The Institution of Engineering and Technology

Security and Risk in Transport Systems and Infrastructure

Introduction

In recent years, terrorist organisations have pursued their objectives through attacks on public places, transport systems and infrastructure and other areas deemed vulnerable. Examples include:

- **Industrial installations** - Natural gas plant in Algeria, where 67 people were killed (2013).
- **Maritime security** - 233 incidents of piracy and armed robbery on a worldwide basis (2012).
- **Urban security** - Mumbai, in and around the Taj Hotel, where 164 people were killed (2008).
- **Underground Train / Public Transport Security in London** - 52 killed and 700 injured (2005).
- **Train Security** - Madrid train bombings where 191 people were killed (2004).
- **Airport security** - 9/11 Twin Towers in New York and associated attacks, where nearly 3,000 people were killed (2001).

Transport

www.**theiet**.org/transport

Such targets have invariably incorporated an element of 'spectacular'. However, calls for 'Electronic Jihad' using cyber attack suggest terrorist organisations are equally turning their attention to new targets and new methods of attack.

To date, they have lacked the resources to successfully launch a cyber attack. If they were to gain that capability the end result could be far more serious than anything that has gone before. Unlike conventional attacks that tend to concentrate on one geographic location with one target, a cyber attack could be launched against multiple targets simultaneously.

Let us consider a couple of potentially serious scenarios in relation to transport and infrastructure:

- Air transport - with the increasing use of electronic systems and Internet connectivity, and with documented media reports on cyber intrusions into satellite systems, it is conceivable that attempts could be made to interfere with aircraft systems in flight, with potentially significant consequences.

- Electrical Distribution Infrastructure - a cyber-attack is perhaps the most serious event that can occur - everything stops. Fuel cannot be pumped so transport comes to a halt, hospitals with people on life support suffer, and food and water cannot be distributed to the population. If not rectified in a short time, civil unrest could occur. There is also a high likelihood that electrical transformers could be damaged in the attack. The lead time for new equipment would be months or years, even in normal circumstances – let alone one where the country has no electricity supply.

Transportation & Urban Security

Safer Cities

To maintain law and order, counter potential terrorist threats and deal with natural catastrophes and emergencies, the concept of "secure cities" has evolved.

As the world population increases, the size of cities increase. According to the United Nations, there are presently 19 cities with populations over 10 million and by 2025 there will be eight more. Mexico City is the world's third largest megacity, has a population of over eight million, but taking into account all 60 municipalities, the population is over 22 million people. Covering over 1,485 square kilometres, the infrastructure to protect the population in the central area from threats is significant and has the world's largest urban security system, consisting of:

- 8,080 CCTV cameras, 80% with video analytics
- 380 gunshot sensors
- 255 Automatic Number Plate Recognition (ANPR) cameras
- 180 traffic monitoring cameras on key routes
- Four unmanned aerial reconnaissance drones
- Two mobile tactical command and control centres
- Five local C2 (command and control operation) centres
- One city-level C4I (command, control, communication, computer and intelligence) centre
- City-wide network of emergency call points and citizen terminals
- 8,000 Public Address speakers
- Vehicle location capability for all 25,000 police cars
- Mobile data terminals and PDAs for police officers

Metrics from 2012, indicate:

- 3x reduction in response times
- 80% - reduction of crime in metro area
- 35% - reduction in crime in certain previously neglected areas

www.**theiet**.org/transport

Rail & Airport Hubs

Transportation hubs for air, sea and rail have been focal points for terrorist threats and other crimes such as people and drug trafficking. Heathrow Airport is a major international hub which in 2012 was ranked as the third busiest airport in the world, with approximately 70 million passengers and 475,000 aircraft movements. With flight restriction times and quotas operational between 0700 hours and 2300 hours, the majority of traffic is during the day, equating to an annualised average hourly throughput of 12,000 people. It is only with the assistance of technology that all passengers can be assessed and monitored, allowing safe transit and identification of threats.

The number of persons within a transport hub can fluctuate during the day depending on the timing of flight or train arrivals / departures. A number of simulation activities have been undertaken to ensure facilities are scaled to support passenger flow, such as check-in gates. However, it is not only passenger flow during normal operations that should be considered, but also during times of emergency. Research by Thales has produced the SE-Star product, allowing virtualised simulations of real environments - reactions of passengers and staff to real world events such as explosions, fires, floods or other hard to manage incidents. These can be visualised allowing buildings and response processes to be designed accordingly - this has been trialled on Paris Gare Du Nord.

Video analytics and biometrics technologies are now commonplace in transportation hubs and are used to identify and track passengers. The recent introduction of e-gates at some airports such as London Gatwick allows each passenger to check in with their e-passport, which has an embedded microchip. When presented to the e-gate, the photograph on the passport scanned, and facial recognition performed which is checked against the photograph on the passport and the details stored on the embedded chip. The benefit to the individual is rapid transit through the e-gate.

