognizing the multitude of targets of attacks against critical infrastructure – from individual hackers to hostile countries in cyberspace – one should not disregard physical attacks or a combination of cyber and physical attacks. These could be facilitated through a multitude of tactics from complex attacks involving the use of explosives (predominantly improvised explosive devices or IEDs) in combination with active shooters, hostage-takings, or the use of unmanned aerial vehicles (or UAVs). While the majority of the recent literature focuses predominantly on cyber rather than on "old school" physical attacks against critical infrastructure, this chapter will only focus on physical threats after first establishing what the concept "critical infrastructure" includes. This is followed by a discussion of the importance of threat, risk, and vulnerability assessments. A section on the manifestation of previous threats and incidents through utilizing the National Consortium for the Study of Terrorism and Responses to Terrorism's (START) Global Terrorism Database (GTD) developed by the University of Maryland will introduce trends, weaknesses, and mitigating measures to be considered.

Working through earlier attacks, one is again reminded of the complex interconnected nature of infrastructure in that an attack on one service can have a direct impact on another. Energy, especially electricity, is the most critical sector, considering that none of the other sectors will be able to function without power. Although (so far) not caused by acts of terrorism, one only needs to consider the impact power outages have on the functioning of other sectors, e.g. the distribution of water, communication (especially internet connection), and fuel for power plants or reactors, whether delivered by road, rail, ship, or pipeline. Moreover, the vast and often long-distance distribution of critical infrastructure networks, for example the distance covered by oil pipelines, bridges, dams, and mobile phone towers further add strain to efforts to protect these facilities. Placing the entirety of critical infrastructure of a country on the table will create the impression of being impossible to protect, considering the resources and manpower required. However, an analysis of previous failed and successful attacks will come in handy while constantly conducting threat, risk, and vulnerability assessments on all levels – country, industry, and facility – while also keeping the unpredictability of terrorists in mind. As a result of this unpredictability of the attacker, any analysis needs to identify the "enemy" as far as possible, assessing their motivations, size, targets, and earlier *modi operandi*. The ultimate objective is to plan for the most probable contingencies, while not losing sight of less probable, but high impact, incidents.

This chapter will focus on the concept "critical infrastructure," the manifestation of attacks directed against critical infrastructure – most notably transportation, utilities, and telecommunications – and how the state and private sector can respond to these ever-changing threats. While a country's communication network, in particular cyber network, is part of critical infrastructure, cyber security is addressed in chapter 29 of this handbook.

Terminology

Determining what "critical infrastructure" should consist of, is almost as difficult as finding a broadly acceptable definition for "terrorism," considering the implications of including and excluding some services and industries.

The US Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience, identified 16 critical infrastructure sectors whose "assets, systems, and networks, whether physical or virtual, are considered so vital to the country that their incapacitation or

DOI: 10.19165/2020.6.0128

destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[1] These include:

1. Energy (e.g., oil, gas, wind turbines, solar farms) that is needed in the production of electricity, its storage and distribution. Nuclear reactors and waste management.
2. Transportation to include all possible forms of transportation from road, rail, air (airplanes and airports, as well as air traffic), sea, and inland waterway transport. Considering that these networks extend beyond the country's borders this section will also make provision for border security and surveillance.
3. Information systems that include, for example, the internet (the system and protecting the physical network as well as mobile and fixed telecommunication and satellites, also needed for navigation).
4. Communication sector that includes broadcasting through television and radio.
5. Water and wastewater systems (sewerage farms) that include dams, and monitoring and maintaining the provision of purified water.
6. Food and agriculture aimed at the production and delivery of food suitable for human consumption.
7. Chemical industries that require caution and management in the production and storage of dangerous substances.
8. Healthcare and public health.
9. Emergency services.
10. Financial services with reference to banking and payment services.
11. Critical manufacturing.
12. Commercial facilities that draw large crowds of people for shopping, business, entertainment, or lodging.
13. National monuments that are important in representing a country's national identity as well as religious institutions with references to churches, mosques, and synagogues. Symbolism in attacking these facilities and the emotional reaction following an attack make it a favorable target in hate crimes (targeting only the facility) to severe incidents of hate crimes and acts of terrorism.
14. Government facilities.
15. Defense sector that enables research, development, design, production, delivery, and maintenance of military weapons systems, subsystems and components or parts.

According to John Moteff, Claudia Copeland, and John Fischer,[2] critical infrastructures also include national monuments "where an attack might cause a large loss of life or adversely affect the nation's morale." Attacks against critical infrastructure and monuments are also clearly incorporated in the African Union's definition of a "terrorist act" as presented in Article 1 (3) of the 1999 Organization of African Unity (OAU) Convention on the Prevention and Combating of Terrorism:

(a) "any act which is a violation of the criminal laws of a State Party and which may endanger the life, physical integrity or freedom of, or cause serious injury or death to, any person, any number or group of persons or causes or may cause

[1] US Department of Homeland Security. Critical Infrastructure Sectors. 2019. Available at: https://www.dhs.gov/cisa/critical-infrastructure-sectors .

[2] Moteff, J., Copeland, C. and Fischer, J. *Critical Infrastructures: What Makes an Infrastructure Critical?* Washington, DC: Congressional Research Service, 2003, p. 8.

DOI: 10.19165/2020.6.0128

damage to public or private property, natural resources, environmental or cultural heritage and is calculated or intended to:

(i) intimidate, put fear into, force, coerce or induce a government, body, institution, the general public or a segment thereof, to do or abstain from doing any act, or to adopt or abandon a particular standpoint, or act according to certain principles; or
(ii) disrupt any public service, the delivery of an essential service to the public, or to create a public emergency; or
(iii) create general insurrection in a State."[3]

While this definition also captures some of the main objectives of terrorism, the possibility exists that what is regarded today as critical by governments, might not be regarded as such by tomorrow's terrorists. The focus might shift from merely physical attacks towards more attacks on critical infrastructure in cyberspace, which would require different countermeasures While terrorist organizations, such as the Islamic State in Iraq and Syria (ISIS) and Al-Qaeda became more active in cyberspace in recent years, and might soon be able to cause substantial damage in new ways, the predominant terrorist inclination still is to rely on physical tangible tactics, at least till cyber-attacks become physically visible. Considering the technical skills required to launch major attacks in cyberspace, it is likely that, in the near future, most terrorists will make use of explosives, firearms, and knives to carry out their next attack.

Determine the Nature of the Threat

The debate around what should be included when referring to "critical infrastructure" is often influenced by cost implications (i.e. costs of resorting an infrastructure object) if and when a building, network, or service is categorized as such. The level of security associated with the protection of above will be influenced by the level of threat (likelihood of becoming a target) and the classification of countermeasures put in place to address potential threats. The former will require risk, threat, and vulnerability assessments.

According to John Ellis,[4] risk assessment "is a concept developed in many settings to analyze the possibilities or probabilities of future events and circumstances, and then forecast the impact this would have on the organization conducting the assessment and on its goals." Risk assessments, however, often only provide a snapshot of the vulnerabilities in what is an ever-changing environment. Good forecasts should be based on the history of threats and incidents, given that there usually is a high probability that history will repeat itself at some point in time. Forecasting will also require a careful consideration of existing circumstances and indicators that will determine the probability of certain outcomes.[5] Ideally, risk assessments should be regularly undertaken to deal with changing trends and capabilities of security forces. This way both current and future threats can be monitored and addressed accordingly.

[3] Italics added by author. African Union, *OAU Convention on the Prevention and Combating of Terrorism*, 1999, Available at: https://au.int/sites/default/files/treaties/7779-treaty-0020_-_oau_convention_on_the_prevention_and_combating_of_terrorism_e.pdf
[4] Ellis, J.W., *Police Analysis and Planning for Vehicular Bombings: Prevention, Defense and Response*, Springfield: Charles C Thomas Publisher, Ltd., 1999, p. 74.
[5] Howell, L.D., *The Handbook of Country and Political Risk Analysis*, New York: The Political Risk Services Group, 1998, p. 9.

DOI: 10.19165/2020.6.0128

Terrorism-related risk analysis has been defined by Hunsicker as:[6]

> "a survey to ascertain how high the probability is of one of these dangers occurring, how well the organization can respond should the threat become a reality, and how well the organization can carry on once that reality materializes. Inherent in the analysis is the identification of the vulnerabilities and threats that go along with the risk. In the course of the analysis, one of the things to be determined is the extent of the organization's exposure, which could materially contribute to loss or damage in the event of a terrorist attack."

Considering that not every sector or facility can receive the same level of protection, the level of risk needs to be calculated. The first step is to determine the value of each asset (e.g., human beings, facilities, services, processes and programs). The second step is to determine what the impact would be if the asset is damaged or destroyed. Based on such calculations the standard classification system will express risk on a five-point scale as: i) very low, ii) low, iii) moderate, iv) high, or v) extremely high.[7] According to Moteff and Parfomak, the value of an asset can also be expressed "in monetary terms in what it will cost to replace an asset from the cost to build the asset, the cost to obtain a temporary replacement for the asset, the permanent replacement cost for the asset, costs associated with the loss of revenue, an assigned cost for the loss of human life or degradation of environmental resources, costs to public/stakeholder relations, legal and liability costs, and the costs of increased regulatory oversight."[8]

The US Department of Defense focuses on the following four critical components to evaluate and prioritize the protection of its assets:[9]

1. Criticality: how essential is the asset?
2. Vulnerability: how susceptible is the asset to surveillance or attack?
3. The ability to reconstitute: how hard will it be to recover from inflicted damage?
4. Threat: how probable is an attack on this asset?

It is important to factor probabilities into the broader threat and vulnerability assessments.

Threat assessments are originated from, and are primarily used by, security forces when they have to decide on the best strategy to address (e.g., a specific threat to national security). In essence, a *threat analysis* is based on the need to identify, prioritize, and monitor the most hazardous threats to human safety and security. In conducting a threat assessment on terrorist activities within a specific region, certain information is required to build a profile that will be used to assess the *level* of threat and the most appropriate counteraction. This information needs to include, for example, the existence of groups that currently or previously resorted to violence and other acts of terrorism in a specific country. This will have a direct bearing on the risk portion and on the validity of the vulnerability analysis. In other words, an important

[6] Hunsicker, A. *Understanding International Counter Terrorism: A Professional's Guide to the Operational Art.* Universal Publishers: Boca Raton, 2006, p. 86.
[7] Kassa, S.G., 'IT Asset Valuation, Risk Assessment and Control Implementation Model', *ISACA Journal*, Vol 3, 1 May 2017. Available at: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/it-asset-valuation-risk-assessment-and-control-implementation-model
[8] Moteff, J., and Parfomak, P., *Critical Infrastructure and Key Assets: Definition and Identification*, Washington, DC: Congressional Research Service, 2004, p. 12.
[9] Brown G., Carlyle M, Salmerón J., Wood K. 'Defending Critical Infrastructure', *Interfaces*, Vol 36, No 6, 2006, p. 531.

