CRITICAL INFRASTRUCTURE PROTECTION

NATO Science for Peace and Security Series

This Series presents the results of scientific meetings supported under the NATO Programme: Science for Peace and Security (SPS).

The NATO SPS Programme supports meetings in the following Key Priority areas: (1) Defence Against Terrorism; (2) Countering other Threats to Security and (3) NATO, Partner and Mediterranean Dialogue Country Priorities. The types of meeting supported are generally "Advanced Study Institutes" and "Advanced Research Workshops". The NATO SPS Series collects together the results of these meetings. The meetings are co-organized by scientists from NATO countries and scientists from NATO's "Partner" or "Mediterranean Dialogue" countries. The observations and recommendations made at the meetings, as well as the contents of the volumes in the Series, reflect those of participants and contributors only; they should not necessarily be regarded as reflecting NATO views or policy.

Advanced Study Institutes (ASI) are high-level tutorial courses to convey the latest developments in a subject to an advanced-level audience.

Advanced Research Workshops (ARW) are expert meetings where an intense but informal exchange of views at the frontiers of a subject aims at identifying directions for future action.

Following a transformation of the programme in 2006 the Series has been re-named and re-organised. Recent volumes on topics not related to security, which result from meetings supported under the programme earlier, may be found in the NATO Science Series.

The Series is published by IOS Press, Amsterdam, and Springer Science and Business Media, Dordrecht, in conjunction with the NATO Emerging Security Challenges Division.

Sub-Series

A.	Chemistry and Biology	Springer Science and Business Media
B.	Physics and Biophysics	Springer Science and Business Media
C.	Environmental Security	Springer Science and Business Media
D.	Information and Communication Security	IOS Press
E.	Human and Societal Dynamics	IOS Press

http://www.nato.int/science
http://www.springer.com
http://www.iospress.nl

Sub-Series E: Human and Societal Dynamics – Vol. 116

ISSN 1874-6276 (print)
ISSN 1879-8268 (online)

Critical Infrastructure Protection

Edited by

Matthew Edwards
Centre of Excellence – Defence against Terrorism
Ankara, Turkey

IOS Press

Amsterdam • Berlin • Tokyo • Washington, DC
Published in cooperation with NATO Emerging Security Challenges Division

Proceedings of the NATO Advanced Research Workshop on
Critical Infrastructure Protection
Ankara, Turkey
2–3 May 2012

ISBN 978-1-61499-356-8 (print)
ISBN 978-1-61499-357-5 (online)

Library of Congress Control Number: 2013 955 222

Publisher
IOS Press BV
Nieuwe Hemweg 6B
1013 BG Amsterdam
Netherlands
fax: +31 20 687 0019
e-mail: order@iospress.nl

Distributor in the USA and Canada
IOS Press, Inc.
4502 Rachael Manor Drive
Fairfax, VA 22032
USA
fax: +1 703 323 3668
e-mail: iosbooks@iospress.com

Critical Infrastructure Protection
M. Edwards (Ed.)
IOS Press, 2014

Preface

The issue of Critical Infrastructure Protection (CIP) against the current threat of terrorist attack continues to feature prominently. But it is not just about terrorism – environmental hazards, industrial accidents and sabotage (deliberate and consequential which includes terrorism) all play a role. Solutions to one are applicable to others. Protecting critical infrastructure (CI) is expensive so in these days of scarce resources multi-sector or multi-threat solutions are preferred. Dealing with this issue demands a balanced strategy and prioritisation. CIP is about measuring risk-informed outcomes. There must be a feedback loop and element of risk accepted and mitigated through consequence management. Two important questions that continue to arise are: firstly, what can we do to increase the resilience of CI? The common answer being that we must cooperate. The second question is whether CI protection is a national or international issue. The answer is of course both and must be deconflicted.

This book presents the proceedings of the NATO Centre of Excellence – Defence against Terrorism (COE-DAT) Advanced Research Workshop entitled "Critical Infrastructure Protection," held in Ankara, Turkey, in May 2012. The workshop brought together 44 participants from 13 countries and consisted of five sessions: a General Overview of Policy, Tools and Techniques; the Realities of Implementation; Protection of Critical Energy Infrastructure; Protection of Critical Communications and Information Infrastructure; and Protection of Critical Transportation Infrastructure. During these sessions, presentations by 16 expert speakers – military and civilian practioners, business leaders, diplomats, and academics – from 6 countries were followed by a detailed discussion and debate. The workshop concluded with a summary of all the topics reflected in the individual papers presented.

Representing a significant contribution to furthering the science of counterterrorism, this book will be of interest to all whose work involves aspects of Critical Infrastructure Protection and the terrorist threat to infrastructure.

This page intentionally left blank

Contents

Critical Infrastructure Protection
M. Edwards (Ed.)
IOS Press, 2014

doi: 10.3233/978-1-61499-357-5-1

NATO and Critical Infrastructure Resilience – Planning for the Unknown

Dinos KERIGAN-KYRO[1]
Dartmouth Strategic Studies Group

Abstract. Critical infrastructure is vital for modern existence. It includes communications and the Internet, the logistics of food and water supplies, and transport on the roads, in the air, on water, and by rail. The supply and distribution of gasoline and electricity is perhaps the most important aspect, as it underpins our entire critical infrastructure and indeed our modern way of life. Without power nothing can operate. Our critical infrastructure is however subject to ever increasing asymmetric threats. Such threats can arise from industrial accidents, extreme weather, and deliberate sabotage caused by terrorists and extreme protest. Moreover, those that wish to do harm have an ever increasing ease of access to vital critical infrastructure systems by way of 'cyber' information technology. Since 9/11, NATO has adapted to face these new challenges. Continuing this adaptation is vital. The paper argues that information-sharing and emergency planning based on resilience and flexibility is the key way in which we can address these new challenges.

Keywords. Critical infrastructure protection, resilience, emergency planning

Introduction

The article will address NATO's polices and plans in critical infrastructure protection and what we can do to help protect our critical infrastructure. Firstly a definition is needed about what is meant by critical infrastructure, before moving on to examine what these challenges are.

A good definition of critical infrastructure has been given by U.S. Senator Susan Collins; her proposed bill before the Senate defines it as infrastructure that, if attacked, would produce "mass casualties, severe economic damage, and a serious threat to national security."[2]

Indeed, our critical infrastructure makes modern society possible. It includes our communications and the Internet, banking, food and water supplies, health systems, defence, transport, air traffic control, logistics and ports. It also includes the supply and distribution of energy and electricity. Fuels, power generation, electricity grids, and the distribution of gasoline and diesel underpin our entire critical infrastructure.

The question that must be asked is: what are these threats to our critical infrastructure Moreover, what form will they take?

[1] Research Associate.
[2] S.201, *Cyber Security Act, 2012*, First Reading, 14 February 2012, 112th US Congress,2nd Session, available at www.opencongress.org/bill/112-s2105/text

Threats can arise from:

- environmental hazards.
- industrial accidents.
- or deliberate sabotage, and what can be defined as 'consequential sabotage'.

Firstly, an examination of environmental hazards.

1. Environmental Hazards

The 2011 Japan earthquake and tsunami tragedy is perhaps the prime example of an environmental threat that caused thousands of fatalities and incapacitating much of Japan's infrastructure. Even under these terrible conditions, Japan demonstrated that parts of its infrastructure, such as its roads and airports, could be repaired and running again very quickly. For example, Sendai Airport was devastated, yet the airport was operating emergency flights just a week later and commercial flights within a month. Indeed, the Japanese authorities received substantial help from the U.S. Army, the U.S. Marine Corps and the U.S. Air Force led by Col Craig Kozeniesky. There are many examples of this rapid recovery; to the north of Sendai the city of Kesennuma was devastated and yet today the city is fully functioning. Nonetheless, other aspects of Japan's infrastructure, such as the Fukushima nuclear power plant, have proved much less resilient; these will be addressed in detail later in this paper.

In Europe, the October 2011 earthquakes in eastern Turkey may have killed 1,000 and made many more homeless. Turkey worked closely with NATO's Euro-Atlantic Disaster Response Coordination Centre (EADRCC) to help the region's civilians. Indeed, EADRCC has an important coordinating role between NATO members, working closely with the military in each country, and with international organizations, enabling expertise and assistance to be on the ground very quickly. After 9/11, EADRCC was tasked with coordinating international assistance in the event of chemical, biological, radiological, and nuclear incidents.

NATO's EADRCC also has an important role as a tool for information sharing and knowledge management – an extremely important issue and perhaps the key to critical infrastructure resilience. Information sharing and knowledge management is an issue that will be addressed further later in this paper.

In 2010, NATO provided humanitarian assistance to the people of Pakistan following extreme flooding. That NATO assistance saved thousands of lives – not just from drowning but also by helping to prevent diseases which occur in such conditions, particularly cholera. In that same year there were torrential rain and mudslides in China and fires in Russia, which killed many thousands.

In May 2011, tornadoes in the United States, particularly in the southern states of Alabama, Tennessee, Mississippi, Kentucky, Louisiana, Georgia, and Virginia killed over 300 people. They were the most powerful tornadoes ever on record for the region. Less than four weeks later tornadoes in Massachusetts and in Joplin Missouri killed over 200, and caused economic devastation. (Although it was contained within a smaller geographical area, the devastation in Joplin was similar to that which occurred

in Japan earlier the same year.) Shortly afterwards, wildfires threatened electric power lines in Arizona and Texas. In August 2011, New Jersey experienced unprecedented hurricanes that killed at least nine, closing bridges and adversely affecting infrastructure. Indeed, the northeastern United States had some of the most severe winter weather on record in 2011. Freezing temperatures and snow caused a state of emergency in Connecticut, New Jersey, Massachusetts, and parts of New York. Three million people were without power; there were horrific accidents on the roads and flights were cancelled across the region. These incidents were followed by catastrophic flooding in Queensland, Australia where flood waters devastated infrastructure such as dams, bridges and power facilities. Some say that climate change is causing this unusual weather; however, from a critical infrastructure resilience perspective it does not actually matter if climate change is causing these events. What matters is that there has been an increase in unusual and highly unpredictable weather patterns across the world. This will continue for decades to come; NATO and its allies need to adapt and be resilient.

Indeed, it is not just physical critical infrastructure that can be affected by environmental hazards. According to data from the World Health Organization and NASA satellite imagery, it appears that diseases - including dengue fever, West Nile virus, and indeed cholera, are spreading to other regions of the world, such as mainland Europe.[3] Likewise, this maybe be the result of climate change; however again it does not actually matter a great deal if climate change is causing these problems or not. These problems are here to stay; health systems will have to adapt to new and unforeseen challenges for many years to come.

2. Industrial Accidents

Environmental hazards affecting critical infrastructure are often closely connected to industrial accidents.

In Hungary in 2007, a spill of toxic aluminum 'red mud' affected drinking water, transport, and health services, killing nine and affected many more. The region's particularly wet summer may have been a contributory factor, weakening the structure of the dam holding the sludge. Companies that build and maintain our critical infrastructure need to become much more aware of how changing weather patterns create new challenges to civil engineering.

In Japan four separate disasters occurred at the Fukushima nuclear power plant. It is important to note that the plant was resilient to the earthquake, which was the most powerful ever to occur. Immediately after the quake the plant shut down, as designed. The problem was the damage caused by the wave occurring nearly one hour later when the protective seawall was topped by a fourteen-meter tsunami wave. Power was needed at a nuclear power station even after shut-down to keep the uranium fuel cool, as it continued to emit heat. The problem was the equipment, control systems, and the diesel back-up generators were submerged, plus the pipes carrying the cooling water

[3]Priya Shetty, "Climate Change and Insect-borne Disease: Facts and Figures," *Science Development and Network, at* http://www.scidev.net/en/features/climate-change-and-insect-borne-disease-facts-and--1.html (last visited Nov. 1, 2012).

were badly damaged. The storage tanks for the used uranium fuel rods, which need to be continually cooled, were left without power. The fail-safe system for such an occurrence is a heat exchange condensation system, but this only lasted a few hours. New emergency back-up generators rushed to the site did not have the right connections or sockets. The Tokyo Electric Power Company (TEPCO) thought that a total power loss was impossible; indeed, this is understandable. There were indeed multiple back-up power generating systems. It is very difficult for an organisation to make plans for situations that it cannot foresee or which it reasonably thinks are impossible. The recent tornadoes in Alabama killed over 300 in the surrounding area, but an even greater tragedy was averted due to the resilience of the Browns Ferry nuclear power plant, which was able to perform a 'cold shutdown' when it lost power, thereby avoiding a potential meltdown of the nuclear reactor core. Although a very different situation than in Japan, the nuclear industry in Japan – indeed across the world – may want to look at why Browns Ferry was able to shut down. Although there was no flooding at Browns Ferry, its storm damage was extensive. To improve our critical infrastructure resilience, governments need to learn from situations that worked – such as Browns Ferry – as well as those that did not, such as Fukushima.

Thus far this article has examined examples of challenges to our critical infrastructure arising from environmental challenges and industrial accidents. Next it will move on to threats from deliberate sabotage and attack.

3. Deliberate sabotage and attack

Attacks on critical infrastructure can be a necessary part of conflict. In May 1943, as part of World War II, a British Royal Air Force squadron set out to attack three dams in the German Ruhr valley. Operation Chastise, which eventually became known as the 'Dambusters,' was an attack on three dams - the Mohne, Edersee, and the Sorpe; all three dams were key parts of the German critical infrastructure. Two particularly interesting things can be learned from these raids. First, attacks on critical infrastructure can help develop ingenious and highly unusual methods. With the 'Dambusters,' it was the development of a 'bouncing' bomb by a genius named Barnes Wallace. Second, how critical infrastructure is built can make all the difference to the resilience of that infrastructure. The Mohne and the Edersee were indeed breached by the Dambusters. The Sorpe, however, suffered only minor damage. The obvious question is: Why? The Mohne and the Edersee were built of concrete but the core of the Sorpe was covered in earth making it far more resilient to attack. Breaching the Sorpe proved impossible because not enough Lancaster bombers could breach the German defences and launch a highly complex attack pattern on the dam – even more complex than the attacks on the Mohne and the Edersee, which required dropping the bouncing bombs at 60 feet above the water, precisely at a particular point at 280 miles per hour, while under anti-aircraft fire. A key aspect to be learned from this World War II episode is this: Innovation – encapsulated in the genius of Barnes-Wallace – and Resilience, as the Sorpe proved to have – were vital components of critical infrastructure in 1943 and they are today in 2012. These factors of innovation and resilience were as important in a raid on German dams 1943 as they are today 70 years later protecting infrastructure from cyberattack.

In modern times, deliberate attacks on our critical infrastructure again came into

focus on 9/11. NATO and its allies suddenly realized just how vulnerable aviation -- a key component of modern society's critical infrastructure – is to the concept of suicide terrorism. This was something that had never been experienced before, even with the many aircraft hijackings of the 1970s and 1980s or indeed with the deliberate aircraft bombings such as Pan Am 103 over Scotland. Aviation remains at risk. Even with a locked cockpit door as a form of defense Turkish Airlines Flight 1476 was hijacked in 2006 by a terrorist 'rushing' the cockpit when the door was opened by cabin crew. (Terrorists have the opportunity to 'rush' or 'crash' the cockpit at least once or twice on even the shortest flights when the door is briefly opened by cabin crew). Flight 1476 was resolved peacefully, due to excellent cooperation between Turkey, Greece (over whose airspace the flight was hijacked), and Italy, where the aircraft eventually landed.

The first record of aviation terrorism was in 1933; a nitroglycerin explosion occurred on a United Airlines Boeing 247 near Chesterton, Indiana killing all seven passengers and crew. The case was never solved. In 1972, terrorists murdered 26 people in the arrivals hall of Lod Airport, Israel. This event changed airport security forever. Transport was identified as a possible way to inflict mass causalities in 1990. A report by Lewis Libby and Paul Wolfowitz at the U.S. Pentagon, where at the time the U.S. was preparing to go to war with Iraq to liberate Kuwait, identified that the American mainland was vulnerable to an Iraqi biological attack using a terrorist group or a team of trained specialists using transport or transit.[4] In other words back in 1990, 11 years before 9/11, it was identified that a state or indeed a non-state actor does not need long-range missiles or submarines to inflict a great loss of life.

In 1995 the Aum Shinrikyo cult attacked the Tokyo Metro with Sarin nerve agent in coordinated attacks killing thirteen and wounding over 1,000, 50 of them very seriously. Had it not been for the disorganized nature of the attacks many more people would have been killed. Transport remains the ideal means for an aggressor to launch such an attack.

The day after 9/11, NATO invoked Article 5 of the NATO Treaty; Operation Active Endeavour began in October 2001 and NATO's Defence against Terrorism was established, utilizing the expertise of the Centre of Excellence - Defence against Terrorism (COE-DAT), in Ankara, Turkey.

Indeed the security services of the countries that comprise NATO have worked tirelessly to prevent many attacks against our infrastructure. Such planned attacks included the 2006 transatlantic liquid explosives plot (led by British Islamic extremists), the plan to attack a fuel pipeline at JFK airport, and the 2007 planned attack at Frankfurt Airport. Ironically, it may be because of these intelligence successes that al-Qaeda and its associates are trying to hit 'softer' infrastructure targets. The 2005 coordinated attacks on London's underground metro and buses is one example. A year earlier, al-Qaeda inspired terrorists struck at the Madrid commuter train system killing 191. Also in 2004 Abu Sayyaf, affiliates of al-Qaeda, bombed a ferry sailing from Manila in the Philippines, murdering 116. In 2011 a PKK terrorist hijacked a Turkish ferry in the Sea of Marmara; thankfully no civilians were killed, although the stand-off lasted for twelve hours.

It is very possible that al-Qaeda was planning to cause a catastrophe in the US on

[4] U.S. DoD, *Draft Defense Planning Guidance* (1992).

the tenth anniversary of 9/11, possibly on the US rail infrastructure, according to notes retrieved by the U.S .Navy SEALs in the house where Osama bin Laden had hidden. Indeed, despite bin Laden's death the role of the security services in preventing such attacks will continue to be crucial. The former head of the UK Security Service has stated that the UK has about 1,600 terrorists plotting up to 30 attacks at any one time.[5]

Moreover, it is not just transport infrastructure that is under threat. For example, in 1996 the Irish Republican Army attempted to attack four electricity substations near London. If the attack had been successful, it would have crippled electricity supplies for many months, potentially crashing the UK economy and much of its critical infrastructure. In 2002 al-Qaeda attacked the oil tanker Limburg with a suicide boat off the coast of Somalia. Indeed, further documents seized from bin Laden's house indicate that oil tankers will continue to be a target. In Saudi Arabia, and recently in Iraq, al-Qaeda operatives have attacked oil refineries and energy facilities causing many casualties and damaging infrastructure. Al-Qaeda in Iraq (AQII), is trying to attack the country's developing economy by targeting oil facilities. Iraq has the second highest proven oil reserves in the world, but its daily oil production of around 2.5 million barrels is relatively low. Iraq has the ambition to increase this four-fold up to the daily production levels of the US, Russia, and Saudi Arabia. For Iraq to have any chance of achieving this goal, long-term stability is needed, particularly stability and safety for workers in the oil industry. This is why AQII struck at the Beji oil refinery in the Salah ad-Din province north of Baghdad, last year, killing three and injuring many more.

Furthermore, sabotage may also be inflicted by the reckless actions of those who do not deliberately seek to destroy our critical infrastructure, the term 'consequential sabotage' could describe this phenomenon.

4. Consequential Sabotage

Consequential sabotage is the unintended damage to critical infrastructure caused by extreme protest or by the side-effects of particular actions. For example, the aims of pirates operating off Somalia are financial, not ideological; yet their actions attack the logistics of world trade as well as the transport of oil. The NATO allies have done excellent work with Operations Allied Protector and Ocean Shield. This work is of vital importance as pirates provide financex by way of a forced 'operating licenses' for the al-Shabaab waterway. They are main terrorist network in the region and allies of al-Qaeda with similar dreadful aims and objectives. The consequence of these pirates' actions is to help and aid the facilitation of terrorism in Africa – it may not be their aim and they may or may not care that this is the result – but it is the result nonetheless.

A growing and particular area of concern in regard to 'consequential sabotage' is environmental extremism. The actions of environmental extremists may produce results just as catastrophic as a terrorist attack. In the UK, groups such as 'Plane Stupid', an anti-aviation campaign group, climb fences at airports and run across live airports. Extreme environmental campaign groups have occupied coal power stations and attacked trains taking coal to the power stations. Indeed, the recent occupation by

[5] BBC, "MI5 tracking '30 UK terror plots,"' *BBC News* (10 November 2006), at http://news.bbc.co.uk/1/hi/uk/6134516.stm (last visited Nov. 1, 2012).

campaigners of the Cairn Energy Leiv Eiriksson oil rig, in transit from Turkey to Greenland, is an example of this development. A few weeks later Greenpeace again occupied the rig, this time off the Greenland coast. The Royal Danish Navy had to remove the protesters for their own safety, the safety of those who work on the rig, and (ironically), for the safety of the environment. In 2011 the Port of Oakland was blockaded by 7,000 demonstrators; this led to a total shut-down of this key part of California's critical infrastructure. Occupation of an oil rig or a power station, the blockade of a port, or the invasion of a live airport could well produce a human or environmental disaster. If environmental protesters were to damage the control room of a nuclear power station, they could produce a situation as catastrophic as the Fukashima nuclear power plant disaster. If anti-aviation campaigners run across a live runway in front of an aircraft in the process of taking-off, they could produce a tragedy as great as 9/11. The perpetrators' aims do not need to be sinister for their actions to prove catastrophic.

5. Critical Infrastructure and Cybersecurity

Sabotage of critical infrastructure may not only consist of physical attacks; critical infrastructure is also at increased risk from communications technology. Control systems are vulnerable to hacking, manipulation, and viruses which can remain undetected for months, perhaps even years. Such a 'cyberattack' could take place against almost any aspect of our critical infrastructure. Power stations are one example of this vulnerability; each power station has vulnerable equipment that issue commands to control the speed of the turbines and the valves for water control and steam production. The United States is one of many NATO members where power stations could come under such an attack - even if they are 'separated' from the Internet. In the US power grids are divided into regions. This fact does provide increased separational security since a problem in one area should not affect another. The problem is that malicious software, similar to the Stuxnet virus (which was used to crash Iran's nuclear program by spinning its centrifuges out of control), can be used in several areas at once, spread by USB thumb drives, accidentally by engineers, or over the network. A sustained electricity blackout in New York could cause a food shortage in just a week with devastating impacts across the country. Moreover, by the time the exact problem in New York has been identified the virus could have been encrypted and placed on other systems across the US, hidden from view. A new attack could be launched days, weeks or even months later. The reality is that although a system may theoretically be isolated from the Internet, it is very difficult in reality to do this, especially with the proliferation of USB devices taking information from one machine to another. Moreover, such an attack on critical infrastructure does not even need a commander with a phone or a remote control – the attack simply launched when the virus identifies a specific control process, causing the turbine to spin at 100 times the appropriate speed, thereby wrecking the entire plant.[6]

As can be seen, resilience is needed in all of our critical infrastructure. In November 2011, US Homeland Security and FBI officials were altered to an apparent

[6] Steven Prtichard, "Hacktivism: Groups Occupy a Grey Area between Protest and Crime," *The Financial Times* (31 May 2012), available at www.ft.com/reports/cybersecurity-2012 (last visited Nov. 1, 2012).

cyberattack on a water treatment facility in Springfield, Illinois. Hackers caused a water pump to burn out of control by accessing the Supervisory Control and Data Acquisition (SCADA) software. Was the attack meant to damage water treatment? Or was it is a test by Russia, China, or a terrorist group? No one is quite sure, but the attack certainly took place and the consequences of such a coordinated attack could be severe.