It is not just facial recognition. Other techniques such as iris recognition or hand geometry that can be used to identify a person. Multimodal feature recognition, raises confidence that a person's identity has been confirmed. As passengers pass through the various stages of the airport from ticket presentation, security screening and through to the departure lounge, techniques such as passive facial recognition can be used to automatically track persons throughout their route within the airport.

Human Recognition Systems, an SME providing biometric identity solutions, has developed techniques to monitor for abnormalities. Where persons stray from pre-set safe zone, across a virtual boundary, an alert is raised. Other techniques can be used to detect persons loitering in a defined area. A variant of this can detect unattended objects, such as suitcases, and back-track to the person who left the object.

In the air

The threat from conventional explosives will not recede but new methods may evolve, as demonstrated by the attempted cargo plane bomb in 2010 when explosives were concealed in printer cartridges and linked to mobile phone timer for detonation - though in this instance the SIM card had been removed and detonation was based on a timer rather than receipt of a call. This is similar to the Madrid train bombings in 2004, where mobile phones with SIM cards were used, but only so that the timer could operate and the tracing of the SIM registration led to the suspects.

www.**theiet**.org/transport

One could imagine threats evolving. The SIM card operation would perhaps be problematic unless it was registered to a carrier in that country. However, with the evolution of in-flight Internet systems offering Wi-Fi, the ability to receive a remote detonation command may become a concern. It is therefore essential that the vendors of these systems address the issue of security lockdown to ensure unauthorised devices cannot connect.

Safety of operations is paramount with the number of planes taking off and landing worldwide. Before passengers get airborne, Baggage Reconciliation Systems (BRS) ensure that bags loaded onto the aircraft are matched against passenger records. If a bag is on an aircraft but not the passenger, then the bag is removed before take-off.

Although the use of UAVs (Unmanned Aerial Vehicles) are well known for surveillance and offensive operations, it is likely that drone technology will evolve for autonomous civilian cargo transportation - though the timeline may not yield commercial systems for perhaps another 15 years. Given the technology for guidance would be satellite GPS, the integrity of this data would need to be maintained to ensure unmanned autonomous systems could not be hijacked by terrorists; by spoofing of the GPS data, a technique demonstrated by the University of Texas in June 2012.

The safety of aircraft in the sky is critical. Cyber threats in air traffic control systems affecting the integrity or availability of the data, perhaps including intrusion into satellite / radio communication systems, or remote changes to data received and acted upon by Flight Management Systems (FMS) are to be detected and stopped. Advanced cyber detection systems that detect Advanced Persistent Threats (APT) and other threats within air traffic command and control systems particularly in the military sphere, have been developed and are currently in use.

With the rise of cyber attacks against real time systems, and the sophistication of those attacks, this must be a primary concern in the long term. As aircraft are being fitted with the capability to allow passenger Internet connectivity, the design of these systems and the interconnecting networks must ensure that malicious threats cannot get into flight control and engine management systems. Conventional bomb attacks by terrorists require a large team of suicide bombers - such as the 2006 transatlantic plot where there was an intention to target at least 10 aircraft travelling from the United Kingdom to the United States and Canada. With a cyber attack, the potential damage could be far more serious if the on-board aircraft systems and methods of remotely compromising those systems were discovered and mastered, enabling a simultaneous attack against many more aircraft.

www.**theiet**.org/transport

Infrastructure Security

The CNI (Critical National Infrastructure) of a country can broadly be categorised into the following nine groups:

- Banking and Finance
- Emergency Services
- Communications
- Energy
- Food
- Government
- Health
- Transportation
- Water

They share similarities with respect to the threats, both physical and cyber, that can be deployed against them and, therefore, the security controls used to protect the CNI will be similar.

For illustration if we take a large gas, oil or nuclear facility there is the need to keep determined intruders out. The first line of defence should be monitoring of approach roads, perhaps using ANPR (Automatic Number Plate Recognition) technology to check and validate license plates of oncoming vehicles. The next layer should be layers of gates and fences into controlled areas of the site. The perimeter fence for high security sites should consist of 2 layers with an inner sterile zone. Other physical security measures may be used such as Bunds (earth mound with sloped sides) to ensure vehicles cannot access the site by crashing through the fence-line. The value of physical barriers have been proven on a daily basis in the conflicts in Afghanistan and Iraq to keep truck bombs out of facilities.

CCTV cameras are used for monitoring of events, typically comprising a large number of fixed fence-line cameras and a smaller number PTZ (Pan Tilt Zoom) cameras - cued to the point of intrusion, either automatically, or by human operator in an Incident Command Centre.