DOI: 10.19165/2020.6.0128

relationship exists between threat and vulnerability that requires constant re-evaluation. Although an existing threat profile might form the foundation of this assessment, other factors also need to be taken into consideration. For example, with reference to critical infrastructure, the profile of the facility or establishment, and the type of shops and events hosted in shopping centers (e.g., live events might include celebrities or prominent officials that most often receive media coverage), need to be taken into consideration. Vulnerability assessments determine whether a specific country or institution might be vulnerable to terrorism or other risks. Therefore, risk and threat assessments serve as a foundation for vulnerability assessments.[10]

Before embarking on a threat analysis, the first question to be asked, is: "For what purpose?" The answer will determine the model and the specific categories used to conduct the assessment. It is again necessary to stress the importance of realizing that although risk, vulnerability, and threat assessments may fall under pre-determined categories, decisions will be determined by the aim and objective of the assessment. Within risk assessment and vulnerability analysis the focus is to determine *what* you are facing and *how* it will affect you. For government security forces the aim will be to prevent or deter the risk (proactive), defend (pro- and re-active), and respond or use the best strategy to manage the actual risk when it occurs (re-active).[11]

Essentially, the vulnerability analysis focuses on the identification of all factors, including safety and security hazards that leave people or critical infrastructures vulnerable to attacks. As a consequence, the aim of a vulnerability assessment is broader than a risk or threat analysis. Accordingly, the aim is not only to identify potential threats, but also to understand their likelihood of occurring. The goal therefore is twofold.

Firstly, the aim is to identify threats - in this case terrorism - based on feasibility and indicators of potential exploitation. For example, the existing presence of a known terrorist organization operating or intelligence on the presence of individuals suspected to be involved in decentralized networks.[12] Al-Shabaab in Eastern Africa is an example of the former that were previously implicated in numerous attacks on above classification of critical infrastructure, namely prominent shopping centers (for example the Westgate shopping mall attack on 21 September 2013[13] and the DusitD2 complex attack on 16 January 2019)[14] and Kenya's mobile communication network in the Northeast region close to the border with Somalia. This type of threat manifests in countries the closest to conflict areas, for example Somalia where attacks are being planned and executed from both Somalia (origin) and/or Kenya (extension).

Another factor that will increase vulnerability is the manifestation and extent of domestic marginalization on the basis of religion and/or ethnicity (often associated with a decreasing national identity) that the organization can exploit. These threats are further categorized by the likelihood that vulnerabilities will be exploited. In the case of Kenya, the presence of its defense

[10] Renfroe, N.A., and Smith, J.L., *Threat / Vulnerability Assessments and Risk Analysis*, Whole Building Design Guide, 2016. Available at: https://www.wbdg.org/resources/threat-vulnerability-assessments-and-risk-analysis
[11] Jones, S., Proactive vs Reactive Risk Management Strategies, *Reciprocity*, 20 February 2020. Available at: https://reciprocitylabs.com/proactive-vs-reactive-risk-management-strategies/
[12] Zio, E., 'Critical infrastructures vulnerability and risk analysis', *European Journal for Security Research*, Vol 1(2), 2016, 97-114.
[13] Howden, D., 'Terror in Nairobi: the full story behind al-Shabaab's mall attack', *The Guardian*, 3 October 2012. Available at: https://www.theguardian.com/world/2013/oct/04/westgate-mall-attacks-kenya
[14] *Agence France-Presse*, 'Terrorists attack Dusit hotel in Nairobi, Bangkok Post', 16 January 2019. Available at: https://www.bangkokpost.com/world/1611674/terrorists-attack-dusit-hotel-in-nairobi

DOI: 10.19165/2020.6.0128

force in Somalia as part of the African Union Mission to Somalia (AMISOM) increased the likelihood of attacks in Kenya. This category is directly linked to the motivation or what attackers hope to achieve. For example, in the case of Kenya, the aim was to intimidate the country through attacks on its population so as to pressure Kenyan armed forces to withdraw from Somalia. However, attacks can also facilitate the future operation of the organization. For example, destroying telephone masts (sabotage) prevents the public from reporting the local presence of al-Shabaab fighters to authorities. Through isolating these often-remote areas, the organization enhances its presence in the country and weakens the Kenyan state by showing the immediate community - but also the broader country - that government is unable to maintain control over its territory and cannot protect its citizens from external threats or from threats emerging from refugee camps and illegal immigrants. Although the presence of illegal immigrants is not an immediate threat per se, limitations associated with the legal status can increase future vulnerability as these individuals will be exploited, while not enjoying the same benefits as citizens. Most critical for assessments is the identification of infrastructure lacking effective security measures.

The second aim of a vulnerability assessment is to provide an informed assessment based on detecting, monitoring and predicting potential threats. As a multivariate analysis, the aim of a vulnerability assessment would be to predict future trends on the basis of current and historical information; and describe and understand the underlying relationship within a country that could ultimately determine the vulnerability of a country to instability and terrorism.

Attraction of Launching Attacks against Critical Infrastructure

Determining the potential threat, risk, and vulnerability is the first step in establishing the value and need to protect a particular asset, from the perspective of those launching an attack as it is important to determine the value of attacking that particular target. In this regard the motive behind spending time (in planning the attack), resources (what is needed to execute the attack) and the risk (of being killed or captured) will be taken into consideration in determining the risk and what is needed to protect and counter a possible attack. It is, therefore, important to recognize the different values that will be attached to an asset by terrorists and criminals, because this difference will influence the type of countermeasures needed to protect that particular asset.

Similar to other criminal activities, the motive (intent) behind the attack is an important factor for understanding, countering, and preventing future attacks as it sheds light onto the potential modus operandi and the value of each target. These can include:

- Attacks directed at the infrastructure aimed at physically destroying the building, airplane, airport, refinery, mobile phone mast etc., to disrupt the service where the aim is not to cause mass casualties.
- Attacks against personnel employed at facilities: These specifically directed attacks (discriminate) through killing, kidnapping etc., persons for their symbolic value, but also to attain access to the facility.
- Attacks against passengers or the broader public, making use of all forms of transportation that is generally indiscriminate (being at the wrong place at the wrong time) and intended to cause mass casualties.

DOI: 10.19165/2020.6.0128

- Intimidation directed at the intended target, but also broader audiences that might find themselves in a similar situation in the future.[15]

From the perspective of terrorists, there are a number of factors that will influence their decision-making process:[16]

- Symbolism: Symbolism can be defined as something that stands for or suggests something else; especially a visible sign of something invisible."[17] Keeping in mind that attacking a specific target is a form of communication, deciding on a specific target is, among other motivations, also driven by symbolism: the greater the symbolic value of the target, the more publicity the attack brings to the terrorists and the more fear it generates. Symbolism can also rationalize the decision to focus on a particular target in representing what the attackers are against.[18] For example, in the minds of those who planned the 9/11 attacks, the World Trade Centre symbolized capitalism and the financial strength of the US, and the Pentagon its military power. The symbolism of these targets was clear and the attacks were categorized as acts of symbolic terror within the framework of political communication.[19] Attacking the Independence Day celebrations in Nigeria, the Movement for the Emancipation of the Niger Delta (MEND) not only ventured outside its normal area of operation (the Niger Delta) and its traditional target selection (oil companies), but it also attacked the Nigerian state, its unity and its accomplishments when celebrating fifty years of independence.[20]
- Vulnerability: When planning an attack, those involved in this process will consider how protected and secure the target is. Although it might be easier to attack a soft target in comparison to a hardened target, the message in successfully attacking a target that is regarded as "secured," associated with the intimidation value (benefit), might surpass the risk. The differentiation between "soft" and "hard" targets, therefore, predominantly rests upon the level of access control and steps being taken to prevent incidents (security).
- Risk*:* What is the risk of detection and being captured? In other words, is the risk worth the effort?
- Feasibility: Is the target accessible? Will the intended level of destruction be achieved? How easy and expensive will it be to rebuild and recover?
- Impact: Will attacking the target bring about the required result (i.e., the anticipated impact on its intended victims and the audiences watching the attacks)?
- Reflection on the organization: How will the organization be perceived after the execution of the attack, considering that "overkill" (resulting in more than the expected casualties) will reflect negatively on the organization?

The last element is particularly important when the terrorist organization relies on the support of a segment within the public. For example, following the attack in Mogadishu, Somalia on

[15] Schmid, Alex P., 'Terrorism-the definitional problem,' *Case Western Reserve University School of Law*, Vol 36(375), 2004, p. 398.
[16] Bennett, Brian T., *Understanding, Assessing, and Responding to Terrorism: Protecting Critical Infrastructure and Personnel*, Hoboken: John Wiley & Sons, 2018, p. 193-194.
[17] Literary Devices. *Symbolism*. Available at: https://literarydevices.net/symbolism/
[18] Martin, Gus, *Understanding Terrorism: Challenges, Perspectives, and Issues*, Thousand Oaks: SAGE, 2006, p. 20-21.
[19] Louw, P. E., 'The War Against Terrorism': A Public Relations Challenge for the Pentagon', *Gazette: The International Journal for Communication Studies*, Vol 65(3), 2003, p. 212.
[20]Nossiter, A., 'Bombs by Nigerian Insurgents Kill 8', *The New York Times*, 1 October 2010. Available at: https://www.nytimes.com/2010/10/02/world/africa/02nigeria.html

DOI: 10.19165/2020.6.0128

14 October 2017 in which 587 people were killed and 316 people were seriously injured, no organization claimed responsibility.[21] According to all indications al-Shabaab (suspected to be responsible) did not intend to cause so many casualties as the device most probably was detonated prematurely by its driver when it was stopped by security officials while stuck in a traffic jam. A nearby fuel tanker ignited and caused a secondary explosion that increased the number of casualties.[22] This same element will be less relevant when the organization or individuals involved in planning an attack is detached from the country and the public targeted. For example, the 9/11 attackers had no attachment to the US, but were external actors launching attacks against the US with the intention to cause as many casualties and as much destruction as possible. The same consideration is also relevant to other attacks in Europe. For example the 2004 Madrid train bombings when ten IEDs detonated on four commuter trains, resulting in the death of 191 people and nearly 2,000 injured,[23] and the 2005 attacks on the London Underground and a bus at Tavistock Square in which 52 people were killed and approximately 700 injured.[24] Although these attacks were executed by nationals, some with links to immigrant communities, those executing the attacks associated themselves with an external cause (withdrawing support from the US alliance and involvement in especially Iraq). It is equally important to note that all of these attacks were directed at a critical infrastructure - the transportation sector of Spain and the UK.

Understanding the organization, its objectives, and its ideology will ultimately shed light onto its target selection process and its modus operandi. Furthermore, from the perspective of the state, responsible for protecting an array of potential targets, it is critical to prioritize vulnerabilities and risks within the framework of its broader terrorism threat assessment, an assessment that need to be constantly updated.

Type of Threats

Although the following section will reflect on previous attacks, this is not at all an indication to those involved in planning for critical infrastructure protection to exclude what may happen in the future. Those tasked with prevention should put themselves in the shoes of potential attackers (think like a "terrorist" also referred to as "red teaming") and, from the adversary's perspective, recognize weaknesses. Terrorists' success lies in their ability to change or adapt old and new tactics to their operations. In preparing for a potential act of terrorism, security forces often prepare only for the known instead of thinking "outside the box" and also prepare for the unfamiliar.