It is of course not just terrorists that engage in 'cyberwarfare' – it is a particularly attractive option to other states or their sympathizers, as there is no outward display of hostility that would indicate the start of an actual conflict. So how can NATO members and allies address this growing problem? Much can be learned from Estonia and from Norway, countries which have addressed cybersecurity issues in advanced ways. Both countries treat cybersecurity as an 'open' problem. The 2007 cyberattacks on Estonia's critical infrastructure, when either Russia or Russian sympathizers attacked computer systems across Estonia, made the country's systems much stronger, not weaker. This is because Estonia sees the Internet as a way to make itself more resilient to its huge eastern neighbor. Estonia created a Cyber Defence League - recruiting volunteers who are similar to a reserve army – but who would work in the cybersphere. Likewise, Norway's excellent NorCERT[7] helped prevent a possible attack on the energy company Statoil in 2011. Several Statoil employees noticed something strange in some emails, so Statoil reported them to NorCERT, who subsequently investigated. The emails indeed contained very well-hidden viruses which could have adversely affected Staoil's oil and gas production. The problem was effectively dealt with early on, well before it became an issue of concern. Staoil, and Norway as a country, have a 'no blame' open culture. That is vital to detect cyberintrusion at an early stage. Many countries, however, have a 'blame culture.' Very few employees would identify a suspect email in these countries as they would worry about being blamed for the problem, even losing their job. Such a 'blame culture' has to end if there is to be any chance of addressing this growing and ever-changing threat. Indeed, those who try to do harm do not have a 'blame culture.' Much can be learned from Estonia and Norway to improve cyber security for critical infrastructure. Effective knowledge sharing is the key to this. Now, cyberthreats are also today the prime tool of anarchist groups, often in the form of 'denial-of-service' attacks, rendering commercial websites unusable. Indeed, all that is needed for such groups and individuals is a computer, access to the Internet, and a grudge against society. Dr. Jamie Shea, NATO Deputy Assistant Secretary General for Emerging Security Challenges, describes cyber warfare as the ultimate example of asymmetric warfare - "the weak and the motivated versus the strong and complacent."[8] To help counter these challenges, NATO' has established the Cyber Defence Management Authority, and the Cyber Defence Centre of Excellence in Estonia. NATO also conducts regular defence exercises such as the Cyber Coalition Exercise in 2011. Up to this point, this paper has addressed some examples of environmental, industrial, and deliberate sabotage threats to out critical infrastructure. Now the paper will examine what NATO has done to improve our critical infrastructure resilience, and what further measures can be taken.

NATO's continually evolving policies on Critical Infrastructure Protection were

[7] See Norwegian National Security Authority, "NorCert," at http:// www.nsm.stat.no/Engelsk-start-side/English2/ (last visited Nov. 1, 2012).
[8] Dr Jamie Shea, "Lecture on Cyber Security" (College of Europe, Brugge, Belgium, January 2011).

greatly developed in the wake of 9/11. Just a week after the attacks, NATO Defence ministers asked for a Military Concept for the Defence against Terrorism. The Concept was formally adopted at the 2002 Prague Summit. It enables NATO to take the lead in providing support to counter terrorism and antiterrorism, including:

- Sharing intelligence and shared lessons learned,

- An emphasis on deterring attacks to prevent having to deal with attacks, and

- Providing assistance to civilian authorities, so involvement of emergency services and operators of critical infrastructure will become more coordinated.

At Lisbon Summit of 2010, the New Strategic Concept was adopted by the NATO members. It highlights protection of critical infrastructure from cyberattacks and the importance of energy security.[9]

A new more integrated counterterrorism and antiterrorism policy was agreed at the May 2012 Chicago summit. Critical infrastructure protection is now a key part of this policy.[10]

Moreover, the 2002 Military Concept for the Defence against Terrorism will need to be reviewed in light of the new policy.

In addition to this is the actual on-the-ground implementation. COE-DAT and the International Security Assistance Force (ISAF) are clear examples of this: Operation Active Endeavour, cyberprotection, counter-improvised explosive device work, energy security, the Euro-Atlantic Disaster Response Coordination Center (EADRCC), and of particular importance the Terrorism Threat Intelligence Unit (now integrated and fully part of the Emerging Security Challenges Division), to share knowledge and information are all key parts of NATO's scheme of critical infrastructure protection (CIP).

The Defence against Terrorism (DAT), Program of Work began in 2004 to add more structure to these efforts. This was approved at the Istanbul summit and was of particular relevance to CIP as it is one of 10 key areas of work. The DAT Program is now a key part of the Emerging Security Challenges Division at NATO.

6. The 'Unknown Unknowns'

Of particular concern to NATO and our allies are those type of emergencies which cannot be planned for – the famous 'Unknown Unknowns.' Without a doubt, these types of asymmetric critical infrastructure emergencies will increase in number in the coming years. Some very relevant research into how we manage unexpected events has been conducted by the Australian government and has produced a strategy on critical infrastructure resilience.[11] A particular quote from the Australian Critical Infrastructure

[9] NATO, "NATO's New Strategic Concept," at http://www.nato.int/cps/en/natolive/topics_67814.htm (last visited Nov. 1, 2012).

[10] NATO, "The Chicago Summit,"at http:// www.nato.int/cps/en/SID-C6395F67-A198B263/natolive/opinions_88137.htm (last visited Nov. 1, 2012).

[11] Australian Government, *Critical Infrastructure Resilience Strategy* (2010), available at http://www.ag.gov.au/Documents/Australian%20Government%20s%20Critical%20Infrastructure%20Resilie

Resilience Strategy sums-up very well what our approach should be:

A resilience approach to managing the risks to our critical infrastructure encourages organizations to develop a more organic capacity to deal with rapid onset shock. This is in preference to the more traditional approach of developing plans to deal with a finite set of scenarios, especially in the context of an increasingly complex environment."[12]

The Australians have summed-up the challenge faced by NATO perfectly. A key question to be asked is: What does this mean in practice?

The key is developing methods and exercises to enhance our surprise-responding capacities.[13] In other words, emergency plans will always be needed in order to respond to contingencies that can be imagined, i.e. rare, but experienced events. However, leaders of organizations should also develop 'at the ready' institutional capacities to encounter catastrophic surprises that could overwhelm conventional capabilities. In other words, countries must practice being 'very surprised' and indeed must prepare to deal with emergencies that cannot possibly be foreseen.[14]

The European Union has recently funded the development of a simulation tool at the University of Greenwich in London known as the Pandora Project; it is a computer-aided simulation of different crises scenarios without the need and expense of a full 'for real' exercise. In other words, emergency simulation is now starting to borrow ideas from aviation simulation to move away from static and often unrealistic desk-based exercises.[15]

Indeed, the militaries know much about managing unconventional circumstances. Many have been engaged in 'red teaming' exercises - where the security of an organization or a facility – such as an oil terminal – is tested by a team without the management of that organization knowing that the testing is taking place. Testing the vulnerabilities of critical infrastructure in this way helps lessen the threat. Such simulations should take place not only to test the infrastructure's vulnerability to sabotage, but also to industrial accidents and environmental hazards. It is very important – in fact it is crucial – that the knowledge from such exercises is managed in a way that lessons are learned so that new ways of thinking and adapting can be followed. Knowledge and learning from such exercises needs to be shared among NATO allies and not hidden away in a military department or an intelligence agency. Indeed, knowledge management and continual learning is key to reconstruction and recovery.

Countries need to enhance surprise-responding capacities. They need to share knowledge and lessons learned - effective and usable knowledge management systems

---

nce%20Strategy.PDF (last visited Nov. 1, 2012).

[12] Ibid, p. 5.

[13] Arjen Boin and Allan McConnell, "Preparing for Critical Infrastructure Breakdowns - The Limits of Crisis Management and the Need for Resilience," *Journal of Contingencies and Crisis Management* 15(1) (2007), pp. 50-59; Todd R. LaPorte, "Critical Infrastructure in the Face of a Predatory Future - Preparing for Untoward Surprise," *Journal of Contingencies and Crisis Management* 15 (1) (2007), pp. 60-64.

[14] Boin and McConnell, "Preparing for Critical Infrastructure Breakdowns - The Limits of Crisis Management and the Need for Resilience."

[15] See University of Greenwich, "PANDORA - Advanced Training Environment for Crisis Scenarios," at www2.gre.ac.uk/research/centres/ecentre/projects/pandora (last visited Nov. 1, 2012).

are vital for this. Complex knowledge-sharing systems that are difficult to use end-up being avoided by all.

In addition to these two factors is the importance of first-line responders and operational commanders. These first-line responders must be identified and trained to act independently in an emergency. First-line responders must be able to seize the initiative, especially if there is a problem with the command structure. They should be trained in accordance with a set of core values and priorities which will guide them in their decisions and their actions. They should be trained how to identify when a plan (or plans) should be followed exactly and when they should deviate from a plan. First-line responders need constant training to encourage them to display resilient behavior during a crisis. To help this process, well before any emergency occurs, organizations need to encourage an open flow of information, with knowledge-sharing systems that encourage cross-collaboration across the organization.[16]

To many in the military some of the recommendations here may seem quite obvious. Nonetheless, most organizations are simply not set-up to manage in asymmetric emergencies; the information flow before and during the crisis is impeded by traditional hierarchical structures which prevent cross-collaboration.

Indeed, Chapter 13.3 of the 9/11 Commission Inquiry, discussed the human, or systemic resistance – to sharing information. It identified the problem of 'compartmentalizing' information (or information hoarding) and the problem of basing information access on a 'need to know' basis. There are no punishments for not sharing information, but one could face severe penalties if information is shared with the wrong person, wrong department or the wrong government organization. Security concerns of who has access to information are of course extremely important – however, the Commission argued that the Cold War assumptions about information security are no longer appropriate. The benefits of keeping information secure need be weighed against the costs. The Commission concluded that systems for information-sharing need to be decentralized and network-based, rather than a centralized hub-and-spoke arrangement.[17]

The Commission's recommendations remain crucial today. Indeed, its recommendations can be applied to very different situations, such as the Fukushima nuclear disaster. The recent International Atomic Energy Agency interim report stated that inadequate information and compartmentalized decision-making contributed to the Fukushima nuclear accident.[18]

There are substantial lessons that can be learned from the 9/11 Commission regarding how we protect our critical infrastructure from industrial accidents and extreme weather, as well as deliberate and consequential sabotage.

Security of information is of course paramount and always will be. Intelligence

[16] See LaPorte, "Critical Infrastructure in the Face of a Predatory Future - Preparing for Untoward Surprise."
[17] National Commission of Terrorists Attacks Upon the United States, *The 9/11 Commission Report,* Chapter 13.3, available at http://www.911commission.gov/report/911Report.pdf (last visited Nov. 1, 2012).
[18] See IAEA, *IAEA Misson to Review NISA'S Approach to the "Comprehensive Assessments for the Safety of Existing Power Reactor Facilities,"* (January 2012), available at http://www.iaea.org/newscenter/focus/actionplan/reports/nisa-mission-report0312.pdf (last visited Nov. 1, 2012).

sharing between the agencies of NATO members and allies has greatly improved over recent years; threats to our critical infrastructure do not respect borders. As the 9/11 Commission Report clearly stated, the 'Cold War assumptions' about intelligence sharing may no longer apply in a world of asymmetric threats. So intelligence sharing needs to continue to develop while at the same time ensuring security of information. It is a difficult yet necessary target to achieve, but NATO is the world's leading example of such smart intelligence sharing.

Conclusion

Asymmetric challenges to our critical infrastructure require asymmetric responses. These responses must be flexible and highly adaptable to the particular circumstances. Challenges to our critical infrastructure can come from a wide range of threats including natural hazards, industrial accidents, and deliberate sabotage. However, whatever the cause of the problem, the results of the challenge can be very similar. The challenges caused by a catastrophic environmental hazard can be the same, indeed even worse, than a terrorist strike. The Japan earthquake and tsunami incident is a key example of this. Innovation and resilience are as important today for our critical infrastructure protection as they were 70 years ago. The threats and challenges to our critical infrastructure over the coming decades will be numerous and diverse. NATO has adapted superbly to these new challenges. Nonetheless, these challenges will change rapidly over time; how NATO, its members, allies, and partners adapt to these ever challenging challenges will be crucial in ensuring that critical infrastructure remains resilient, now and into the future.

Bibliography

Australian Government. *Critical Infrastructure Resilience Strategy* (2010).

BBC, “MI5 tracking '30 UK terror plots,'” *BBC News* (10 November 2006).

Boin, Arjen amd Allan McConnell, "Preparing for Critical Infrastructure Breakdowns - The Limits of Crisis Management and the Need for Resilience," *Journal of Contingencies and Crisis Management,* (2007).

IAEA, *IAEA Misson to Review NISA'S Approach to the “Comprehensive Assessments for the Safety of Existing Power Reactor Facilities,”* (January 2012).

LaPorte, Todd R., "Critical Infrastructure in the Face of a Predatory Future - Preparing for Untoward Surprise," *Journal of Contingencies and Crisis Management* 15(1) (2007).

National Commission of Terrorists Attacks Upon the United States, *The 9/11 Commission Report.*

Critical Infrastructure Protection
M. Edwards (Ed.)
IOS Press, 2014

doi: 10.3233/978-1-61499-357-5-13

Critical Infrastructure Protection: The EU Perspective

Francois NAUCODIE
EU Mission to Turkey

Abstract. Although the issue of critical infrastructure protection would normally be a national concern, the cross-border aspects of the problem do cause concern for the European Union (EU). The EU has created a number of bodies to address this issue and they have begun to tackle this issue through a series of seminars. The EU is currently developing a road map for the protection of critical infrastructure.

Keywords. European Union, critical infrastructure protection, subsidiarity

Introduction

Critical Infrastructure (CI) is above all a national affair, hence at the European level, the aim is to bring to light the issues which are cross-sectoral and cross-Member State. The principles of subsidiarity and proportionality are central to this argument; on the former, EU does not take action unless it can be more effective than action taken at national, regional and local levels; on the latter, any new measure should not be proposed where it is not needed. The number of sectors covered (energy, transport, information-communication-technologies, water, food, health, finance, space….) and actors involved (Council – 6 month Presidency + CT coordinator, EC, HRVP and agencies such as ENISA – Network and IT security or Europol – European police office) make this a difficult issue.

1. Background

The European Council Meeting of June 2004 asked for the preparation of an overall strategy to protect critical infrastructure (CI). On 20 October 2004, the European Council adopted a Communication on Critical Infrastructure Protection in the fight against terrorism which put forward suggestions on what would enhance European prevention, preparedness and response to terrorist attacks involving CI.

European Council conclusions on the "Prevention, Preparedness and Response to Terrorist Attacks" and the "EU Solidarity Programme on the Consequence of Terrorist Threats and Attacks" adopted by the Council in December 2004 endorsed the intention of the EC to propose a European programme for CIP (EPCIP) and agreed to the setting up by the EC of a Critical Infrastructure Warning Information Network (CIWIN).

2. State of Play at the EU Level Regarding CIP

In 2006, the Commission proposed a European Programme for Critical Infrastructure Protection (EPCIP) designed to raise critical infrastructure protection capability across all EU Member States and in all relevant sectors of economic activity. It identified the relevant areas with a view to achieving the common objective of improving the protection of critical infrastructures in the European Union. By respecting the principles of subsidiarity and proportionality, the EU activities are meant to support national and regional initiatives without duplicating them.

As part of the EPCIP, a Directive on European Critical Infrastructure was adopted in December 2008. This Directive focused on the identification of European critical infrastructure in the transport and energy sectors, plus introduced requirements on information exchange and basic security measures. Under the Directive, every two years all Member States are required to forward to the Commission information on threats and risks encountered in each sector in which European critical infrastructure was designated. Work has also advanced on the establishment of the CIWIN system to facilitate the exchange of information concerning critical infrastructures.

3. Main Features of EPCIP

EPCIP is intended to provide an overall framework for action, much of which on a sector by sector analysis.

The first sector level initiative in the framework of EPCIP has been on protecting Europe's critical energy and transport infrastructure, focused on identifying what is European critical infrastructure in each transport and energy sectors.

The methodology followed was:

- In the transport area, EC held a number of workshops with MSs and industry stakeholders during seminars organised in 2005 and 2006.

- In the energy field, similar discussions were held at the same seminars. The EC also participated in meetings of the energy security platform, an industry-organised grouping that brings together representatives of European energy associations to discuss security issues.

In addition, between March and June of 2006, expert meetings took place for the maritime, land transport, oil and gas, airports, electricity and air traffic management sectors.

Consultations with stakeholders have been continuing.

4. The Way Ahead: What's Next in 2012?

The Commission has agreed with Member States that the EPCIP should be reviewed in 2012. It is intended to propose a revised programme in November.

To that aim, the EC is preparing a road map for the creation of a European Reference Network for Critical Infrastructure Protection (ERN-CIP). ERN-CIP aims at linking together existing laboratories and facilities in Europe in order to carry out CIP-related security experiments as well as tests of new technology.

The EU is currently engaged in a discussion process on the external dimension of the EPCIP. In June 2011, the Council adopted conclusions on the development of the external dimension of the EPCIP. The conclusions invite both the Commission and the Member States to step up their cooperation with third countries, in order to exchange good practices, but also in order to identify critical infrastructures in third countries, which would potentially affect them.

Conclusion

The COE-DAT initiative is timely. On 14-16 March, a meeting took place with Member States to review the policy including the Directive and CIP sectoral work, such as finance, ICT, space, transport, energy, health, etc.

To conclude, Europol stated in its latest "EU Terrorism Situation and Trend Report TE-SAT 2012": "2011 presented a highly diverse terrorism picture in which the most notable trend was the increasing prominence of lone and solo actor plots."

In that context, use of Internet is a key facilitator for terrorism-related activities:

> Apart from its use as a communication tool, the Internet offers new and additional possibilities to carry out electronic terrorist attacks, for example on the operating systems of critical infrastructure in EU Member States, like energy production facilities and transport systems. Leading members of al-Qaeda have already encouraged “electronic jihad” against critical infrastructure in Western countries.

This page intentionally left blank

Critical Infrastructure Protection
M. Edwards (Ed.)
IOS Press, 2014

doi: 10.3233/978-1-61499-357-5-17

Leveraging Partnerships to Better Utilize Declining Resources: The Critical Infrastructure Risk Management Enhancement Initiative

Michael Beland[1]
U.S. Department of Homeland Security

Abstract. The homeland security enterprise is entering a new stage in its evolution. Focus is shifting to considerations of all-hazards, while resources are becoming increasingly scarce due to the challenging budget environment. Therefore, partnerships of all types must be leveraged to ensure that resources are used in the most effective ways possible. As the National Coordinator[2] for critical infrastructure protection and resilience activities, the U.S. Department of Homeland Security (DHS), National Protection and Programs Directorate, Office of Infrastructure Protection (NPPD/IP) has addressed this challenge by establishing a Critical Infrastructure Risk Management Enhancement Initiative (CIRMEI) and an associated Regional Initiative. These initiatives ensure that DHS and its partners are identifying risks to critical infrastructure, measuring program effectiveness in managing those risks, and aligning resources to develop and execute the tasks and activities that are most successful in addressing those risks. Through the establishment of a set of desired outcome statements and associated metrics, NPPD/IP is assessing critical infrastructure protection and resilience programs and activities; the results will inform programmatic investments. The Regional Initiative, a public and private sector outreach campaign that is part of CIRMEI, will leverage public-private partnerships to collect information from DHS partners that will be used to enhance delivery of regionally tailored capabilities in each geographic section of the United States. As DHS confronts the dynamic and ever-changing environment facing critical infrastructure, CIRMEI provides a defense for the expenditure of valuable monetary and human resources and strives to close identified gaps in risk management capabilities.

Keywords. Critical Infrastructure Risk Management Enhancement Initiative, homeland security, risk management, interagency cooperation.

Introduction

When DHS was created in the wake of the attacks of September 11, 2001, it had a singular focus. The Department was tasked with ensuring that a terrorist event such as

[1] Chief of Staff of the Office of Infrastructure Protection; e-mail Michael.Beland@hq.dhs.gov.
[2] Presidential Decision Directive 63 established a National Coordinator for infrastructure protection, appointed by the President and reporting to the Assistant to the President for National Security Affairs. Critical Infrastructure Protection, PDD/NSC/63(May 22, 1998), available at http://www.fas.org/irp/offdocs/pdd/pdd-63.htm (last visited Nov. 1, 2012).

the one the United States had just endured would never happen again. The Homeland Security Act of 2002 (Public Law 107-296), Title I, Section 101 states:

> (a) Establishment. - There is established a Department of Homeland Security, as an executive department of the United States within the meaning of Title 5, United States Code.
>
> (b) Mission
>
> (1) In General. - The primary mission of the Department is to
>
> (A) prevent terrorist attacks within the United States;
>
> (B) reduce the vulnerability of the United States to terrorism; and
>
> (C) minimize the damage, and assist in the recovery, from terrorist attacks that do occur within the United States.[3]

To accomplish this mission, several existing agencies with long traditions of protecting the homeland were brought into the new department.[4] These agencies, including the United States Coast Guard (USCG) and the Federal Emergency Management Agency (FEMA), came to the Department with a defined, pre-existing mission and a solid understanding of their unique responsibilities to the country.

Although envelopment of the original 22 separate agencies into one department was considered a positive step in realigning the confusing network of government agencies dedicated to protecting the United States, an outstanding need emerged with respect to critical infrastructure protection and resilience. This relatively new mission area required the establishment of an organization and processes that had not existed before. The establishment of a governance structure was also necessary to help coordinate the many risk management activities conducted by DHS partners in the private sector and at all levels of government.

In order to implement a risk management framework, the National Infrastructure Protection Plan (NIPP) was released in 2006 and established a partnership structure for coordination across seventeen (now eighteen) critical infrastructure sectors. Administered by DHS, the NIPP was developed through a major collaborative effort among critical infrastructure partners, including Federal departments and agencies, State and local government agencies, and private sector entities.

The NIPP's overarching goal is "to build a safer, more secure, and more resilient America by preventing, deterring, neutralizing, or mitigating the effects of ... [a terrorist attack or natural disaster], and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency."[5] After Hurricane Katrina devastated a large portion of the Gulf coast

[3] Homeland Security Act of 2002, Pub. L. 107-296.
[4] Like ministries.
[5] DHS, *National Infrastructure Protection Plan* (2006), p. 1.

region of the United States and the Post-Katrina Emergency Management Reform Act of 2006 was passed, more attention began to be placed on preparing for hazards other than terrorism, including natural disasters. Updated in 2009, the revised NIPP integrated the concepts of resilience and protection and broadened the focus of NIPP-related risk management programs to an all-hazards environment.[6]

1. The Current Challenge

The homeland security enterprise is now entering a new stage in its evolution. The once-singular focus on physical acts of terrorism has shifted to considerations of all-hazards. The effect of this shift for homeland security stakeholders is an expansion of the dynamic threat environment to encompass events in addition to terrorism, including weather and cyber-related events. The Department, including NPPD/IP, is now required to be more nimble and flexible in order to provide capabilities that truly enable partners to manage a growing number of risks.

At the same time, like many countries, the United States is facing a challenging budget environment where resources are becoming increasingly scarce. Government agencies must demonstrate effective stewardship over resources as a prerequisite for receiving funding. In order to defend continued investment in their programs, governmental organizations must both identify innovative ways to make established mechanisms work even harder and document how programs benefit partners. These mechanisms – including partnerships of all types – must be leveraged to ensure that resources are applied in the most dynamic ways possible. With budgets expected to contract further, there is a delicate balance between the widening universe of risks to critical infrastructure and the difficulty in acquiring additional resources to manage these risks.

2. The Current Environment for Critical Infrastructure Protection and Resilience

The NIPP has successfully provided the strategy for integrating the many critical infrastructure initiatives of the United States into a single national effort and has defined roles and responsibilities for the partnership. Furthermore, the associated public and private sector partner councils have brought to life an unprecedented partnership to help promote the preparedness of critical infrastructure in the United States.[7] However, the councils have not yet fully realized their potential. These partnerships can be leveraged at the national level to help DHS field-level personnel identify and deliver capabilities where they are needed, at the local level. Desired outcomes and metrics for evaluating the effectiveness of critical infrastructure protection and resilience capabilities were collaboratively developed and implemented by DHS and its partners. The continually evolving threat environment and limited availability of resources require the critical infrastructure community to streamline and maximize the impact of all efforts across sectors and regions. It is imperative that

[6] DHS, *National Infrastructure Protection Plan* (2009)[hereinafter 'NIPP'], available at http://www.dhs.gov/nipp (last visited Nov. 1, 2012).

