Transactions of the VSB - Technical University of Ostrava Vol. XV, No. 1, 2020
Safety Engineering Series, ISSN 1805-3238 pp. 22-37, DOI 10.35182/tses-2020-0004

PRE-TERRORIST ATTACK INDICATION RELATED TO ELECTRICITY CRITICAL INFRASTRUCTURE: A 'RED CELL' VIEW

David BIRKETT[1]

Research article

Abstract: This paper identifies, examines, and analyses the variable intricacies and the most significant vulnerability from potential future acts of terrorism, related to the electricity sector grids of Europe's Power Grid. More specifically this paper illustrates a 'Red Cell' View from the external terrorist targeting tactics and behavioural strategies when planning an attack on Electricity Critical Infrastructure (ECI). This unique research additionally identifies potential future initiatives and opportunities, which may enhance and provide increased protective resilience, to European ECI, against this form of external adverse human intervention, prior to any potential future terrorist attack.

Keywords: Critical infrastructure, Business continuity, Terrorism, Security, Electricity.

Introduction

A 'Red Cell' Analysis is identified by the Pentagon, USA as:

"Red teams and red teaming processes have long been used as tools by the management of both government and commercial enterprises. Their purpose is to reduce an enterprise's risks and increase its opportunities……. Red teams are established by an enterprise to challenge aspects of that very enterprise's plans, programs, assumptions, etc." (DSB, 2003).

And further as the British Department of Defence suggests:

"The idea of using red teams has been around for a long time. Commercial enterprises, such as IBM, and government agencies such as Defence Intelligence and the Central Intelligence Agency, have long used them to reduce risks and to improve their problem solving" (Shape, 2013).

This paper "Red Cell"[1] analyses and examines the potential future terrorist attack cycle in relation to the electricity sectors of European identified Electricity Critical Infrastructure (ECI). This examination views from an external targeting perspective from outside the grid, as a terrorist would grade a potential target. This form of assessment may well further identify potential vulnerabilities and security gaps that may be identified indicators in the terrorist pre-planning process related to ECI, prior to any potential future terrorist attack.

The main focus of this paper is that as security has tightened on airlines, transport, and other popular targets, the future target shift and displacement effect observed in transnational terrorism may well be directed at a significant public utility, such as ECI. Should this occur, a greater number of people will be affected in European society, which may operationally, economically and socially cripple European financial hubs?

The discussion within this paper presents constructive lines of thought to support this paradigm, with an explanation of how the European electricity industry model operates.

The protection of crucial ECI systems is of significant importance in verifying the continuity of electricity, to assure the continual daily operation of the social and economic function of society (Bompard et al., 2009). In the twenty first century our European society is also significantly and increasingly dependent on Electricity, which is considered as one of the most interdependent sectors of CI relative to the other 10 CI sectors.

[1] Red teaming is also the independent application of a range of structured, creative and critical thinking techniques, as a terrorist would view the infrastructure from the outside looking in, to assist the end user make a better informed decision, or produce a more robust product and increase protection of the infrastructure.

[1] Mettle Crisis Leaders, Perth, Australia, dbirkett@crisisleaders.com

Safety Engineering Series, ISSN 1805-3238 pp. 22-37, DOI 10.35182/tses-2020-0004

Current Electricity Initiatives in the European Union

The European Transmission Network, under the control of the European Union (EU), has issued a 'Planning Road Map' in June 2020, which outlines the future planning of the Generation & Transmission networks with an overview of the European gas system which now supplies most Electricity Generation, apart from Nuclear Power Stations[2]. Gazprom, the Russian gas corporation, supplies EU countries such as Bulgaria, Serbia and Hungary via the Turk Stream pipeline system. Nordstream 2, which is predicted to be functional by the end of 2020, is again managed by Gazprom and will supply Germany & the Czech Republic (IEA, 2020). The Gas Grid in Europe is also becoming more significant in 2020, due to industrial requirements, heating and many other uses.

The movement towards gas in lieu of coal for Power Station operation potentially elevates the risk issue of gas supply from governments' political and strategic moves to restrict or cut supply to individual countries. This now accentuates gas for generation, with the new accent on clean energy. Furthermore, terrorist attacks on the gas network may also be considered, which will impact the generation of electricity.

An EU expert group on electricity interconnection has extended its mandate to 2030, to extend the electricity grid interconnections further across Europe and some neighbouring countries. The primary objective is to implement eighty two additional Transmission interconnections across borders within the EU, and ten neighbouring countries, affecting twenty two border crossings. The advantages of this initiative is to enhance the security of supply and reduce electricity costs across the EU positively impacting some neighbouring countries (such as the Western Balkans; Ukraine and Moldovia) (European Union, 2019). However, this future action may well increase the risk exposure, in creating additional transmission interconnection nodes which may well be a target of future terrorist attacks. Of specific interest the 2020 EU Energy Policy Review, under Electricity Security, addresses the security issues of load balancing control and continuity of supply between EU countries, but fails to address the rising security issues of the ECI grid system interruption from acts of terrorism with the gas grid becoming a higher risk issue, such as 'Turkstream' and the impending 'Nordstream 2' pipelines systems.

[2] In January 2010, 14 out of 27 countries in Europe have Nuclear Reactors. https://en.wikipedia.org/wiki/Nuclear_power_in_the_European_Union#:~:text=The%20countries%20with%20reactors%20are,Sweden%2C%20and%20the%20United%20Kingdom.

European Electricity and Terrorism

As discussed, Electricity is one of the most highly interdependent nodes of European identified Critical Infrastructure sectors. A significant terrorist attack on ECI may potentially damage areas of the EU economies, and create a high degree of fear and panic across the European population due to the increasing social and economic dependency of the public, industry and commerce on ECI.

In addition, Ackerman et al. (2007) suggest that there appears to be a deficit of intellectual analysis related to terrorist attack methodologies on critical infrastructure, on a global basis. Indeed, Ackerman et al. (2007) advise that a literature review confirms that there is a research deficiency regarding methodologies and terrorist target section of critical infrastructure, currently sourced from publicly accessible domains. Indeed, Ackerman et al. (2007) in their comprehensive review further clarify:

"The review confirmed initial expectations that little to no existing work focuses specifically on the reasons why terrorists choose to attack critical infrastructure targets. Surprisingly, the review also revealed a paucity of material regarding the more general process of target selection by terrorist groups".

The electric power transmission and distribution system across various countries has been identified by Davidson (Davidson, 2010) as the largest geographic engineering system in the world. Furthermore the concept of electricity systems on a global basis is claimed by the United States of America National Academy of Engineering to be the world's largest integrated machine, and is part of the most significant engineering achievement of the 20th Century (NRCNA, 2012). The interdependent significance of electricity is highlighted by Robinson (Robinson et al., 1998) that the affects and frequency of ECI failures is increasing over time from all-hazard incidents due to the ECI systems becoming increasingly interlinked and interdependent due to modern technology with associated supply chain failures.

As indicated in Fig. 1, Electricity is generated in Power Stations, often at between 20,000 to 66,000 Volts, which is then boosted to a higher voltage for transmission via a Transmission Line, often over long distances. The High voltage is then stepped down within a Transmission Substation to a Distribution