The modus operandi and target selection will be determined by the objective of the attack and the availability of appropriate means. For instance, ISIS had a dedicated article in its magazine *Rumiyah* on how to use fire as a modus operandi: "Ideal target locations for arson include houses and apartment buildings, forest areas adjacent to residential areas, factories that produce

[21] *Hiiraan Online,* 'Committee: 587 Dead in Oct 14 Terror Attack', 5 March 2018. Available at: https://hiiraan.com/news4/2018/Mar/157047/committee_587_dead_in_oct_14_terror_attack.aspx .
[22] Burke, J., 'Mogadishu Bombing: al-Shabaab behind Deadly Blast, Officials Say', *The Guardian,* 16 October 2017. Available at: https://www.theguardian.com/world/2017/oct/16/mogadishu-bombing-al-shabaab-behind-deadly-blast-officials-say
[23] Sciolino, E., 'Bombings in Madrid: The Attack; 10 Bombs Shatter Trains in Madrid, Killing 192', *New York Times*, 12 March 2004. Available at: https://www.nytimes.com/2004/03/12/world/bombings-in-madrid-the-attack-10-bombs-shatter-trains-in-madrid-killing-192.html
[24] Campbell, D. and Laville, S., 'British Suicide Bombers Carried out London Attacks, Say Police', *The Guardian,* 13 July 2005. Available at: https://www.theguardian.com/uk/2005/jul/13/july7.uksecurity6 .

DOI: 10.19165/2020.6.0128

cars, furniture, clothing, flammable substances, etc., gas stations, hospitals, bars, dance clubs, night clubs, banks, car showrooms, schools, universities, as well as churches, Rafidi temples, and so forth. The options are vast, leaving no excuse for delay."[25]

In addition to arson, terrorist weapons and methods include:

- Explosives: Particularly Improvised Explosive Devices (IEDs) come in many forms and use various delivery methods. Bombing is, historically, the most common terrorist tactic for two main reasons: Relative low risk to the organization when compared to the benefits and the physical (destruction) and psychological impact on the target, especially when the attacker is willing to commit suicide. The UN through the International Convention for the Suppression of Terrorist Bombing in 1997 criminalized bombings, "including the delivery, placing, discharging or detonating an explosive or other lethal device in, into or against a place of public use, a state or government facility, a public transportation system or an infrastructure facility with the intent to cause death or serious bodily injury or extensive destruction to property."[26]
- Firearms: terrorists use various types of firearms for attacks that are discriminate (for example in the case of assassinations) or indiscriminate (when the attacker indiscriminately shoots into a group of people).
- Knives (including for decapitation): the propaganda and intimidation value of knifing has been refined by Al-Qaeda in Iraq under Abu Musab al-Zarqawi and, more recently, by ISIS. The latter in its magazine Rumiyah dedicated a feature on the use of knives, including for decapitation, by giving detailed instruction of the type of knives that should be used for various forms of killing.[27]
- Kidnapping and hostage taking: this tactic is used to achieve a number of objectives, ranging from extorting ransom (money to fund the organization and other activities – not for personal financial gain) to propaganda purposes (particularly when hostages are being executed and the video material is distributed on the Internet). ISIS in the ninth issue of Rumiyah: "The scenario for such an attack is that one assaults a busy, public, and enclosed location and rounds up the kuffar who are present. Having gained control over the victims, one should then proceed to slaughter as many of them as one possibly can before the initial police response …"[28] Under the heading "Ideal target locations" the article continues "… generally any busy enclosed area, as such an environment allows for one to take control of the situation by rounding up the kuffar present inside and allows one to massacre them while using the building as a natural defense against any responding force attempting to enter and bring the operation to a quick halt."[29]
- Hijacking: this signifies the hijacking of airplanes, vessels, and other forms of public transport. The propaganda value (and media coverage) of attacking people in transit was realized early in the development of transnational terrorism. As a result, the first

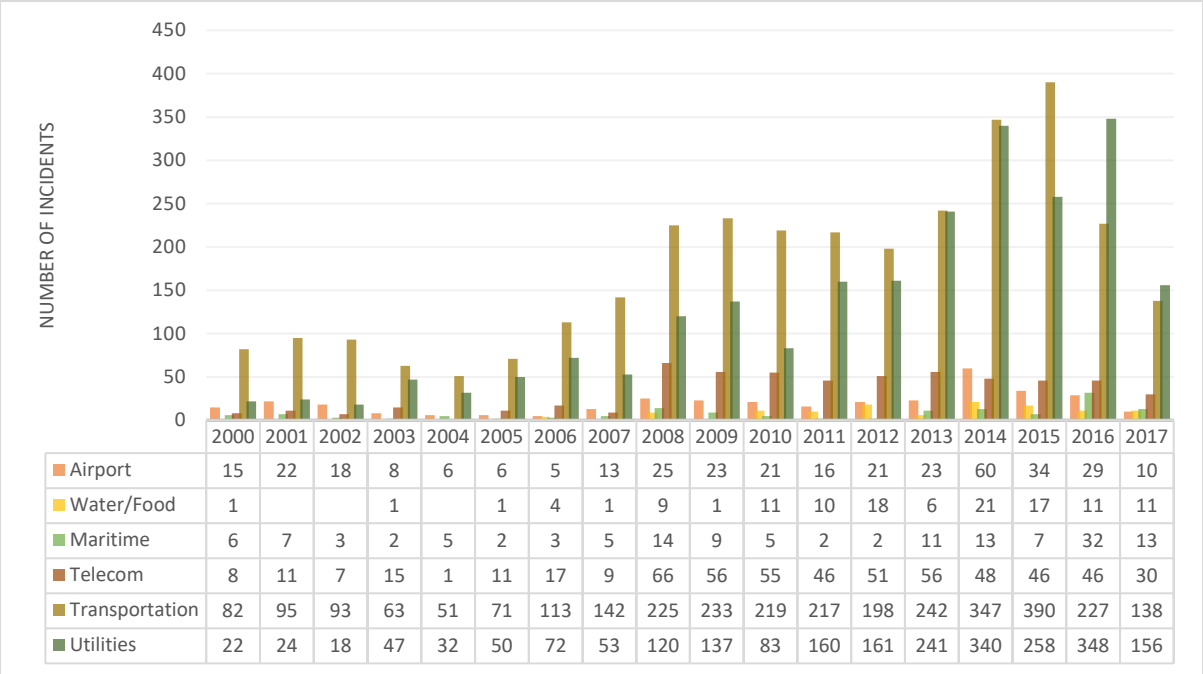
[25] *Rumiyah*, Issue 5, 6 January 2017. Available at: http://clarionproject.org/wp-content/uploads/2014/09/Rumiyah-ISIS-Magazine-5th-issue.pdf
[26] United Nations, *International Convention for the Suppression of Terrorist Bombings* New York: UN, 15 December 1997. Available at: https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-9&chapter=18&clang=_en
[27] *Rumiyah*, Issue 2, 4 October 2016, pp. 12-13. Available at: http://clarionproject.org/wp-content/uploads/Rumiyh-ISIS-Magazine-2nd-issue.pdf
[28] *Rumiyah*, Issue 9, 4 May 2017, p. 46-51. Available at: https://qb5cc3pam3y2ad0tm1zxuhho-wpengine.netdna-ssl.com/wp-content/uploads/2017/05/Rumiyah-9.pdf
[29] Ibid., p. 48.

DOI: 10.19165/2020.6.0128

international conventions dealing with terrorism concentrated on the hijacking of airplanes and the security of aviation on the ground.

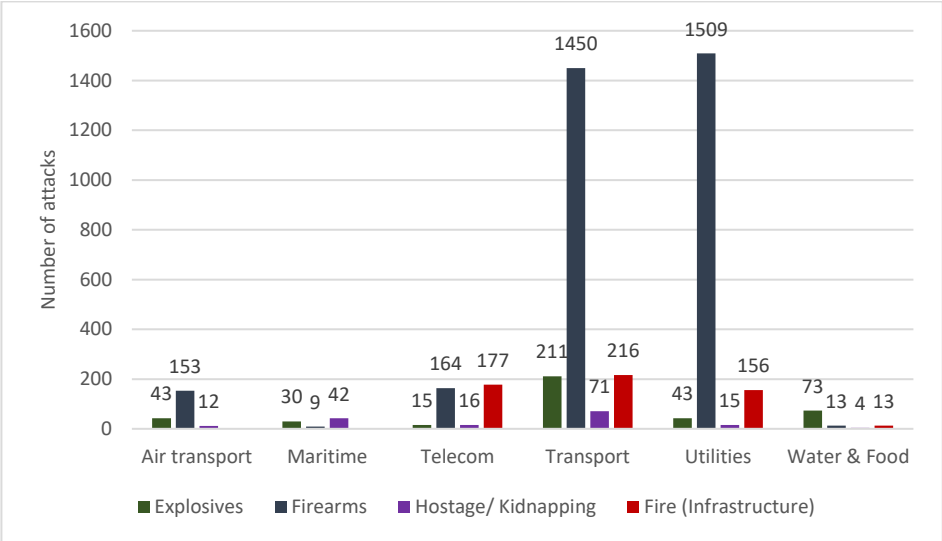
With the above arsenal at their disposal, numerous terrorist attacks were directed at utilities (electricity, gas, and oil) and transportation systems (see Figure 1 for a breakdown of attacks between 2000 and 2017), with firearms as the preferred weapon of choice (see Figure 2).

Figure 1: Attacks against Critical Infrastructure 2000 until 2017[30]



	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Airport	15	22	18	8	6	6	5	13	25	23	21	16	21	23	60	34	29	10
Water/Food	1			1		1	4	1	9	1	11	10	18	6	21	17	11	11
Maritime	6	7	3	2	5	2	3	5	14	9	5	2	2	11	13	7	32	13
Telecom	8	11	7	15	1	11	17	9	66	56	55	46	51	56	48	46	46	30
Transportation	82	95	93	63	51	71	113	142	225	233	219	217	198	242	347	390	227	138
Utilities	22	24	18	47	32	50	72	53	120	137	83	160	161	241	340	258	348	156

Figure 2: Targeting Modus Operandi 2010 until 2017[31]



[30] Based on information obtained from the National Consortium for the Study of Terrorism and Responses to Terrorism: Global Terrorism Database, University of Maryland. Available at: https://www.start.umd.edu/gtd/
[31] Ibid.

DOI: 10.19165/2020.6.0128

Transportation

Transportation in all its different forms is vulnerable to sabotage and terrorism as all systems require public access and as least as possible disruption - with at least as possible bottlenecks - when making use of it. The latter is particularly challenging to effectively monitor but can also increase the number of casualties if attacked. In the following section, air and rail transportation will be highlighted.

Airports and Airplanes

Although attacks on aircraft in flight is not new, the format has slightly changed over the years, as has been reflected in the UN conventions and protocols against the different forms of terrorism. The 1961 Tokyo Convention, focusing on offences committed on aircraft, and the 1970 The Hague convention, addressing plane hijackings, were followed by the 1971 Montreal Convention that criminalized the placement of explosives on board and sabotage, interfering with the navigation systems of the aircraft and damage to the plane that will endanger the safety of an aircraft in flight.[32] Following 9/11, the UN responded by introducing the Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation, signed at Beijing on 10 September 2010. The 2010 Protocol Supplementary to The Convention For The Suppression of Unlawful Seizure of Aircraft (1970 The Hague Convention) criminalized "violence against any person on board an aircraft in flight, endangering the safety of an aircraft, destroy or damage an aircraft in service, destroy or damage air navigation system or interfering with its operation, use an aircraft in service for the purpose of causing death, injury or damage to property, transporting explosives or any biological, chemical and nuclear weapon (BCN) or radioactive material for the purpose of causing death, injury or damage, and threatening to commit such acts."[33]

In the period 2000 - 2017 the number of hijackings decreased substantially from 27 incidents during the period 2000 – 2009 (including 9/11) to only five incidents between 2010 and 2017.