[7] See DHS, "Critical Infrastructure Protection Partnerships and Information Sharing," at http://www.dhs.gov/files/ programs/gc_1292347375129.shtm (last visited Nov. 1, 2012)..

partnerships are amplified and demonstrate consistent progress in enhancing the protection and resilience of the Nation's critical infrastructure. Otherwise, resources must be re-allocated elsewhere.

3. The Critical Infrastructure Risk Management Enhancement Initiative (CIRMEI)

Addressing the stark new reality of increased demands coupled with decreased resources led DHS to implement the Critical Infrastructure Risk Management Enhancement Initiative (CIRMEI). CIRMEI's purpose is to create a continuous, repeatable, performance management cycle that ensures that risks to critical infrastructure are identified, effectiveness in managing those risks is measured, and resources are aligned to execute those activities that are most successful in addressing the risks. The ability to successfully support partners is assessed by gathering feedback on programs through a variety of data collection methods, including the NPPD/IP Regional Initiative, discussed below. CIRMEI leverages existing partner relationships and aids in the building of new local communities of interest, which are, in turn, expected to help close gaps in risk management efforts. In summary, the CIRMEI strengthens the relationships among risk assessments, mitigation efforts, and desired risk management outcomes by using risk information and feedback from partners to guide budget decisions, so that precious resources are applied where they will be most effective. Figure 1 depicts the CIRMEI feedback loop.

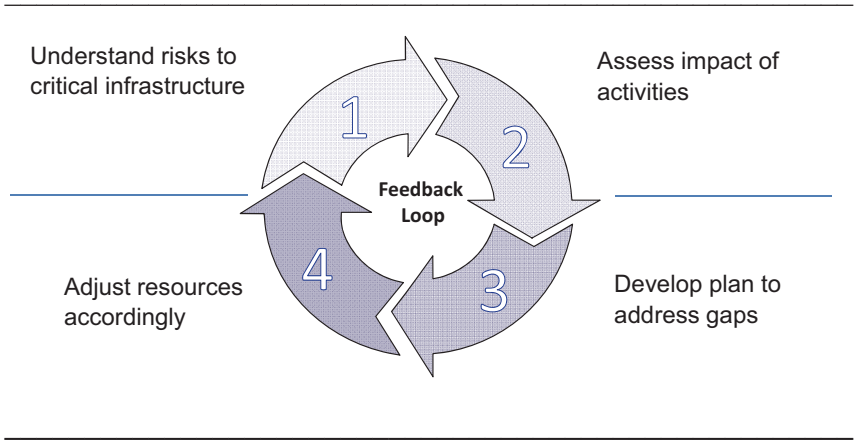

Figure 1. Critical Infrastructure Risk Management Enhancement Initiative

4. Managing Risk

Under CIRMEI, a set of nine National Coordinator Outcome Statements, developed with extensive input from partners, define the end goals for critical infrastructure protection and resilience efforts at the national level. The NIPP partnership also maintains an ongoing effort to collect data and maintain metrics that help measure

progress toward the desired outcomes and identify areas for improvement.[8] Risk, as referred to by the National Coordinator Outcome Statements and associated metrics, is defined by the National Risk Profile (NRP), [9] produced annually as part of the first component in the CIRMEI feedback loop.

The National Risk Profile describes the critical infrastructure risk environment and identifies the risk universe in the short and medium terms. This analysis drives the outcomes and metrics against which risk management efforts are evaluated and also helps to define actions for a risk management plan that outlines how DHS and its partners plan to address any gaps. The only way to accurately claim that efforts are risk informed is by linking the risks highlighted in the National Risk Profile to collective planning efforts. The Profile also describes the implications of risks to each region of the country and each critical infrastructure sector, so that partners can effectively incorporate risk information into their planning.

Once the risks of greatest concern have been identified, the efficacy of current programs in helping to manage those risks and other efforts described by the outcome statements must be assessed. Programs and activities are assessed in relation to the outcome statements and the findings are reported in the Critical Infrastructure Protection and Resilience National Annual Report (NAR). The NAR: (1) contains a comprehensive analysis of that year's metrics data; (2) describes the extent to which desired outcomes are being achieved; and (3) identifies opportunities for improvement. This information is then used to develop a four-year Critical Infrastructure Risk Management Plan (CIRMP) that informs partnership-wide resource allocation. Successive reporting can then quantifiably determine whether the objectives described in the Plan are being accomplished and resources can be realigned accordingly during the budgeting process.

5. DHS Critical Infrastructure Regional Initiative

A key part of the data collection process in the second stage of the CIRMEI feedback loop rests on the ability to gather feedback on programs directly from partners. NPPD/IP has approached this requirement by establishing the Regional Initiative, which provides various forums, including interviews and focus groups, to determine whether its regional partners, in both the public and private sectors, have access to the programs and tools necessary to effectively manage risks to critical infrastructure in their regions. To do this, national-level partnerships must be heavily leveraged at the local level to gather regionally focused feedback from public sector partners and private sector owners and operators. Information gathered as a result of this effort will allow the CIRMP to address opportunities for improvement in the Department's ability to provide the necessary risk management support to the critical infrastructure community. This process will assist DHS in adapting programs and prioritizing resources according to stakeholder-identified needs. The Regional Initiative has become a primary driver of NPPD/IP's annual budgeting process, in order to inform its budgetary requests and ensure it can demonstrate proper stewardship over appropriated resources.

[8] NIPP, Chapter 3, Sections 3.6–3.7.
[9] NIPP, p. 42.

While the Regional Initiative helps to deliver important information that NPPD/IP would not otherwise have on its programs, it produces other tangible benefits as well, which the organization has been able to leverage to continue to advance its mission with reduced resources. The Regional Initiative uses the national-level partnership to identify regional partners who will establish public-private partnerships to further the development of local critical infrastructure communities of interest for the purposes of sustained regional collaboration, coordination, and information sharing. DHS expects that among the benefits of these public-private partnerships will be more organic sharing of intelligence concerning dependencies and interdependencies within a region, which will be extremely valuable during an event threatening critical infrastructure.

It is not only Federal agencies that are dealing with budget reductions and loss of resources – states and local communities are struggling to maintain an acceptable level of preparedness while coping with shrinking resource levels. The operationalization and sustainment of these partnerships helps DHS and its local partners organize to share information and draw upon available tools for maximum benefit. The benefits of these partnerships have already proved their value. In August, 2011, public and private sector partners in the northeastern United States used a network established through a Regional Initiative venue to prepare for and respond to emerging situations during Hurricane Irene. This network helped to facilitate the sharing of important information and lessen the impact of the weather event on the community. Resilience can be supported through the growth of similar regional public-private partnerships nationally.

Although it has been demonstrated that a project such as the Regional Initiative can serve multiple purposes, much of the value is derived from the data captured during the initiative's outreach. Once data from the Regional Initiative is combined with local-level and NPPD/IP programmatic data, it is analyzed and reported annually as progress against the National Coordinator Outcome Statements. As noted above, the NAR is the vehicle for reporting this progress and sets the stage for identifying opportunities to improve critical infrastructure protection and resilience efforts in the CIRMP.

The CIRMP, therefore, addresses gaps in critical infrastructure protection and resilience programs and is the focus of the third component of the CIRMEI feedback loop. Whereas the NAR looks backward and answers questions about how effectively the partnership managed risks to critical infrastructure, the CIRMP looks forward and supports an action plan with specific steps that can be taken to respond to identified opportunities for improvement. This plan will contain goals, milestones, and timelines for risk management activities developed in collaboration with partners. Ultimately, the CIRMP will inform resource allocation decisions. The plan will articulate DHS goals and require that Federal programs coordinate for achievement of a larger purpose.

An additional benefit of the CIRMP is improved coordination of critical infrastructure risk management activities within the Department and increased efficiency across the partnership for driving activities on the ground, because the plan directly links planning and programming processes. In the final stage of the feedback loop, the plan is operationalized, as resources are shifted to support the risk management needs identified by the partners.

To accomplish this last step, resources are prioritized to support programs that have been proven successful through metrics assessment and feedback from partners.

The budget process is the vehicle for prioritizing the allocation of resources to those programs and activities that most directly lead to the achievement of desired risk management outcomes for critical infrastructure protection and resilience. The CIRMEI can only be successful when resource allocation decisions are truly informed by risk and an assessment of past performance. While the NIPP presents an organizing framework that structures partnerships across sectors to deliver a risk management framework,[10] CIRMEI, including the Regional Initiative, elevates these partnerships to a level where, in a decreased resource environment, every dollar delivers real, tangible benefits that meet partner needs. The only way to maintain resource levels to secure critical infrastructure is to demonstrate that the programs and capabilities in place are effectively managing risk.

6. CIRMEI in Practice

During the last year, CIRMEI has gone from a concept to an organized effort among partners. All four components of the feedback loop are currently being executed and leading practices for the implementation of this type of initiative are being established.

The CIRMEI feedback loop is best understood through a simplified, hypothetical example. Assume that one of the desired outcomes is the management of risk to significant critical infrastructure assets. Assume also that the National Risk Profile described an evolving threat and the need to protect against small-scale, swarm attacks on critical infrastructure. The National Annual Report would account for the desired outcome – the management of risk to significant critical infrastructure – and would include metrics that could be used to assess its achievement. Two metrics that could be included in the NAR are: (1) the number of assessments conducted on critical infrastructure facilities that accounted for small-scale attacks; and (2) the number of these facilities that took corrective action as a result of the findings of the assessments. DHS would engage the partnership structure to collect information about assessments conducted nationally, and that data would inform the NAR. The NAR, for example, may report that half of the nationally significant critical infrastructure received such an assessment and took corrective actions. While drafting the quadrennial Critical Infrastructure Risk Management Plan, DHS would consequently consider how many more assessments should be conducted at nationally significant critical infrastructure facilities within the next four years, and the relevant NAR would report upon progress under this objective annually. DHS resources should then be applied to this objective, since the CIRMP will be constructed within a time-period that enables it to inform resource allocation.

[10] The critical infrastructure risk management framework described in the NIPP integrates the elements of risk management relative to human, cyber, and physical threats into a process that allows continuous improvement. NIPP, Chapter 3.

7. Responding to the Findings: Regional Resiliency Assessment Program (RRAP) as a Case Study

Although it is important to justify resource requirements and secure funding for the continuity of critical infrastructure protection and resilience programs, ultimately the efficacy of investments will be evaluated in subsequent years when the NAR evaluates progress against the National Coordinator Outcome Statements. Therefore, as discussed previously, it is imperative that partner needs are understood and action is taken. It is only by responding directly to partners that resources are appropriately leveraged and gaps are addressed. A successful example of CIRMEI at work is NPPD/IP's Regional Resiliency Assessment Program (RRAP), established in 2009. While conducting outreach for the Regional Initiative, partners specifically identified a need for more RRAPs. The RRAP began in 2009 as a pilot program, out of efforts to assess security of individual critical assets. DHS recognized the need to better address the inherent connectivity of assets and systems and the merits of conducting assessments on a regional basis. The RRAP's goal is to identify opportunities for regional homeland security officials and critical infrastructure partners to strengthen resilience to all-hazards. This regional resilience can be achieved through a combination of research, vulnerability assessments, and regional analysis related to the RRAP focus area. The RRAP process identifies current critical infrastructure security and resilience; regional dependencies, interdependencies, and cascading effects; and gaps in State, local, tribal, and territorial agency capabilities. The success NPPD/IP has achieved with RRAPs bolsters its position when justification is required for the request of resources, as it can show that the program successfully addresses a specific need. Partners receive valuable information that enables them to strengthen risk management efforts in their facilities and within their regional context; thereby enhancing overall regional security.

8. Tapping the International Community

As resources continue to be squeezed and the threat environment becomes increasingly dynamic, those executing critical infrastructure protection and resilience programs will need to rely on partners to share leading practices and fresh ideas. International forums for the sharing of these ideas will strengthen the ability of the global critical infrastructure protection and resilience community to become more nimble and adaptable in the face of a variety of threats. DHS is working with interested international partners to develop a Global Infrastructure Security Toolkit (GIST), which is designed to promote the sharing of best practices, lessons learned, standards, methodologies, and other useful materials among countries committed to building robust infrastructure security programs. Examples of included information are approaches to public-private partnerships and information sharing, critical infrastructure assessment and analysis tools, continuity planning exercises, and active shooter training. The GIST is only one example of how successful approaches can be shared to enhance the state of global critical infrastructure protection activities. By harnessing and amplifying global resources, security is increased for the entire critical infrastructure protection community.

Conclusion

Over the past decade, great strides have been made in strengthening the protection and resilience of critical infrastructure. However, a shifting focus toward all-hazards, constantly evolving threats, and increasingly limited resources require the adaption of new approaches and the evaluation of efforts. The Critical Infrastructure Risk Management Enhancement Initiative addresses these challenges by leveraging existing partnerships at the national level to link the identification of risks with the resourcing for programs that have demonstrated the ability to successfully address those risks. Clearly defined risk management outcomes and metrics are vital to measuring progress in closing capability gaps and understanding where realignments must be made during the budget process. The benefits of the CIRMEI approach to the mission of critical infrastructure protection and resilience are evident—a method for identifying risks, a path to assess efforts to manage those risks, and a framework for making risk-informed budget decisions in the future.

Bibliography

DHS, *National Infrastructure Protection Plan* (2006).
DHS, *National Infrastructure Protection Plan* (2009).

This page intentionally left blank

Critical Infrastructure Protection
M. Edwards (Ed.)
IOS Press, 2014

doi: 10.3233/978-1-61499-357-5 -27

Critical Infrastructure Protection in a Post-9/11 World

David Klain[1]
Ultra Electronics – 3e Technologies International

Abstract. This paper focuses on CIP (Critical Infrastructure Protection) and posits an approach to implementing it following the attacks of 11 September 2001 (hereafter referred to as 9/11). While the phrase 'Critical Infrastructure Protection' is used frequently in government, academia, the private sector, and within the NATO alliance, there are many different approaches and constructs to the topic. What is clear is that the terrorist attacks of 9/11 changed how organizations defined critical infrastructure and what strategies were used to protect it.

Keywords. Critical infrastructure,

Introduction

The concept of critical infrastructure is not new; in fact it has existed for thousands of years. Castles and forts were built to protect critical infrastructure, be it a mine, road, bridge, city or government. What has changed over the years is what a nation considered critical infrastructure and what strategies were used to protect it. In 1996, the President's Commission on Critical Infrastructure Protection was formed as an interagency advisory body tasked with developing a strategy to protect certain parts of the United States' infrastructure.[2] In the mid-2000s, NATO formally recognized a need to look at protecting critical infrastructure and an ad-hoc group on critical infrastructure protection was formed to look at the problem. The result was the publication of a white paper that recognized that CIP crosses multiple domains from an organizational as well as functional basis.[3] This was simply an acknowledgement of reality – CIP is situation dependent and what is critical to one person/organization/nation may not necessarily be critical to another.

Following the attacks of 9/11, many countries began to consider threats to their critical infrastructure in light of the evolving threats and struggled to define exactly what was critical infrastructure and how to protect it. In the United States, this effort culminated in the National Infrastructure Protection Plan,[4] while the UK published (and

[1] Vice President, Program Management.
[2] Federal Register, "President's Commission on Critical Infrastructure Protection," at https://www.federalregister.gov/agencies/president-s-commission-on-critical-infrastructure-protection (last visited Jul. 18, 2012).
[3] NATO, *Critical Infrastructure Activities within NATO* (NATO/EAPC(CAPC)WP(2009)003,MULTREF 2009).
[4] Department of Homeland Security, *The 2009 National Infrastructure Protection Plan* (DHS, 2009).

updated) Sector Resilience Plans.[5] These plans (and others like them) took a 'whole of government' approach to CIP and detailed a wide variety of sectors deemed critical infrastructure. While the lists differed in minor ways, in general, the following sectors are considered to be critical:

- Energy
- Information and Communications
- Healthcare
- Food
- Water
- Transportation
- Safety
- Government
- Chemicals
- Defense Industrial Base
- Finance
- Other Sectors or Activities (including monuments/symbols)

A review of the list demonstrates the almost all-encompassing nature of the problem – one would be hard put to find any aspect of a nation which could not arguably fall into one of these categories. The result was that (in many cases), everything became important, making it difficult to prioritize efforts to provide national CIP, and doing so required a risk-based assessment.

1. What Threatens Critical Infrastructure?

While there are many threats to critical infrastructure, they can generally be placed into one or more of five categories: (1) military action, (2) natural disasters, (3) industrial accidents, (4) cyberattacks, and (5) terrorism.

For the purposes of this paper, military action is defined as a deliberate attack on critical infrastructure by another nation-state's military forces to support a military and/or political objective. This includes traditional military action, such as the strategic bombing campaign against industrial production facilities and railway networks during the Second World War, but also includes ballistic missile attacks that may even precede military hostilities when a state of war does not even exist.

Natural disasters originate from weather and other natural phenomena including earthquakes, tornadoes, hurricanes and tsunamis. When considering CIP, the concern is not the loss of life associated with the disaster, but rather the physical effects on critical infrastructure resulting from the natural disaster. A recent example is the radiological contamination and secondary effects of the nuclear disaster at the Fukushima Daiichi Reactor Complex in Japan following the Tsunami in March 2011.

Industrial accidents are failures in the critical infrastructure system itself, resulting from a system failure, operator error or both that is not triggered by a natural disaster.

[5] Cabinet Office, *Sector Resilience Plans for Critical Infrastructure 2010/2011* (UK, 2011).

Examples include the Chernobyl nuclear accident in 1996 and Hungary's red sludge disaster in 2010.

Cyberattacks are deliberate attacks on the information systems used by critical infrastructure operators or the information systems used to control critical infrastructure. An example is the Stuxnet malicious computer virus discovered in June 2010 which attacked Siemens industrial control systems and is widely believed to have been written specifically to attack Iran's nuclear program.

While terrorist attacks are traditionally defined as 'a surprise attack involving the deliberate use of violence against civilians in the hope of attaining political or religious aims,'[6] in recent years terrorists have utilized attacks on critical infrastructure to magnify the effects of their decidedly asymmetric capacity to harm a nation. Recent examples include the 2004 Madrid train bombings and 2005 London train and bus bombings.

This paper postulates that the terrorist attacks of 9/11 truly represented an attack on critical infrastructure – both that of the United States as well as the world at large. While not minimizing the horrific loss of life, the attacks also significantly impacted the information and communications, transportation, safety, government, finance, and monuments/symbols sectors in far reaching ways that are still felt to this day. Arguably those six critical infrastructure sectors were either primary or secondary targets of the attack.

2. Post 9/11 CIP – A Case Study

During the Cold War, the United States and Soviet Union devoted vast resources to ensure survivability in the event of a strategic nuclear exchange. Facilities such as the Cheyenne Mountain Complex were built to protect the military command and control complex.[7] In the case of the United States' legislative branch of government, a bunker was secretly built at the Greenbrier Resort in West Virginia with the aim of providing a relocation site for the US Congress.[8] The facility's existence was a secret until an article was published in the Washington Post in 1992.[9] Following public disclosure about the facility, Congress made the decision to decommission the bunker and many of the plans were put on the shelf.

Following the attacks of 9/11, the author was assigned to the Legislative Branch Emergency Preparedness Task Force, an ad-hoc group chartered to evaluate all aspects of emergency preparedness with an eye towards protecting the critical infrastructure of the United States Congress. While most people think of the U.S. Capitol Building when they think of the U.S. Congress, in fact the U.S. Capitol Complex is actually comprised of a significant number of buildings and locations including: seven office buildings, the Library of Congress, the U.S. Supreme Court, the U.S. Botanic Garden, the Capitol Police headquarters building, a power plant, a mail sorting facility, a steam

[6] Webster's English Dictionary, 2011.
[7] See North American Air Defense Comamnd, "Cheyenne Mountain Complex," at http://www.norad.mil/about/cmoc.html (last visited Jul. 18, 2012).
[8] See The Greenbrier, "Welcome to the Bunker," at http://www.greenbrier.com/play-here/the-bunker.aspx (last visited Jul. 18, 2012).
[9] Ted Gup, "The Ultimate Congressional Hideaway," *The Washington Post* (31 May 1992).

plan, a receiving facility, several parking garages and a day care facility spread out over several square miles.[10] The task was to protect all of the infrastructure of the legislative branch, not just the Capitol building, and ensure that the Congress could continue functioning were another attack to take place.

In considering how to protect the legislative branch itself, the task force needed to consider not just attacks on the people (both members and staff) who are the Congress, but also attacks on the various physical facilities mentioned above, the information technology and communications systems necessary for Congress to function, as well as the unique challenges and threats posed by an attack using a weapon of mass destruction. There were also other complications associated with protecting the CIP of the capitol complex:

- Unlike most critical infrastructure sites located in remote areas or a single campus facility which can be secured, the capitol complex is located in the heart of Washington DC.
- A major rail line on which the majority of people and freight moving up and down the Eastern seaboard passes south of the complex while a spur line connecting the line to Union Station (which is immediately north of the complex) passes beneath the complex.
- The Washington Metro subway system has four stations on the edge of the complex and the subway lines pass beneath various parts of the complex.
- Interstate Highways 395 and 695 (two major transportation routes through Washington) meet just south of the complex with one of the highways passing through a tunnel beneath the mall immediately west of the Capitol building.
- A number of major thoroughfares including Independence, Constitution and Pennsylvania Avenues pass through the complex.
- Much of the complex consists of public buildings accessible to tourists and other visitors coming to meet with members of Congress and their staffs.

The result was a complex CIP environment far more reflective of 'real world CIP' than textbook examples where CIP is accomplished in a vacuum without regard for other factors. The true goal of CIP in most cases is not to protect the critical infrastructure itself, but rather to provide for continuity of operations. Restated – the goal of CIP is to ensure continuity of the function performed by the critical infrastructure. While this obviously does not apply in all cases (monuments and symbols being an example), it provides a slightly different rubric on how to accomplish CIP.

CIP has traditionally focused on protecting the infrastructure/facility/system itself; however, in many cases redundancy can provide for the continuity of operations despite the loss of infrastructure. This is not a new concept – backup systems, alternate facilities or even establishment of multiple facilities with excess capacity are all examples of redundancy used to ensure continuity of operations by distributing risk. It is also important to note that while distribution is traditionally thought of as geographic distribution, in the world of information technology the focus also includes logical distribution.

[10] See Architect of the Capitol, "Capitol Campus/Map," at http://www.aoc.gov/cc/cc_map.cfm for a map highlighting major capitol complex buildings (lastvisited JU. 18, 2012).

How was CIP accomplished in the Capitol complex? It was accomplished through a holistic approach that focused on what functions needed to be protected/preserved and establishing multiple means to do so. CIP planning was not accomplished based on addressing each possible threat – every possible type of terrorist attack, every possible type of industrial accident, etc. Rather a survey of the potential kinds of threats followed a detailed assessment as to the functions and vulnerabilities of the complex and the operations of the Congress itself. This allowed development of CIP plans to address a spectrum of threats and vulnerabilities in an efficient manner (both in terms of cost and disruption) while also integrating CIP into all aspects of operational planning in the organization.

Conclusion

CIP is traditionally the concern of a specialized group who worry about this problem – be it government on the federal, regional or local level or the private sector at varying levels in an organization. Historically, those responsible for CIP planning have accomplished it in a stove-piped manner, often worrying only about their specific sector or infrastructure to address specific threats or risks. CIP has been viewed by leadership as a way to derisk the organization but typically at a cost because excess capacity or capability was being purchased. What was implemented was an evaluation of "the minimum necessary to do the job" to control the costs involved.

CIP is now properly considered in implementing every aspect of an organization's operations. If considered when making implementation or acquisition decisions, CIP becomes entrenched in the very base of the organization's infrastructure and addresses a variety of operational needs, including CIP itself. Solutions which address multiple sectors or threats can provide great value while minimizing costs in a resource-constrained environment. This holistic approach to CIP considers protection, detection, response and continuity/restoration of operations in a manner that provides for effective CIP against threats or risks that were not even imagined when the planning and implementation took place.

While CIP is traditionally spoken of with regards to nations and governments, the reality is something different. Significant portions of a nation's critical infrastructure are in private hands, fully owned and operated by commercial organizations with priorities that may be different than that of the government. A refinery may be critical infrastructure for the country, but the multinational oil corporation that owns it may consider the large numbers of refineries they own and operate around the world to provide dilution of risk. These differing views (and recognition of the differences) mean that public-private sector cooperation is necessary to truly accomplish effective CIP.