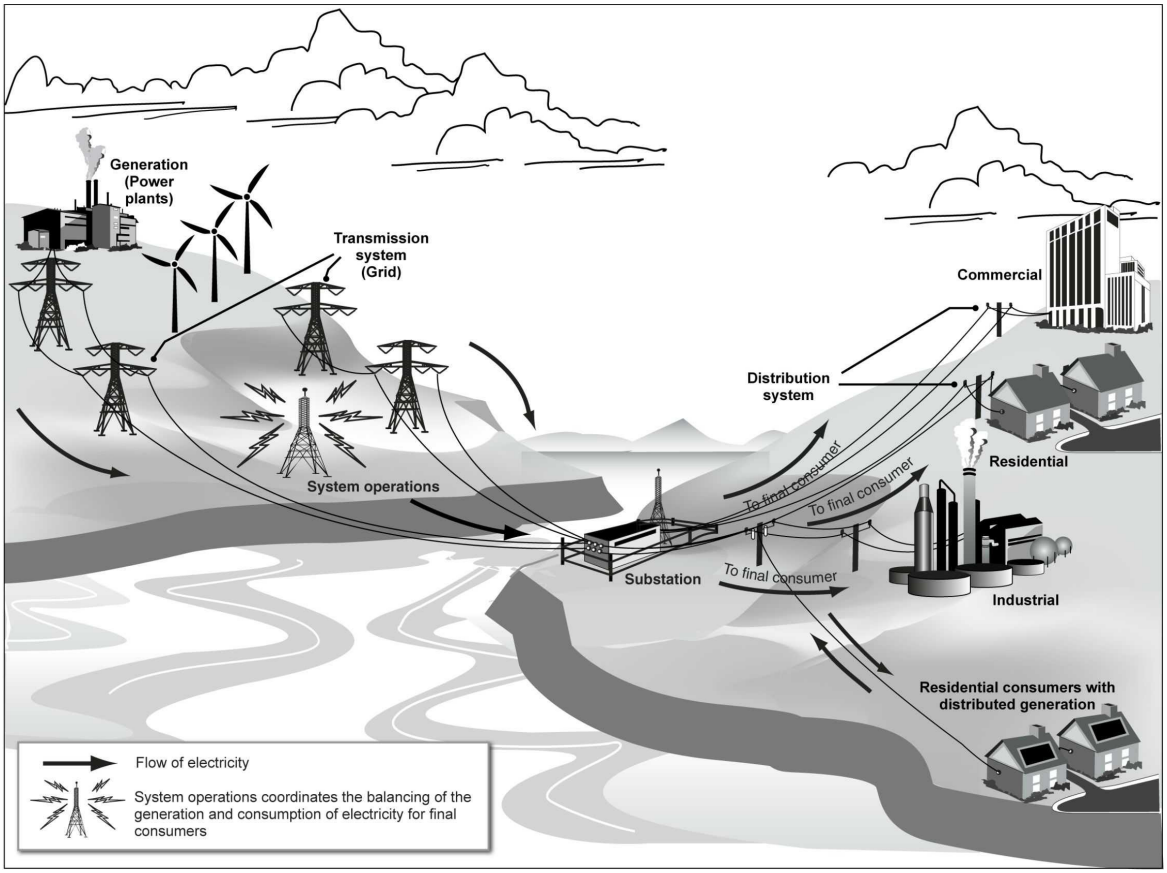


Fig. 1 Illustration of the Electricity Grid System flow from Generation to the Consumer (Rusco, 2017)

Voltage (often 22,000 Volts), which is then lowered to 400 volts and 220 volts for distribution supplies to industrial, business, agricultural and residential consumers.

Electricity grids, with merges, privatisation in general, reflect a perceived movement away from the management of electricity by government. This is especially the case on a global basis, where the Electricity industry has been broken up and segmented into private Generation companies, Transmission entities and Distribution management organisations (refer to Fig. 1). This has been conducted to change the previously vertically integrated utilities to encourage competition and initiate potential financial savings to the consumer (NRCNA, 2012).

The electricity is controlled, as indicated, by system operations and usually by the use of SCADA[3] (Krutz, 2006) for remote and centralised internet computer control systems.

As discussed, from the Power Station, the generated electricity is boosted up to a higher transmission voltage in the Power Station switchyard, to reduce the power losses that will occur over large distances, as is evidently quite frequent across large geographic areas in Europe. This is in consideration of the large distances between the generating source and the consumer (Gray, 1980). Within the European electricity system there are multiple sources of interconnected electricity generation stations across countries within the EU, which tends to reduce the criticality of generation as a 'single point of failure' (SPOF). Subsequently, in consideration of the increasing European dependency on these two essential systems, the electricity grid, as a terrorist target could well be the future selected European 'target of choice' by organised transnational terrorist groups, with a potential to significantly socially, and economically, impact European society. This potential movement in targets may well reflect a more intelligent 'historical generational change' within terrorist groups over time.

[3] SCADA is a model-driven electrical SCADA platform that provides a real-time monitoring and control software applications integrated with data acquisition and control hardware to offer intuitive visualization and analyses via intelligent graphical user interface, one-line diagram, geospatial view, and digital dashboards.

Terrorism in Europe: Strategies and Planning

Terrorists measure the success of an attack by the extent of media reporting; the expenditure required to carry out the attack and the costs and time of reinstatement of the infrastructure or location, such as is typically described in Fig. 2, in the 'CARVER' Terrorist planning model:

Score	Criticality	Accessibility	Recoverability	Vulnerability	Effect on Populace	Recognisability
5	Needed for survival	Public	Difficult	Unable to harden	Mass casualties: high symbolism	Unique
4	Needed for economic	Government or political process recognisable	Admission criteria	One year or more	Can be hardened	Deaths occur; symbolism to some
3	Disruption severe	Screening	One month to one year	Hardened for natural disasters	Injuries; symbolism important	Moderate difficulty to identify
2	Disruption moderate	Inspection of packages	One week	Hardened against snipers and attacks	Major injuries; undetermined symbolism	Very difficult to identify
1	Disruption light	Escort needed	Less than seven days	Hardened against bombs	Minor injuries; not symbolic	Indistinguishable from surroundings

Fig. 2 CARVER Terrorist Planning Guide (Birkett et al., 2011)

terrorist groups in infrastructure target assessments[4] (Miller, 2015; Schnaubelt et al., 2014). Terrorists assess a target's 'value' with a high numerical rating on the Carver Matrix (Fig. 2).

Designated points within the planning cycle are where terrorism-related behavior can be most readily observed as vulnerabilities in the terrorist attack cycle. Indeed, Toben, extends this discussion further (Toben, 2013) suggesting that examinations of the process, observed in most successful terrorist attacks, may be translated and applied as a preventative measure to disrupt future attacks. The American California example will be examined within this paper to seek to confirm this concept, in consideration of the context of the suggested commonality and synergy within elements of terrorist targeting. Romyn et al. (2013) further suggest that there are two areas of terrorist attack prevention: the detection

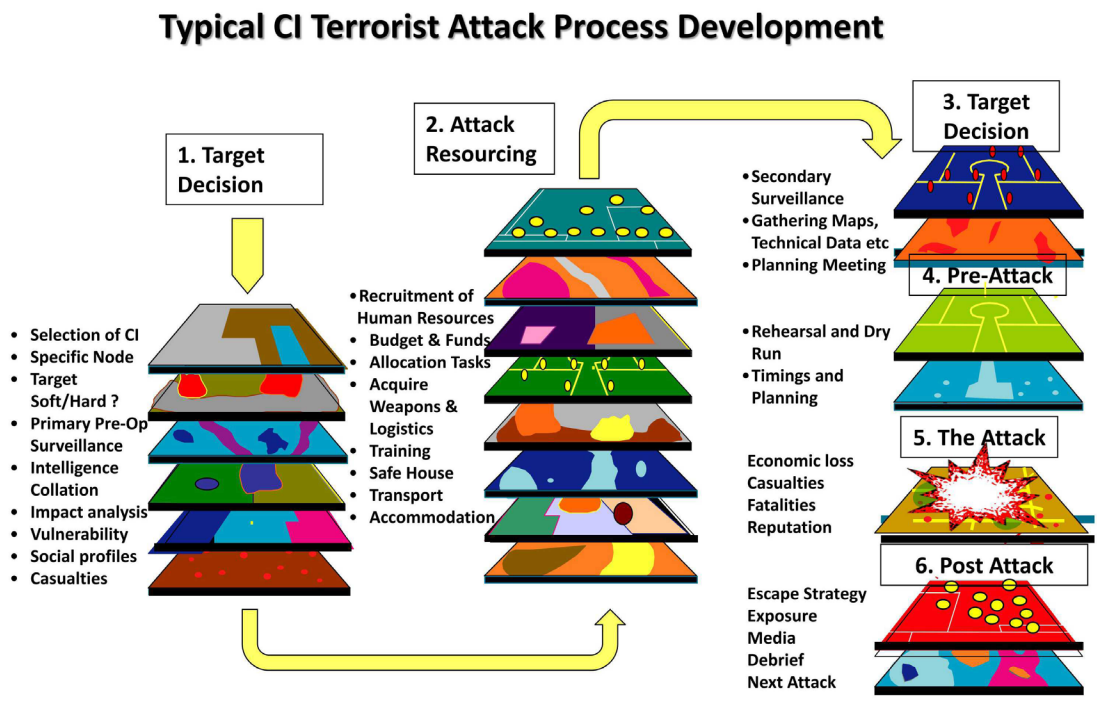


Fig. 3 Systematic Activities Conducted by a Terrorist Group against CI during Attack Process

The 'CARVER' matrix, which originates from the U.S. Special Forces in the 1950's to support U.S. national objectives in South America, identifies soft and critical nodes in critical infrastructure as specific targets. This methodology is now applied by various

[4] CARVER is an acronym that stands for 'Criticality, Accessibility, Recoverability, Vulnerability, Effect and Recognisability'. CARVER is used to extend success, in order to succeed in an attack on CI. (https://redteams.net/redteaming/2013/using-carver-to-identify-risks-and-vulnerabilities).

of terrorists before they are able to carry out an attack; and predicting likely attractive targets for a terrorist attack on ECI. However, as discussed, the topic of terrorist targeting is considered somewhat neglected, despite the vast amount of research and literature related to terrorist attacks (Toft et al., 2010).