The threat of explosives onboard airplanes was real and, despite the introduction of reactive measures following the uncovering of plots, bore witness to the negative application of people's imagination. On 22 December 2001, Richard Reid ("the shoe bomber") attempted to ignite explosives hidden in the heel of his shoes on a flight from Paris to Miami.[34] In another failed attack, on 25 December 2009, Umar Farouk Abdulmutallab ("the underwear bomber") attempted to detonate explosives hidden in his pants on a flight from Amsterdam to Detroit.[35]

[32] United Nations, *The Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, 1971* ('the Montreal Convention'*).* Available at: https://treaties.un.org/doc/Publication/UNTS/Volume%20974/volume-974-I-14118-English.pdf

[33] United Nations, *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation*, Beijing, 10 September 2010. Available at: https://cil.nus.edu.sg/wp-content/uploads/2017/08/2010-Convention-on-the-Suppression-of-Unlawful-Acts-Relating-to-International-Civil-Aviation-1.pdf

[34] Sample, Ian. 'PETN - hard to detect and just 100g can destroy a car', *The Guardian*, 27 December 2009. Available at: https://www.theguardian.com/world/2009/dec/27/petn-pentaerythritol-trinitrate-explosive

[35] Scott, Shane, 'Inside Al Qaeda's Plot to Blow Up an American Airliner', *The New York Times*, 22 February 2017. Available at: https://www.nytimes.com/2017/02/22/us/politics/anwar-awlaki-underwear-bomber-abdulmutallab.html?rref=collection%2Ftimestopic%2FAbdulmutallab%2C%20Umar%20Farouk&action=click

DOI: 10.19165/2020.6.0128

In potentially the most devastating airline plot, in 2006 security forces arrested 24 suspects in London, who were associated with the liquid bomb plot intended to target seven transatlantic planes in flight. Key components of the homemade explosives were acetone peroxide (TATP) and hexamethylene triperoxide diamine (HMTD) carried in 500ml soft drink bottles.[36] As a result, 2006 regulations imposed a 100ml limit for liquids, aerosols, and gels to be carried inside a plane. Although this restriction is still in effect, the argument against these measures is that if a few passengers each carrying 5 x 100ml containers under this rule will not raise suspicion. Similarly, countering the underwear bomber and shoe bomber (although certain airline security companies require the x-ray screening of shoes) the central question is: do those operating x-ray machines know what to look for? In all this author's travels across Africa, none of the security personnel could tell her why they had to screen shoes or why it is not allowed to carry more than 100ml in a container. Considering that airport security and the person manning the x-ray machine is the last line of defense, much more needs to be done to move from window-dressing security to a constructive barrier.

Following the successful detonation of explosives hidden in a laptop on a flight in Somalia on 2 February 2016, the US government restricted the ability to travel to the US with electronic devices from a number of countries, including: Jordan, Egypt, Turkey, Saudi Arabia, Morocco, Qatar, Kuwait, and the United Arab Emirates. Similar to this measure, the UK banned tablets, laptops, games consoles, and other devices larger than a mobile phone on inbound flights from Egypt, Jordan, Lebanon, Saudi Arabia, Tunisia, and Turkey.[37] The main objective of detonating small charges in mid-flight has to do with the consequences of detonating even a very small charge in a pressurized cabin when reaching cruising altitude of approximately 35,000 feet (about 20 minutes after takeoff).[38] Approximately 340 grams (12 ounces) of explosives detonated at an altitude of 31,000 feet brought down Pan Am 103 over Lockerbie, Scotland, in 1988.[39]

Although explosives traditionally raised the most concern, airport security also placed a ban on knives, nail clippers, scissors, and even tweezers after 9/11. During the 9/11 hijackings the perpetrators used box cutters to gain access to the cockpit. However, despite these measures, the reality is that where there is a will there will nearly always be a way. Therefore, instead of boarding with a potential weapon, terrorists might use what is available on the plane. For example, buying a glass bottle on duty free and breaking it can produce an instant weapon. The most effective way of managing this type of attacks will most probably be to enhance sky marshal programs – a strategy predominately introduced in the aftermath of 9/11.

&contentCollection=timestopics&region=stream&module=stream_unit&version=latest&contentPlacement=2&pgtype=collection

[36] Laville, Sandra, *'Five Key Questions for Anti-Terror Investigation'*, *The Guardian*, 19 August 2006. Available at: https://www.theguardian.com/uk/2006/aug/19/terrorism.world

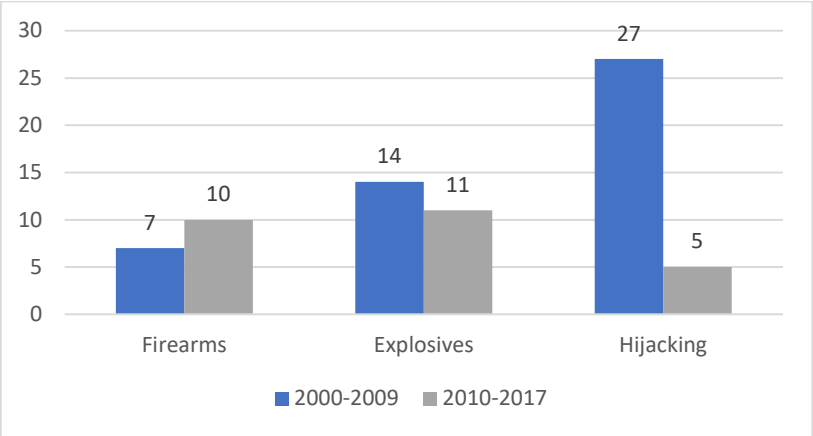
[37] MacAskill, Ewen, 'Laptop Ban on Planes came after Plot to put Explosives in iPad', *The Observer*, 26 March 2017. Available at: https://www.theguardian.com/world/2017/mar/26/plot-explosives-ipad-us-uk-laptop-ban

[38] Larson, George C., 'How Things Work: Cabin Pressure', *Air and Space Magazine*, January 2002. Available at: https://www.airspacemag.com/flight-today/how-things-work-cabin-pressure-2870604/

[39] Jansen, Bart, 'Aviation Experts: Small Explosives cause big Damage in Planes', *USA Today*, 18 November 2015. Available at: https://www.usatoday.com/story/news/2015/11/18/aviation-experts-small-explosives-cause-big-damage-planes/76014432/

DOI: 10.19165/2020.6.0128

Figure 3: Attacks against Airplanes[40]



Surface-To-Air Missiles or Man Portable Air Defense Systems (SAM/MANPADS)

The Surface-To-Air Missiles (SAM) or Man Portable Air Defense Systems (MANPADS) presents probably one of the most severe challenges to airplanes today, having an engagement rate up to 25,000 feet. Especially (though not exclusively) after takeoff and before landing (at an engagement range of approximately four miles) airplanes are particularly vulnerable. Although these weapon systems are particularly used in conflict zones and even directed at planes transporting humanitarian aid (most notably in Afghanistan and Somalia), the use of SAMs against commercial airliners has increased in recent years.[41]

For example, on 20 July 2019, British Airways and Lufthansa suspended flights to Cairo and North Sinai, due to security concerns. While Lufthansa resumed flights on 21 July, British Airways kept the ban for seven days.[42] Although the exact nature of the threat was not made publicly known, unconfirmed intelligence sources indicated that violent extremist groups in Egypt planned to down a commercial airplane with a MANPAD. Five years prior, in January 2014, Ansar Bait al-Maqdis (which later became the Sinai branch of ISIS in, had used a MANPAD it obtained from Libya to shoot down an Egyptian military helicopter in the Sinai Peninsula.[43] The following year, on 31 October 2015, the same organization had claimed responsibility for the attack on Metrojet Flight 9268, an Airbus A321-237, after it had taken off from Sharm El Sheikh International Airport. In this attack a small explosive device had detonated in mid-air at 31,000 feet.[44]

Considering the number of planes that were targeted by SAMs in recent years, other airlines should consider following Israeli commercial airline El Al's example by rolling out anti-ballistic technology. This step came in response to attacks on 28 November 2002 in Mombasa,

[40] Data obtained from National Consortium for the Study of Terrorism and Responses to Terrorism: Global Terrorism Database, College Park: University of Maryland. Available at: https://www.start.umd.edu/gtd/
[41] Chankin-Gould, Sarah and Schroeder, Matt, 'MANPADS Proliferation', *Federation of American Scientists*, Issue Brief 1, 2004. Available at: https://fas.org/asmp/campaigns/MANPADS/MANPADS.html
[42] Mendonca Duarte and Ralph Ellis, 'British Airways Cancels Flights to Cairo for 7 Days; Lufthansa does the same, for 1 Day', *CNN*, 21 July 2019. Available at: https://edition.cnn.com/2019/07/20/world/british-airlines-lufthansa-cancel-flights-to-cairo/index.html
[43] Broder Jonathan, 'ISIS in Libya: How Muhammar Gaddafi's Anti-aircraft Missiles are Falling into the Jihadists' Hands', *The Independent*, 11 March 2016. Available at: https://www.independent.co.uk/news/world/middle-east/isis-libya-muhammar-gaddafi-anti-aircraft-missiles-jihadists-a6926216.html
[44] France24, 'Russian Plane that Crashed in Egypt 'broke up in Air', 1 November 2015. Available at: https://www.france24.com/en/20151101-russian-plane-crash-sinai-egypt-broke-air-says-aviation-official

DOI: 10.19165/2020.6.0128

Kenya when two Strela 2 missiles were fired during take-off at an Israeli Arkia airline plane, - a Boeing 757 carrying 261 passengers - but missed.[45] In February 2014 Israel's Ministry of Defense (Misrad HaBitahon) announced that it successfully tested a "Commercial Multi-Spectral Infrared Countermeasures (C-MUSIC) system. According to Janes, a commercial intelligence firm, this new system consists of a pod under the fuselage that houses an infrared missile-tracking camera, an "infrared (IR), ultra-violet (UV), or radar missile-approach warning (MAWS) sensor to detect a missile launch in the very early stages of an attack" and a laser system meant to jam the incoming missile's "seeker" and "cause [the missile] to be diverted away from the aircraft."[46] The system, however, only protects against shoulder-launched heat-seeking missiles and not against radar-based anti-aircraft missile systems, as in the case of the Russian SA-11 that downed Malaysian Airlines MH17 while the plane was at cruising altitude over the Ukraine, killing nearly 300 people[47] While the Israeli system is costly, more airlines ought to consider similar defense systems, especially when operating in high-risk environments or if the country itself has a high-risk profile.