Lastly, when taking that holistic view towards CIP, it is very easy to fall into the trap of making everything critical – and when everything is critical, nothing is critical. The large amounts of infrastructure (particularly at the national level) and the variety of threats and risks they face require prioritization and creative techniques to addressing the problem. In some cases, the amount of physical infrastructure to be protected may be reduced. Use of new and emerging technological solutions may reduce costs (e.g., cloud based storage vice dedicated servers or video analytics surveillance vice guards),

but it all stems from an accurate assessment of what actually requires protection (e.g., data vice physical hard drives). Critical Infrastructure Protection is not just about security of the physical plant – it includes protecting every aspect of operations!

Bibliography

Cabinet Office, *Sector Resilience Plans for Critical Infrastructure 2010/2011* (UK, 2011).
Department of Homeland Security, *The 2009 National Infrastructure Protection Plan* (DHS, 2009).
Gup, Ted, "The Ultimate Congressional Hideaway," *The Washington Post* (31 May 1992).
NATO, *Critical Infrastructure Activities within NATO* (NATO/EAPC(CAPC)WP(2009)003, MULTREF 2009).

Critical Infrastructure Protection
M. Edwards (Ed.)
IOS Press, 2014

doi: 10.3233/978-1-61499-357-5-33

Practical Issues Facing Businesses in the Implementation of Critical Infrastructure Protection

Patrick BLACK[1]
OMV Akteingesellschaft, Austria

Abstract. This article discusses the concept of critical infrastructure protection (CIP) from an international business standpoint. Governments and their agencies need to recognize that international businesses, by their very nature, have resilience embedded into their systems, processes, manning and skillsets. Therefore, businesses may not be as keen to protect a particular asset when an alternative is available, often in another country or on another continent. The decisions made by businesses to invest in protection is made based on risk assessment and may result in only a select number of points being protected in order to provide cost-effective protection of the whole system. CIP will also move as business models and processes change in relations to changing business conditions. Lastly, private-public partnerships can help national governments and agencies improve effectiveness and to align solutions with business financial tolerances and better understand the business models.

Keywords. Business infrastructure, CIP, protection investment, public-private partnerships

Introduction

The relationship between government, agencies and industry in Critical Infrastructure Protection (CIP) cannot be understated. Often governments and agencies do not recognize the challenges faced by international businesses. These challenges range from on-going market constraints, uncertain and changing environments through to the dynamic nature of international business and decisions promulgated on a business's international footprint rather than the needs of one particular country. As a result, the designation of sites, infrastructure and processes as 'CIP' are viewed by businesses from both a positive and negative perspective. Whilst this paper seeks to highlight some of the issues that international businesses have in working with governments and agencies, it also acknowledges there is a vast amount of excellent work being undertaken in the public-private partnership field. There is no intention to degrade the commitment, expertise and knowledge that some countries have consistently demonstrated. It does seek, however, to highlight some inconsistencies and shortfalls that can be viewed as 'positive insights' rather than overarching negativity.

[1] CPP (Certified Protection Professional), Global Security Advisor; e-mail: partick.black@omv.com. This article is based on his experience in this field.

1. Implementing CIP Protection in Business

Although there is no doubt that a threat to infrastructure exists, there are a number of challenges in establishing an infrastructure protection programme from a business lens. The following paragraphs contain the most common concerns.

International business models and government business models are different, although, in basic terminology, they seek to be responsible, make a profit, please 'stakeholders' and invest in the future. Therefore the designation of a particular site as 'CIP' often means significant investment with little or no return. This is of particular concern where 'CIP' sites are designated in areas/countries where there is a low threat. Conversely, it could be argued that, by providing such resilience measures in 'higher risk' countries, it provides an 'opportunity' to sustain itself in a country with a fragile infrastructure or political stability. International businesses may consider the designation as expensive with little or no impact to their business model if that site, process or infrastructure is lost in one country. In such cases, it is a challenge to explain to governments and agencies that, what is really important to the functioning of that country may not be mirrored by international businesses which have resilience due to duplicated sites, systems and processes in other countries. In such cases, businesses may prefer to insure for loss rather than make significant security investments. This is particularly applicable in the oil and gas industry which operates a devolved operating model with, for instance, a portfolio of international refineries. The loss of a refinery in one country, whilst it may be devastating economically locally, may have little impact as production and capability maybe enhanced elsewhere in the business to compensate. Critically, there is often a misalignment between threat and reality when business leaders are not fully conversant of the threats to their businesses. As a result, it is sometimes difficult to align the government-driven threat awareness with local and national understanding.

Governments and their agencies need to acknowledge that international businesses, by their very nature, have resilience embedded into their systems, processes, manning and skillsets. Historically, 'CIP' businesses have demonstrated they can survive man-made and natural disasters. It should also be recognized that, in some cases, international businesses may not be investing in one particular country, because the business key site, process or node is located in another country or continent with no linkage to that country. In engaging with international businesses, governments and agencies should review the criticality of that particular, site, process or infrastructure to that business to confirm the appetite for such expensive measures and be prepared to invest if that appetite is absent.

Secondly, and closely related to the first, is the need to undertake detailed risk assessments of the site, process or infrastructure to be protected. This can result in one particular part of a site, process or infrastructure being designated 'CIP', with only that part of the whole requiring protection. This is termed 'citadelling.' There are however, exceptions, with pipeline protection and maritime security being examples. Fixed assets are, however, subject to detailed risk assessments by experts in their field, and it is often a business decision to harden such facilities because of criticality to the international business, compliance with international safety and resilience measures and to protect people, plant, processes and reputation. In some cases too, there is an option to 'do nothing' when the CIP physical and technical security enhancements

could change the posture of the business profile locally. This is termed 'sign-posting' that something has changed. In some cases, however, by leaving a pipeline or other cross-country infrastructure in a 'used' and 'discreet' manner with discreet technical security measures, it maintains its low profile.

There is also a very positive aspect of being designated a CIP site and implementing the physical and technical security upgrades. This is termed 'deflection'. It is however, less-welcomed by neighbouring businesses that may have to upgrade their facilities to counter perceived vulnerabilities. This provides a business dilemma – even if not part of a country's CIP, it may appear that their security, even though proportionally postured to meet the threat and/or industry expectations, is insufficient.

International businesses are always looking for opportunities to increase and reshape their portfolios. As a result, parts of the business may have been designated for divestment or are being deliberately run down. For commercial reasons, these plans may not be in the public domain and business leaders may be reluctant to divulge plans forming part of a longer-term strategy.

Another issue is the absence of a common international CIP standard and methodology. What is critical in one country may not be critical in the next. There is often an issue that governments and agencies may not understand that, in designating a site, process or infrastructure as 'CIP' there may be a lack of awareness of the business model; that sites are rarely 'standalone' and may have interdependencies that are not being addressed in parallel. This absence of a common international CIP framework causes unnecessary complexity as there are many regulatory compliance issues that international businesses also have to deal with.

Governments and their agencies must also recognize that CIP facilities 'move.' This may be as a result of a new technology or process or change from one source of raw material or power to another. As a result, international businesses may choose to divest the business or even shut it down because the product, output or service is no longer financially viable, forms a part of a package of mature options to be divested or a reshaping its direction. There are also 'game changing' activities which impact CIP. The development of 'fracking' has completely changed the international gas landscape and, in doing so, impacted on strategic business models. It has also resulted in a global rebalancing of the energy market with some countries becoming self-sufficient in gas, whilst suppliers face looking for new markets. As a result, CIP investments made that may take 5-10 years to fully fund and implement could, rapidly, lack relevance.

Finally, corporate security staffs are generally small but highly-experienced with deep functional knowledge. Because of the comparative size and geographical spread of that expertise, corporate security staffs rely on local content, technology and information-led security measures. Cost will always be a driver and the ability to use integrated technological solutions is advantageous. . There is a growing understanding too, that governments and their agencies could enhance information-led security to help manage corporate security risk. This includes the sharing of intelligence to permit security staffs to implement timely and proportionate measures. In recent years considerable steps forward have been achieved with the UK Centre for Protection of National Infrastructure and the US Department for Homeland Security in particular. These initiatives are welcomed, and recognize too, that many corporate security staffs are, in many cases, drawn from the government military and intelligence circles. Such

engagement not only enhances the ability of international businesses to respond, but also provides an auditable account why investment in security measures is required.

Coupled with the need to interact with government and agencies is the need for corporate security staffs to interact with employees. Staff morale plays a big part of the way that international businesses operate, so considerable investment is made into motivating and retaining them. CIP measures can have a considerable degrading impact on staff morale. Often recommendations are made to provide 'defense in depth' using physical barriers, stand-off, physical checks of cars and individuals entering and leaving a site. Employees may rightly wish to understand what has changed and why their quality of life may be degraded. Working closely with corporate security staffs provides governments and agencies with additional options to meet national CIP baseline measures without creating an adverse or austere working environment using such methods as crime prevention through environmental design and innovative security technologies.

2. The Government Dilemma

The reluctance to invest in CIP without clear justification is not just a business issue: governments are reluctant too. This is the case when raising the issue of 'how do you control something that you don't own?' Governments also face the challenge of seeking to align themselves with an international standard that currently does not exist. Currently there is no lead organization or body to direct this and, as a result, the approach to CIP is, in some countries, very well-developed and maturing, whilst in others, the need is not understood and therefore the process not embarked upon.

It is very rare that CIP sites stand alone. CIP businesses may be interdependent and interrelated but a considerable amount of cross- and pan-sector work needs to be carried out to align such jigsaw pieces as power and utility independencies, pipelines, ports, railways, raw materials and markets. This is a complex task that often extends well beyond a single country's borders. To fully understand how the infrastructure of a country works as a whole is time-consuming, complex and subject to considerable resistance on both commercial and national secrecy terms. Where CIP cross borders or feeds more than one country, it may lead to considerable debate and discussion on responsibilities, cost sharing and lead nation role.

An issue for many businesses with large geographical 'footprints' is the cost of installing, running and maintaining complex security regimes linked to national police and military agencies. In many cases costs remain the burden of the business rather than shared. In some cases however, government assistance can be offered, but there can be frustration with the speed of government planning cycles which are, in most cases, much slower than that of responsive and market-facing businesses.

A further issue is the gap between government and agency security 'generalists' and deep-seated expertise within international businesses in providing cost-efficient, proportionate and future-proofed protective security solutions. In such cases, government and agency recommendations may only address the issue of providing site security. This may not take address parallel issues which may overrule these recommendations. These can include health, safety and environmental concerns, existing industry-wide best practice and compliance issues. In some cases, this relates

to a limited awareness of security technologies and solutions that can be implemented. Of more concern is the issue of an armed response to an incident requiring entry to a site where hazardous materials are in use or stored and kinetic weaponry could be employed. Early engagement and working very closely with corporate health, safety, security and environmental staffs ensures that all stakeholders have expectations met.

In summary, it is difficult for governments to 'lead' in CIP implementation; it requires recognition that both the private and public sectors provide particular skill sets, access to information and finance to synergize the relationship. Once understood by both parties, a positive and dynamic relationship can be built.

3. Private-Public Partnerships

Private-public partnerships are the future. International businesses have, in general, demonstrated excellence in developing accurate global information and intelligence information to deal with security threats. To complement information-led security, corporate security staffs must also develop analytical forecasting, enhanced and cutting-edge protective security measures, deeper planning, training and increased staff situational awareness. Governments and agencies can improve effectiveness by working to achieve broad understanding and commitment at an international level, greater information-sharing, improved funding and faster financial cycles and to align solutions with business financial tolerances and better understand the business models.

Conclusion

Implementing CIP is a difficult, expensive, time-consuming and complex process involving numerous stakeholders. Whilst there may have been difficulties in the past, there is a growing recognition that the public-private partnership approach is the most efficient way to assess, implement and inform CIP across a range of sectors. By fusing the corporate knowledge, business models, agility, revenue streams and tolerances of the private sector with the access to information, international engagement, funding and expertise in the public sector there is considerable synergy, proportionality, pragmatism and costs-savings to be accessed using the public sector. In doing so, both sectors mutually benefit.

This page intentionally left blank

Critical Infrastructure Protection
M. Edwards (Ed.)
IOS Press, 2014

doi: 10.3233/978-1-61499-357-5-39

Critical Infrastructure and Its Impact on Energy Security

Mitat ÇELİKPALA[1]
Istanbul Kadir Has University, Turkey

Abstract. Energy security has emerged as an issue of great importance. As well as the traditional aspects of energy security, a myriad of new aspects has emerged and continues to emerge such as tight oil and gas markets, increasing prices, alternative energy sources and their role, the threat of terrorism, instability in some exporting and importing countries, geopolitical rivalries, and the increasing need for energy to fuel economic growth. The concept of energy security is vague. Energy security is an umbrella term that covers many concerns linking energy, economic growth and political power.

Keywords. Energy, security, terrorism.

Introduction

As Daniel Yergin has suggested, energy security became an issue on the eve of the First World War, when First Lord of the Admiralty Winston Churchill made a historic decision to shift the power source of the British Navy's ships from coal to oil.[2] Churchill's basic intention behind this decision was to make the British fleet faster than its German counterpart. This underlying decision was a watershed event that made the issue of energy security an important issue of national strategy and security.

With this decision, British decision makers shifted their attention towards the Middle East. This switch meant that the Royal Navy could rely not on coal from British sources anymore but instead had to rely on oil supplies from the Middle East. This meant a new strategy for the British decision makers and a new threat for security structures. Thus, from then on, energy security became a question of national strategy and energy security means in Churchill's words "safety and certainty in oil lie in variety and variety alone." Since Churchill's momentous decision, energy security has repeatedly emerged as an issue of great importance and it is so once again in today's world.

Currently, as well as the traditional aspects of energy security, a myriad of new aspects has emerged and continues to emerge: tight oil and gas markets, increasing prices, alternative energy sources and their role, the threat of terrorism, instability in some exporting and importing countries, geopolitical rivalries, and the increasing need for energy to fuel economic growth. At present, the issue of energy security is not

[1] Department of International Relations, e-mail: mitat@khas.edu.tr
[2] Daniel Yergin, "Ensuring Energy Security," *Foreign Affairs* 85 (2006), pp. 69-70.

restricted to oil. High natural gas prices and the situation in the gas sector, the electric power blackouts in the US and power cuts in Europe, hurricanes and their negative effects on supply, and nuclear energy-related issues together with alternative resources make the issue more complicated. This presentation aims at discussing and analyzing the basic parameters of energy security by taking different aspects into account.

1. Definition: What does Energy Security Mean?

The concept of energy security is vague. Definitions range from uninterrupted oil supplies to the physical security of energy facilities to support for biofuels and renewable energy sources. Therefore, it is not wrong to say that the energy security is an umbrella term that covers many concerns linking energy, economic growth and political power. Traditionally, the concept of energy security was limited to the security of consuming countries and energy security issues focused on disruptions of the crude oil supply from the Middle East. From this perspective, the traditional elements of energy security were classified as supply sources, demand centers, geopolitics and market structures. Especially during the energy crisis of the 1970s, the primary focus for the Western industrial countries was on sources of oil supply and geopolitics.[3]

The current energy security system was created in the 1970s to counter the crude oil disruptions in the Middle East. As a response to the 1973 Arab oil embargo, the industrialized countries, most of whom were the members of the OECD, established the International Energy Agency. The basic aim of this organization was to ensure coordination among those countries to counter the disruption of energy supply, encourage collaboration on energy policies, avoid bruising scrambles for supplies, and deter any future use of an oil weapon by the exporters.[4] Thus the term 'energy security' was narrowly viewed as reduced dependence on oil consumption and imports, particularly in the OECD and other major oil importing countries.

From those days on, the term 'diversification' then became the main or key concept in energy security. Nevertheless, despite the fact that the term diversification is still a key concept in energy security, the environment and content has changed a lot in the last couple of decades. Some issues remained the same of course but some has changed. Regional and social turmoil are still unsettled in the main producing areas but there are new aspects in the system. The potential for global terrorism focused on energy supply systems was not a consideration in the mid-1970s.

Currently global or local terrorism threatens the entire system. The Iraqi war or Iran's nuclear program has led to oil and gas disruptions and could lead to new ones. Political turmoil in Nigeria and Venezuela could have serious consequences in the energy supply chain and have disrupted significant oil supplies. Climate change and related regulations as a new aspect of the energy security are also on the agenda. Natural disasters and their consequences are new phenomena that researchers have to take into account. The hurricanes in the Gulf of Mexico in 2005 showed everyone that consumers in the US or elsewhere are at risk and have to face new risks in terms of higher and more volatile prices, both at the gasoline pump and in their heating bills.

[3] Cambridge Energy Research Associates, *The New Energy Security Paradigm* (World Economic Forum, 2006), available at http://www.weforum.org/pdf/Energy.pdf (last visited June 4, 2012).
[4] Yergin, "Ensuring Energy Security," p. 75.

As a result, the G-8 meeting in St. Petersburg in July 2006 took energy security as the key concept in its agenda. The G-8 countries renewed their focus on energy security and discussed the tight oil market, high oil and gas prices, the threat of terrorism, instability in some exporting countries, a nationalist backlash in those regions, geopolitical rivalries and developing countries' increasing need for energy to power their economic growth. The oil and gas crisis just before the economic crises in 2008 forced everyone to think about the issue of energy security on a wider dimension. With the overall energy system stretched to its limits, the critical physical connections between gas and power, between oil refineries and power, and between pipeline distribution systems and power led everyone on the planet to think about energy security-related issues once more. Thus the term energy security does not encompass only the flow of oil and diversification. It now extends to the entire infrastructure of energy supply that supports the global economy – off-shore platforms, long distance oil and gas pipelines, oil and gas tankers, as well as refineries, storage and generating facilities, transmission lines and distribution systems.

More narrowly, energy security is defined as the "reliable and adequate supply of energy at reasonable prices" or as "securing adequate energy supplies at reasonable and stable prices in order to sustain economic performance and growth." Within this definition, prices and supply diversity are critical components of energy security. It should be stressed that energy security (the continuous availability of energy in varied forms, in sufficient quantities and at reasonable prices) has several aspects. It means limited vulnerability to transient or longer disruptions of imported supplies. It also means the availability of local and imported resources to meet growing demand over time at reasonable prices. This perspective put three basic elements in front of us, essentially encapsulated in the energy security: availability, accessibility and affordability. Among those three elements, availability means availability on demand. We may clarify this by saying that when a country needs or wants energy, it should be available. Accessibility means the nation should be able to access energy sources globally in order to ensure uninterrupted growth. Affordability also means the affordability of the energy being procured to ensure that the growth engine is not impacted by the price impact. From this perspective, it could be said that while rich countries are able to find willing sellers, the issue of energy security gains importance for developing countries which have invested huge amounts of money in infrastructure but still face issues of high costs for energy. As a result, the energy security issue is becoming related with reducing risks and dealing with risks.[5]

Reducing risks is meant to reduce energy requirements by increasing efficiency in the production and use of energy. Looking at the global sources to stake equity and generate alternate sources of energy are other aspects. When it comes to the issue of dealing with risks, topics such as strategic storage, infrastructure, technology and in-place resources are coming to the fore. Thus the current definition of energy widens from how to handle any disruption of oil supplies from producing countries to include the protection of the entire energy supply chain and infrastructure. The challenge of energy security grows because the scale of the global trade in energy grows substantially as world markets become more integrated.

[5] Hisham Khatib, "Energy Security," in *Energy and the Challange of Sustainability* (UNDP, 2000), pp. 112-131.

In line with this perspective, Daniel Yergin defines ten key principles of energy security:

1. Diversification of energy supply source is the starting point for energy security.

2. There is only one oil market.

3. A 'security margin' consisting of spare capacity, emergency stocks and redundancy in critical infrastructure is important.

4. Relying on flexible markets and avoiding the temptation to micromanage them can facilitate speedy adjustment and minimizing long-term damage.

5. Understand the importance of mutual interdependence among companies and governments at all levels.

6. Foster relationships between suppliers and consumers in recognition of mutual interdependence.

7. Create a proactive physical security framework that involves both producers and consumers.

8. Provide good quality information to the public before, during and after a problem occurs.

9. Invest regularly in technological change within the industry.

10. Commit to research, development and innovation for longer-term energy balance and transitions.[6]

As can be seen clearly from this analysis, the definition of the energy security widens to encompass different aspects of political, financial, technological, social and security agendas.

2. Maximizing Energy Security

By taking these myriad aspects of the issue, some authors suggest different dimensions of energy security for both energy-consuming and energy-producing countries in order to reach a comprehensive and clear definition of the term. Alhaji identifies six competing dimensions of the term: economic, environmental, social, foreign policy, technical and security.[7] He argues that these dimensions reflect the integration of energy policy into other policies; balancing all these dimensions within an energy policy is not an easy task because, despite their universal and general character, the weight of each of these dimensions differs by place and time; the interaction between them also differs from country to country and from time to time. Thus, he sees the concept of energy security is "an amoebaean concept at its best."[8] It changes shape and dimensions continuously. Thus, a careful and efficient policy maker in the long run can only maximize energy security.

[6] Daniel Yergin, "Energy Security and Markets," in *Energy and Security: Toward a New Foreign Policy Strategy* (Jan H. Kalicki and David L. Goldwyn, eds., Woodrow Wilson Press and Johns Hopkins University Press, 2005).
[7] A. F. Alhaji, "What is Energy Security," *Energy Politics* IV (2008), pp. 62-82.
[8] Ibid, p. 73.

The economic dimension of energy security is related to the strength of the relationship between energy consumption and GDP. That necessitates the use of fiscal and monetary policies. The economic dimension of energy security ensures that the scarcity of energy resources does not stall economic growth, increase inflation, raise unemployment, weaken the balance of payments or reduce the value of a country's currency. The impact of the scarcity of those resources on these key macroeconomic variables depends on the strength of the relationship between energy consumption and the GDP. The solution does not lie in the energy sector nor is it related to the policy makers in the ministries of energy but requires the use of fiscal and monetary policies. Therefore, fiscal and monetary policies should be integrated into any energy policy and vice versa. Policy makers can enhance the economic dimension of energy security through the implementation of a combination of fiscal and monetary policies.

The environmental dimension is related to the incorporation of environmental objectives into energy policies. Pollution or increasing prices are aspects of the environmental dimension. Since the environmental impact of producing, transporting and burning fossil fuels has health and economic consequences, several countries have incorporated environmental objectives into their energy policy. Nevertheless the dichotomy of development and environmental concerns is still on the table.

The social dimension is most ignored dimension of energy security. Most energy policies do not focus on the social dimension. The energy security debate mostly focuses on external factors that are related to the security of supplies and the political situation in the producing countries. The environmental dimension of the domestic aspects has precedence currently but the social dimension has barely attracted attention. The social dimension of energy security might require governments to intervene to reduce the energy gap between the rich and poor. The larger the proportion of the poor who are not able to get energy resources, the more energy insecurity the country experiences. When energy prices are high, the gap between the rich and the poor became obvious. The result of such an energy gap could well be political unrest, which will reduce economic growth.

The foreign policy dimension of energy security deals with the relationship between energy sources and politics. Energy and politics are intertwined each other. A fear of shortage of energy resources may force a country into some disadvantageous relationships with countries having energy producing powers with which it would not otherwise cooperate. The need for energy might force some countries to take foreign policy decisions that would compromise them on other important issues or principles. Accordingly, several countries have linked energy security to strategic and defense considerations, an indication that they realize the foreign policy dimension of their country's energy security. The need for energy might force some countries to limit their foreign policy options. This dimension thus focuses on diplomatic and trade relations.

The technical dimension is a government's push to improve energy security by supporting technologies that facilitate the production of renewable energy resources. Technology is the eternal partner of energy security.

The security dimension of energy security deals with the physical security of the energy infrastructure and the energy needs of the security apparatus. Threats to the physical security of the energy infrastructure include terrorist attacks, human error,

natural disasters and technical malfunctions. Measures of the security dimension include the geographical location of energy resources and facilities relative to the location of the market, the locations of various threats and the natural disaster prone areas. These measures also include frequency of terrorist attacks and energy consumption.