Video object tracking and classification techniques and technology can be used to reduce the number of false alarms and prioritise important events.
A Hypervisor based system is used at Fleury-Merogis prison near Paris. With 4,000 inmates, it is the largest jail in Europe and is linked via secure network and communication subsystems to more than 46,000 items of field equipment - the potential for alarm indications is significant.

It is not only the facilities such as oil and gas facilities that require protection but also the pipelines and pumping stations to and from these facilities. If we examine some of the longest gas pipelines:

- China West East Pipeline - (internal China) – 5,410 miles
- Gasun Pipeline (Bolivia to Brazil) – 3,100 miles
- Trans-Saharan (planned Nigeria, Niger to Algeria) – 2,565 miles

It is clear that these distances are huge - the China pipeline is almost the same distance as London to Los Angeles (5,446 miles). Often the pipelines pass through regions where militia may try to attack the pipeline and techniques are required using acoustic detection methods to identify attacks, persons trying to tap-off the pipeline, or leaks.

Command Centres

Due to the prevalence of command centres in modern films and TV programmes, the general public have a reasonable awareness of what constitutes a command centre and thanks to modern technology, the reality has now caught up but there is still a significant cost for integrating technologies. Thales have worked with a large number of customers to deploy Hypervisor integration technology with packaged modular solutions, to deliver large scale integrated solutions such as:

- Mexico City, Mecca - crowd monitoring / urban security
- Dubai, Doha, Durban, Singapore - airport security
- Gazprom, Saudi Aramco, ADNOC - oil & gas security
- Latvia, North Africa - border security

These command centres have operator stations with multiple monitors, large video walls to overlay CCTV, maps, newsfeeds, and any other item of interest including GPS tracking of personnel & assets responding to an incident.

Incidents are unpredictable and require a variety of responses. For example, a terrorist attack on a gas processing plant, chemical factory or nuclear facility may require an armed response. If explosives were detonated, the need for emergency evacuation of local populations may also be required. Similarly, the response to a physical attack versus a cyber attack may be very different. Therefore, the scenarios that must be handled should be modelled and practised. Appropriate interfaces need to be created to allow the transfer of necessary data into the command centre and instructions to external parties and stakeholders.

Big Data

The London Metropolitan Police in March 2013 stated that they were foiling a terrorist plot as big as the 7/7 (2005) attacks every year. The old adage with respect to terrorists "they only have to get lucky once, we have to get lucky every time", is a true statement, but given that an event as significant as The Twin Towers attack has not occurred since 2001, is testament to the behind the scenes investigative work and correlation of data - Big data.

Big data is a phrase used in recent times and will become more prevalent. Data exists in many sources (terrorist watch lists, car licensing databases, passenger flight lists, Facebook / social media pages & related contacts, bank / card transaction data, company registration data, criminal records, ANPR data, Internet search data .... for those with access the list goes on). The challenge is to capture, curate, store, search, share, analyse and visualise the data - such that a human can easily interpret and act on the results.

Examples of such systems are Thales OSInt Lab which has the ability to perform social web mining and monitoring, based on crawling, annotation search, mining of textual and relational data and visual analytics. Other technologies exist for the handling of diverse datasets, with the US DOD use of DCGS-A and Palantir.

Although very much "big brother" in the eyes of some, the consequences of letting a terrorist attack slip through is significant. If technology can be used in a non-intrusive way, benefitting the everyday traveller, allowing rapid transit through customs; the objections will be minimised.

Countering Cyber Threats

Cyber incidents and threats usually cover:

- Cyber Crime (theft of money)
- Cyber Espionage (theft of intellectual property & secrets)
- Cyber Warfare / Cyber Terrorism / Cyber Accident

The latter category is difficult to quantify. It mainly affects real-time or operational systems. The incident may not have malicious intent but could have serious consequences for operational systems. For example, when Heathrow Terminal 5 opened in 2008, there were significant problems with the operation of the automated baggage handling system, causing the cancellation of 430 flights, mishandling of 20,000 bags and lasted 8 days. There was no malicious intent, just technical teething problems and human reactions to events. In this case, the "availability" of the system was affected.

In future, there may be targeted incidents which affect the "integrity" (malicious changing of data), as well as availability. For example, the much publicised Stuxnet cyber attack in 2010 on the Natanz nuclear enrichment facility in Iran, caused the destruction of an estimated 1,000 centrifuges out of a total of 5,000 present. The method of attack was to change the software logic of the connected programmable controllers to spin the centrifuges at a high speed, causing high vibration, then destruction. This was very much a landmark incident and possibly opens up the west to similar attacks on infrastructure controlled by SCADA and other real-time systems, using resources such as Shodan search tool to locate vulnerable systems.