Unmanned Aerial Vehicles (UAVs - Drones)

Although the use of UAVs by security forces are well documented, the use of commercial drones by terrorists is increasing and raising is concerns. Early on, ISIS started to use UAVs to collect intelligence before executing attacks, but the group soon learned to use it also as a mini-bomber. On 24 January 2017, the ISIS media office in Iraq's Ninawa province released a video with the title "The Knights of the Dawawin."[48] It highlighted a new ISIS drone capability: dropping small bomb-like munitions on its enemies from the air. The capability displayed was not a once-off achievement as in scene after scene the video shows the group dropping small bombs from remotely controlled drones with some degree of accuracy. This included ISIS being able to successfully drop munitions onto crowds, and to hit stationary vehicles and tanks while another drone lingered above and filmed the attacks. A few days later, on 30 January 2017, ISIS' Wilayat al-Furat media office released a video entitled "Roar of the Lions"[49] in which ISIS featured its aerial operation in the Anbar Province of Iraq. At the end of the video, the group showed a video clip of the drone being used to deliver an IED in Anbar.[50] A year later, on 26 July 2018, Houthi rebels from Yemen claimed they had launched a drone attack on the Abu Dhabi airport. Although the United Arab Emirates (UAE) deny that the incident

[45] Knight, W., ''Incompetence' saved rocket-attack airliner', *New Scientist*, 29 November 2002. Available at: https://www.newscientist.com/article/dn3127-incompetence-saved-rocket-attack-airliner/

[46] Ferran Lee, 'Israeli Airline with Missile Defenses Goes to Israel When US Carriers Won't', ABC News, 23 July 2014. Available at: https://abcnews.go.com/Blotter/israeli-airline-missile-defenses-israel-us-carriers-wont/story?id=24684650

[47] *NBC News*, 'MH17: Why Commercial Jets Aren't Equipped to Avoid Missiles', 19 July 2014. Available at: https://www.nbcnews.com/storyline/ukraine-plane-crash/mh17-why-commercial-jets-arent-equipped-avoid-missiles-n159421

[48] *Jihadology*, 'New Video Message from The Islamic State: "Knights of the Departments – Wilāyat Nīnawā,"' 24 January 2017. Available at: https://jihadology.net/2017/01/24/new-video-message-from-the-islamic-state-knights-of-the-departments-wilayat-ninawa/

[49] *Jihadology*, 'New Video Message from The Islamic State: "Roar of the Lions – Wilāyat al-Furāt"', 30 January 2017. Available at: https://jihadology.net/2017/01/30/new-video-message-from-the-islamic-state-roar-of-the-lions-wilayat-al-furat/

[50] Rassler Don, Muhammad al`Ubaydi and Vera Mironova, 'The Islamic State's Drone Documents: Management, Acquisitions, and DIY Tradecraft', *Combating Terrorism Center at West Point*, 31 January 2017. Available at: https://www.ctc.usma.edu/posts/ctc-perspectives-the-islamic-states-drone-documents-management-acquisitions-and-diy-tradecraft

DOI: 10.19165/2020.6.0128

occurred,[51] information available in the public domain claims evidence that the Houthis' Sammad-3 drone launched three attacks on the airport[52]

Nine days after this incident, on 4 August 2018, two DJI M600 drones (manufactured in China), each carrying one kilogram of C-4 explosives, were used in a failed assassination attempt against Venezuelan President Nicolás Maduro, when one or both drones detonated explosives above the audience at a nationally televised military event. Although several people were injured, the president and his wife who was standing next to him onstage remained unharmed.[53]

This was followed in December 2018 by an incident at London's Gatwick Airport when a number of drone sightings brought the airport's entire air traffic to a standstill. It later became known that this was not the first drone experience at Gatwick. In July of the same year there had been a near-miss between an unmanned aircraft and a passenger plane. According to the British Airline Pilots Association, the number of incidents involving drones and other aircraft has grown dramatically, from none in 2013 to 93 in 2017, to 117 incidents between January and November 2018.[54]

Weaponized drones offer tactical advantages that only wait to be harnessed by terrorists (and criminals alike):[55]

1. Versatility*:* with fixed-wing drones being able to fly much further from their controller than quad-copter versions, while the latter are able to hover and stay in one place.
2. Stealth*:* as most drones can fly lower than current technology (for example, radar) is capable to detect.
3. Thinking bomb: payload and utilization enables drones to be used in almost every phase of a terrorist operation. Being equipped with a camera, drones can be used to conduct surveillance on a potential target, whereas a camera with video link to the controller can be used in the execution of an attack to ensure accuracy that translates into executing the strike at the right moment. This allows the attacker to utilize the benefits of a suicide bomber as a 'thinking bomb' while enabling the controller to leave the scene unscathed to strike – unlike suicide bombers - at another target in the future.
4. Lethality*:* considering that even a small quantity of explosives can bring down a civilian aircraft in flight, commercial airliners are vulnerable to drone attacks during take-off and landing. There is limited time for pilots to react in an attempt to prevent collision. Airports are also not designed to ward off drone bombs attacks from the sky.

Following attacks against aircraft in flight, attacks directed at airports were addressed in the

[51] Hudson Bernard, 'Drone Attacks are Essentially Terrorism by Joystick', *Washington Post*, 5 August 2018. Available at: https://www.washingtonpost.com/opinions/drone-attacks-are-essentially-terrorism-by-joystick/2018/08/05/f93ec18a-98d5-11e8-843b-36e177f3081c_story.html?utm_term=.44fab7a35c53

[52] Al Jazeera, 'Yemen's Rebels 'Attack' Abu Dhabi Airport Using a Drone', 27 July 2018. Available at: https://www.aljazeera.com/news/2018/07/yemen-rebels-attack-abu-dhabi-airport-drone-180726155103669.html

[53] Brocchetto Marilia, Jonny Hallam, Joe Sterling and Stefano Pozzebon, 'Venezuela Makes Six Arrests in Alleged Maduro Assassination Attempt', *CNN*, 6 August 2018. Available at: https://edition.cnn.com/2018/08/05/americas/venezuela-maduro/index.html

[54] Coulter Martin and Naomi Rovnick, 'How Big a Threat are Drones at Airports*?*' *Financial Times*, 20 December 2018. Available at: https://www.ft.com/content/ee9bb576-0455-11e9-99df-6183d3002ee1

[55] Clarke, Colin P., 'Approaching a 'New Normal': What the Drone Attack in Venezuela Portends', Rand Corporation, 13 August 2018. Available at: https://www.rand.org/blog/2018/08/approaching-a-new-normal-what-the-drone-attack-in-venezuela.html

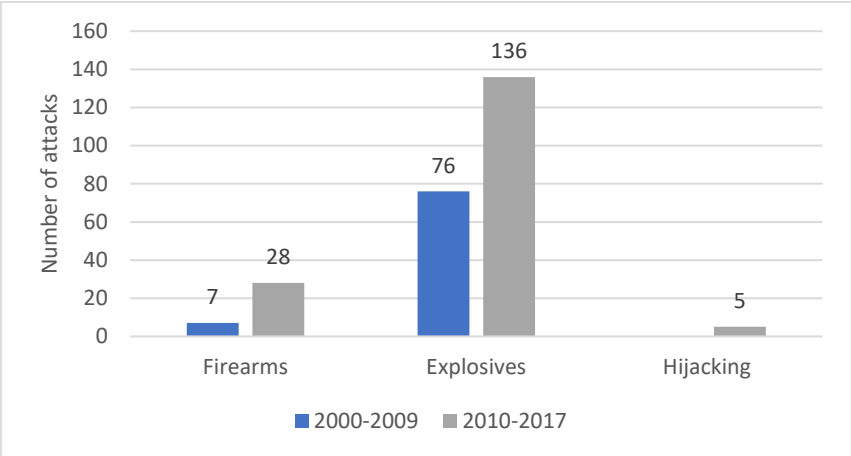
DOI: 10.19165/2020.6.0128

Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Montreal Convention, 1988 (Montreal Protocol) This protocol criminalizes violence, destruction and disruption at airports.[56]

The biggest challenge in airport security (as well as in other forms of transportation) is the massive influx of people, the majority with luggage. Although luggage may be screened during check-in or before boarding, these steps might be too late in the execution phase of the attack where the airport entrance hall is the intended target. For example, on 22 March 2016, two brothers executed coordinated attacks targeting transportation infrastructure in Brussels. In the first attack, Brahim el-Bakraoui, and a second suicide bomber, Najim Laachraoui, carried explosives in their suitcases and detonated these at a check-in counter at Brussels Airport in Zaventem, killing 11 people. In the second attack, Khalid el-Bakraoui targeted the Maelbeek metro station in downtown Brussels, in which twenty people died. At least 270 people were injured due to these incidents. ISIS claimed responsibility for the attacks by the two Belgian brothers. [57]

Countering the terrorist threat at airport entrance halls, Kenya requires passengers to get out of their vehicle approximately two kilometers from the airport building) and go through a metal detector while their hand luggage is scanned through an X-ray machine. The biggest flaw in this system is that after a quick screening of the vehicle by an officer, larger pieces of luggage are allowed to go through unchecked. The use of sniffer dogs to detect explosives could add another layer of security.

Figure 4: Attacks against Airports[58]



[56] United Nations, *Protocol on the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, 1988*. Available at: https://www.un.org/ruleoflaw/blog/document/protocol-on-the-suppression-of-unlawful-acts-of-violence-at-airports-serving-international-civil-aviation-supplementary-to-the-convention-for-the-suppression-of-unlawful-acts-against-the-safety-of-civ/

[57] BBC News, '*Brussels Attacks: Two Brothers behind Belgium Bombings'*, 23 March 2016. Available at: https://www.bbc.com/news/world-europe-35879141

[58] Data obtained from National Consortium for the Study of Terrorism and Responses to Terrorism: Global Terrorism Database, College Park: University of Maryland. Available at: https://www.start.umd.edu/gtd/

DOI: 10.19165/2020.6.0128

Subway and Railway Stations, Trains and Tracks

In comparison to the period 2000 - 2009, attacks against railways and road systems increased between 2010 and 2017 (see Figure 4). Similar to airport security, preventing a potential attacker to enter a bus terminal or train station remains a major challenge. However, in the Shanghai Metro Station, the Chinese government imposed compulsory x-ray screening of all luggage and bags, while also performing random checks of purses at over 700 checkpoints. This has, however, resulted in long queues when the number of entrances to the station was reduced for the purpose of passenger screening.[59]

Using CCTV and facial recognition can be helpful in identifying and apprehending individuals known to security agencies. But what if the attacker is unknown? The already growing use of artificial intelligence (AI) in the security sector is likely to further increase. According to a report written in 2019, the US Transportation Security Administration (TSA) is engaged in a project that enhances airport security through a Dynamic Aviation Risk Management Solution (DARMS). It is meant to "… integrate information across the aviation sector to tailor a personalized security profile for each person, on a per-flight basis. A smart tunnel will check people's security while they walk through it, eliminating the need for inefficient security lines."[60] Although implementation is still a few years away, the potential of using a similar system for other transportation systems looks promising. In the UK the introduction of trials in 3D scanning of carry-on luggage will no longer require passengers to remove items from bags or limit the amount of liquids taken onboard a plane. With the help of computer tomography (CT), cabin baggage is displayed as 3D rotatable images. Material that could be an explosive is highlighted by color upon which the operator can further investigate the item through studying cross-sectional images.[61] The application of this technology at all airports and beyond will add an important security layer to transportation checkpoints.