Conclusion

In sum, all indications point to a broadening in the definition of energy security. There is improvement in energy security in all parts of the world, thanks to technological advances, adequacy of resources, and regional cooperation. The world will continue to depend on fossil fuels for decades to come. These fuels, nevertheless, have detrimental impacts on the environment that must be dealt with to achieve sustainable development. This requires promoting clean energy technologies, pursuing energy efficiency, developing renewable forms of energy, and providing technical assistance to developing countries, where most growth in energy use will take place. Being aware of all these facts, it has to be mentioned that no energy policy is complete or successful without focusing on energy security. A discussion of energy security is useless without understanding its meaning in order to able to measure and assess it. The energy market is global. Deregulation and market liberalization pose questions for energy security and for the future role of the state with respect to energy security. To improve energy security, any country needs to collect relevant, up-to-date data, measure the various dimensions and assess energy security. Only then can policy makers make an informed decision and protect their country from future crises. A market leading to innovation reduces costs, increases trade, improves allocation of resources, and spurs technological development, all of which enhance energy security. Markets also normally pursue short-term objectives, while energy security demands long-term planning, investment and political will. The state therefore needs to continue to play a role in ensuring national long-term security of supplies and protecting consumers.

Bibliography

Alhaji, A. F., "What is Energy Security," *Energy Politics* IV (2008).

Cambridge Energy Research Associates,*The New Energy Security Paradigm* (World Economic Forum 2006).

Khatib, Hisham, "Energy Security," in *Energy and the Challange of Sustainability* (UNDP, 2000).

Yergin, Daniel, Energy Security and Markets, in *Energy and Security: Toward a New Foreign Policy Strategy* (Jan H. Kalicki and David L. Goldwyn, eds., Woodrow Wilson Press and Johns Hopkins University Press, 2005).

Yergin, Daniel, "Ensuring Energy Security," *Foreign Affairs* 85 (2006).

Critical Infrastructure Protection
M. Edwards (Ed.)
IOS Press, 2014

doi: 10.3233/978-1-61499-357-5-45

Threats to Energy Resources and Infrastructure

Staff[1]
COE-DAT, Ankara, Turkey

Abstract. The world energy infrastructure is vulnerable to a variety of man-made and natural disasters. Cyberattacks are an emerging threat that grows daily in its ability to create energy shortages on a grand scale. War, both conventional and unconventional, has the possibility to cause huge energy disruptions in a region or even in the whole world. Crime, both economic and political, rages from the small, localized stealing to the piracy (and often ransom) or large tanker ships. The world needs to come together to be able to address these threats in a comprehensive manner.

Keywords. Energy infrastructure, piracy, cyberattacks, war and energy

Introduction

Energy is a prime commodity in international trade that relies on a worldwide system of production and delivery. Such a complex system is very vulnerable to man-made and natural disruptions. This article will deal with, in turn, the threats to the energy infrastructure by cyberattack, conventional warfare, unconventional warfare, and criminal activity. Although economic factors and weather can also affect energy infrastructure, they are beyond the scope of this article.

1. Cyberattack

Cyberattack is an emerging vulnerability for energy systems. The vast expanse of infrastructure required to bring energy, particularly liquid fossil fuels and electricity, to markets makes the energy infrastructure vulnerability to cyberattack. Because the system is so complex and long, remote controls and surveillance systems are often used; for example, many switches or pump stations are controlled by SCADA (supervisory controls and data acquisition) systems that use either radio signals, or, increasingly, Internet connectivity to control the flow of energy resources. Surveillance systems can be deceived to show that all is normal when in fact a physical threat is approaching. Although the threat started with amateur 'hackers," the attacks are coming now from state cyberwar units or by state-controlled groups.[2] One of the

[1] This is a summary of the presentation made by Senior Energy Analyst Frederick Pollack of the NATO *NATO Intelligence Fusion Centre*; please direct any questions to e-mail: Frederick.Pollack@ifc.bices.org.
[2] See NATO, "The History of Cyberattacks," *NATO Review, at* http://www.nato.int/docu/review/2013/Cyber/ timeline/EN/index.htm (accessed 08 Oct 2013).

advantages of this type of attack is that one can be safely at home, conducting the attacks remotely, so that there is less risk of detection and less physical risk as well. The limits on this type of attack are not known but are becoming widely spread and numerous.

2. Conventional Warfare

In a conventional war (nation vs. nation) the energy infrastructure can be targeted directly or indirectly. With a declaration of general war, all military targets can be attacked, so if the energy structure is part of the military apparatus (generally, yes), then it can be destroyed legally. However, even if not part of the military structure, the energy infrastructure can be attacked indirectly as 'collateral damage' incident to an attack on a valid military target. The test for this is whether the collateral damage is greater than the military value of the target (normally not), so the energy infrastructure can suffer indirect damage in this way.

A very vivid on destruction of the energy infrastructure occurred during the tanker war associated with the Iran-Iraq war. In the span of 4 years (1984-1988), 546 commercial vessels were damaged by the sides targeting ships transiting the region; as a result Iraqi oil exports dropped 85% while Iranian oil exports dropped 80%.[3] Another example is attacks on oilfields during the on-going hostilities between Sudan and the new state of South Sudan where critical components of oilfield pipelines have been attacked and destroyed.[4]

Although the legality of these attacks can be questioned, they certainly have an impact.

3. Unconventional Warfare

Unconventional warfare, particularly insurgencies and other types of internal conflicts, can be another source of threat to the energy delivery system. In these types of situations, the insurgents want the populace to lose faith in the central government. Light (electricity) and heating (fuel oil) are two particularly sensitive utilities that definitely influence the people. By disrupting the energy supplies that keep electricity and fuel oil distributed, insurgents can create unrest that fosters their goals. Byproducts of these attacks on the energy systems can also prevent the government from using these resources against the insurgents while keeping the insurgents supplied and undermining international support for the government.

A good example of this is post-war Iraq (2004-2011) when insurgents kept disrupting oil pipelines and electricity supplies. Not only did this cause economic losses but also turn the tide of sympathies away from the government that could not secure/protect these services.

[3]Bradley S. Russell and Max Boot, "Iran Won't Close the Strait of Hormuz," *The Wall Street Journal* (January 4, 2012)

[4] BBC, Sudan Accues South Sudan of Attacking Oilfield," *BBC News Africa* (April 10, 2012), available at http://www.bbc.co.uk/news/world-africa-17671091 (last visited 08 October 2013).

4. Criminal Activity

Threats to energy infrastructure from criminal activity can be divided into two categories: terrorism (politically motivated) and normal criminal activity (financially motivated).

The energy system is a natural target for terrorists. Everybody is dependent upon energy for their daily personal and professional lives. Economic growth is directly related to energy usage so attacking the energy infrastructure of a country can be a way for terrorists to severely affect nations. Just like for the insurgent who wants to cause a loss of confidence in the government, terrorists want to leverage their attacks or threats of attacks to compel the target government to change a policy or take some action.

"As the economies of the world grow and societies develop, so does the importance of energy. And so does the importance of the infrastructures that produce and supply this energy."[5] The U.S. National Counterterrorism Center counts 2750 terrorist incidents on energy infrastructure occurring between 2004 and 2011.[6] These are not limited to a few nations, but are spread all around the work and range from attacks on refineries or pipeline to attacks on power stations to attacks on oil company executives. They one thing these attacks have in common is the loss of confidence in the energy delivery process.

Theft can vary from small petty theft to large grand theft. On the lower end, illegal tapping of power lines or oil pipelines causes small losses but exposes the vulnerabilities of the systems that other may decide to exploit. On the other end, piracy (which is a financial crime) causes the loss of millions of dollars in ransom, increased insurance costs, and delays in deliveries; 2010 saw a high of 445 piracy incidents; with half of those in the high transit area off the coast of Somalia.[7] Piracy incidents against tankers increased from 9 in 2006 to 49 in 2010.[8] However, as a result of a number of counterpiracy measures, this dropped on 28 incidents in 2011.[9] These criminal activities have a large aggregate effect on energy supplies.

Conclusion

The threats to the world energy infrastructure are credible and diverse. Both man-made and natural disasters can take their toll, but the man-made threats can be countered to a certain extent and both threats can be countered to a certain extent. However, it is clear that the threats to world energy are not abating but are generally increasing in number and scope, requiring all of us to do our best to protect and defend the world energy system.

---

[5] Raphael F. Perl, "Protecting Critical Energy Infrastructures against Terrorist Attacks: Threats, Challenges and Opportunities for International Co-operation"(Reinforced NATO Economic Committee Meeting, Brussels, 22 September 2008), full text in Annex.
[6] National Counterterrorism Center, "Counterterrorism 2013 Calendar," at http://www.nctc.gov/site/ index. html (accessed 09 October 2013).
[7] International Maritime Bureau Piracy Reporting Center, "Piracy & Armed Robbery News & Figures," at http://www.icc-ccs.org/piracy-reporting-centre/piracynewsafigures (accessed 08 October 2013).
[8] Ibid.
[9] Ibid.

Bibliography

BBC, Sudan Accues South Sudan of Attacking Oilfield," *BBC News Africa* (April 10, 2012).

Perl, Raphael F., "**Pr**otecting Critical Energy Infrastructures against Terrorist Attacks: Threats, Challenges and Opportunities for International Co-operation"**(**Reinforced NATO Economic Committee Meeting, Brussels, 22 September 2008).

Russell, Bradley S., and Max Boot, "Iran Won't Close the Strait of Hormuz," *The Wall Street Journal* (January 4, 2012).

ANNEX A

Protecting Critical Energy Infrastructures

Against Terrorist Attacks: Threats, Challenges and Opportunities for

International Co-operation

Reinforced NATO Economic Committee Meeting

22 September 2008, Brussels

Address by Dr. Raphael F. Perl

Head of the OSCE Action against Terrorism Unit*

Ladies and Gentlemen,

Dear Colleagues,

Let me start by thanking NATO's Defence and Security Economics Directorate for having invited me to address the important topic of energy security. It is a pleasure and a great honor for me to address such a distinguished audience.

The importance of energy security, and energy infrastructure security, cannot be overstated. Think about what would be the potential consequences of a terrorist attack against the energy infrastructure system. Think about the consequences of a successful terrorist attack on a nuclear power plant – radioactive clouds spreading across borders, very much like the Chernobyl disaster in 1986. Or think of a successful terrorist attack against a super tanker in the Strait of Hormuz – wreaking havoc in the oil market

Clearly, energy security is among the most serious security and economic challenges both today, and in the future. As the economies of the World grow and societies develop, so does the importance of energy. And so does the importance of the infrastructures that produce and supply this energy. Critical energy infrastructures provide the fuel that keeps the global economy moving and our societies working.

Disruptions of energy distribution, natural or manmade, are likely to have cascading effects on the entire system, in fact on all aspects of society. And the destruction or disruption of critical energy infrastructure such as nuclear power plants, dams of hydroelectric power plants or major pipelines, would have a potentially serious, if not catastrophic impact on the health, safety, security and economic well-being of citizens.

For the international community, energy security and critical energy infrastructure security presents both challenges in terms of the threats we face, and opportunities in terms of how we can respond to those threats. Enhancing energy security, very much like combating terrorism, is a complex, multifaceted and interdisciplinary challenge. It requires a comprehensive approach and all countries have a stake in it. Important contributions can be made by all of us, in our different fields of expertise.

And let me stress that the topic of energy security is particularly relevant for the OSCE. My organization spans North America and Eurasia, including Central Asia, the Caucasus, the Caspian Sea, and the Black Sea. We have 56 participating States, among which are found some of the biggest producers of energy commodities, and some of the largest consumers of energy, as well as strategic transit countries. And the OSCE, like NATO, is considering how it can add value to enhancing energy security. OSCE participating States have adopted in November last year a Ministerial Decision on *Protecting Critical Energy Infrastructure from Terrorist Attack* (MC.DEC/6/07). In implementation of this decision, we are examining opportunities for cooperation with relevant international organizations in this field, and we will soon report to our participating States for further deliberation on an appropriate OSCE involvement.

So what I suggest to you in my remarks today is first that I share some of my thoughts on the terrorist threat to critical energy infrastructures. And then I will attempt to identify some needs and options for response, including opportunities for international cooperation.

Assessing the Terrorist Threat to Critical Energy Infrastructure and Vulnerabilities

The reality of the terrorist threat to critical energy infrastructure is often discussed, especially by the private sector: the companies owning and or operating these infrastructures. As a case in point, the International Association of Oil and Gas Producers (OGP) ranks terrorism only in 6th position in terms of threat to the industry, behind violent crime, organized crime, militant activism, civil unrest and political instability. But such assessment of the threat may well be underestimated.

I would suggest that terrorists, particularly Al Qaeda inspired terrorists think different in terms of targets and target priorities. An avowed goal of Al-Qaeda inspired terrorists is to inflict damage of catastrophic proportions, not only physical but also economic damage.

Disruption of the global economic system and of the western lifestyle has become a goal and a rallying call for Al-Qaeda inspired terrorists. From this perspective, energy infrastructures, given their economic importance, could be particularly attractive as targets for terrorists.

If one wants to cause economic damage, attacks on energy infrastructure are clearly an attractive option for terrorists. The economic impact of such attacks, even if they are localized, has the potential to be greatly amplified given the volatility of the energy market and other economic implications. Think for instance of the consequences of the failed Al Qaeda suicide attack against Saudi Arabia's largest oil refinery in Abqaiq, early 2006 – oil prices jumped $2 a barrel on news of the attack. And following the terrorist attack on the French super tanker Limburg in 2002 off the coast of Yemen, oil maritime transportation costs tripled!

Moreover, as the energy infrastructure system is highly networked, a potential exists for a cascade of disruptions, thereby multiplying the impact of a single localized attack. Just think of the massive blackout experienced by the United States and Canada in the summer of 2003, which affected some 50 million people in the Northeast. And

this started with a single generating plant unexpectedly shutting down in Ohio, sparking a cascade of failures across the whole grid.

Much of Al Qaeda leadership is engineers – they think in term of systems and networks. We need do the same, and we need to think in terms of multiple attacks.

I would also suggest to you that energy is often perceived as being at the core of some controversial decisions, policies, and attitudes of western countries. Hence, some energy infrastructures could also be attacked for their symbolic value.

So the terrorist threat is real, but how vulnerable are we? I would suggest that despite all our commendable efforts, vulnerabilities still exist. These vulnerabilities derive from a number of different factors. Overall, the system today is complex, highly networked along a transnational supply chain, from extraction/production to local distribution, with thousands of kilometers of pipelines and power lines, cutting across wide open areas, or dense urban environments. Critical junctions, nodes, choke points and bottle necks exist along transportation routes and transmission grids. Important single facilities exist, like hydroelectric dams or nuclear power plants.

In addition, these energy infrastructures are connected and/or dependent upon other infrastructures, such as transportation networks and facilities, but also information and communication infrastructures, which represent yet another source of vulnerability. Many experts argue indeed that the threat of cyberattacks against energy infrastructures today is underestimated.

Some researchers also point to the potential employment of Electromagnetic Pulse (EMP) technology by terrorists. It only takes a microwave and some amplifiers for an individual to remotely target, interfere with, and potentially disable operating and control systems, without the immediate appearance of an attack.

Globalization and deregulation also create vulnerabilities. The energy infrastructure system today is profit-oriented and arguably suffers from under investment, especially in terms of security enhancement. The drive for profit and optimal efficiency has resulted in decreased resiliency and decreased redundancy in back up in the sector. The industry itself recognizes the existence of competitiveness / security trade-offs, but arguably still favors competitiveness.

Needs and Options for Response

So the threat is potentially great, arguably increasing, and vulnerabilities abound. But what can we do? To put everything in a nutshell: we need to foster a proactive – comprehensive – inclusive and cooperative approach to securing the energy infrastructure system. We need to take a holistic approach, thinking in terms of securing the entire energy supply chain – not in fragmented terms – not just security of some physical infrastructures.

Moreover, I suggest to you that rather than focusing specifically on the terrorist threat, security enhancement measures should be designed, promoted and treated as an investment against security hazards in general. We should not think of this as a costly response to a threat, but rather an investment opportunity.

The security measures we take to protect energy infrastructures from terrorist attacks also apply to mitigating other criminal threats, as well as possible accidents or natural disasters.

Clearly, as we cannot protect everything to the same extent we need to prioritize our efforts and allocation of resources. The approach followed by most countries here is to identify the "critical" component of their energy infrastructure systems, the Critical Energy Infrastructures located on their territory. However, these criticality criteria vary from one country to another, thus perhaps, it could be useful to strive towards an harmonized definition of what is critical.

A need also exists for comprehensive and regular assessments of vulnerabilities and threats to the energy infrastructure system. For this, analytical methods and capabilities must be strengthened, ideally again on a harmonized basis. A broad range of energy

infrastructure protection issues must be addressed, including cyber threats, electromagnetic threats. Infrastructure situational awareness should be enhanced to the maximum extent possible and private owners and operators should be compelled, to the maximum extent possible, to regularly report to state authorities on the status of their infrastructures. In addition, state authorities could arguably do more to share threat information with the private sector.

Developing public-private partnerships (PPPs) is a potentially effective tool here. This is an area where my organization, the OSCE, is particularly active. Effective PPPs require clarifying roles and responsibilities, building mutual trust, as well as highlighting mutual benefits and the shared valued outcome of co-operation. These are results we want to achieve. To maximise the effectiveness of such partnerships, a variety of stakeholders, public and private, must be involved to discuss their needs, concerns and priorities, to identify compromise approaches and joint actions, and first of all to share information.

Building on this honest exchange of information and assessment of vulnerabilities, threats, and risks, we must aim at cost-effective mitigation measures, to enhance both physical and cyber security. Importantly, security arrangements should be tailored to take into account the specific characteristics of a given infrastructure. For example, when dealing with nuclear power plants, hardening and military protection seems only reasonable. When addressing the security of other infrastructures, it might simply be desirable to build more redundancy into the system and prepare for the eventuality of acceptable, perhaps inevitable or unpreventable losses.

As we cannot protect everything, preparedness, resiliency and recovery capacity are paramount to ensuring continuity of service. It is quite telling in this regard that the division of the United States Department of Energy that deals with energy infrastructure security is called the *Infrastructure Security and Energy Restoration* (ISER) Division.

And with this, I come to the issue of institutional capacity-building. The approach to securing the energy infrastructure system that I am promoting here is very much a strategic approach. For such a strategically-oriented comprehensive strategy to be adequately devised, let alone implemented, institutional capacity is *sine qua non*.

National inter-agency co-ordination has to be strengthened and this could take the form of special national interagency bodies or taskforces for instance. A need also exists to maintain and/or to enhance civil emergency planning and disaster response capabilities in the event of a successful attack.

Conservation can also do much to reduce efforts required to bring energy supplies up to speed and to backfill supplies or compensate for decreases in supply in wake of a terrorist attack. Arguably, this is an area where we need to do more.

Opportunities for International Cooperation

I would now argue that international co-operation is essential with respect to most, if not all needs and action areas that I have just identified. Given the transnational character of the energy supply chain, countries have a vested interest in co-operating to ensure the integrity of the energy infrastructure system. More experienced and resourced countries have a vested interest in sharing their expertise and providing assistance to other less resourced or experienced countries.

As energy security of a particular country is closely linked to that of others, each country needs to know what others are doing. Compliance with existing international safety and security standards is a key element of transparency and essential to regional energy stability. International co-operation is obviously indispensable to further promote such compliance, including through the provision of assistance, expert advice and training.

Besides, many actors of the energy sector feel that as the energy infrastructure system is transnational, a need exists for international efforts towards development of a uniform cross-border regulatory framework and comprehensive set of international standards for energy infrastructure security.

But we need not wait for such a comprehensive framework to take action. There is already a wealth of experience, good practices and lessons learned that are waiting to be disseminated. Countries would also benefit from more exchanging data and information, as well as from pooling resources to promote further research on energy infrastructure security.

Due to their particular location or importance, some critical energy infrastructures arguably require targeted cross-border co-operation. In this regard, I would like to recognize here the ongoing efforts of the European Union towards the identification of *European* Critical Infrastructures. The United States Global Critical Energy Infrastructure Protection (GCEIP)

Strategy is a model one might also want to draw from, which aims at assisting foreign countries in improving the security and resilience of overseas petroleum infrastructures identified as critical for the United States.

International co-operation could also be specifically enhanced with initiatives focusing on key energy corridors or areas. Establishing a *Critical Energy Infrastructure Emergency Response Network* might also be an option worth considering as a possible mechanism for enhanced international co-operation.

And at the confluence of objectives between counter-terrorism and energy security, we might want to put more emphasis on the need for further international co-operation in terms of enhancing maritime security, transport security, and cyber security.

Finally we should not overlook the role of international organizations such as the OSCE and NATO. International organizations have also an important role to play here, in their different field of expertise, where they can add value to existing efforts. My organization, the OSCE, has the potential to play a key role in raising awareness and mobilizing political support; it could promote intergovernmental as well as public-private co-operation; and it could support the enhancement of national capabilities. The OSCE, with its 56 participating States, has a comprehensive security mandate with a soft power focus, as opposed to the specialized mandates of other organizations. It is arguably therefore well positioned to serve as a platform to promote a comprehensive approach to critical energy infrastructure protection.

Conclusion

I would like now to briefly conclude by reiterating a few thoughts. The economic importance of the energy infrastructure system and interdependencies in the energy supply network leave us vulnerable to terrorist attacks on major facilities, nodes or routes, aimed at paralyzing the whole system by cascade effect.

The threat is potentially great, increasing. But we must not over react. We cannot protect everything – we must protect wisely and ensure against potential losses. Excessive redundancy and back up are generally not perceived as cost effective. But major damage to the energy infrastructure system, where supplies remain disrupted for long periods of time, is even less cost effective. And clearly, as we cannot protect everything, building resiliency and recovery capacity must be emphasized.

Energy security like terrorism is a truly global issue in which we all have a stake. Hence international co-operation is indispensable – we are all on the same boat. And we all need to work together to maximize our ability to effectively protect the energy infrastructure system from attacks and to maximize our resiliency and ability to recover in the wake of such attacks.

I thank you again for this opportunity to offer my thoughts on this important and timely topic.

Thank you for your attention.

Critical Infrastructure Protection
M. Edwards (Ed.)
IOS Press, 2014

doi: 10.3233/978-1-61499-357-5-55

Protecting Pipelines - BTC as a Case Study

Staff[1]
COE-DAT, Ankara, Turkey

Abstract. Energy security does not depend upon just the supply but also the transportation infrastructure, much of which are pipelines. Pipelines can be vulnerable to attack, particularly in Turkey where 22,000 km of pipelines carry 4% of the world's daily oil production. In addition to terrorism, there are other threats to pipelines. Unless it is willing to post guards at every ten meters, a company will have to take measures to allocate resources to meet the highest risk. This article discusses the BTC approach to pipeline security.

Keywords. Transit, pipelines, infrastructure security

Introduction

Energy security is not just about the energy supply; it is also about ensuring it gets there. The energy transportation system is a massive category of infrastructure that is hard to protect. With so many vulnerable locations, it presents a real problem with regards to management of security assets. This article addresses this issue by looking at what energy security is within the meaning of infrastructure protection, then will discuss the specific case of Turkey with emphasis on the BTC pipeline that transits Azerbaijan, Georgia, and Turkey. The last portion will deal with the security threats and measures taken to address those threats.

1. Critical Energy Infrastructure Security

Analysis on the global system of energy security often focuses on two components of 'diversity of supply' and 'reliability of supply' but often fail to mention 'energy infrastructure security.' Despite its critical and integral role in the sector, energy infrastructure security is often neglected in policy circles and academic studies. However, regardless of how energy security is defined, it always includes the protection of critical energy infrastructure as a crucial element of the energy sector.