As indicated in Fig. 3, the illustrated eidetic representation of the typical terrorist attack activity development against ECI indicates the pre-operative stage, where the selection of which specific target occurs, with considerations of the levels of security and protection at the facility. Terrorists generally appear to select a 'soft' target, in lieu of a hard target to maximise the success of the attack. With the collation of such inputs as the pre-operative surveillance, relevant intelligence and the vulnerability, a decision is made by a planning group of varying sizes dependent on the size and complexity of the attack. Resources are then acquired from the funds and budget of the attack cost estimate. Amongst the resources are contingencies for weapons, training, accommodation, safe house, logistics and storage and transport. The final confirmation of the target is generally made subsequent to inputs from secondary surveillance, gathering of target specific data, a rehearsal and dry run with timings and escape contingencies. The attack may result in economic losses for the infrastructure owners, some potential reputational damage, and possible casualties. After the attack there would be an escape strategy, considerable media exposure which is monitored by the terrorists as the oxygen for further attacks. A debrief, further recruitment, and planning for the next attack then progressively occurs. Developed criteria, based on the understanding of the terrorist attack process, will add to the ECI industry sector protection and hardening from any future act of terrorism. Recent examples of significant planning include the Paris attacks of 2015, where 137 people were killed and 416 injured, and also the 6 location attacks in 2020[5], Vienna, where 4 civilians and one attacker were killed, with many wounded, on the evening of 02.11.2020[6].

Drake (1998) advises that there four primary aspects to evaluate when considering the potential for terrorist attack, which is particularly relevant in relation to potential attacks on ECI. These aspects are:

- Ideology of the particular Group;
- The Strategy behind the attack;
- The motivation of the Group;
- The purpose of the attack.

The ideology of a terrorist group provides a foundation for the motive, and is a means by which a terrorist group defines its political identity to provide some internal and external justification or rationale for its actions. Drake further expands the ideological perspective by illustration of the meaning, within a terrorist's interpretation and perspective, that ideology provides a terrorist group with beliefs, values, principles and objectives, however unrecognised or rejected by others outside of the group (Drake, 1998).

Dependant on the strength of belief of the terrorist ideology, a more significant affect is the tendency to dehumanise and transform the perception of the human being into objects or representative symbols, thereby transforming the target into a perception easier for the terrorist palate to digest for the potential future maiming, murder or disfigurement of victims of any potential attack.

Indeed, Combs highlights the 'propaganda of the deed' attributed to early revolutionaries such as Morozov, to attain successful revolution with the use of non-selective violence to initiate social and political change in czarist Russia (Combs, 1997). This rationalisation and the promotion of the imagery of violence within the broad modern spectrum of terrorism appears to have extended the ideology to provide credence and justification to support the type of terrorist attack, whatever it may be.

A sample example of a transnational terrorist group's CI ideological view in declaring its political identity in justifying extreme actions is demonstrated by the 'Earth Liberation Front' (ELF) whose ideological issues are closely allied with their perspective on an ecological basis to preserve the environment and save the planet utilising extreme action[7]. Whilst not specifically targeting Electricity utilities, the ELF has engaged in violent acts on a global basis (Beering, 2002), and did target the CEO of the Hazelwood Power Station (Victoria, Australia) in March 2006 with a threat of violence against the CEO unless Hazelwood coal fired Power Station was closed (Buttler, 2009).

5 https://www.bbc.com/news/world-europe-34818994

6 https://www.theguardian.com/world/2020/nov/03/vienna-shooting-what-we-know-so-far-about-the-attack?CMP=fb_gu&utm_medium=Social&utm_source=Facebook&fbclid=IwAR3Hs2JHQBEWUPBOczB0MA0aqnREoDQvznyj3lzlsaSbB1ZUG4AsfLF1nOM#Echobox=1604361131

7 http://earth-liberation-front.com/

Bennett suggests that the ideology of a terrorist group is intrinsically linked to the motivational aspects of the group (Bennett, 2007). An example of this is the Islamic Fundamentalist terrorist motivation of religion, with a further illustration, where Osama bin Laden (OBL) issued his first 'fatwa'[8] to provide some justification and 'credibility' in the perceptions of Islamic fundamentalists and followers of Islam. This first Fatwa was a declaration of war against the Americans occupying the land of the two holy places and was issued in August 1966 (Bennett, 2007). Bennett considers further that OBL[9] was concerned that the incremental presence and occupation of areas of the Islamic Gulf States was a major threat to the legitimate owners of the world's largest oil reserves. This example links the ideology into a practical example of how terrorist statements translate and loom through the media amplification fog, into a more tangible and clear understanding, to encourage public support for their actions.

Drake claims that a terrorist group's ideology is an extremely important consideration in determining target selection (Drake, 1998). It defines how the group perceive the world around them, reflecting a certain degree of cognitive dissonance, dependent on the ideological strength and belief in the terrorist group cause. Thus when a group takes the decision to apply violence in their actions and activities, a primary consideration is to determine who or what is attacked. The ideology of the group then identifies the main attack focus, dependent on how the selected target 'scores' against how the target is perceived against the ideological direction of the group. Some targets then become increasingly 'legitimised' as being attacked to disenfranchise the perceived and identified enemy.

As indicated by Drake (1998), Lee (2009) and Stewart (2012), there is a pattern of planning and process adopted by all terrorists. Whether the 1970's models of left wing terrorism, such as the Red Brigades in Italy, the Irish Republican Army or the Baader Mienhoff cell in Germany, or the more modern Islamic Fundamentalists such as al-Qaeda and al Shabaab. These terrorist groups all appear to adopt and exhibit defined planning procedures with some commonalities (Lee, 2009).

An outcome of recent Australian research conducted by Romyn et al. (2013) indicated that those planning a terrorist attack concern themselves primarily with target selection prior to the selection of weapons. Romyn et al. (2013) further advise that attributes typical of 'occupied, easy, vital, iconic and destructible' are considered to be of greater importance than how exposed or the proximity of a potential target.

However, post analysis of successful terrorist attacks indicates that terrorists are often ruthless, relentless, patient (with some attack planning occurring over a period of years), opportunistic and flexible. They have learned from their exposure and experience and have modified their processes, operational tactics and targeting strategies with consideration of counter measures and target hardening (Bennett, 2007).

The successful global terrorist incidents have involved considerable planning, training and resources to achieve the level of success they seek. Although Michaelson argues that al-Qaeda, Jemaah Islamiyah and home-grown terrorists pose minimal threat to the Western Society (Michaelsen, 2010), there is always the possibility of an attack on critical infrastructure, in proportion to Europe's international political stance on many security issues as an international community member.

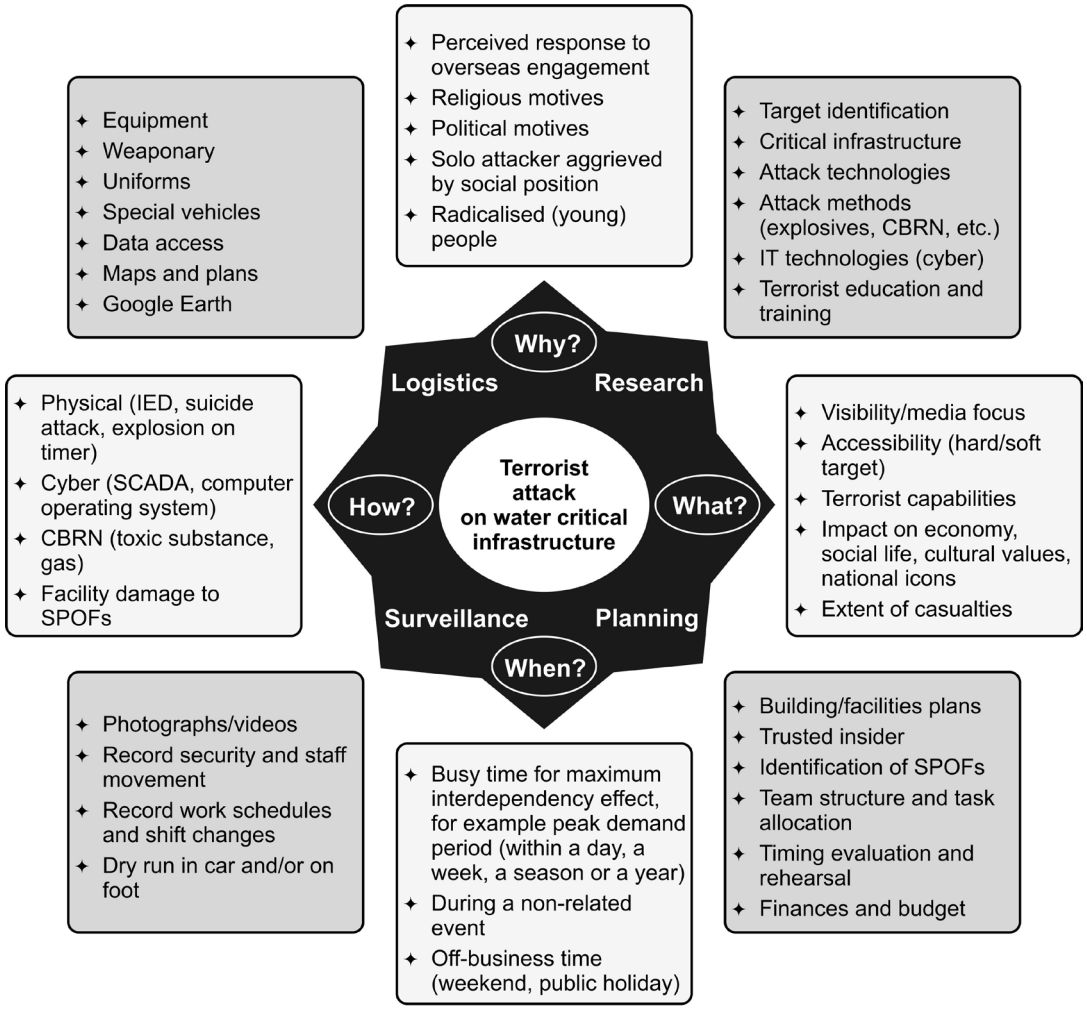
There are many varying groups with differing agendas from the ecological (examples are Earth Liberation Front - ELF and Campaign against Nuclear Energy - CANE) to the Islamic Fundamentalist (examples are al-Qaeda - AQAP[10] and Jemaah Islamiyah - JI). There is also the rise of right wing nationalist groups to consider (such as the Norwegian 'Sons of Odin' and the USA 'Montana Freemen'), with anti-abortionist, animal protection and anti-immigration lobbyists.