The protection against attacks carried out by a passenger on board a train is, however, only one part of the security solution. The other part is determining how to protect tracks against sabotage causing a train to derail. Although not a common feature in Al-Qaeda's or ISIS's modus operandi, derailing trains has been a favorite tactic of certain separatist movements. Following a drastic increase in events that included the usage of explosives and obstacles and barriers in since 2016, the Indian government established the Railway Protection Force (RPF) to address this challenge.[62]

[59]Aldama Zigor, 'Shanghai Metro: keeping world's longest mass-transit rail system on track', *Post Magazine*, 12 August 2017. Available at: https://www.scmp.com/magazines/post-magazine/long-reads/article/2106229/shanghai-metro-keeping-worlds-longest-mass

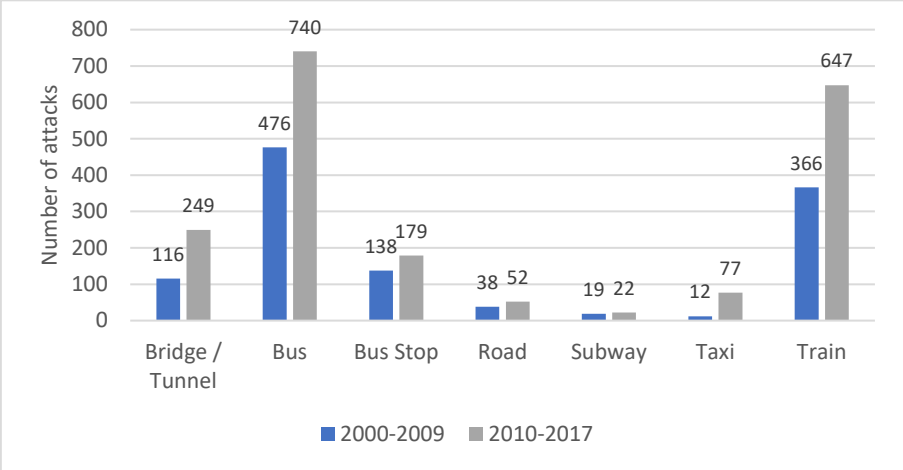
[60] Faggella Daniel, 'Artificial Intelligence and Security: Current Applications and Tomorrow's Potentials', *Emerj Artificial Intelligence Research*, 20 May 2019. Available at: https://emerj.com/ai-sector-overviews/artificial-intelligence-and-security-applications/

[61] Schwaninger, Adrian and Sarah Merks, 'Single-View, Multi-View and 3D Imaging for Baggage Screening: What should be considered for effective training?' *Aviation Security International*, 19 February 2019. Available at: https://www.asi-mag.com/single-view-multi-view-and-3d-imaging-for-baggage-screening-what-should-be-considered-for-effective-training/

[62] Chauhan, Chanchal, '*18 Sabotage Attempts on Indian Railways in 40 Days: Suresh Prabhu Expresses Serious Concern'*, *India,* 19 February 2017. Available at: https://www.india.com/news/india/18-sabotage-attempts-on-indian-railways-in-40-days-suresh-prabhu-expresses-serious-concern-1823503/

DOI: 10.19165/2020.6.0128

Figure 5: Attacks against Transportation Systems[63]



Remote Targets

Attacks against the energy and telecommunication infrastructures, being often conducted from a distance, are usually easy to access which increases the likelihood of attacks intended to damage and disrupt such facilities. Although strikes seldom lead to massive casualties, the economic consequences can be severe. It should therefore come as no surprise that the majority of attacks against critical infrastructures are directed against telecommunication facilities and utilities like electricity, oil, and gas lines.

Strikes against energy facilities, including power plants, transmission lines, and generating stations have shown a drastic increase since 2010, with 88 percent of the attackers resorting to explosives as the preferred modus operandi, followed by arson which account for 9 percent of the assaults.

Communication facilities include the Internet, radio, and TV broadcast, telephone facilities as well as other forms of written media (for example newspaper offices). Mobile telephone facilities require special attention, especially in conflict areas, considering the 260% increase in attacks (see Figure 7).

Recognizing that the vulnerability of energy infrastructure increases as a result of being above the ground and therefore visible as well as remote (similar to the telephone network), technological solutions in association with traditional security measures are required as will be briefly discussed in the next section.

[63] Data obtained from National Consortium for the Study of Terrorism and Responses to Terrorism: Global Terrorism Database, College Park: University of Maryland. Available at: https://www.start.umd.edu/gtd/

DOI: 10.19165/2020.6.0128

Figure 6: Attacks directed at Utilities[64]

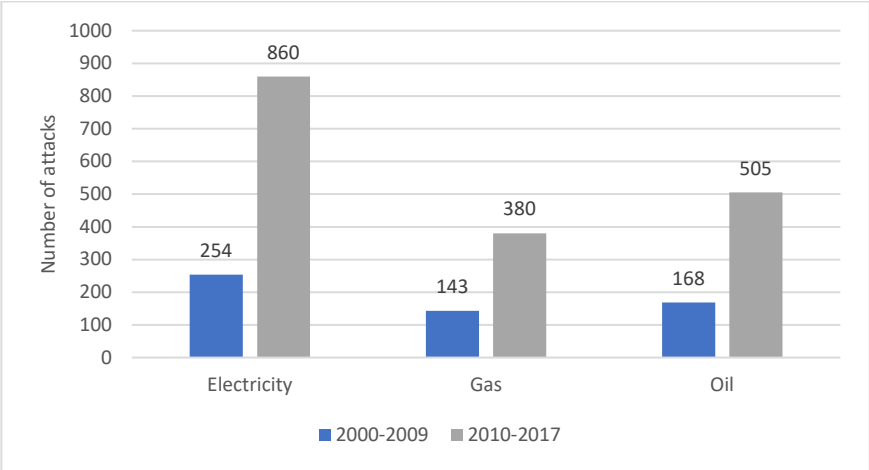
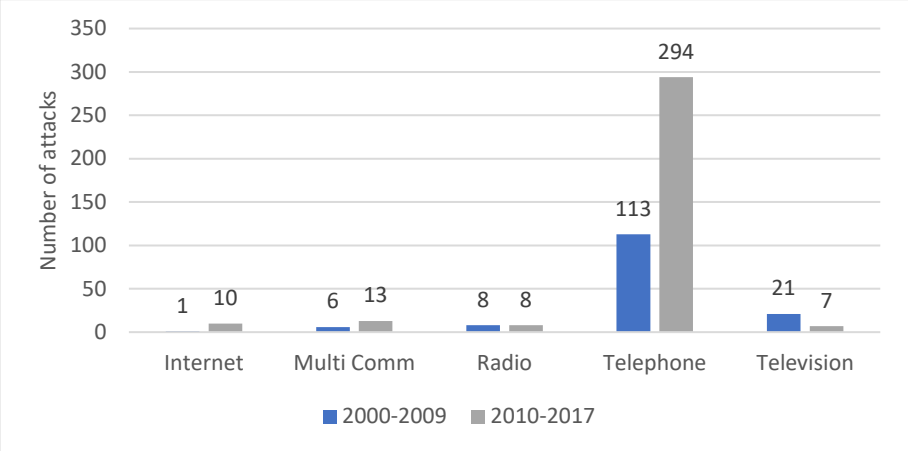


Figure 7: Attacks against Communication Infrastructure[65]



Planning for the Worst

The maxim "hope for the best, plan for the worst" applies both in areas constantly targeted, and in areas where there is no prior history of terrorist attacks on infrastructures. Though, from practical experience, it is much harder to convince policymakers to plan for the latter and implement measures against what is regarded as a remote possibility, especially when the cost implications are substantial. It is, therefore, understandable that in addition to the vulnerability assessment of a specific region and the country as a whole, it is crucial to identify areas of special concern which then should be placed on an appropriate level of preparedness. Furthermore, security officials also need to assess the vulnerability of each venue or facility within the broader environment and introduce specific measures to counter and/or minimize the impact an attack might have. The best mental approach in this regard is to plan as if an attack were already in progress, instead of asking oneself whether it could ever happen. With

[64] Data obtained from National Consortium for the Study of Terrorism and Responses to Terrorism: Global Terrorism Database, College Park: University of Maryland. Available at: https://www.start.umd.edu/gtd/
[65] Ibid.

DOI: 10.19165/2020.6.0128

this being said, governments or corporate managements need to be reminded that the success of terrorists rest to a large extent in their ability to surprise and use the unexpected to their advantage as part of their asymmetric warfare. In light of this reality, the following measures and practical steps need to raise awareness and initiate other practical steps to plan and prepare for the worst:

1. Within the framework of a broader threat assessment, management in partnership with security experts need to conduct a risk assessment that identifies key vulnerabilities in- and outside the facility. This is done by identifying: potential routes, traffic flow patterns in and out of the facility, areas where there is a large concentration of people, times of the day where vulnerability is higher (e.g., rush hour), etc. The overall objective is to develop a layered security solutions design that balances the need for open public access (where required) and concern for public security.
2. Another feature of this framework is the development and implementation of a formal security awareness program. This in turn, ought to be discussed with personnel; in this phase it is also important to ask for the personnel's input since employees will often present a very different angle to potential risks and vulnerabilities than "outside" assessors. Employees need to understand and accept that their security is both their own responsibility and that of the company or institution. This step is important for informing personnel (especially security personnel) how attacks are planned and what their role is in detecting suspicious activities, most notably during the intelligence collection phase of a planned attack by reporting:
    i) Individuals asking irrelevant questions, for example:
        - An employee at a service center being asked when they open or close is one thing but asking questions around the movement of personnel or other schedules is another.
        - Asking questions about the inside of the building, and the way it was constructed.
    ii) Individuals acting suspicious:
        - Taking "irrelevant" pictures. Today it is extremely easy to take pictures of buildings (with a mobile phone or other device), the positioning of CCTV cameras, fences, and other security measures in place.
        - Potential indicators might include the taking of "selfies" or taking pictures of friends "posing" at the least tourist friendly areas or positions.
        - Strolling might be a sign of boredom but seeing the same person over time in different areas without having a reason to be there needs to be followed up. Algorithms are becoming increasingly available to detect suspicious behavior, including what a person might do next.
3. In addition, it is important to conduct realistic live exercises to develop, implement, and rehearse incident response plans. It is important that these plans should not stagnate but should stay relevant for changing modus operandi and new inventions and trends. Information will empower employees, but it needs to be followed with equipping people with the skills to turn anxiety into preparedness.

Depending on the type of service or facility, proactive measures should take the following key principles – borrowing from basic security[66] – into consideration when developing and implementing dedicated countermeasures. I discuss five below.

[66] Duff, B., 'The 5 Ds of Home Security: Deter, Detect, Deny, Delay, and Defend', Mind 4 Survival, 28 March 2017 Available at: https://mind4survival.com/5-ds-of-home-security/

DOI: 10.19165/2020.6.0128

Deter

These proactive measures reduce attackers' interest in the target, most notably by means of hardening the target through increasing the risk of being detected prior to an attack (as briefly indicated above) or through implementing measures that will decrease potential success if terrorists should decide on launching an attack. In short, it sways the cost-benefit balance to the negative side.

Detect

These are proactive measures which identify a potential threat through threat, risk, and vulnerability assessments. Using CCTV with facial recognition software to identify individuals acting suspiciously is the most well-known of such measures. The utilization of artificial intelligence (AI) to detect changes in behavior may become a valuable tool in uncovering potential plots during the intelligence collection phase. While CCTV has been useful in the investigation of already executed attacks, – for example identifying perpetrators and their movements leading up to an attack – more can be done to prevent attacks through this technology. It will also require a closer relationship between facility-based security personnel and security agencies (especially intelligence agencies) with a clear mandate to investigate potential perpetrators, taking into account privacy considerations of ordinary law-abiding citizens.

Although the majority of high-risk facilities may already have such measures in place, previous attacks on utilities, communication, and transportation systems indicate that remote sites of some of these facilities added to their vulnerability. It is, therefore, necessary to protect the most vulnerable areas during the most likely times attacks occur even in peripheral areas For example, attacks against mobile phone transmission masts in conflict areas have been a favorite tactic for the Taliban, al-Shabaab, and Maoist militants in India. Telecommunication transmission towers are often easy access targets. If successful, attacks can cause the collapse of telecommunications and further facilitate the operation of terrorist groups in those areas by preventing the public from communicating their whereabouts and movements to security forces. The inability to communicate attacks to security forces allow armed groups to operate with impunity, meaning that by the time security forces are informed attackers have already fled the scene. Similarly, attacks on oil pipelines not only cause environmental damage, but also have a major economic impact, making companies question whether it is viable to remain and/or invest in conflict zones.