Terrorist attacks and illegal tapping have important economic implications on oil and gas prices since there appears to be a "security premium" of between $1 - $25 per barrel. Thus, terrorist sabotage and theft from oil and gas facilities exposes economies to rising energy prices. As an example, al-Qaeda has argued that priority should be given to attacking energy facilities in the Middle East. After Osama bin Laden's call

[1] The staff of COE-DAT prepared this summary of a presentation made by Hasan ALSANCAK of British Petroleum, Turkey. Questions should be directed to the author at Hasan.Alsancak@ec1.bp.com.

for attacks against oil, the terrorist attack on Abqaiq, Saudi Arabia's giant oil processing facility in 2005 was the first direct attack by al-Qaeda. Even though the attack was termed a 'failed terrorist attack' by official Saudi statements, on news of the attempted attack, the price of crude oil increased 3.4%.[2]

2. Pipelines in Turkey

Pipelines going through Turkey are very important to Turkey as well as to the world. With more than 22,000 km of pipelines traversing Turkey, more than 4% of the daily world oil production flows through Turkish pipelines. Turkey has a valuable geostrategic position in this regard, by sitting between the world's largest energy market in Western Europe and 70% of the world's oil reserves in the Middle East, Turkey is central to the world energy infrastructure and therefore world energy infrastructure security. This transit function also provides substantial income for Turkey.[3] More pipelines in Turkey are planned for the future.

One of the pipelines in Turkey is the Baku-Tbilisi-Ceyhan (BTC) pipeline, which at 1776 km is the longest in the world (1,076 km are in Turkey). It transports one million barrels per day (1.2% of world oil production) of Azeri, Kazakh and Turkmen crude to the Turkish port of Ceyhan. The BTC Corporation, a consortium of eleven companies, owns the pipeline, with majority stockholder (31%) British Petroleum operating it. It is an impressive engineering feat – with a diameter varying between 42 and 46 inches, it has 720 road/rail crossings and 1500 water crossings. In case of breach, flow can be controlled with 100 block valves.

3. Security Threats against Pipelines

BTC see four types of threats against the pipeline: illegal tapping, vandalism, cyberattacks, and terrorism. Of these, illegal tapping and terrorism will be discussed.

Illegal tapping itself is more of a nuisance than a threat but does expose the fact that large amounts of the pipeline can be accessed unobserved. This is especially true in Turkey where there are no dedicated state security forces patrolling the pipeline and land owners may farm the land that the pipeline crosses. Coupled with the economic factors of the high price of petroleum in Turkey and the low penalties for illegal tapping, makes this a continuing problem. After a high of seven incidents in the third quarter of 2004, the norm now is two incidents per year, but is still indicative of a security problem for vandalism or other damage. This is a move afoot to increase penalties under Turkish law for illegally tapping pipelines.

Terrorism is another matter. Beyond the normal terrorism problem in Turkey from PKK and related organizations, the geopolitical balance between Turkey, Iran, Iraq, Syria, Israel, the U.K., Russia, and the U.S. can all affect this. For example, if Iran

[2] Khalid R. al-Rodhan, "The Impact of the Abqaiq Attack on Saudi Energy Security (CSIS, 27 February 2006), at http://csis.org/files/media/csis/pubs/060227_abqaiqattack.pdf (last visited Aug. 19, 2013).
[3] John Daily, "Yet Another Attack on Turkish Pipelines," *OilPrice.com* (14 October 2012), at http://oilprice.com/Energy/Crude-Oil/Yet-Another-Attack-on-Turkish-Pipelines.html (last visited Aug. 19, 2013).

were to shut down oil transportation through the Straits of Hormuz either directly or indirectly, the importance of the BTC pipeline increases and so does its value as a target. This vulnerability is best illustrated by the 5 August 2008 atatck on the pipeline that occurred just prior to the Russia-Georgia war.[4]

The impact of disruptions can have a number of effects. There is of course always the possibility of fatalities or injuries to either workers or innocent bystanders. Oil spills can have lasting effects on the environment by damaging land so as to make it unuseable but can also ruin water supplies and kill wildlife. The business owning the pipeline itself can suffer reputational issues within the business community or the community as a whole from its failure to deliver product in a timely manner. This can lead to financial losses from the oil lost, penalities for failing to meet contract performance or governmental fines. In the bigger picture, reduction in the supply of energy can lead to worldwide or regional rising oil and gas prices.

4. BTC's Holistic Security Strategy

> "Security should be taken into consideration during the proposal, planning and implementation stages of all new capital projects."[5]

To secure the pipeline, BTC has employed a holistic approach that uses risk management to identify the need for physical security measures and to focus the efforts of private security personnel.

The security of the pipeline is implemented via responsibilities outlined in the Intergovernmental Agreement (IGA), the Host Government Agreement (HGA) and the Turkish Law on the Transit of Petroleum (Law 4586[6]).

Through physical security measures, the goal of the BTC security is to deter, detect, delay and deny. By creating physical obstacles to access, critical portions of the pipeline can be protected. When that fails, detection systems will notify the security forces of an intrusion; while the intruders are dealing with physical security measures, security forces are closing in on the intruders.

5. The Way Forward

Pipeline security is not an easy task and BTC has tried to approach this from a smart point of view (rather than a blunt force approach) by integrating risk management, state security forces, private security forces, personnel security and cooperative measures to mitigate the danger. Measures taken to address the tapping problem include community awareness and elimination of microrefineries as well.

[4] Ibid.
[5] BP Group Security Policy
[6] Promulgated in Official Gazette 24094, 29 June 2000.

Conclusion

Pipeline security is absolutely vital to the security of the world's energy supply. Disruption of energy supplies can have disastrous effects on the lives of people as well as on businesses and governments. Pipeline security cannot be guaranteed but can be managed through the efficient use of smart resources.

Bibliography

al-Rodhan, Khalid R., "The Impact of the Abqaiq Attack on Saudi Energy Security (CSIS, 27 February 2006).

Daly, John, "Yet Another Attack on Turkish Pipelines," *OilPrice.com* (14 October 2012).

Critical Infrastructure Protection
M. Edwards (Ed.)
IOS Press, 2014

doi: 10.3233/978-1-61499-357-5-59

An Analysis of a Cyberattack on a Nuclear Plant: The STUXNET Worm

Staff[1]
COE-DAT, Ankara, Turkey

Abstract. The STUXNET worm has come into daily lexicon by accident. A very powerful piece of malware, designed to target specifically Iranian nuclear facilities using certain Siemens software, has shown us the possible vulnerabilities to such measures.

Keywords. Malware, virus, worm, targeting

Introduction

The name STUXNET is very well-known to the computer world and the general public as well. This 'worm,' found in many countries of the world, demonstrates that ability of potent software to penetrate into secure facilities. The possibilities of such malware causing substantial damage have now gone from the theoretical to the possible.

1. A History of Malware

Almost as long as there have been computers, there has been malware. Ignoring for the purposes of this paper, the 'bugs' or unintentional errors in software, 'viruses' have been used to 'infect' a target computer by inserting One of the earliest viruses inserted a 'backdoor' into a program so that it could be accessed by people other than the programmer or system administrator.

The idea of infectious programming was carried a step further with the development of 'worms' – software that was capable of replicating itself in order to travel from computer to computer without further instruction. The worm exploits vulnerabilities in software to take control.

One particular type of system is quite vulnerable – Industrial Control Systems (ICS) – which are normally of three types: Supervisory Control And Data Acquisition (SCADA) systems; Distributed Control Systems (DCS) and Programmable Logic Controllers (PLC). These systems can control a wide range of other systems, the disruption of which can be catastrophic.

[1] The summary was prepared by the staff of COE-DAT. Please direct any questions to the presenter: Associate Professor Ahmet Koltuksuz, Yasar University, Izmir, Turkey at ahmet.koltuksuz@yasar.edu.tr.

2. The STUXNET Worm

The STUXNET worm has become almost common knowledge as a result of substantial news coverage. It was first discovered in June 2010 by a security company called VirusBlokAda.[2] Analysis of the code showed it to be specific to target the SCADA and PLC systems of the Iranian nuclear research and development activities. It did this by attacking an application based on Microsoft Windows that was used by an ICS used to control machinery (centrifuges) built by Siemens of Germany. The worm could spread through linked computers as well as "air-gapped" machines through the use of storage media (such as 'flash drives').

There were five specific vulnerabilities exploited by STUXNET:

- MS08-067 RPC Vulnerability – allowed a remote user rights equal to a local user
- MS10-046 – LNK Vulnerability – allowed remote insertion of malware
- MS10-061 – Spool Server Vulnerability – allowed a malicious print request to take control of a server
- MS10-073 – Win32k.sys Vulnerability – opens a vulnerability to execute kernel privileges
- CVE-2010-2772 – Siemens SIMATIC Win CC Default Password Vulnerability – use of known default password to access the system[3]

The worm could then spread by removable storage media, local areas network (LAN) communications, and through infected data files.

The source of this code has been subject to much speculation, focusing on possible nation-states with access to Siemens code provision and the motive to attack the Iranian nuclear system.[4]

3. The Impact of STUXNET

Although the STUXNET worm appears to have been designed to attack a very specific target, its ability to move from computer to computer resulted in widespread distribution. By September 2010, the STUXNET worm had infected 59% of

[2] Gregg Keizer, "Is Stuxnet the 'Best' Malware Ever?," *InfoWorld* (16 September 2010), at http://www.infoworld. com/print/137598 (accessed Oct. 11, 2013).
[3] Aleksander Matrosov, *et al*, "Stuxnet under the Microscope," *ESET* (undated, Version 1.31) available at http://go.eset.com/us/resources/white-papers/Stuxnet_Under_the_ Microscope.pdf (accessed Oct.11, 2013).
[4] A recent report attributes STUXNET to a joint US-Israeli operation. David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *New York Times* (1 June 2012), available at http://www.nytimes.com/2012/ 06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all (accessed ct. 11, 2013).

computers in Iran, but also 19% of computers in Indonesia and 9% in India.[5] Although found in lesser concentrations in other countries, it was assessed to have infected almost 5% of the computers worldwide.[6]

One worry of computer security professionals has been that the STUXNET worm could be modified to attack other systems without losing the ability to move from system to system that made it so effective. Therefore, the total effects of STUXNET may not be known for years.

Conclusion

The STUXNET worm was a very powerful piece of malware that was developed for a specific purpose. However, its wide distribution shows how quickly even secure systems can be infected with harmful software. Although the damage this time was limited, we may not be so lucky the next time.

Bibliography

Keizer, Gregg, "Is Stuxnet the 'Best' Malware Ever?," *InfoWorld* (16 September 2010).
Matrosov, Aleksander, *et al*, "Stuxnet under the Microscope," *ESET* (undated, Version 1.31) .
Sanger, David E., "Obama Order Sped Up Wave of Cyberattacks Against Iran," *New York Times* (1 June 2012).

[5] Symantec, "W32.STUXNET" (26 February 2013), at http://www.symantec.com/security_response/writeup.jsp? Docid=2010-071400-3123-99 (accessed Oct. 11, 2013).
[6] Ibid.

This page intentionally left blank

Critical Infrastructure Protection
M. Edwards (Ed.)
IOS Press, 2014

doi: 10.3233/978-1-61499-357-5-63

Strategies to Counter Cyberattacks: Cyberthreats and Critical Infrastructure Protection

Bilge KARABACAK and Ünal TATAR[1]
TÜBİTAK-BİLGEM, Ankara, Turkey

Abstract. Today, cyberthreats have the potential to harm critical infrastructure which may result in the interruption of life-sustaining services, catastrophic economic damages or severe degradation of national security. The diversity and complexity of cyberthreats that exploit the vulnerabilities of critical infrastructures increase every day. In order to lessen the potential harm of cyberthreats, countermeasures have to be applied and the effectiveness of these countermeasures has to be monitored continuously. In this study, a brief definition and history of critical infrastructure are introduced. Cyberthreats are examined in four fundamental categories with the vulnerabilities of critical infrastructure categorized and examined. Finally, countermeasures that may play a key role in critical infrastructure protection programs are discussed.

Keywords. Cyberattack, critical infrastructure, cyberthreats

Introduction

Critical infrastructure is those physical and cyberspace-based systems essential to the minimum operations of the economy and the government.[2] Critical Infrastructure Protection (CIP) is an important program in which governments have to take action to cope with threat to that infrastructure, to include cyberthreats. The first formal document that uses the term 'critical infrastructure' dates back to 15 July 1996, which was an executive order signed by the U.S. president.[3] Physical threats and 'cyberthreats' are stated as two major threat types in this executive order. The purpose of the executive order is to set forth the basic outline of CIP.

According to the Presidential Decision Directive, much of the critical infrastructure has historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity to improve efficiency, however, this infrastructure has become increasingly automated and interlinked.[4] Therefore, it is important to note that the term of "critical infrastructure protection" was proposed after the widespread use of information

[1] Chief Researcher and Researcher, respectively.
[2] Presidential Decision Directive/NSC-63 (22 May 1998), available at http://www.fas.org/irp/offdocs/pdd/pdd-63.htm (accessed 12 June 2012).
[3] Presidential Executive Order 13010, "Critical Infrastructure Protection" (15 July 1996), p. 3, available at http://www.iwar.org.uk/cip/resources/eo/eo13010.pdf (accessed 8 December 2012).
[4] Presidential Decision Directive/NSC-63.

technologies in that infrastructure. Critical infrastructure and information technologies have strong relationships in many different ways and at many different levels.[5]

Cyberthreats are evolving with each passing day. Almost every week, a new cyberincident appears in the media. Cyberthreats are asymmetric in nature;[6] They can harm critical infrastructure to A great extent by making minor changes to operations. This paper, categorizes cyberthreats against critical infrastructure. The vulnerabilities of critical infrastructure are defined with the countermeasures for the resulting risks categorized and listed.

1. Strategies to Counter Cyberattacks

In this part of the paper, cyberassets, cyberthreats, vulnerabilities of critical infrastructures and countermeasures are explained in the following four subsections, respectively.

1.1 Cyberassets: Critical Infrastructures

Today, almost all critical sectors use cybersystems. The transportation, banking and finance, health and emergency, defense and government sectors use conventional information technologies. The telecommunications sector is also a part of the critical infrastructure and it is entirely composed of information technologies.[7] Some of the critical sectors are controlled and monitored by Supervisory Control and Data Acquisition (SCADA) systems, which are specially crafted software and equipment. Energy, water and critical manufacturing are key sectors that use SCADA systems.

In the 1970s, 1980s and even in the 1990s, SCADA systems were legacy systems. They were composed of exotic, proprietary and even obscure hardware and software. SCADA systems were almost always unique to the specific system and isolated as well. There weas no access to corporate networks and the Internet..

Today, SCADA systems use open international standards for most operations. They use standard hardware, software, operating systems, and protocols. SCADA systems make use of commercial off the shelf (COTS) products in most cases. Today, SCADA systems are well-documented as well. Finally, SCADA systems are connected to corporate networks and even to the Internet by wired or wireless means.[8] Therefore, energy and water industries may be directly exposed to cyberthreats.

In general, almost all of the critical sectors are connected to the Internet. Although the Internet is a physically-distributed infrastructure, it is logically unified. In this unique logical infrastructure, we live with cyberthreats like cyberattacks,

[5] Wipul Jayawickrama, "Managing Critical Information Infrastructure Security Compliance: A Standard Based Approach Using ISO/IEC 17799 and 27001," in *On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops* (Zahir Tari, ed. Springer Books, 2006), p. 563.
[6] Nir Kshetri, "Information and Communications Technologies, Strategic Asymmetry and National Security" *Journal of International Management* 11 (2005), p. 564.
[7] Fernando Beltran, Alain Fontenay, and Marcio Alameida, “Internet as a Critical Infrastructure: Lessons from the Backbone Experience in South America,” *Communications & Strategies* 58 (2005), p. 1.
[8] Vinay M. Igure, Sean A. Laughter, and Ronald D. Williams, "Security Issues in SCADA Networks," *Computers & Security* 25 (2006), p. 500.

cybercriminals and cyberspies. In the next subsection, cyberthreats are discussed in four categories.

1.2 Cyber Threats

Cyberthreats can be categorized in four main groups.[9] These groups are hacktivism, cybercrime, cyberespionage and cyberwar. However, there is sometimes no clear-cut distinction between these groups as shown in Figure 1. These categories of cyberthreats can intersect with each other in many different ways. A member of a hacktivist group may get into cybercrime activity. The same person may take part in coordinated cyberwar or cyberespionage.

An action in cyberspace can be categorized or perceived as both cyberwar and hacktivism. As an example, a country can consider a cyberincident to be cyber war while on the contrary, another country can consider the same act to be hacktivism.

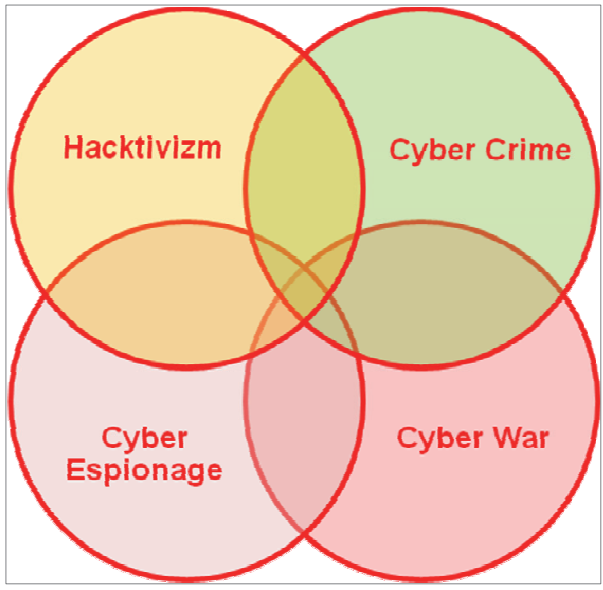

Figure 1. Four types of cyber threats

When critical infrastructure is taken into consideration, cyberespionage and cyberwar are much more harmful than hacktivism and cybercrime.

1.2.1 Hacktivism

Hacktivists create opportunistic attacks against weak targets. Hacktivism is the activity of a group of hackers; their power comes from their number.. The hacker group

[9] Janet J. Prichard and Laurie F. MacDonald, "Cyber Terrorism: A Study of the Extent of Coverage in Computer Security Textbooks," *Journal of Information Technology Education* 3 (2004), p. 280.

'Anonymous' is a hacktivist group. The main purpose of hacktivists is not to make money, but rather to protest something. For example, they protest governmental restrictions on the Internet and they take aim at the websites of public organizations.

Hacktivists usually perform denial of service (DoS) attacks. A DoS attack can be defined as purposefully flooding the targeted system with a huge number of legitimate service requests. Hacktivists usually target the availability of networks and systems by performing DoS attacks. In addition to DoS attacks, hacktivists try to deface websites, especially websites of public organizations. They do not usually try to deface a specific website for a long time. Rather, they search for a specific vulnerability on a number of websites and deface all of the websites within their search scope that contain the specific vulnerability. Hacktivist use botnets or contact owners of botnets in order to perform Distributed DoS (DDoS) attacks to guarantee the unavailability of networks and systems.

1.2.2 Cybercrime

In contrast with hacktivists, the main purpose of cybercriminals is to make money. Cybercriminals are individuals. Usually, they do not act in groups like hacktivists. They steal credit card information, bank account credentials and passwords. The critical target sector for cybercriminals is banking and finance. Compared to the other threat types, cybercrime does not normally have a prominent effect on critical infrastructures.

1.2.3 Cyberespionage

Cyberespionage is basically the act of stealing documents from networks of foreign countries.[10] The loss of confidentiality is the major consequence of cyberespionage. The term 'Advanced Persistent Threat' (APT) is used in the context of cyberespionage. According to Mandiant, which is a well-known information security company, APT is used by a group of sophisticated, determined and coordinated attackers that have been systematically compromising (U.S.) government and commercial computer networks for years. The vast majority of APT activity observed by Mandiant has been linked to China.[11]

According to the Department of Defense Strategy for Operating in Cyberspace, every year an amount of intellectual property larger than that contained in the Library of Congress is stolen from networks maintained by U.S. businesses, universities, and government departments and agencies. [12]

The US - China Economic and Security Review Commission prepared a report to Congress in 2008. According to this report, China has an active cyberespionage program. This report said that China's cyberwarfare is so sophisticated that the United States may be unable to counteract or even detect the efforts.[13]

---

[10] James A. Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," (Center for Strategic & International Studies, December 2002), p. 9.
[11] Mandiant, "The Advanced Persistent Threat," *M Trends Report* (2010), p. 1.
[12] U.S. Department of Defense, "Strategy for Operating in Cyberspace" (July 2011), p. 4, available at http://www.defense.gov/news/d20110714cyber.pdf (accessed December 8, 2012).
[13] US - China Economic and Security Review Commission, "2008 Report to Congress" (GAO, November 2008), p. 164, available at http://www.uscc.gov/annual_report/2008/annual_report_full_08.pdf (accessed 8 December 2012).

1.2.4 Cyberwar

Cyberwar is the use of coordinated attacks to specific critical sectors of a country. Every critical sector is a potential target of cyberwar. Most cybersecurity experts think that the Stuxnet virus, discovered in Jun 2010, was the beginning of real cyberwar. The target of the Stuxnet virus was the Iranian nuclear energy infrastructure. According to a New York Times report of 1 January 2012, President Obama secretly ordered increasingly sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, significantly expanding America's first sustained use of cyberweapons, according to participants in the program.[14] The cyberattacks against the Estonian and Georgian websites, as well as their network infrastructures are other examples of cyber war. Although Russia did not undertake those attacks as a government, the coordinated attacks were performed by Russians. The target of cyberwar is not only the availability of systems and networks. A virus called 'duqu' affected the confidentiality of Iranian energy infrastructure. Duqu was discovered after Stuxnet but both are thought to have the same origin because of their similarities. Duqu provided services to the attackers; currently this includes information-stealing capabilities. The last discovered malware is called Flame, Flamer or Skywiper. According to the New York Times, Flame appears to be part of the state-sponsored campaign that spied on and eventually set back Iran's nuclear program in 2010.[15]

1.2.5 Cyberthreats - Final Remarks

The number of cyberespionage and cyberwar activities is low compared to the number of cybercrime and hacktivist attacks. When economic damage and national security is the main concern, the impact level of cyberespionage is very high compared to the impact level of other threats types.[16] Although cyberespionage attacks are low in number, they cause intellectual property losses, which has a great value for a country. Although cybercrime activities are large in number, the loss is limited to credentials and money. When public safety is the main concern, the impact level of cyberwar is high compared to the impact level of other threat types because cyberwar can affect the availability of SCADA systems and corporate networks.

According to the draft Cyber Security Act of 2012, an industry can be defined as "critical" if damage or unauthorized access to that system could reasonably:

a) Result in the interruption of life-sustaining services,

b) Cause catastrophic economic damages, or

c) Cause severe degradation of national security. [17]

By using this damage classification, the prominent effects of the four threat

[14] David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks against Iran, *New York Times* (1 June 2012), available at http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all (accessed 13 June 2012).

[15] Nicole Perlroth, "Researchers Find Clues in Malware," *New York Times* (31 May 2012), available at http://www.nytimes.com/2012/05/31/technology/researchers-link-flame-virus-to-stuxnet-and-duqu.html (accessed 13 June 2012).

[16] Nir Kshetri, "Patterns of Global Cyber War and Crime: A Conceptual Framework," *Journal of International Management* 11 (2005), p. 552.

[17] The Cyber Security Act of 2012 (draft).

categories on critical infrastructures are shown in Table 1. Although there is no crystal-clear classification and correlation between threat types and impact types, Table 1 shares the notion that cyberespionage and cyberwar are much more harmful than cybercrime and hacktivism.

Table 1. Threat categories versus impacts

THREAT TYPE	IMPACT TYPE
Hacktivism	The interruption of life-sustaining services (Minor)
Cybercrime	Economic damages (Minor)
Cyberespionage	Economic damages (Major) Severe degradation of national security
Cyberwar	The interruption of life-sustaining services (Major) Economic damages (Intermediate)

1.3 Vulnerabilities

Vulnerabilities of critical infrastructures can be classified into two major groups: technical vulnerabilities and non-technical vulnerabilities.