The observed shifting continuum, of significant 'high visibility' terrorist attacks often appears one step in front of intelligence analysts and predictive ability by Western Intelligence agencies and law enforcement groups. This is as distinct from the many successes, such as in Germany, France, the UK and USA, achieved by cohesive team work between State law enforcement and Intelligence Agencies.

[8] An Islamic legal pronouncement issued by a religious law specialist, concerning a specific issue. Bennett, B. T. 2007. Understanding, Assessing and Responding to Terrorism - Protecting Critical Infrastructure and Personnel. New Jersey, USA: John Wiley & Sons. ISBN 978-0-471-77152-4.

[9] Osama bin Laden.

[10] Al Qaeda in the **Arabian Peninsula** (AQAP) is a Sunni terrorist organization. (https://cisac.fsi.stanford.edu/mappingmilitants/profiles/al-qaeda-arabian-peninsula).



LEGEND: CBRN = chemical, biological, radiological, nuclear; IED = improvised explosive device; IT = information technology; SCADA = supervisory control and data acquisition; SPOF = single point of failure

Fig. 4 Potential Future ECI Terrorist Planning Considerations (Birkett, 2017)

Observed international attacks are illustrated by the New York 9/11 attacks, to the London, Moscow, Bali, Jakarta, Mumbai and Madrid transport and Mass Gathering attacks, and to the 2016 Algerian Statoil Gas Plant attack (Statoil, 2013). The elimination of OBL has not ceased the threat as the Jihadist ideology is continuing on a global basis, with other fundamentalists gravitating upwards to seize command and control. Organisations similar to Al-Shabaab in Somalia, and Boko Haram in Nigeria, appear to be competing for international media space for media amplification of the cause and their ambitions

The above diagrammatic representation (Fig. 4) of the perceived elements of a terrorist planning process, although illustrative, may be applied to any attack on critical infrastructure across all defined areas.

The planning process conforms to the motivation and long term ideological vision of the group. In consideration of these planning considerations, a strategic, ideological and tactical objective is developed. In adopting the military questions of 'Why, What, When, and How', Fig. 4 is divided into the terrorist strategic and tactical areas of Logistics, Research, Surveillance and Planning. The diagram encapsulates a wide variety of significant planning nodes prior to an attack, which in practice, a terrorist group may apply some, most, or all features displayed to effectively enable a successful attack. When the activities related to each function in the diagram are considered, opportunities exist to capture some awareness of the pre-planning activities and behaviors, to alert ECI owners prior to the incident occurring. For example, the gathering of data, maps, staff timings and physical surveillance if observed and noted, may provide an image indicator related to a pre-attack behavioral alert.

Safety Engineering Series, ISSN 1805-3238 pp. 22-37, DOI 10.35182/tses-2020-0004

Terrorism and associated interdependency attacks should be of ongoing concern to all 21st Century critical infrastructure owners and operators. Consequently, there is a defined planning process prior to an attack, which may be analysed and understood by alert staff, with preventative measures taken to prevent terrorist acts, and to mitigate the effects of attacks. It should be considered that the most significant concept to understand, regarding potential Critical infrastructure attacks, is that attacks do not appear out of 'the ether', without the presence of pre-incident indicators (Stewart, 2012). Individuals planning a terrorist attack follow the previously mentioned established and defined cycle (refer to Fig. 3). This cycle and the behaviors linked to it can be identified should the educated observer be alert to identify indicative and unnatural occurrences. Alert, early identification and recognition of terrorism related behavior may be observed and identified as potential vulnerabilities in the terrorist attack cycle (Stewart, 2012).

Terrorist strategy is considered by Howard to be the plan by which a terrorist group seeks to deploy and use its logistics and resources to achieve its political objectives (Howard, 1984). In practical terms this is the 'Why, What, When and How', as illustrated in Fig. 4.

The 9/11 major terrorist incidents in the United States of America have produced a global defining point in modern history relative to the interpretation and context of 21st Century non-state asymmetrical warfare. Researchers, such as Bennett, claim that September 11th 2001 is now identified as a 'watershed moment' in the United States of America's history, and possibly of generationally associated significance, in comparison with the Japanese attacks on Pearl Harbour in Hawaii during World War II (Bennett, 2007). Global terrorist attacks from 2001 to 2020 appear to again be seeking increasingly more significant targets, such as London, Madrid, Paris and Moscow with higher victim death counts.

New essential security concepts have had significant impacts into personal accountability and privacy, with the previous terrorist target focus on public transportation and significant target identification involving large groups of people, such as London[11] (Jenkins et al., 2012), Paris (CNN, 2020), Madrid[12] (Martí et al., 2006), Belgium (Fakude, 2016) and Moscow[13] (Gupta, 2011). These attacks appeared to have reflected a modern 21st century target objective of killing and injuring a maximum number of people, in lieu of a previously more strategic objective.

Despite the loss of land based gains in Syria, ISIS or ISIL, has progressed globally, utilising clever internet communication to 'cyber' recruit and inspire others, with 143 attacks in 29 countries other than Syria and Iraq, with 2,043 people killed (Lister et al., 2017).

The increase in airline security, which was the previous popular target from the 1970s, involving airline hijacking and bombing, has tended to 'harden' the target creating a shift in target focus. This appears to have created a visible 'displacement' effect, shifting the recent terrorist target focus to subways, buses, trains, transport terminals and places of public mass gatherings, due to the necessary freedom of movement in these locations. Transport hubs and feeders are still a popular terrorist target due to freedom of access, and high concentrations of people (Jenkins et al., 2012). However, with an increase in security, involving the installation of high resolution CCTV, more accurate identification of passengers, elevated scanning of luggage and passengers; it has become increasingly more difficult for any aspiring terrorist to effectively plan and conduct a terrorist operation within transport hubs.

There is a distinct advantage for the target seeking terrorist seeking to attack CI 'soft targets'. The soft targets as distinct from hard targets are those which the business owners risk analysis process outcome results in a lower level of security (physical and cyber). The advantage for the terrorist is that they can observe and identify, in their own time the progressive and variable hardening of various CI to identify, decide and select on which area of CI, and when to attack (Brandt, 2009).

There has been an indicative synchronous movement in target selection by terrorists from the suggested genesis of modern State sponsored terrorism (Brandt, 2009), indicated with the November 4th 1979 capture of 52 U.S. hostages from the U.S. Embassy in Tehran, to the current cellular transnational profile of groups such as al Qaeda, ISIL and Boko Harem. As indicated, there has

[11] London Rail Tube poison gas plots 2002 & 2004 (unsuccessful); London Rail Tube & Bus bombings July 7th 2005 (52 people killed) and similar attempted London Rail & Bus bombings July 21st 2005 (unsuccessful).

[12] The Madrid Rail System bombings March 11th 2004, where 191 passengers were killed and 2,000 injured.