It is physically impossible to have enough boots on the ground to protect many telecommunication facilities. Even if security personnel are stationed at such a facility, the possibility of being overrun is real as witnessed in a recent attack in Kenya. On 7 August 2019 in Garissa, Kenya, ten National Police Reservists were kidnapped after the telecommunication mast they were protecting was overrun by suspected al-Shabaab operatives.[67]

Detecting threats before an attack, purely for the logistical challenges it represents, proves to be extremely difficult. The use of UAVs and other picture/video-based network systems may be useful for identifying attackers, but can usually not prevent attacks and physical intrusions,

[67] Morani Anderson, 'Al-Shabaab Militants Destroy Safaricom Mast, Overpower Officers', *Havisasa*, 8 August 2019. Available at: https://hivisasa.com/posts/30107553-al-shabaab-suspects-destroy-safaricom-mast-overpower-officers?source=latestHome

DOI: 10.19165/2020.6.0128

given reaction times and distances to the scene of an incident. Perimeter Intrusion Detection Systems (PIDS), such as fibre-optic Distributed Acoustic Sensing (DAS) technology hidden below the ground or a pressure sensitive cable or one that builds up an electromagnetic field allow early detection of the footsteps of intruders. Instead of applying this technology within the attack-range of a telecommunication transmitter mast, or an oil or gas pipeline, such a system could be installed at a larger distance from the object to be protected to provide early warning for a timely response. New security systems are able to provide an "acoustic fingerprint" which will allow the system operator to distinguish between people, vehicles, and animals crossing perimeter lines, and also tell him whether a specific activity is occurring (such as digging or fence climbing). This allows them to take the required countermeasures in time to prevent an attack.[68]

The introduction of UAV technology not only presents a threat to the aviation industry as discussed earlier, but it can also easily be applied to conduct surveillance before launching a 'traditional type' attack or launch the actual attack by delivering chemical and biological agents or detonating explosive payloads. With the latter in mind, governments, security companies (commercial), and security agencies (state controlled) need to rethink access control to facilities and other countermeasures. UAV detection and countermeasures has become a growing industry. One new system, marketed by Radar Zero, can detect small drones in three dimensions with static or mobile detectors. The system includes a radar sensor that tracks a moving object while separating it from other objects such as trees or birds. Secondly, a radio frequency (RF) sensor provides a direction of bearing to the target, matching a set of RF signatures. Lastly, a camera and thermal sensors visual confirm the target. Once detected the UAV can be brought to the ground, returned to the operator, or destroyed.[69]

Delay

While early detection will allow the deployment of appropriate countermeasures, additional measures should be in place to delay attackers from reaching their intended goals and gaining access to the target. Physical barriers are most common and include fences, gates etc. These measures need to buy as much time as possible. Over the years, fence technology advanced substantially to include fences that have anti-cut and anti-climb features while some fence and gate types are intended to withstand vehicles. Such crash-rated barrier fences can prevent one or more vehicles from ramming or crashing into a secured facility by absorbing their kinetic energy.[70]

Defense and response capabilities

Depending on the nature of the facility to be protected and the result of threat and risk assessments, high value facilities need to be able to withstand attacks. Even if this self-defense capability will be limited, it should be sufficient until the arrival of reinforcements.

[68] Bandweaver, *Perimeter Intrusion Detection System*. Available at: https://www.bandweaver.com/sectors/fire-and-security/perimeter-intrusion-detection-system/
[69] DroneShield, *Detect. Assess. Respond*. Available at: https://www.droneshield.com/
[70] Aberdeen, *Security Fences – The Most Impenetrable Types in the World*. Available at: https://aberdeengate.com/security-fences-impenetrable-types-world/

DOI: 10.19165/2020.6.0128

Devalue

All of the above will minimize the impact of an attempted attack, including preventing or at least limiting the number of casualties and the destruction of the facility. This, in turn, will decrease the value of attacking the particular target. When assessing the value of a target, impact on life and limb will be the first criteria, but the impact on the environment (for example an oil spill as a result of a damaged pipeline) and lost income, depending on how long the facility will be inactive, also need to be taken into consideration.

Conclusion

Irrespective of being classified as a "hard" or "soft" target, critical infrastructure will remain in the crosshairs of terrorists as it ticks all the boxes in conveying a message, causing massive casualties or disruption, hurting a country and/or industry economically, attracting massive media attention, and intimidating as many as possible. Considering the diverse nature of potential targets, it is impossible to protect them all. Accurate intelligence about the motives, intentions, and capacities of the adversary is necessary to prioritize preparations. Yet, those responsible for protecting infrastructure against terrorist attacks need to plan also for less probable scenarios - not only by considering what happened in the past (and being reactive), but also by considering what is likely to happen in the future (and being proactive). Possible countermeasures can be expensive, but policymakers should keep in mind that these countermeasures can often also be applied for preventing and countering natural disasters and man-made non-terrorist accidents.

This chapter started by explaining the concept of "critical infrastructure" and how it relates to the overall aim of terrorists to attack associated sector facilities. Specific reference was made to the OAU's categorization of intent by targeting "public or private property, natural resources, and environmental or cultural heritage."[71] The second part of the chapter emphasized the need to conduct periodic threat-, risk-, and vulnerability assessments to be continuously abreast and prepared for potential threats, especially since attacks seldom take place outside situational developments within a particular time and place. While the purpose of assessment analysis needs to be clear, those responsible need to constantly keep the purpose of attacking critical infrastructure in mind. In other words, what makes a country's critical infrastructure attractive to attack? Taking into consideration that the planning of such attacks requires a basic cost-benefit analysis: those tasked with preventing and countering acts of terrorism and sabotage need to increase the cost of attacking a particular facility or sector, while decreasing the benefit the group or organization may attain from executing the attack(s).
Shedding light on the type of threats critical infrastructure may potentially have to deal with, this section of the chapter tried to explain future *modi operandi* and target selection by highlighting previous incidents Furthermore, specific reference was made to the transportation industry, (most notably airports and airplanes, and the railways), utilities (electricity, gas, and oil networks and facilities), and the communication infrastructure. The use of UAVs, drones, and SAM/MANPADS were briefly highlighted as their use requires additional and specific countermeasures.

[71] African Union, *OAU Convention on the Prevention and Combating of Terrorism*, 1999. Available at: https://au.int/sites/default/files/treaties/7779-treaty-0020_-_oau_convention_on_the_prevention_and_combating_of_terrorism_e.pdf

DOI: 10.19165/2020.6.0128

Anneli Botha, Ph.D., is a senior lecturer at the Department Political Studies and Governance at the University of the Free State in South Africa. She also serves as an independent consultant on radicalization, deradicalization, reintegration and terrorism in Africa and worked on a number of projects with the Finn Church Aid (FCA) and different UN agencies. During the period 2003 till 2016 she worked as a senior researcher on terrorism at the Institute for Security Studies (ISS) in Pretoria, South Africa. Dr. Botha has travelled extensively throughout Africa where she conducted research on terrorism and delivered specialized training on various aspects of the threat of terrorism, extremism, radicalization and counterterrorism to law enforcement and criminal justice officials. Prior to her position at the ISS, she served in the South African Police Service (SAPS) for 10 years. Highlights included being a founding member of the Religious Extremism and Terrorism Desk at Crime Intelligence Head Office and serving in the Rapid Reaction Unit and the Special Task Force on Urban Terror in the West Cape. At the end of her police career, she provided strategic support to the Head of South Africa's Crime Intelligence Unit.

DOI: 10.19165/2020.6.0128

Bibliography

Aberdeen, *Security Fences – The Most Impenetrable Types in the World.* Available at: https://aberdeengate.com/security-fences-impenetrable-types-world/

African Union, *OAU Convention on the Prevention and Combating of Terrorism, 1999*. Available at: https://au.int/sites/default/files/treaties/7779-treaty-0020_-_oau_convention_on_the_prevention_and_combating_of_terrorism_e.pdf

Agence France-Presse, 'Terrorists attack Dusit hotel in Nairobi, Bangkok Post', 16 January 2019. Available at: https://www.bangkokpost.com/world/1611674/terrorists-attack-dusit-hotel-in-nairobi

Aldama, Z, *Shanghai Metro:'* Keeping World's Longest Mass-Transit Rail System on Track', *Post Magazine*, 12 August 2017. Available at: https://www.scmp.com/magazines/post-magazine/long-reads/article/2106229/shanghai-metro-keeping-worlds-longest-mass

AlJazeera, *Yemen's Rebels "Attack" Abu Dhabi Airport Using a Drone'*, 27 July 2018. Available at: https://www.aljazeera.com/news/2018/07/yemen-rebels-attack-abu-dhabi-airport-drone-180726155103669.html

Bandweaver, *Perimeter Intrusion Detection System*. Available at: https://www.bandweaver.com/sectors/fire-and-security/perimeter-intrusion-detection-system/

BBC News, '*Brussels Attacks: Two Brothers Behind Belgium Bombings'*, 23 March 2016. Available at: https://www.bbc.com/news/world-europe-35879141

Bennett, Brian T., *Understanding, Assessing, and Responding to Terrorism: Protecting Critical Infrastructure and Personnel'*, Hoboken: John Wiley & Sons, 2018.

Brocchetto, M. Jonny Hallam, Joe Sterling and Stefano Pozzebon, 'Venezuela Makes Six Arrests in Alleged Maduro Assassination Attempt', *CNN*, 6 August 2018. Available at: https://edition.cnn.com/2018/08/05/americas/venezuela-maduro/index.html

Broder, J., 'Isis in Libya: How Muhammar Gaddafi's Anti-aircraft Missiles are Falling into the Jihadists' Hands', *The Independent*, 11 March 2016. Available at: https://www.independent.co.uk/news/world/middle-east/isis-libya-muhammar-gaddafi-anti-aircraft-missiles-jihadists-a6926216.html

Brown G, Carlyle M, Salmerón J, Wood K., 'Defending Critical Infrastructure', *Interfaces*, Vol. 36, No. 6, 2006, pp. 530-544.

Burke, J., '*Mogadishu Bombing: al-Shabaab Behind Deadly Blast, Officials say'*, *The Guardian*, 16 October 2017. Available at: https://www.theguardian.com/world/2017/oct/16/mogadishu-bombing-al-shabaab-behind-deadly-blast-officials-say

Campbell, D. and Laville, S., 'British Suicide Bombers Carried out London Attacks, Say Police', *The Guardian*, 13 July 2005. Available at: https://www.theguardian.com/uk/2005/jul/13/july7.uksecurity6

Chankin-Gould, Sarah and Schroeder, Matt, 'MANPADS Proliferation', *Federation of American Scientists*, Issue Brief 1, 2004. Available at: https://fas.org/asmp/campaigns/MANPADS/MANPADS.html

Chauhan, C., '18 Sabotage Attempts on Indian Railways in 40 Days: Suresh Prabhu Expresses Serious Concern', *India*, 19 February 2017. Available at: https://www.india.com/news/india/18-sabotage-attempts-on-indian-railways-in-40-days-suresh-prabhu-expresses-serious-concern-1823503/

Clarke, Colin P., 'Approaching a 'New Normal': What the Drone Attack in Venezuela Portends', *Rand Corporation*, 13 August 2018. Available at:

DOI: 10.19165/2020.6.0128

https://www.rand.org/blog/2018/08/approaching-a-new-normal-what-the-drone-attack-in-venezuela.html

Coulter, M and Rovnick, N., '*How Big a Threat are Drones at Airports*?' *Financial Times,* 20 December 2018. Available at: https://www.ft.com/content/ee9bb576-0455-11e9-99df-6183d3002ee1

Department of Homeland Security, *Critical Infrastructure Sectors 2019*. Available at: https://www.dhs.gov/cisa/critical-infrastructure-sectors

DroneShield, *Detect. Assess. Respond*. Available at: https://www.droneshield.com/

Duff, B., 'The 5 Ds of Home Security: Deter, Detect, Deny, Delay, and Defend', *Mind 4 Survival*, 28 March 2017. Available at: https://mind4survival.com/5-ds-of-home-security/

Ellis, J.W., *Police Analysis and Planning for Vehicular Bombings: Prevention, Defense and Response*, Springfield: Charles C Thomas Publisher, Ltd., 1999.