1.3.1 Technical Vulnerabilities

Technical vulnerabilities can be further divided into two subgroups: basic protocol vulnerabilities and application vulnerabilities. Basic protocol vulnerabilities are the vulnerabilities of common Internet protocols.[18] The core protocols of the Internet such as Internet Protocol (IP), Transmission Control Protocol (TCP), Domain Name System (DNS), Hypertext Transfer Protocol (HTTP) and routing protocols were designed and implemented without focusing on security features since the Internet was initially used in academic and governmental environments. In these environments, humans were the trusted entities. Security countermeasures were included in Internet protocols as add-ons after the proliferation and widespread use of the Internet. Therefore, the Internet is vulnerable to basic and competent attacks like denial of service, eavesdropping, spoofing and sniffing. Apart from basic protocols, there are a number of applications, including operating systems that logically run on top of basic protocols. According to the IBM X-force report, there has been an exponential increase in cumulative

[18] Alcaraz-Tello, Cristina, et al., "Secure Management of SCADA Networks," *The European Journal for the Informatics Professional* 9 (December 2008), p. 23.

vulnerability disclosures from 1996 to 2010.[19] These application vulnerabilities are exploited by attackers to gain access privileges to remote systems, to steal information and to stop services.

1.3.2 Non-Technical Vulnerabilities

In spite of the state-of-the-art security systems – such as digital signatures, cryptography, biometric security, stateful firewalls, intrusion prevention systems, access control systems – the number of security breaches has increased. Even closed networks are infected with targeted worms and viruses, as in the case of Stuxnet. It has been argued by security experts that Stuxnet infected the closed energy network of Iran by means of USB thumb drives used by the workers of the nuclear enrichment facilities. The reason for security breaches is non-technical vulnerabilities. Non-technical vulnerabilities are related to people and their processes.[20] Unfortunately, the weakest link for security is the human being. As an example, in November 2008, the US-CERT issued a warning that malicious code was increasingly being propagated via USB flash drive devices. The fact that USB thumb drives are being used by so many people makes them an attractive target for malware writers.[21] In those days, the US Department of Defense had temporarily banned the use of thumb drives, CDs and other removable storage.[22] Although technical countermeasures are vital for the security of critical infrastructure, they will not be as effective as expected without improvements in the behavior of people and security processes.

1.3.3 Vulnerabilities - Final Remarks

Certain threat types exploit certain vulnerabilities as shown in Table 2. Although it is not a golden rule, hacktivists generally exploit basic protocols at first, then application vulnerabilities. Cybercriminals usually exploit application vulnerabilities. Cyberwarriors use application and infrastructure vulnerabilities like hacktivists. Finally, cyberspies exploit people and process vulnerabilities.

1.4 Countermeasures

Most of the vulnerabilities can be patched by using simple technical preventive countermeasures. There will still be a considerable amount of risk even after applying preventive countermeasures. Corrective countermeasures should be used in order to minimize the level of risk. Even if all of the preventive and corrective countermeasures are applied, there will be some minor residual risk. Hundred percent security is not possible in the real world. There is no technology and budget that eliminates risk totally. The residual risks would generally originate from the vulnerabilities of people

[19] IBM X-force, "2010 Trend and Risk Report" (March 2011), p. 75.
[20] Keith Stouffer, Joe Falco, and Karen Scarfone, "Guide to Industrial Control Systems (ICS) Security," (National Institute of Standards and Technology, Special Publication 800-82, June 2011), pp. 3-7.
[21] Elinor Mills, "USB Devices Spreading Viruses," *CNET* (20 November 2008), available at http://news.cnet.com/8301-1009_3-10104496-83.html (accessed 13 June 2012).
[22] Noah Shachtman, "Under Worm Assault, Military Bans Disks, USB Drives," *Wired* (19 November 2008), available at http://www.wired.com/dangerroom/2008/11/army-bans-usb-d (accessed 13 June 2012).

Table 2. Threat categories versus vulnerabilities

THREAT TYPE	EXPLOITED VULNERABILITY TYPE
Hacktivism	Basic Protocol Vulnerabilities Application Vulnerabilities
Cybercrime	Application Vulnerabilities
Cyberespionage	Non-technical Vulnerabilities Application Vulnerabilities
Cyberwar	Application Vulnerabilities Basic Protocol Vulnerabilities

and processes. Cyberespionage teams and spies usually use these vulnerabilities in order to steal information.

Countermeasures can also be divided into two main categories, which are technical countermeasures and non-technical countermeasures.

1.4.1 Technical Countermeasures

Patching the systems against vulnerabilities and implementing the latest technical security measures are the most prominent technical countermeasures. Security tests and audits should also be performed periodically. Active cybersecurity teams that are working for governments should gather cyberintelligence. Based on this cyberintelligence, predictions could be made and preventive actions taken. Also, research and development facilities should be supported by governments. The security for SCADA networks is a new and extremely important subject. Security must be a design issue for SCADA systems; it should not be an add-on. Certified software and hardware usage should be prioritized.[23] Both technical and policy-based access control mechanisms should be used.[24]

1.4.2 Non-technical Countermeasures

There are two important non-technical countermeasures, which are awareness and cooperation. The most effective countermeasure for human vulnerabilities is security awareness. Security awareness is a vital countermeasure for not only computer users. Everyone, whether computer user or not, in an organization should be included in security awareness programs.

Security is a matter of coordination, cooperation, collaboration and communication. In 2009, a Department of Homeland Security official said that hackers

[23] Miller, Ann, "Trends in Process Control Systems Security," *IEEE Security & Privacy* 3 (2005), p. 58.
[24] Kilman, Dominique, and Jason Stamp, "Framework for SCADA Security Policy," (Sandia National Laboratories, 2005), p. 4, available at http://energy.gov/sites/prod/files/Framework%20for%20SCADA%20Security%20Policy.pdf (accessed 9 December 2012).

are better organized than governments.[25]

For all the types of threats that are stated in this paper, cooperation is a vital countermeasure. For all four threat categories, the methods for possible cooperation are shown in Table 3. For a government, cooperation with critical infrastructure operators and owners is an essential and imperative countermeasure. Cooperation with Internet Service Providers (ISPs) and Computer Emergency Response Teams (CERTs) is a significant countermeasure against hacktivist attacks. Cooperation with police and law enforcement agencies is essential in order to combat cyber-crime. Cooperation with CERTs and other countries are crucial in order to deal with cyberwar. Cooperation with employees and cutting-edge technology makers is an indispensable countermeasure against cyber espionage.

Table 3: Threat categories versus sides of cooperation

THREAT TYPE	COOPERATION WITH ...
Hacktivism	Cooperation with ISPs Cooperation with CERTs Cooperation with infrastructure operators and owners
Cybercrime	Cooperation with police Cooperation with law enforcement agencies Cooperation with infrastructure operators and owners
Cyberespionage	Cooperation with employees Cooperation with technology developers Cooperation with infrastructure operators and owners
Cyberwar	Cooperation with CERTs, ISPs International cooperation Cooperation with infrastructure operators and owners

1.4.3 Countermeasures - Final Remarks

Countermeasures are imperative in order to deal with cyberrisks and to ensure an acceptable level of critical infrastructure protection. The application of all types of countermeasures should be considered as a life-cycle process. Once a countermeasure is applied, the effectiveness of the countermeasure should be measured continuously and improved as necessary. In Table 4, prominent countermeasures are listed for each threat category. Cooperation and technical countermeasures should be applied for all types of threats. Although security awareness is also applicable in order to deal with all

[25] Eric Chabrow, "Testimony: Hackers Better Organized Than Government," *GovInfoSecurity.com* (14 September 2009), available at http://www.govinfosecurity.com/articles.php?art_id=1775 (accessed 13 June 2012).

threat types, it is especially important to counteract cyberespionage.

Table 4: Threat categories versus countermeasure types

THREAT TYPE	COUNTERMEASURE
Hacktivism	Cooperation Technical Countermeasures
Cybercrime	Cooperation Technical Countermeasures
Cyberespionage	Cooperation Security Awareness Technical Countermeasures
Cyberwar	Cooperation Technical Countermeasures

Conclusion

Today, cybersystems serve as key infrastructures for critical sectors. Almost all sectors use information technologies to automate their core business processes. Automated business processes are connected to the Internet and corporate networks to optimize processes and decrease costs. Cybersystems of critical infrastructures are attractive targets for cyberthreats. There are different types of threats with different motivations, qualifications and capacities, but all of these threats exploit certain vulnerabilities of cybersystems of critical infrastructures. Therefore vulnerabilities have to be mitigated in order to cope with threats. There are different types of countermeasures in order to mitigate the vulnerabilities. The impact level and diversity of cyber threats will increase steadily in parallel with the widespread use of cybersystems. Therefore, critical infrastructure protection will be one of the most important agenda items of all governments in the near future.

Bibliography

Alcaraz-Tello, Cristina, et al., "Secure Management of SCADA Networks, " *The European Journal for the Informatics Professional* 9 (December 2008).

Beltran, Fernando, Alain Fontenay, and Marcio Alameida, "Internet as a Critical Infrastructure: Lessons from the Backbone Experience in South America," *Communications & Strategies* 58 (2005).

IBM X-force, "2010 Trend and Risk Report" (March 2011).

Igure, Vinay, M., Sean A. Laughter, and Ronald D. Williams, "Security Issues in SCADA Networks," *Computers & Security* 25 (2006).

Jayawickrama, Wipul, "Managing Critical Information Infrastructure Security Compliance: A Standard

Based Approach Using ISO/IEC 17799 and 27001," in *On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops* (Zahir Tari, ed. Springer Books, 2006).
Kilman, Dominique, and Jason Stamp, "Framework for SCADA Security Policy," (Sandia National Laboratories, 2005).
Kshetri, Nir, "Information and Communications Technologies, Strategic Asymmetry and National Security" *Journal of International Management* 11 (2005).
Kshetri, Nir, "Patterns of Global Cyber War and Crime: A Conceptual Framework," *Journal of International Management* 11 (2005).
Lewis, James, A., "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," (Center for Strategic & International Studies, December 2002).
Mandiant, "The Advanced Persistent Threat," *M Trends Report* (2010).
Miller, Ann, "Trends in Process Control Systems Security," *IEEE Security & Privacy* 3 (2005).
Eric Chabrow, "Testimony: Hackers Better Organized Than Government," *GovInfoSecurity.com* (14 September 2009).
Perlroth, Nicole, "Researchers Find Clues in Malware," *New York Times* (31 May 2012).
Prichard, Janet, J., and Laurie F. MacDonald, "Cyber Terrorism: A Study of the Extent of Coverage in Computer Security Textbooks," *Journal of Information Technology Education* 3 (2004).
Sanger, David E., "Obama Order Sped Up Wave of Cyberattacks against Iran, *New York Times* (1 June 2012).
Shachtman, Noah, "Under Worm Assault, Military Bans Disks, USB Drives," *Wired* (19 November 2008).
Stouffer, Keith, Joe Falco, and Karen Scarfone, "Guide to Industrial Control Systems (ICS) Security," (National Institute of Standards and Technology, Special Publication 800-82, June 2011).
US - China Economic and Security Review Commission, "2008 Report to Congress" (November 2008).
U.S. Department of Defense, "Strategy for Operating in Cyberspace" (July 2011).

This page intentionally left blank

Critical Infrastructure Protection
M. Edwards (Ed.)
IOS Press, 2014

doi: 10.3233/978-1-61499-357-5-75

Transportation Security in the Context of Defense against Terrorism

Cristian Coman[1]
NATO Communication and Information Agency

Abstract. Terrorist threats to transportation systems, particularly the air transportation systems, are of great concern because of the magnitude of the possible effects, both direct and indirect. Although multiple layers of security are in place at airports using technological tools, they are still not enough to deal with emerging threats. Not only do we need to continue improving our security technology, we also need to address the terrorist attack systems as a whole. NATO has learned in recent operations that air hubs are the main entry and exits points from an area of operation and protecting these nodes is of significant importance.

Keywords. NATO, transportation security, security screening

Introduction

For many years, Defence against Terrorism (DAT) has been one of the top priorities for NATO nations, and in 2010 the importance of being able to address new emerging threats (e.g. terrorism) was furthermore underlined by setting up the Emerging Security Challenges Division (ESCD) within the NATO Headquarters.

The active participation in military conflicts has taught NATO many lessons about combating terrorist activities. The problem of controlling entry points in a military facility has been addressed by NATO through a comprehensive approach involving technological and operational components.

The present technological solutions for detection of IEDs have reached a level of strong deterrence and functionality on a component level. The limitations at the sensor level are often compensated by expensive operational procedures with a negative impact on the traveller experience (e.g. long queues and privacy violation).

Airport security is moving towards the application of better technologies and procedures to counter the IED threat, in particular the one hosted by a suicidal attacker (e.g. IEDs hidden in luggage and on the person). Despite sophisticated security procedures, the international (and national) airports are not able of detecting all kinds of possible IEDs. For example, it is difficult to detect plastic and liquid explosives and ceramic weapons with a conventional security checkpoint setup equipped with metal detectors and hand luggage screening sensors (e.g. single view X-ray). The passenger screening is a vital component in aviation security designed to maximize effectiveness in identifying potential threats that could be used for a terrorist attack.

[1] PhD., Capability Development, e-mail: cristian.coman@nc3a.nato.int.

The development of the screening technology and procedures reflects a reactive approach. In 2006 an attempt to use liquid explosives created the restriction on liquids carried on board and the requirements for liquid explosive detection capabilities as a component of the security checkpoint portfolio. In 2009 explosives were carried on board a transatlantic flight and created an acceleration of the development of the next wave of technology to be used in a security checkpoint. The Millimetre Wave (MMW) imaging or the X-ray security scanners have been proposed as supplements and potentially as replacements of the metal detector.

Terrorists pose a continuing risk to our transportation systems. Perhaps this threat is no greater apparent then the air transportation system. Security of the air transportation system has traditionally focused on the airports and other hubs where planes can be more easily targeted because, when airborne, airplanes are difficult for the terrorist to target. Although there is a great deal of security employed, to protect the air transportation systems, we need to do better.

1. Security Challenges in Airports and Air Hubs

When looking at the business of air travel, the security process presents some interesting challenges.

Airports generally employ multiple levels of security that intensify as one gets closer to the aircraft themselves. There is the physical security of the airport itself that is generally isolated and patrolled to some extent. Next comes the terminal area where access is limited by a number of measures, then the most controlled area is the boarding zone and access to the airplanes.

To a great extent, these security measures rely on a variety of sensors, coupled with personnel following operating procedures. These sensors are not perfect, nor are they obvious – even computer-assisted interpretation of the displays requires trained operators to properly screen for threats. Not all threats can be detected through technical means so we have to train personnel to watch for warning signs – not only do we have possible terrorist trying to sneak in weapons, you also have your garden variety smuggler trying to sneak in cash, drugs or other controlled substances, as well as people trying to bring in exotic pets or souvenirs. Security by humans has its own sets of problems – security personnel can be bribed, they can be inattentive or they can be fatigued.

Most of the detectors have been built to detect earlier threats – metal detectors for guns, for example. However, with the ability to make weapons of plastic or ceramic, these are outdated. The greater threat now comes from explosives – sensitive equipment is needed to quickly screen for explosives. Some explosives are binary – harmless in separate parts but lethal when combined.

The IED threat is definitely not confined to an area of military operations and many nations are facing this threat in day-to-day life. IED networks extend across borders and cooperation between civil and military organizations is required to efficiently counter them. The need of cooperation between in-theatre and out-of-theatre

security forces is outlined in the NATO doctrine as well.[2] In-theatre activities are often under the responsibility of military authorities whereas out-of-theatre actions are coordinated by civilian authorities.

Although technology has continued to develop, the question is whether we can continue to develop sufficient technology to cope with the business realities – can multisensory technology improve security or is more screening time going to be required?

2. Transportation Security Technologies

This section will look at both an overview of the security technologies and emerging solutions**.**

2.1 Overview

The most common security equipment used at international airports consists of walk-through metal (WTM) detectors and carry-on luggage X-ray scanners. The design of security checkpoints at airports is mainly aimed at detecting metal on passengers and potential threat objects in the carry-on luggage (based on X-ray imaging techniques). In some airports, the detection of non-metallic threats is supported with active MMW security scanner as the primary technological platform. In December 2011, the European Union (EU) endorsed regulations facilitating the use of non-ionising millimetre-wave (MMW) security scanners as the primary technology for persons. X-ray imaging technologies used in person security screening provides better imaging capacity compared with the MMW technology. However privacy and health concerns are significant factors that prevent this technology for being used widely.

Radiation in the millimetre-wave (mm) and the lower end of the terahertz (THz) range has the useful property of being able to penetrate clothing. Thus using imaging systems at these frequencies allows for the detection of weapons and explosives, both metallic and non-metallic, hidden on a person.[3] This is achieved by detecting the naturally emitted and reflected radiation at these wavelengths which varies depending on the material and its temperature. In addition, certain bands in the millimetre wavelength range have very high atmospheric transmission (forming the so-called atmospheric windows) and therefore also enable stand-off detection and imaging through adverse weather conditions such as fog and clouds, as well as dust and smoke.

Non-imaging radar techniques have also been used for detecting the body borne IEDs. In general, these techniques allow detecting targets at large distances (50-100m), although the cause that generated the detection is not explicitly presented to the operator. Often the non-imagining radar systems are equipped with video or infrared cameras to support the representation of the target.

[2] NATO Standardization Agency, "Allied Joint Doctrine For Countering – Improvised Explosive Devices", AJP-3.15(B), STANAG 2295 (May 2012).
[3] William Harris, "How Millimeter Wave Scanners Work," *How Stuff Works* (undated), at http://science.howstuff works.com/ millimeter-wave-scanner.htm (accessed 08 October 2013).

Infrared cameras have been recently used in the fight against body-borne IED devices.[4] The infrared spectrum is situated in a region which does not allow the waves to penetrate clothing. However innovative processing and visualization techniques have been used to detect if rigid objects are hidden under cloths.

A classical solution for security scanning of personnel is based on x-ray. The resolution and the penetration performance are the most attractive feature of these systems. The main limitations of the x-ray techniques are related to the long scanning time, radiation hazard and very short distance between the imaging system and the person under test.

Figure 1. X-ray Vehicle Scanning Systems Installed at a NATO base in Afghanistan

In areas of operations the security risks are at a high level and the technology used should provide the adequate level of protection. In Figure 1, an x-ray vehicle scanning systems is visible at an entry control point at an NATO airfield in Afghanistan.

The imaging capacity of x-ray technology is illustrated in Figure 2. The high resolution and the penetration capacity are key characteristics that make this technology popular in airports. However the ionizing effect of this technology is still a point of concern mainly in body scanning applications.

2.2 Emerging Solutions

Among the emerging solutions proposed to enhance the security level at airports, there are two technologies that have being investigated by the NCI Agency on the past years: passive millimeter wave scanners for stand-off detection of explosives/weapons and psychological profiles of suicide bombers.

Alfa Imaging, in Spain is a company that develops MMW scanners for security applications. The MMW cameras produced by Alfa are passive stand-off millimetre-wave imager for the detection of person-borne hidden objects. The camera operates at real-time video rates (10fps), which, together with the stand-off architecture, provides a walk-by security screening solution.

[4] Franco Fiore, "The NATO C3 Agency Support to the IED Fight: A Comprehensive Approach," *Information & Security* 27 (2011), p. 79.

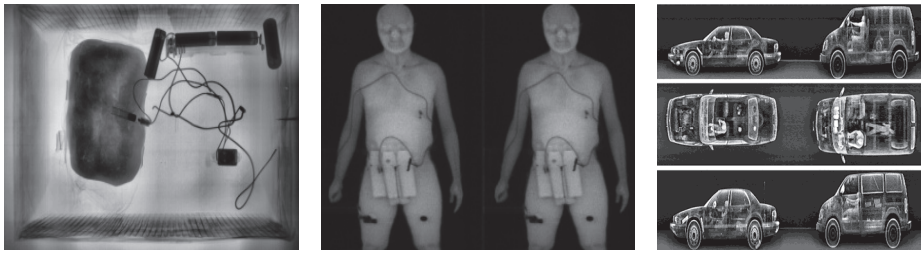

Figure 2. Images collected with X-ray scanning systems,
a) Luggage Scanner, b) Body Scanner, and c) Vehicle Scanner

The integrated automatic threat detection software automatically outlines the object detected in red, thus showing its position and size. This can be presented to the operator on the millimeter-wave video, on the visible video or on a fixed computerized generic silhouette (see Figure 3).

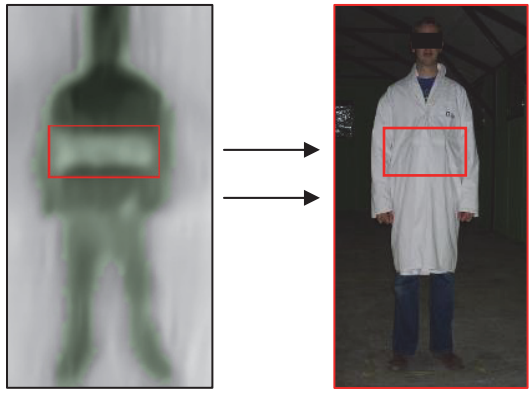

Figure 3. Automatic Threat Detection (red rectangle) Performed on MMW Image and Overlapped on Visible Image.

Some of the key features of MMW cameras are:

- The output can be saved, however no anatomical details are ever shown or saved (privacy).
- Covert operations are possible (the imager can be hidden behind a screen).
- Anomaly detection: Hidden objects of any material composition are detected, including explosives, metallic weapons, liquids and gels. Object cannot be identified. Due to the intrinsic characteristics of materials there may be times when certain objects are not detected.
- All regular clothing is transparent for these imagers.
- The imagers do not see through skin, thus the subjects must pass the imagers one by one, and if the subjects do not lift their arms and stand in a "stride" position there are areas that will not be thoroughly screened.
- The integrated automatic threat detection software automatically detects the hidden objects and outlines them in red, thus showing the location and size. The minimum size of the automatic detected object is 2 x 2 pixels, as long as there is sufficient thermal contrast and the subject's body is behind the object (from the imager's perspective).

Passive scanners look for shadow areas indicating objects or anomalies that disrupt the normal emission of radiation from the human body. Active emitters can be used to enhance the penetration capacity and see more details. The high frequency used provides a reasonable angular resolution and allows detecting small and thin objects. The technology has been tested in simulated conditions as well as in actual operational conditions in Afghanistan.

The use of facial characteristics to identify potential bombers is also being pursued. By focusing on the analysis of facial expressions, it may be possible to quickly identify those persons trying to deceive or those having certain psychological profiles that pose a possible threat.[5] Facial recognition may be effective all the way out to 50 meters so that this screening may be used somewhat surreptitiously.

NCI Agency organized a demonstration with support from a start-up company (Inteliwatch, Delft, NLD) focusing on capturing data from a high resolution camera coupled with a Kinect 3D video sensor to provide detection and tracking of person's face as well as other relevant information to determine the emotion and mind-set of the person. To determine such emotions, the camera will capture the slightest changes and movements of the facial muscles, which are called Action Units. The combination of several Action Units can be used to categorize the physical expression of emotions and therefore the emotional state of the person under analysis.

Facial video analysis techniques are specialized in collecting information that can be used to estimate the emotion of a person or its level of stress, and can also support the positive identification of a person. The goal would be to provide counterterrorism actions and critical infrastructure protection against suicide bomber IED (SBIED) attacks.

[5] See Ekaterina Kamenskaya and Georgy Kukharev, "Recognition of Psychological Characteristics from Face," *Metody Informatyki Stosownej* 1 (2008) pp. 59-73, available at http://library.binarydissent.com/MetInfStos_2008_01_Art_06.pdf (accessed Oct. 11, 2013).

The initial results are encouraging. At this stage, six action units have been implemented in the system. However, if the analysis of the results is convincing, more actions units could be integrated and processed to determine more precisely the emotional state of a person. Moreover, further improvement, such as the remote recording of the heartbeat of the passenger, will be integrated into the system in the near future. The data collected would not be used directly to take a decision but would be processed and taken into account as one of the parameters of a multisensor system.

3. The IED Fight: A Comprehensive Approach

However much we would like to think of the fight against IED to be an isolated problem, it is not. IEDs are part of a much bigger problem where they are linked with terrorism, human trafficking, weapons smuggling, and illegal drugs. Therefore, we must train the forces to target the networks in which IEDs play a role.

Although technology can help us detect and neutralize the IED when it is being deployed, it is far better to break the chain before the IED is emplaced. By developing such capabilities, we will also be capable of small rockets, dirty bombs, and other weapons that would enjoy a similar employment profile. Methods to do so include large-scale screening capabilities to detect the weapons in transit, software tools to search for strange e-mail or money transfers, all-source intelligence, and biometrics of personnel involved.