[13] Moscow 2004 suicide bombing of train between the Avtozavoskaya and the Paveletskaya stations, which resulted in 39 killed and over 100 injured. Attack by Chechen Terrorist Group Gazoton Murdash. Also, Moscow 2010 suicide bombings (2) at Lubyanka station and at Park Kultury station resulted in 40 deaths and over 100 injured.

been an escalating introduction of metal detectors, screening devices and more intrusive security at airports with increased application and monitoring of CCTV cameras and high technology devices at transport locations, shopping centres and inner cities locations. The introduction of this technology appears to be as a reaction to increased perceptions of vulnerability, subsequent to enhanced business and military defence measures (Brandt, 2009).

Bennett (2007) illustrates the terrorist tactical attack process into a four stage progression:

1. The 'Initiation phase' selects a target (compatible with objectives and ideology); gathers relevant intelligence, data, plans and maps; conducts operational planning (with timings, rehearsals and 'dry runs); Recruits and trains teams and obtains defined logistics, and required supplies for the attack.
2. The 'Escalation phase' assembles and tests weapons and explosives; transports the trained recruits to the target area and executes the attack.
3. The 'De-Escalation phase' withdraws from the target area and the safe house.
4. The 'Termination phase' clears all loose ends and potential evidence associated with the attack; conducts a post attack review and commences planning for the next attack.

Although there are varying concepts by researchers in the terrorism discipline of exactly which planning process is adopted by terrorist groups, it is generally accepted that there is a process, and there are indicators of this planning occurring prior to any terrorist attack. As suggested, these indicators may be observed by the informed organisation, as a form of pre-warning of an impending attack, and if action is taken, may well either lead to the attack being aborted, or the terrorists apprehended prior to an attack occurring.

European Electricity System Vulnerabilities

Electricity Critical Infrastructure is considered by Farrell to be more vulnerable than other CI, such as gas and oil due to the fact that gas and oil can be stored, whereas electricity is generated and used, and not stored easily (Farrell et al., 2004).

Electricity has been significantly impacted by weather within an all-hazard category of failure, with Farrell highlighting the 1965 and 2003 New York blackouts from weather related incidents (Farrell et al., 2004). In the 1965 electricity outage, there was an observed general acceptance of the all night blackout affecting the 30 million inhabitants of New England Ontario and New York. This outage was an equipment failure, and Farrell claims that good communication from the utility led to an absence of widespread fear, panic and breakdown of public order. However, the 1977 New York blackout, although a smaller outage, illustrated a more troubling social response across the city. Widespread looting occurred, in conjunction with a general sense of community insecurity across New York and a documented corresponding increase in crime across the city for the duration of the outage (Farrell et al., 2004). It could be considered that the increase in community dependence on electricity with modern technological developments, and a level of cultural generational change may well provide some answers related to the community reactions between 1965 and 1977.

Terrorist attacks in Europe appear to be progressing as a significant issue related to risk and threat analysis. The 28 EU Countries have estimated that expenditure due to acts of terrorism between 2004 and 2016 was €180 Billion in terms of the Gross Domestic Product (GDP). The EU countries with the highest expenditure were the United Kingdom (€43.7 Billion); France (€43 Billion); Spain (€40.8 Billion) and Germany (€19.2 Billion). Furthermore there are additional estimates of the human and physical capital costs within this period of €5.6 Billion, which includes costs of homicides; losses of lifetime earnings and other ancillary costs (Rand Corporation, 2018a,b). The psychological effects on organisations, and members of the public who view and are affected by the incident, witnessing the incident, or viewing it on the internet need to be considered in assessing the social and emotive impact of terrorism

Although terrorist attacks in Europe have declined by 50 % since 2018, there were 191 terrorist attacks in Europe within the 12 month period 2018-2019 and 6,722 terrorist attacks on a global basis with 13,822 total deaths and 14,542 total injured (START National Consortium, 2020).

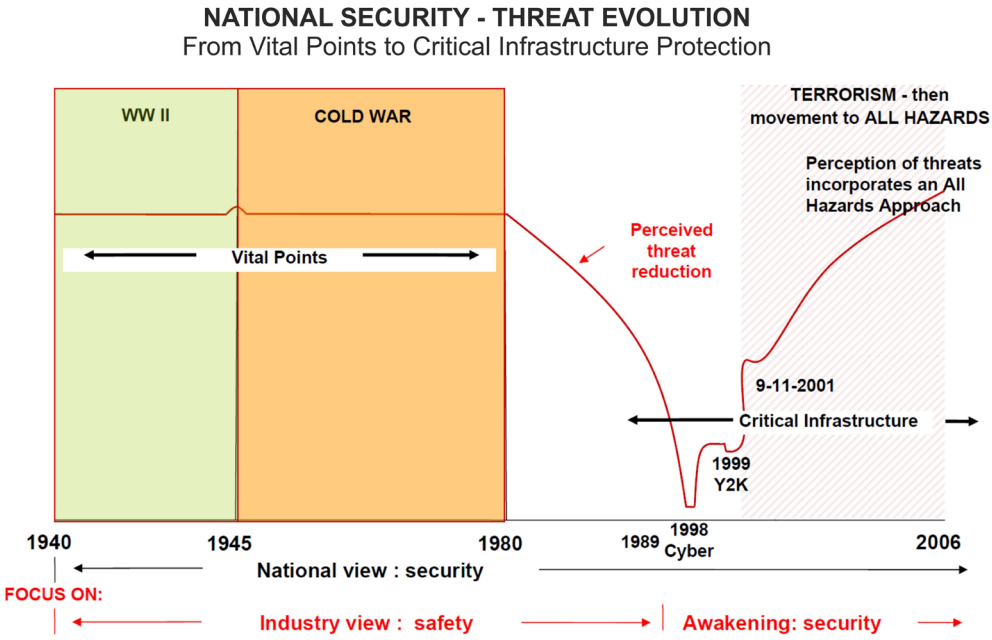


Fig. 5 Critical Infrastructure Threat Evolution 1940 to 2006 (Nelson et al., 2007)

As indicated in Fig. 5, a sequential evolving history of security in the workplace of Critical Infrastructure has occurred, from a focus on industrial safety, from 1940 to 1989, with a corresponding perceived threat reduction, progressing to a significant rise in threat levels in 2001. This is interpreted as a consequence from the Y2K[14] cyber threat, and also subsequent to the Jihadist aeroplane attacks in the U.S. On 11th September 2001 (9/11).

Furthermore, to support an evidence-based illustration of the identified terrorist pre-planning vulnerabilities, an incident is examined relating to an actual successful attack on ECI in the USA, and more specifically, with evidence of the context of the use of the terrorist planning cycle. This is an electricity attack case study in California[15]. This example identifies some commonality in terrorist organisational attack structures, tactics, techniques, and procedures prior to an attack. This incident clearly demonstrates firstly, the synergies within the planning stage of a terrorist attack across organised domestic and transnational incidents. Secondly, to identify intelligence indicators which may be observed in these case studies to create a more effective future strategic and tactical estimate of terrorist intention and capability that can fit into a future ECI attack preventative model. The Offenders in this case have never been identified or arrested for this crime (Memmot, 2020) .

Hence, in consideration of the vast distances of transmission and distribution lines in conjunction with the geographic spread of significant assets across Europe, such as substations and transformer stations, electricity could be considered a 'soft' target displaying some difficulty in adequate defence against hostile attack, such as a terrorist attack. Furthermore with the broad introduction of SCADA[16] most assets are no longer staffed, with control and

[14] The Year 2000 problem, also known as the Y2K problem, the Millennium bug, Y2K bug, the Y2K glitch, or Y2K, refers to events related to the formatting and storage of calendar data for dates beginning in the year 2000. Problems were anticipated, and arose, because many programs represented four-digit years with only the final two digits - making the year 2000 indistinguishable from 1900.

[15] Attack on the Metcalf Transmission Substation in San Jose, California (USA) on 16.04.2013.

[16] 'These industrial control systems (ICS), which include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other smaller control system configurations such as skid-mounted Programmable Logic Controllers (PLC) are often found in the industrial control sectors. ICSs are typically used in industries such as electric, water, oil and gas, transportation, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing'. Stouffer, J., Falco, J., Kent, K. 2006. Guide to Supervisory Control and Data Acquistion (SCADA) and Industrial Control System Security. Gaithersburg, MD 20899-8930.