Faggella, D., 'Artificial Intelligence and Security: Current Applications and Tomorrow's Potentials', *Emerj Artificial Intelligence Research*, 20 May 2019. Available at: https://emerj.com/ai-sector-overviews/artificial-intelligence-and-security-applications/

Ferran, L., 'Israeli Airline with Missile Defenses Goes to Israel when US Carriers Won't', *ABC News*, 23 July 2014. Available at: https://abcnews.go.com/Blotter/israeli-airline-missile-defenses-israel-us-carriers-wont/story?id=24684650

France24, 'Russian Plane that Crashed in Egypt 'Broke up in Air', 1 November 2015. Available at: https://www.france24.com/en/20151101-russian-plane-crash-sinai-egypt-broke-air-says-aviation-official

Hiiraan Online, 'Committee: 587 Dead in Oct 14 Terror Attack', 5 March 2018. Available at: https://hiiraan.com/news4/2018/Mar/157047/committee_587_dead_in_oct_14_terror_attack.aspx

Howden, D., 'Terror in Nairobi: the full story behind al-Shabaab's mall attack', *The Guardian*, 3 October 2012. Available at: https://www.theguardian.com/world/2013/oct/04/westgate-mall-attacks-kenya

Howell, L.D., *The Handbook of Country and Political Risk Analysis*, New York: The Political Risk Services Group, 1998.

Hudson, B., 'Drone Attacks are Essentially Terrorism by Joystick', *Washington Post*, 5 August 2018. Available at: https://www.washingtonpost.com/opinions/drone-attacks-are-essentially-terrorism-by-joystick/2018/08/05/f93ec18a-98d5-11e8-843b-36e177f3081c_story.html?utm_term=.44fab7a35c53

Hunsicker, A., *Understanding International Counter Terrorism: A Professional's Guide to the Operational Art*, Boca Raton: Universal Publishers, 2006.

Jansen, B., 'Aviation Experts: Small Explosives Cause Big Damage in Planes', *USA Today*, 18 November 2015. Available at: https://www.usatoday.com/story/news/2015/11/18/aviation-experts-small-explosives-cause-big-damage-planes/76014432/

Jihadology, 'New Video Message from The Islamic State: "Knights of the Departments – Wilāyat Nīnawā"', 24 January 2017. Available at: https://jihadology.net/2017/01/24/new-video-message-from-the-islamic-state-knights-of-the-departments-wilayat-ninawa/

Jihadology, 'New Video Message from The Islamic State: "Roar of the Lions – Wilāyat al-Furāt"', 30 January 2017. Available at: https://jihadology.net/2017/01/30/new-video-message-from-the-islamic-state-roar-of-the-lions-wilayat-al-furat/

Jones, S., 'Proactive vs Reactive Risk Management Strategies', *Reciprocity*, 20 February 2020. Available at:

DOI: 10.19165/2020.6.0128

https://reciprocitylabs.com/proactive-vs-reactive-risk-management-strategies/

Kassa, S.G., 'IT Asset Valuation, Risk Assessment and Control Implementation Model', *ISACA Journal*, Vol 3, 1 May 2017. Available at: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/it-asset-valuation-risk-assessment-and-control-implementation-model

Knight, W., ''Incompetence' saved rocket-attack airliner', *New Scientist*, 29 November 2002. Available at: https://www.newscientist.com/article/dn3127-incompetence-saved-rocket-attack-airliner/

Larson, G.C., 'How Things Work: Cabin Pressure', *Air and Space Magazine*, January 2002. Available at: https://www.airspacemag.com/flight-today/how-things-work-cabin-pressure-2870604/

Laville, S., 'Five Key Questions for Anti-Terror Investigation', *The Guardian*, 19 August 2006. Available at: https://www.theguardian.com/uk/2006/aug/19/terrorism.world

Literary Devices, *Symbolism*. Available at: https://literarydevices.net/symbolism/

Louw, P. E., *'The War Against Terrorism': A Public Relations Challenge for the Pentagon'*, *Gazette: The International Journal for Communication Studies* Vol 65(3), 2003, pp. 211–230 DOI:10.1177/0016549203065003001

MacAskill, E., *'Laptop Ban on Planes Came after Plot to put Explosives in iPad'*, *The Observer*, 26 March 2017. Available at: https://www.theguardian.com/world/2017/mar/26/plot-explosives-ipad-us-uk-laptop-ban

Martin, G., *Understanding Terrorism: Challenges, Perspectives, and Issues,* Thousand Oaks, Cal.: SAGE, 2006.

Mendonca, D. and Ellis R., 'British Airways Cancels Flights to Cairo for 7 Days; Lufthansa does the same, for 1 Day', CNN, 21 July 2019. Available at: https://edition.cnn.com/2019/07/20/world/british-airlines-lufthansa-cancel-flights-to-cairo/index.html

Morani, A., *'Al-Shabaab Militants Destroy Safaricom Mast, Overpower Officers'*, *Havisasa*, 8 August 2019. Available at: https://hivisasa.com/posts/30107553-al-shabaab-suspects-destroy-safaricom-mast-overpower-officers?source=latestHome

Moteff, J., Copeland, C. and Fischer, J., *Critical Infrastructures: What Makes an Infrastructure Critical?* Washington, DC: Congressional Research Service, 2003.

Moteff, J., and Parfomak, P., *Critical Infrastructure and Key Assets: Definition and Identification*, Washington, DC: Congressional Research Service, 2004.

NBC News, 'MH17: Why Commercial Jets Aren't Equipped to Avoid Missiles', 19 July 2014. Available at: https://www.nbcnews.com/storyline/ukraine-plane-crash/mh17-why-commercial-jets-arent-equipped-avoid-missiles-n159421

Nossiter, A., 'Bombs by Nigerian Insurgents Kill 8', *The New York Times*, 1 October 2010. Available at: https://www.nytimes.com/2010/10/02/world/africa/02nigeria.html

Rassler, D. al`Ubaydi, M and Mironova, V., 'The Islamic State's Drone Documents: Management, Acquisitions, and DIY Tradecraft', Combating Terrorism Center at West Point, 31 January 2017. Available at: https://www.ctc.usma.edu/posts/ctc-perspectives-the-islamic-states-drone-documents-management-acquisitions-and-diy-tradecraft

Renfroe, N.A., and Smith, J.L., *Threat / Vulnerability Assessments and Risk Analysis*, Whole Building Design Guide, 8 August 2016. Available at: https://www.wbdg.org/resources/threat-vulnerability-assessments-and-risk-analysis

Rumiyah, Issue 2, 4 October 2016. Available at: http://clarionproject.org/wp-content/uploads/Rumiyh-ISIS-Magazine-2nd-issue.pdf

DOI: 10.19165/2020.6.0128

Rumiyah, Issue 5, 6 January 2017. Available at: http://clarionproject.org/wp-content/uploads/2014/09/Rumiyah-ISIS-Magazine-5th-issue.pdf

Rumiyah, Issue 9, 4 May 2017, p. 46-51. Available at: https://qb5cc3pam3y2ad0tm1zxuhho-wpengine.netdna-ssl.com/wp-content/uploads/2017/05/Rumiyah-9.pdf

Sample, I., *'PETN – 'Hard to Detect and just 100g can Destroy a Car'*, *The Guardian*, 27 December 2009. Available at: https://www.theguardian.com/world/2009/dec/27/petn-pentaerythritol-trinitrate-explosive

Schmid, Alex P., 'Terrorism: The definitional problem,' *Case Western Reserve University School of Law*, Vol 36(375), 2004.

Schwaninger, Adrian and Merks, Sarah, *'Single-View, Multi-View and 3D Imaging for Baggage Screening: What should be considered for effective training?' Aviation Security International,* 19 February 2019. Available at: https://www.asi-mag.com/single-view-multi-view-and-3d-imaging-for-baggage-screening-what-should-be-considered-for-effective-training/

Sciolino, E., 'Bombings in Madrid: The Attack; 10 Bombs Shatter Trains in Madrid, Killing 192,' *New York Times*, 12 March 2004. Available at: https://www.nytimes.com/2004/03/12/world/bombings-in-madrid-the-attack-10-bombs-shatter-trains-in-madrid-killing-192.html

Shane, S., 'Inside Al Qaeda's Plot to Blow Up an American Airliner', *The New York Times*, 22 February 2017. Available at: https://www.nytimes.com/2017/02/22/us/politics/anwar-awlaki-underwear-bomber-abdulmutallab.html?rref=collection%2Ftimestopic%2FAbdulmutallab%2C%20Umar%20Farouk&action=click&contentCollection=timestopics&region=stream&module=stream_unit&version=latest&contentPlacement=2&pgtype=collection

United Nations, *The Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, 1971 ('Montreal Convention').* Available at: https://treaties.un.org/doc/Publication/UNTS/Volume%20974/volume-974-I-14118-English.pdf

United Nations, *Protocol on the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, 1988.* Available at: https://www.un.org/ruleoflaw/blog/document/protocol-on-the-suppression-of-unlawful-acts-of-violence-at-airports-serving-international-civil-aviation-supplementary-to-the-convention-for-the-suppression-of-unlawful-acts-against-the-safety-of-civ/

United Nations, *International Convention for the Suppression of Terrorist* Bombings, New York, 15 December 1997. Available at: https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-9&chapter=18&clang=_en

United Nations, *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation*, Beijing, 10 September 2010. Available at: https://cil.nus.edu.sg/wp-content/uploads/2017/08/2010-Convention-on-the-Suppression-of-Unlawful-Acts-Relating-to-International-Civil-Aviation-1.pdf

Zio, E., 'Critical infrastructures vulnerability and risk analysis', *European Journal for Security Research*, Vol 1(2), 2016, 97-114; DOI: 10.1007/s41125-016-0004-2

DOI: 10.19165/2020.6.0128

Web-Based Resources

Clarion Project, Islamic State's (ISIS, ISIL) Magazines. Available at: https://clarionproject.org/islamic-state-isis-isil-propaganda-magazine-dabiq-50/

Jihadology, a clearing house for Jihadi source material. Available at: https://jihadology.net/

National Consortium for the Study of Terrorism and Responses to Terrorism: Global Terrorism Database, University of Maryland. Available at: https://www.start.umd.edu/gtd/

The Quality Infrastructure Investment Database, An initiative of the G20 under the 2019 Japanese Presidency, in collaboration with the Global Infrastructure Hub, the OECD and the World Bank. Available at: https://www.gihub.org/quality-infrastructure-database/

US Homeland Security, Critical Infrastructure Security. Available at: https://www.dhs.gov/topic/critical-infrastructure-security

DOI: 10.19165/2020.6.0128