Further integrity / availability attacks have been observed. In 2012 Saudi Aramco was struck by Shamoon wiper malware, which overwrote disk data with fragments of a photo of a burning American flag, then corrupted the master boot record rendering the 30,000 PCs inoperable.

It is estimated in media reports that the majority of Fortune 500 companies in the USA have suffered at the hands of cyber intrusions; this supposition is most probably accurate, and the extent is far worse than published, with large scale exfiltration of intellectual property and trade / national secrets. It should be noted that many companies that were compromised had sophisticated IT security controls in place but malware still got through. Customers require better technologies as an alternative or supplement to the current signature based anti-virus industry. "Zero-day" attacks pass straight through undetected and there is the release of over 100,000 new signatures each day. The intent of the malware may presently be IPR theft but in-future the consequences may be far more serious allowing Cyber-Terrorism, with outsiders perhaps taking down electricity supplies or affecting major transportation infrastructure.

The solution lies in:

- Better detection of threats.
- Organisations should assume that current controls are not good enough to keep the malware out, and should segment their networks to ensure direct connections from outside cannot interact with internal networks from Internet connected user PCs, perhaps using virtualised browse down Internet connectivity.
- Using sophisticated technologies for identity and access management.
- Treating cyber-security not as a tick-box compliance exercise but one of an ongoing battle against cyber adversaries, where indicators of compromise and systems are monitored before, during and after attacks - and corrective measures put in place to ensure further intrusions are kept out.
- Having response plans to ensure that once intrusions are detected, they are contained and removed from the wider network.

Future Outlook

Early experiences of threats against transport systems and infrastructure have revolved around explosives, hostage taking and physical attacks. The nature of such attacks has escalated as terrorist-inspired groups have sought to wreak havoc, inflict mass casualties and secure maximum publicity.

The risk is not receding and technology will play a greater part in the analysis of multiple sources of data, alerting the authorities to the threat before an event happens or before the perpetrators get anywhere near the transport hub, plane/train or public space they plan to attack.

The threat of cyber-attacks targeting transport and infrastructure systems remain very real, not least as an ever increasing dependence is placed on IT systems to manage these functions.

Is there a danger that attacks, like that unleashed in summer 2012, knocking out computers managing oil and gas supplies in the Gulf, may become commonplace? Avoiding 'cyber Pearl Harbour', a potential threat outlined by former US Secretary of State for Defense, Leon Panetta, requires urgent, united action to deter possible attacks on power grids, infrastructure, transportation, financial and government systems across the globe. All available technologies and resources to address this threat are needed as a matter of priority.

Visit our website for all the latest news, information and downloads from the IET Transport Sector or email transport@theiet.org

www.**theiet**.org/transport

This Sector Insight has been written in collaboration with Dr. Paul A. Irving, Principal Consultant for Thales UK.

The Institution of Engineering and Technology

IET Offices

London*
Savoy Place
2 Savoy Place
London
WC2R 0BL
United Kingdom
www.theiet.org

Stevenage
Michael Faraday House
Six Hills Way
Stevenage Herts
SG1 2AY
United Kingdom
T: +44 (0)1438 313311
F: +44 (0)1438 765526
E: postmaster@theiet.org
www.theiet.org

Beijing
Suite G/10F
China Merchants Tower
No.118 Jianguo Road
Chaoyang District
Beijing China
100022
T: +86 10 6566 4687
F: +86 10 6566 4647
E: china@theiet.org
www.theiet.org.cn

Hong Kong
4412-13 Cosco Tower
183 Queen's Road
Central
Hong Kong
T: +852 2521 1611
F: +852 2778 1711

Bangalore
Unit No 405 & 406
4th Floor, West Wing
Raheja Towers
M. G. Road
Bangalore 560001
India
T: +91 (0) 080 4089 2222
E: india@theiet.in
www.theiet.in

New Jersey
379 Thornall Street
Edison NJ 08837
USA
T: +1 (732) 321 5575
F: +1 (732) 321 5702

IET Venues

IET London: Savoy Place*
London
T: +44 (0) 207 344 5479
www.ietvenues.co.uk/savoyplace

IET Birmingham: Austin Court
Birmingham
T: +44 (0)121 600 7500
www.ietvenues.co.uk/austincourt

IET Glasgow: Teacher Building
Glasgow
T: +44 (0)141 566 1871
www.ietvenues.co.uk/teacherbuilding

*Savoy Place will be closed for refurbishment from summer 2013 until autumn 2015. During this time IET's London home will be within the Institution of Mechanical Engineers building at:

1 Birdcage Walk
Westminster
London
SW1H 9JJ

If you are attending an event during this period, please check the venue details carefully.

www.**theiet**.org