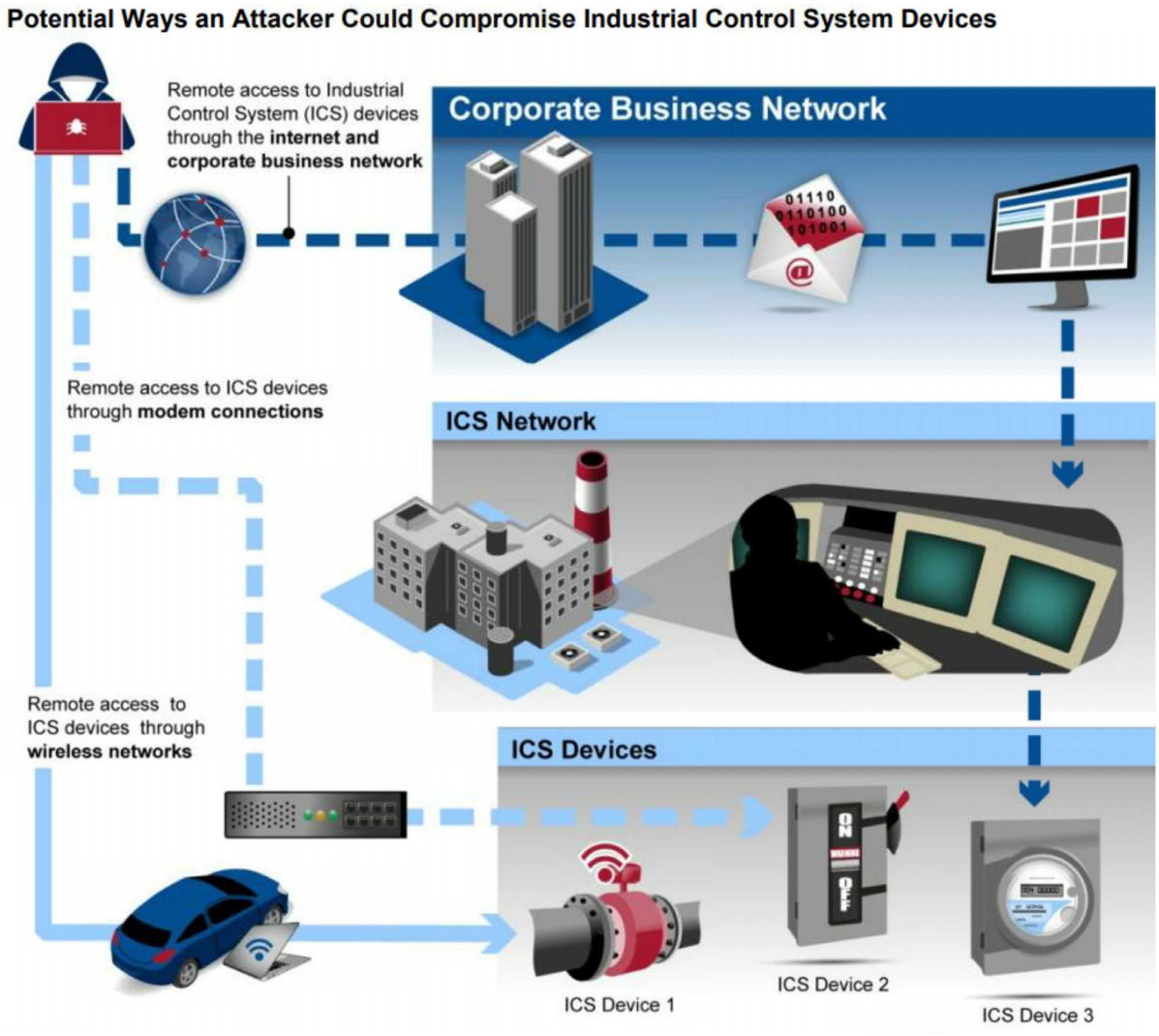


Fig. 6 Industrial Control System Vulnerability (GAO, 2019)

system observation from a central control room, distant from the asset (Hildick-Smith, 2005; Stouffer et al., 2006). Although SCADA is an economic and work-force efficiency innovation, the lack of staff at these facilities in electricity nodes tends to increase the risk exposure from physical adverse human intervention, such as terrorism. Consequently, it is not only physical attacks against ECI, but more likely as an internet cyber-attack aimed at the SCADA cyber infrastructure which now controls ECI in most locations. The electricity protection systems are designed to protect the electricity system from various internal external electrical influences and impacts on the total system, such as overload, weather occurrences, and electrical fluctuations that may affect or impact upon the electricity grid as a whole (Gray, 1980). These systems are vulnerable to external cyber-attack, due to the increasing industry reliance on 'SCADA'[17] (Stouffer et al., 2006). SCADA, in a remote control operational concept, operates electrical switches, and transformers in switchyards, often to move electricity to control overloads, individual line failures and to maintain system operation without human intervention at the particular site.

The SCADA system can be operated by authorised operators, and generally the electricity system is monitored from a central control centre, which is a high security facility, with a central system surveillance and operational control centre. Due to the operation of the SCADA dependency on

[17] SCADA is an abbreviation for Supervisory Control Access Data Acquisition, and are computer and internet operated industrial control systems, which, in this case, remotely control operational aspects of the electricity grid across Europe.

a wireless system configuration SCADA systems have been subject to high threat levels in the past due to the increasing use of wireless applications, particularly those in close proximity (Stouffer et al., 2006). Indeed, Stouffer considers that the threats to SCADA Control systems can come from numerous sources inclusive of hostile governments, Terrorists, disgruntled employees, malicious intruders, accidents, natural disasters and malicious acts by internal or external employees.

SCADA systems are designed to collect field information, transfer it to a central computer facility, and display the information to the operator graphically or textually, thereby allowing the operator to monitor or control an entire system from a central location in real time[18] (Stouffer et al., 2006).

Brandt (2009) confirms the increasing growth of the gap between private-party business attacks and official or government attacks, driven by the sequential hardening of official, government, and large corporate bodies. Over the past 20 years, substantial dramatic changes and expansions have occurred across the ECI and the extent of the Electricity Grid.

Of specific interest is a recent U.S report on the potential for terrorism related to power delivery systems indicates that incentives for private firms who own elements of the system have become mixed, and that the physical capabilities of the transmission system have not kept pace with the increasing modern requirements (NRCNA, 2012). The original concepts for electricity systems were initially designed and constructed to cater for ease of access and future maintenance with limited considerations for the 21st century contingencies of an event of adverse human intervention, such as an act of terrorism.

The European distribution system node caters for voltages from 22,000 volts to 220 volts, supplying electricity to the consumer. Apart from the individual 'nuisance value' within the distribution system, there are no indications of a SPOF in this area.

Historical Terrorist Attacks on Electricity Grids

Targeted terrorist attacks on CI have occurred in various parts of the world over the past 40 years. Farrell et al. (2004) document attacks in the United States of America, where The New World Liberation Front (NWLF) bombed assets of the Pacific Gas & Electric Company (USA) in more than 10 locations in 1975. Additionally, Seger (2003) informs that the Klu Klux Klan (KKK) and the San Joaquin Militia have been convicted (USA) of conspiring or attempting to attack energy infrastructure. Research of Ackerman et al. (2007) suggests that attacks on CI may require careful coordination and planning, as indicated by the Chukaku-ha (Nucleus Faction or Middle Core Faction), the largest active domestic terrorist group in Japan. The Chukaku-hu Group (ChG) is a radical Marxist organization that operates exclusively in Japan and has an estimated membership of 3,500, has been in existence since the 1950s, and is recorded as planning and conducting the most carefully coordinated and consequential CI-specific terror attacks ever conducted (Ackerman et al., 2007).

It is also of interest that Seger documents that the Klu-Klux Klan and the San Joaquin Militia have been convicted (USA) of conspiring or attempting to attack energy infrastructure conducted (Ackerman et al., 2007). Furthermore, Domingo reports that the Philippine Energy Authority reports that 100 attempted ECI cyber-attacks had been blocked in 2019 and also that a similar cyber-attack occurred in 2016, which was responsible for leaving thousands without power (Domingo, 2020).

An extreme 'Right Wing' group North of Seattle, USA implemented Chainsaw "Sabotage" on 12,000 Volt Power Poles in Washington, United States. In this attack five utility poles were attacked using a chainsaw, with one pole completely felled (TRAC, 2020).

Example of an Electricity Physical Attack

On 16.04.2013, near San Jose, California, USA (Harris, 2013), an organised attack occurred on a Transmission substation. Initially, two fibre optic communications cables in the ground were severed, adjacent to this critical transmission substation, compromising communications such as landlines, security monitoring and mobile phones. This occurred at 0100 hrs, with 100 bullets fired from a high powered weapon into the oil cooling tubes of 10 H.V. transmission transformers within the substation. The incident appeared well planned and was over quickly, with indiscernible CCTV images of two people in dark clothing and the bullets being fired (Memmot, 2020). Multiple transformers were damaged with the oil leaking out of the bullet holes causing overheating and damage to the 10 transformers. The unknown offenders secreted themselves in a gap between the CCTV cameras, indicating either pre-knowledge

[18] Page 22, Stouffer et al. (2006)

or previous surveillance (Fig. 7). As illustrated in Fig. 7, the offenders exited the site 1 minute prior to Police attendance indicating perhaps Police communications monitoring. The incident resulted in long power blackouts as spare components were difficult to acquire (Harris, 2013). The attack was highly organised and may have illustrated a 'dry run' or pre-attack trial to evaluate security, effect and response[19].

Of specific interest is that one of the most critical SPOFs, in electricity systems, is the large Transmission transformers within critical Transmission Sub-Stations in lieu of the actual electricity generation source in a Power Station. This is due to the multiplicity of interconnected generating sources that invariably exhibit surplus generating capacity that can maintain generated supply under single or duplicate generation outage conditions. Under prolonged electricity outage conditions there is a compounding social and economic 'flow-on' effect of electricity blackouts that strategic terrorist targeting may achieve, affecting all sectors of society and the economy. Transmission Transformers are extremely large and are now manufactured in South Korea, with a 12 month lead time for manufacture. The Transformers are also difficult to transport, requiring a sea voyage to the required location.

Discussion and Conclusions

The European electricity transmission system generally covers a large area with multiple isolated transmission towers to deliver high voltage electricity to communities ranging from domestic to industrial, retail and rural. These, often remotely located, structures are difficult to individually protect due to the multiple nature and location far from inhabited areas. In the event of a single transmission line failure from all hazard events, built in redundancy is planned to cater for a single transmission line outage. However single points of failure (SPOFs) exist in the event of multiple deliberate critical transmission line failures and additionally, in the Transmission zone substations, where multiple transmission lines feed in to a common point and within large Transmission transformers. The failure of an 'angle

[19] http://complex.foreignpolicy.com/posts/2013/12/24/power-station-militaryassault#sthash.Rvk9BRIG.re9jzhfv.dpbs.

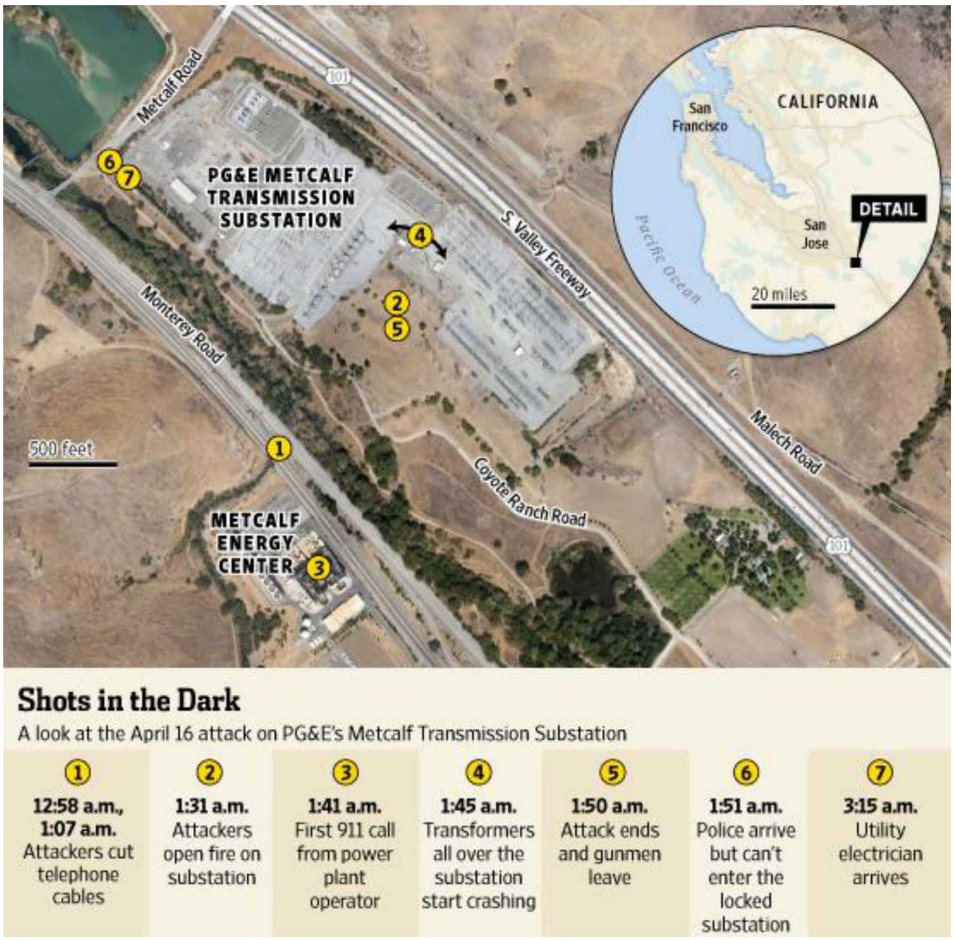


Fig. 7 Metcalf Transmission Substation, San Jose, USA, 16.08.2013 (Smith, 2014)

tower' in the transmission system can lead to a 'cascade' failure, destroying multiple towers in the system. A more associated supply chain risk exists from the unplanned interruption to gas supply from the European gas grid, which becomes more relevant with the closure of coal fired power stations and greater dependency on gas for electricity generation.

In determining the potential target selection by any specific terrorist group, there are a number of criteria and choices impacting on the actual selection and determination of the actual target and specific location. These choices, as part of a preliminary planning process is additionally influenced by the nature, classification or category of terrorist group, such as what the objective or strategy of the specific group is. However, various types of attack on ECI can be considered such as:

- Cyber Attack, (SCADA[20] or DOS[21]), to damage or interrupt ECI.
- Mass destruction of critical assets.
- Targeted attack on specific and vulnerable ECI critical nodes (such as Transmission Transformers and Transmission Substations).
- Siege and/or hostage situation within a sector of ECI, such as the ECI Control Centre.
- Mass Casualty Attack on ECI.[22]
- Attacks on one or more Nuclear Power Stations.

Within the EU, security context an international modern high profile terrorist attack on ECI has not yet occurred on main land Europe. To a certain extent this has contributed to an environment of relaxed security by critical infrastructure owners and operators, resulting in low levels of security, as compared with other similar countries where devastating attacks have occurred. For example, London, Madrid and New York have experienced increased levels of security and mitigation strategies. The issue is one of lagging mitigation, or tightening up security after the event rather than prior to the event. An appropriate eidetic illustration is being on the front of the wave instead of the back of the wave, or anticipating the parameters of the iceberg, when only 30 % is visible. The association with the planning for a terrorist attack are to a certain extent similar to the iceberg, that the only indications are a series of 'dots' that may be connected prior to an attack, which may only provide 20-30 % of an indication.

The scenario example from California, USA provided is extremely credible and realistic to any potential future attack in Europe (based on this Author's exercises and observations conducted over 20 years with Australian Electricity & Water entities), and could occur with the appropriate ideology, strategic focus, motivation and purpose by a 'home-grown' terrorist group, an international group gaining access to Europe, or a solo terrorist, as has been observed recently in Norway (Christensen, 2012): the United States and New Zealand, on many recent occasions.

A terrorist attack on the Generation or Distribution nodes can be easily rectified, whereas the Transmission system, and more specifically the large transmission transformers Within the Transmission Substations represent a single point of failure (SPOF) across the system.

- This criticality is based on the lead time involved in obtaining, transporting and installing back-up transmission transformers, some of which are not available in Europe or are of limited supply (Memmot, 2020). Many Transmission companies keep a few spare transformers but owing to the expense: physical size and transport difficulties, not many.
- Substations are publicly identified as many substations, including those critical for supplying electricity to some of our major cities, are clearly marked in publicly available material (e.g. street directories and Google Maps).
- Terrorist attack planners are likely to assess the relative impact on the electricity system in targeting different substations, including substations supplying capital cities compared with substations supplying regional and rural communities. It is considered feasible that a physical terrorist attack against a critical substation supplying large or symbolic capital cities could well occur. AQ media releases have also directly threatened Western electricity substation infrastructure.

Due to the large geographic distances and remote locations, the transmission systems are extremely difficult to protect and mitigate. However, additional remote security monitoring via SCADA could be achieved in the future, with heightened monitoring from Electricity Control Centres.

[20] SCADA is an abbreviation for Supervisory Control and Data Acquisition.

[21] DOS translates to an externally originated cyber overload or 'Denial of Service' designed to cripple an organisation's on line capacity to conduct BAU (Business as Usual).

[22] Designed to kill and injure as many people as possible, thereby highlighting the Terrorist Group's cause across national and global media.

Safety Engineering Series, ISSN 1805-3238 pp. 22-37, DOI 10.35182/tses-2020-0004

References

Ackerman, G., Abhayaratne, P., Bale, J., Bhattacharjee, A. et al. 2007. Assessing Terrorist Motivation for Attacking Critical Infrastructure. In Weapons of Mass Destruction Team Publications. Monterey, California, U.S.: Center for Non-Proliferation Studies, Monterey Institute of International Studies, University of California, 273.

Beering, P. S. 2002. Threats on Tap: Understanding the Terrorist Threat to Water. Journal of Water Resources Planning and Management, 128(3): 163-167.

Bennett, B. T. 2007. Understanding, Assessing and Responding to Terrorism - Protecting Critical Infrastructure and Personnel. New Jersey, U.S.: John Wiley & Sons. ISBN 978-0-471-77152-4.

Birkett, D., Truscott, J., Mala-Jetmarova, H., Barton, A. F. 2011. Vulnerability of Water and Wastewater Infrastructure and its Protection from Acts of Terrorism: A Business Perspective. In R.M. CLARK, S. HAKIM AND A. OSTFELD eds. Handbook of Water and Wastewater Systems Protection, Series Protecting Critical Infrastructure. New York, U.S.: Springer, 457-483.

Birkett, D. M. 2017. Water Critical Infrastructure Security and its Dependencies. Journal of Terrorism Research, 8(2): 1-21.

Bompard, E., Napoli, R., Xue, F. 2009. Analysis of Structural Vulnerabilities in Power Transmission Grids. International Journal of Critical Infrastructure Protection, 2(1): 5-12.

Brandt, P. T. 2009. What do Transnational Terrorists Target? Has It Changed? Are We Safer? California: U.S. Department of Homeland Security, Center for Risk and Economic Analysis of Terrorism Events.

Buttler, M., Mcmahon, S. 2009. Earth Liberation Front Threaten Hazelwood Power's Graeme York. In Herald Sun. Melbourne, Victoria, Australia: News Corporation (Rupert Murdoch).

Christensen, T., Laegreid, P., Rykkja, L. H. 2012. How to Cope With a Terrorist Attack? - A Challenge for the Political and Administrative Leadership. In European Commission Research Area, European Union. Oslo, Norway: COCOPS, 36.

CNN. 2020. 2015 Paris Terror Attacks Fast Facts [online]. Edition.cnn.com, 2020 [cit. 2020-11-09]. Available at: https://edition.cnn.com/2015/12/08/europe/2015-paris-terror-attacks-fast-facts/index.html.

Combs, C. C. 1997. Terrorism in the Twenty-First Century. New Jersey, U.S.: Pearson-Prentice Hall. ISBN 0-13-193063-X.

Davidson, M. 2010. Australian Electricity Market Overview. Belair, South Australia: Wessex Consult Pty Ltd.

Domingo, K. 2020. Philippines' Power Grid Blocked 100 'Attacks' in 2019: Operator. ABS-CBS NEWS.

Drake, C. J. M. 1998. Terrorists' Target Selection. London, U.K.: MacMillan Press. ISBN 0-333-72006-7.

DSB. 2003. The role and Status of DoD Red Teaming Activities. Washington, DC: U.S. Department of Defense.

EUROPEAN UNION. 2019. Electricity Interconnections With Neighbouring Countries. Luxembourg: Publications Office of the European Union.

Fakude, T. 2016. Media Coverage of the Paris and Brussels Attacks - What was Different? Al Jazeera.

Farrell, A. E., Zerriffi, H., Dowlatabadi, H. 2004. Energy Infrastructure and Security. Annual Review of Environment & Resources, 29(1): 421-469.

GAO. 2019. Preparing for Evolving Cybersecurity Threats Facing the U.S. Electric Grid. United States Government Accountability Office (GAO), Washington, U.S.: WATCHBLOG.

Gray, C. M., Spencer, A. M. 1980. The Linemans' Handbook. Wellington, New Zealand: Electric Supply Authority Engineers' Institute of New Zealand Inc.

Gupta, R. 2011. Utilizing Network Analysis to Identify Critical Vulnerability Points in Infrastructure and Explain Terrorist Target Selection. Masters Thesis, Georgetown University, Washington, DC.

Harris, S. 2013. 'Military-Style' Raid on California Power Station Spooks U.S. Washington, DC: Washington Post (Graham Holdings).

Hildick-Smith, A. 2005. Security for Critical Infrastructure Scada Systems. SANS Reading Room, SANS Institute, Bethesda, Maryland.

Howard, M. 1984. The Causes of War. London, U.K.: Unwin.

IEA. 2020. European Union 2020 - Energy Policy Review. Paris, France: International Energy Agency (IEA).

Jenkins, B. M., Trella, J. 2012. Carnage Interrupted: An Analysis of Fifteen Terrorist Plots Against Public Transportation. San Jose, California, United States of America. CA-MTI-12-2979.

Krutz, R. L. 2006. Securing SCADA Systems, Nov 2005, e-Book-DDU. Indianapolis, IN: Wiley Publishing Inc. ISBN-13 978-0-7645-9787-9, ISBN-10: 0-7645-9787-6.

Lee, E. 2009. Homeland Security and Private Sector Business: Corporations' Role in Critical Infrastructure Protection. Boka Rato, Florida: Auerbach Publications. ISBN 1420070789.

Lister, T., Sanchez, R., Bixler, M., O'kay, S. et al. 2017. ISIS Goes Global: 143 Attacks in 29 Countries Have Killed 2,043. CNN.

Martí, M., Parrón, M., Baudraxler, F., Royo, A. et al. 2006. Blast Injuries from Madrid Terrorist Bombing Attacks on March 11, 2004. Emergency Radiology, 13(3): 113-122.

Memmot, M. 2020. Sniper Attack on Calif. Power Station Raises Terrorism Fears [online]. Nhpr.org, 2020 [cit. 2020-11-06]. Available at: https://www.nhpr.org/post/sniper-attack-calif-power-station-raises-terrorism-fears#stream/0.

Michaelsen, C. 2010. Australia and the Threat of Terrorism in the Decade after 9/11. Asian Journal of Political Science, 18(3): 248-268.

Miller, M. 2015. Think Like a Green Beret: The CARVER Matrix. SOFREP.

Nelson, B., Godson, E. 2007. Development of the Ontario Critical Infrastructure Program. In 17th Conference on Disaster Management. Ontario, Canada.

NRCNA. 2012. Terrorism and the Electric Power System. National Research Council of the National Academies (NRCNA), National Academies of Sciences, Washington, DC, U.S.

Rand Corporation. 2018a. Terrorism Cost the EU €180 Billion Between 2004 and 2016. Rand Corporation.

Rand Corporation. 2018b. The Financial Cost of Terrorism in Europe. World Economic Forum.

Robinson, C. P., Woodard, J. B., Varnado, S. G. 1998. Critical Infrastructure: Interlinked and Vulnerable. Issues in Science and Technology, 15(1): 61-67.

Romyn, D., Kebbell, M. 2013. Red-Teaming Terrorist Attacks: A Simulation Approach. Nathan, QLD: ARC Centre of Exellence in Policing and Security.

Rusco, F. 2017. Status of Residential Deployment of Solar Energy and Other Technologies and Potential Benefits & Challenges. In United States Government Accountability Office (GAO). U.S. GAO, Washington, DC: U.S. GAO, 51.

Schnaubelt, C. M., Larson, E. B., Boyer, M. E. 2014. Vulnerability Assessment Method Pocket Guide. Santa Monica, California, U.S.: RAND Corporation. ISBN 978-0-8330-8689-1.

Seger, A. K. 2003. Utility Security: The New Paradigm. Pennwell Corporation. ISBN 13-978-0878148820.

Shape, A. 2013. Red Teaming Guide, Ministry of Defence. Shrivenham, Swindon, Wiltshire, United Kingdom: The Development, Concepts and Doctrine Centre.

Smith, R. 2014. Assault on California Power Station Raises Alarm on Potential for Terrorism. In The Wall Street Journal. Washington, U.S.: The Wall Street Journal, 8.

Start National Consortium. 2020. Global Terrorism Index 2019 Measuring the Impact of Terrorism. California, U.S.: Institute for Economics & Peace.

STATOIL. 2013. The In Amenas Attack, Report of the Investigation into the Terrorist Attack on In Amenas. Oslo, Norway: STATOIL.

Stewart, S. 2012. Detection Points in the Terrorism Attack Cycle. Security Weekly: Fundamentals of Terrorism, Thursday 01 March 2012, Chapters 3 and 5.

Stouffer, J., Falco, J., Kent, K. 2006. Guide to Supervisory Control and Data Acquistion (SCADA) and Industrial Control System Security. Gaithersburg, MD: National Institute of Standards and Technology.

Toben, A. 2013. Terrorism Case Studies. Tel Aviv, Israel.

Toft, P., Duero, A., Bieliauskas, A. 2010. Terrorist Targeting and Energy Security. Energy Policy, 38(8): 4411-4421.

TRAC. 2020. Chainsaw "Sabotage" on 12,000 Volt Power Poles Washington, USA. In Terrorism Research and Analysis Consortium (TRAC).