NATO's comprehensive approach to the C-IED problem involves the partition of the security problem at hand into three views: operational, architectural and technical.

The NATO C-IED Concept of Operation is exposed in AJP_3.15. The concept is constructed around the popular decomposition of the C-IED problem onto three areas:

- Defeat the Device (DtD),
- Attack the Network (AtN), and
- Prepare the Forces (PtF).

The underlying element of these three domains is represented by understanding and intelligence. The decision on the countermeasures to be deployed is fully depended on the understanding of the situation. Information collected through command and control (C2) channels and from intelligence analytic activities is combined to provide effective understanding. The accuracy of the information plays an important role in the combination process particularly when multiple sources of information are used.

Conclusion

Although the security of the air transportation system against terrorism is an important one, it cannot be left to just the airports and other hubs of the air transportation system. Within this system, there is a constant trade-off between security requirements and time/costs required. We rely a great deal on technology to help us with this system, where research and development continue, but technology is not the only tool. We

need to continue a systemic approach to defeat the employment of bombs and other weapons against our air transportation system.

Although randomness in the security procedures remains the main strategy in protecting transportation systems against new terrorist threat, the technology is also evolving rapidly and provides credible solutions in increasing the security level.

In military operations an ultimate security screening solution would have the capacity to perform stand-off screening under various weather conditions (e.g. rain, fog, humidity) by also avoiding contact between security personnel and potential suicide bomber before the screening process.

Bibliography

Harris, William, "How Millimeter Wave Scanners Work," *How Stuff Works* (undated).

Fiore, Franco, "The NATO C3 Agency Support to the IED Fight: A Comprehensive Approach," *Information & Security* 27 (2011).

Kamenskaya, Ekaterina, and Georgy Kukharev, "Recognition of Psychological Characteristics from Face," *Metody Informatyki Stosownej* 1 (2008), pp. 59-73.

NATO Standardization Agency, "Allied Joint Doctrine For Countering – Improvised Explosive Devices," AJP-3.15(B), STANAG 2295 (May 2012).

Critical Infrastructure Protection
M. Edwards (Ed.)
IOS Press, 2014

doi: 10.3233/978-1-61499-357-5-83

Valuable and Vulnerable: Protecting Maritime Infrastructure

Brian Wilson[1]
U.S. Coast Guard

Abstract. For nations bordering on oceans, security of the sea borders is a must. The oceans are not the only place where illicit activity occurs, but they are uniquely vast, jurisdictionally challenging, and operationally complex. Merchant vessels do not strictly move in controlled channels or according to fixed time parameters like planes and can carry potentially legitimate cargo capable of causing great destruction. Not every threat manifests itself clearly: the scope of maritime security challenges is immense. Maritime infrastructure protection consists of risk management and maritime domain awareness (MDA). Protecting maritime infrastructure is particularly challenging because threats are not always clear and are often preceded by ambiguous signals, uncertain events and incomplete information.

Keywords. Maritime infrastructure, maritime security, maritime risk

Introduction

A foreign-flagged cargo ship en route to the United States disclosed that it was carrying liquid urea, a fertilizer that could potentially be used as an explosive.[2] Information was then received that the ship was in poor materiel condition, had not made a call on a U.S. port in more than 15 years and intended to dock at a port with critical infrastructure.

Reports later followed of potential links between the vessel's owner and a terrorist organization. Even with this data, it was far from clear whether the ship represented a grave danger or was simply carrying legitimate commerce.

The issues surrounding the Warms Seas Voyager are not unusual: Is there a threat, how will information be shared, and what is the appropriate response.

Fortunately, the response could unfold over hours, not minutes. Representatives from several U.S. Government agencies met to collectively assess the situation, decide on courses of action, and take aligned action.

---

[1] Captain, US Navy (Ret). Deputy Director of the United States' Global Maritime Operational Threat Response Coordination Center and is an adjunct professor at the United States Naval Academy. The views expressed are those of the author and do not reflect the official policy or position of the U.S. Coast Guard or the Departments of Homeland Security or Defense. Email: brianstwilson@gmail.com.

[2] Gary L. Tomasulo, Jr., *Evolution of Interagency Cooperation in the United States Government: The Maritime Operational Threat Response Plan* (June 2010), pp. 52-55, available at http://dspace.mit.edu/bitstream/handle/1721.1/59157/659552377.pdf?sequence=1 (last visited Dec. 11, 2012).

A focus on protecting maritime trade and port facilities is not new, but is particularly challenging today. Since 2000, several devastating strikes have occurred on or from the water including the Mumbai attacks and those on the USS Cole, SuperFerry 14, and the M/V Limburg, among others. The challenge is not just about transnational trade, linked economies, or more lethal weapons; it is about a transformed security and transportation environment. Maritime infrastructure represents a central component of this transformed environment and its protection is vital to security and economic interests.

The oceans are not the only place where illicit activity occurs, but they are uniquely vast, jurisdictionally challenging, and operationally complex. Maritime trade frequently involves cargo moving across multiple countries with a multinational crew, ownership in one country and registry in another. The country that has registered the ship, the flag state, along with the coastal state or port state may seek to assert jurisdiction. However, depending on the location, activity, and national laws, a gap in jurisdiction may exist.

Adding to the challenge: Merchant vessels do not strictly move in controlled channels or according to fixed time parameters like planes and can carry potentially legitimate cargo capable of causing great destruction. Moreover, like the Warm Seas Voyager, not every threat manifests itself clearly: Is a ship loitering 15 miles off the coast for 8 hours waiting to enter port or poised to conduct illicit activity or is the failure of a master to respond to repeated radio contacts two miles off the coast the result of faulty equipment or something more?

This article first discusses the scope of maritime security challenges and then examines infrastructure protection and its two critical components: risk management and maritime domain awareness (MDA), also referred to as maritime situational awareness.

1. Maritime Security

Protecting maritime infrastructure is directly linked to economic stability and national security. Critical infrastructures and key resources (CI/KR) in the maritime environment include ports and waterways lined with gas platforms, oil refineries, passenger terminals, businesses, restaurants, conference centers and physical and cyber networks. These assets represent 'attractive terrorist targets' because of their value and vulnerability.[3]

A report by the U.S. Government Accountability Office (GAO) on port security and the marine transportation system noted that: "The estimated economic consequences of a successful attack and resulting shutdown of this system total billions of dollars. Ports also represent attractive targets because they contain a myriad of vulnerabilities. In all, the nation's 300-plus ports have about 3,700 cargo and

[3] United States Government Accountability Office, Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure (GAO-06-91, December 2005) [hereinafter "GAO Risk Management Study"], available at http://www.gao.gov/new.items/d0691.pdf (last visited Dec 11, 2012). The GAO is, "an independent, nonpartisan agency that works for Congress [that] investigates how the federal government spends taxpayer dollars."

passenger terminals. Chemical factories, oil refineries, power plants, and other facilities are often located in port areas and add another set of possible targets. Roads crisscross many ports, allowing access by land as well as by water, and the number of people working in or traveling through ports is in the millions."[4]

The movement of just one product, oil, illustrates the global vulnerability and exposure to attack: Of the 85 million barrels of oil that travel daily, approximately 43 millions barrels transit on the water, easily within the reach of criminal networks and terrorists.[5]

Multiple studies have examined the methods by which an attack can take place in the maritime environment, including ports and infrastructures. The U.S. Congressional Research Service (CRS) divided attacks into five areas of concern:

- Perpetrators: Al Qaeda and affiliates…disgruntled employees, others;
- Objectives: Mass casualties, port disruption, trade disruption, environmental damage;
- Locations: 360+ US ports, 165 foreign trade partners, 9 key shipping bottlenecks;
- Targets: military vessels; cargo vessels; fuel tankers; ferries/cruise ships; port area populations; ship channels; port industrial plants; offshore platforms; and
- Tactics: explosives in suicide boats; explosives in light aircraft; ramming with vessels; ship-launched missiles; harbour mines; underwater swimmers; unmanned submarine bombs; exploding fuel tankers; WMDs in cargo ships.[6]

The US Port Security Training Exercise Program (PortSTEP)[7] explored scenarios that included "targeted or exploited cruise ships, container ships, a harbor truck, a barge, a rail yard, port industrial facilities, bridges, and a national landmark."[8] Other threats have been identified in various governmental and non-governmental studies.[9]

---

[4] Id.

[5] Daniel Yergin, "Ensuring Energy Security," *Foreign Affairs* 85 (March/April 2006). By 2020, the number of barrels transiting the oceans, "could jump to 67 million," a day. Id.

[6] Paul W. Parfomak and John Frittelli, *Maritime Security: Potential Terrorist Attacks and Protection Priorities* (CRS Report for Congress, May 14, 2007), p. 7, available at http://assets.opencrs.com/rpts/RL33787_20070514.pdf (last visited Dec. 11, 2012).

[7] This collaborative US Transportation Security Administration program is conducted in association with the US Coast Guard.

[8] Parfomak and Fritelli, *Maritime Security: Potential Terrorist Attacks and Protection Priorities*, p. 8.

[9] "Explosives attack on a chlorine storage tank in port; hostage-taking and executions aboard a vessel in port; a marine mine attack on a Navy frigate in port; underwater explosive devices planted on multiple vessels in port; a nuclear device aboard an incoming vessel in a 55-gallon drum; attack on a port with a biological disease agent; detonation of a dirty bomb in a shipping container in port; aircraft attack on a passenger ferry or cruise ship; ammonium nitrate bombs shipped by rail to a port; Sarin gas attack on a cruise ship in port; various types of an explosives attack on a ship in port; "dirty" bombs in cargo containers at multiple U.S. ports; radioactive materials carried on a cargo ship 90 miles offshore; underwater and fishing boats explosives attacks on riverboat; bombing and sinking of a liquefied propane gas (LPG) tanker in a major commercial and naval shipping channel; hijacking of a river tanker for use as a "floating bomb"; ramming and "dirty" bombing a ferry with a hijacked cargo ship; coordinated bombing of docks and bridges, and mining of the harbor at a major commercial port; attack on a liquefied natural gas (LNG) terminal and tanker in port." Parfomak and Frittelli, *Maritime Security: Potential Terrorist Attacks and Protection Priorities*, pp. 10-11.

Ports and maritime infrastructure will always be vulnerable: high value assets with relatively easy access and large numbers of ships moving in close proximity to dense populations.[10] Risk management[11] and separately, mechanisms that provide senior policy officials and operational commanders with situational awareness of maritime activities best position a country to identify, respond, and as appropriate, eliminate or mitigate threats.

2. Assessing Maritime Infrastructure Risk

Effectively recognizing anomalies and trends to assess risk and evaluate alternative measures requires structured protocols at both the national- and operational-level.[12] The U.S. Coast Guard has developed a computer-based program that enables ports to measure risk and make assessments regarding where assets are best needed. This program establishes a baseline level of risk and identifies measures to enhance security, evaluating threat, vulnerability and consequence.[13]

Determining risk, in part, involves assessing how likely it is that an event will occur, what can go wrong, and what are potential impacts of an event. The foundation for determining risk includes historical experience, analytical methods, knowledge, and intuition. Targets could be direct or indirect, such as mailing anthrax. This data is entered into a risk calculator and enables a port and a nation to most effectively evaluate the risks of a vessel or other events to infrastructure assets.

After entering information into this program, some ports realized that fire was their greatest concern, and thus, they bought additional fire equipment and trucks to put an increased emphasis on fire response training; other ports recognized security was their highest concern and were able to similarly focus on increasing assets and addressing gaps. The Coast Guard has shared PSRAT (Port Security Risk Analysis Tool) with dozens of countries. The data that is entered remains with the country using the program.

PSRAT also supports national objectives, which may include the uninterrupted flow of maritime commerce and ensuring that ships making port calls are not carrying illicit cargo or facilitating illegal activity. PSRAT supports those objectives by identifying

[10] "Ports are often sprawling enterprises that contain key infrastructure besides docks, piers, ships, barges, and warehouses. Many ports are also home to power plants, chemical factories, bridges and tunnels, and a variety of other assets of critical importance to the nation's economy and its defense." GAO Risk Management Study.

[11] Risk management, "involves a continuous process of managing—through a series of mitigating actions that permeate an entity's activities—the likelihood of an adverse event and its negative impact. Risk management addresses risk before mitigating action, as well as the risk that remains after countermeasures have been taken." GAO Risk Management Study.

[12] United States Government Accountability Office, "Maritime Security Responses to Questions for the Record" (GAO-11-140R, October 22, 2010), available at http://www.gao.gov/assets/100/97153.pdf (last visited Dec. 11, 2012).

[13] The U.S. Government Accountability Office defined threat, vulnerability and consequence as, "Threat is the probability that a specific type of attack will be initiated against a particular target/class of targets…The vulnerability of an asset is the probability that a particular attempted attack will succeed against a particular target or class of targets…[and] The consequence of a terrorist attack is characterized as the expected worst case or worse reasonable adverse impact of a successful attack." GAO Risk Management Study.

critical infrastructures within ports along with the resources that may be used against the greatest risks.

PSRAT workshops develop capacity to effectively increase maritime security and include port security officials and managers. The workshops are intended to provide instruction in the use and execution of PSRAT and allow participants to become trainers in PSRAT.[14]

The opening day of a PSRAT workshop features a detailed briefing on PSRAT methodology, defining the aims, objectives, and deliverables that participants will be presented. The focus on the second and third day is on entering port facility data in the PSRAT risk assessment and modeling tool. Several scoring scenarios are executed and the results quantified. The results provide a means to rank and subsequently reduce risk within the port or port facility. The scoring scenarios and resulting data are critical to accurately assessing and mitigating risk to a port or port facility and allows for optimum allocation of resources in order to address key targets identified as being at risk.

The final day of the workshop involves an extensive review of the software manual and a discussion of employing PSRAT data to more effectively enhance existing port security strategies such as developing data focused drill and exercise scenarios for ISPS Code Compliance. Participants receive copies of the PSRAT software to conduct additional courses within their own countries.

A GAO report on port security remarked, "Local Captains of the Port have used the assessment information in coordination with input from local stakeholders to (1) establish security zones around key port infrastructures; (2) improve security in and around passenger vessels; and (3) coordinate security improvements, such as fences, cameras, and barriers around port infrastructures."[15]

Risk modeling does have limitations: "Without sensitivity analysis or formal feedback loops to reassess all scenarios and therefore provide greater assurance that the rankings are as reliable as possible, the risk of being unprepared for strategic surprise may increase….[Moreover…] applying risk management to terrorism has no well-established precedent."[16]

3. Maritime Domain Awareness

Awareness is crucial to effectively protecting maritime infrastructure. "We cannot hold polluters accountable unless we can match them to their spills; we cannot keep vessels from colliding if we don't know where they are; we can't rescue survivors unless we

[14] A PSRAT workshop: establishes a baseline level of risk; identifies the key drivers of risk scores and measures to enhance security; provides comprehensive instruction and evaluation of the PSRAT; identifies nationwide port critical infrastructure; establishes best security measures to reduce risk thereby providing the greatest return on investment; establishes security measures providing a more robust layered security regime to countries and owners and operators of the critical infrastructure; and provides a country with risk mitigation data for developing port wide risk plans by identifying critical infrastructure in ports that require protection while creating strong multi-sector connectivity and communication among a range of stakeholders.

[15] Id. The report also noted, "At the national level, the Coast Guard is designing and planning to implement an array of radar systems, sensors, and information systems to identify and track possible threats in the maritime domain."

[16] Id.

find them; and we cannot intercept those who would do us harm if they are able to blend in with the millions of recreational boaters who lawfully enjoy our ports and coastal waters."[17]

MDA, or maritime situational awareness, seeks to attain an actionable understanding of anything in the oceans that could affect the safety, security economy or environment at sea. This awareness is a key component of maritime defense and a critical factor in effective infrastructure protection.[18] MDA systems also may be used to increase the security of commercial shipping, fishing and other lawful users of the sea.

Though a focus on attaining maritime awareness has existed for many years,[19] the current MDA concept took form in the late 1990s. After 9/11, a combination of new vulnerabilities in maritime homeland security and infrastructure assets along with advances in technologies for vessel tracking highlighted the importance of MDA.

While possessing data, being data rich, is important, it represents just one component of attaining maritime situational awareness. Achieving maritime security situational awareness depends on the ability to monitor activities so that trends can be identified and irregularities differentiated. Data must be collected, fused, and analyzed in a timely manner for senior policy officials and operational commanders to take effective action.

U.S. Coast Guard Admiral Brian Salerno noted that "MDA represents a continuum of maritime knowledge from situational awareness through current and predictive intelligence that supports decision makers across all mission areas. It is developed through a process of: (1) collection ["see"], (2) fusion and analysis ["understand"]; and (3) dissemination ["share"] of information and intelligence on vessels, cargo, people, infrastructure, and the environment."[20]

A U.S. Presidentially approved Maritime Domain Awareness Plan in 2005 defines MDA as "…the effective understanding of anything associated with the maritime domain that could impact the security, safety, economy, or environment of the United States…[The] Maritime Domain is all areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all maritime-related activities, infrastructure, people, cargo, and vessels and other conveyances."

[17] Testimony of Rear Admiral Brian M. Salerno, "U.S. Coast Guard's Maritime Domain Awareness Efforts" (Before the House Transportation and Infrastructure Subcommittee on Coast Guard & Maritime Transportation, December 9, 2009), available at http://republicans.transportation.house.gov/Media/file/TestimonyCGMT/2009-12-09-Salerno.pdf (last visited Dec. 11, 2012).

[18] "Maritime domain awareness seeks to identify threats as soon as possible and far enough away from domestic ports to eliminate or mitigate the threat." GAO Risk Management Study.

[19] Rear Admiral Brian Salerno, U.S. Coast Guard, traced the origins of maritime domain awareness to the earliest days of the USCG. "In Alexander Hamilton's 1791 letter of instruction to commanding officers of the Revenue Cutters he noted that "[t]he provisions of these sections admonish you to keep a careful eye upon the motions of coasting vessels, without, however, interrupting or embarrassing them unless where some strong ground of suspicion requires that they should be visited and examined. " This, in essence, was the birth of Maritime Domain Awareness (MDA). Throughout nearly 220 since, the Coast Guard assets, including its cutters, aircraft, stations, boats, sensors, and people have provided the nation with MDA." Id.

[20] Id.

The Safety of Life at Sea Convention (SOLAS), developed approximately a century ago as a result of the Titanic disaster of 1912, provides the standards for the safe navigation of ships and improved maritime awareness. SOLAS amendments have been adopted to enhance the security of the global shipping cargo chain by bringing greater transparency to the maritime domain. Using technology to precisely locate merchant shipping, the amendments provide the commercial fleet and port, coastal and flag state with greater authorities and capabilities. An awareness of legitimate shipping activities enables authorities to better focus scarce resources on anomalous contacts and sort civil commerce from suspicious activity.

The two primary systems for collecting and sharing information are attached to the SOLAS Convention—the Automatic Identification System (AIS) and the satellite-based Long Range Identification & Tracking (LRIT) system. The section on safety of navigation in Chapter V of SOLAS was revised to require all ships over 300 gross tons or that carried 12 or more passengers on international voyages to install AIS. These two systems complement other data sources to secure information, including air surveillance, radar, video cameras and patrol craft.

A ship with AIS is able to display to similarly equipped vessels or shore receivers information such as vessels size, heading and speed. Originally, AIS was developed as a navigational aid in the 1990s to make transit through the Panama Canal safer. The system is based on VHF maritime band, so the range is restricted to line-of-sight coverage, approximately 60 km. A long-range AIS that could potentially track vessels up to 2,000 nautical miles at sea is being developed, but is not projected to be fully operational until 2014. The AIS signal is transmitted on a continuous basis, but when vessel stations are transiting the ocean it cannot always be picked up and used by shore-based security centers. The system is used throughout the world, especially along chokepoints such as the Strait of Gibraltar.

Cooperation is a critical component of attaining maritime situational awareness and the protection of infrastructure protection. Bilateral, regional, and international collaboration is occurring in multiple venues. In 2002, member-states of the International Maritime Organization (IMO) developed and implemented the International Ship and Port Facility Security (ISPS) Code. This agreement provides a construct for ensuring port security throughout the world. Thus, a template now exists for examining security issues ranging from the movement of people and cargo to port services.

The Container Security Initiative (CSI) program is another endeavor that heightens security by collaboratively screening containers. Under CSI, containers, including those that may pose a terrorist risk, are inspected in foreign ports before being shipped. In part, CSI employs "intelligence and automated information," pre-screening of cargo, and detection technology, and it encourages "smarter, tamper-evident" containers.

Collectively, these programs and systems support a layered security approach to maritime security that recognizes the value of unified, and at times, redundant action. Targeting is part of a layered approach and involves screening of vessels that may, for example, be transporting certain dangerous cargoes.[21] Screening is also part of a

[21] United States Government Accountability Office, "Homeland Security; Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection," (Statement of Richard M. Stana, Testimony before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of

layered approach and could include examining ship management – owner, operators, charterer; the flag of the ship – where it is registered; the type of ship; the vessel's history; its last five ports; security compliance history; whether there are reliable reports of serious security deficiencies or a random examination.

The United States Coast Guard seeks to involve the maritime industry and the public in recognition of the fact that the shipping industry as well as citizens can help reduce the potential for illicit activity. The U.S. Coast Guard also embraces the strategy of "pushing the borders" in its effort to protect maritime infrastructure and reduce the threat of maritime terrorism.[22]

Screening in the United States begins, for the most part, when a vessel provides an advance notice of its arrival (ANOA) at the 96 hour point, or 4 days out. Like the ship discussed earlier, the Warm Seas Voyager, information disclosed in an ANOA may trigger additional examinations, further inquiries or pre-entry boardings, security boardings, or prompt the vessel to be escorted.

Similar to limitations on the use of risk assessment models, "even when vessels carrying transponders are tracked in ports, recognizing hostile intent is very difficult…[Information disclosed in a GAO Report noted the existence of…] vessels intruding into security zones where unauthorized access was prohibited. While no attacks occurred, such vessels were able to travel freely near potential targets. The difficultly in recognizing potentially threatening activity and the limited response capability indicate that expanding tracking to small vessels would not necessarily diminish the risk posed by small vessels."[23]

A separate and uniquely challenging issue in the maritime environment is disposition: determining what we going to do with the cargo, the people and the vessel after it is interdicted. For governments with separate judicial, diplomatic, military and police agencies, along with different chains of command, a national-level process to align efforts and speak as one voice is absolutely critical.

Coordination for national-level issues in the United States unfolds through the interagency process,[24] in the space below the President and above the individual

---

Representatives, GAO-04-557T, March 31, 2004). See also United States Government Accountability Office, Cargo Security, Partnership Program Grants Importers Reduced Scrutiny with Limited Assurance of Improved Security (GAO-05-404, March 2005).

[22] "Current programs and policies can be grouped under the following generic categories, which include pushing the border outwards to intercept unwanted people or goods before they reach the United States (as in the passenger pre-screening program); hardening the border through the use of technology (as shown by biometric identifiers); making the border more accessible for legitimate trade and travel (as in "trusted traveler" programs); strengthening the border inspection process through more effective use of intelligence (with the integration of terrorist watch lists); and multiplying the effectiveness of interdiction programs through the engagement of other actors in the enforcement effort (as displayed by bi-national accords with Canada and Mexico). It is also possible to use the strategies as a checklist for what new efforts might be explored." Lisa M. Seghetti, Jennifer E. Lake and William H. Robinson, *Border and Transportation Security: Selected Programs and Policies* (Congressional Research Service RL32840, March 29, 2005), available at http://www.fas.org/sgp/crs/homesec/RL32840.pdf (last visited Dec. 11, 2012).

[23] United States Government Accountability Office, "Maritime Security Responses to Questions for the Record."

[24] See Presidential Policy Directive 1, Organization of the National Security Council System, February 13, 2009. More than twenty federal agencies are involved in maritime issues, including the Departments of Defense, State, Justice, Homeland Security, Transportation and Commerce, as well as the Council on Environmental Quality, the Office of Science and Technology and the intelligence community. The National

departments (ministries in most countries). A key challenge within the interagency or inter-ministerial level, is expeditiously securing consensus, as each agency brings distinct perspectives, capabilities and authorities to issues.

In the United States, national-level plans have evolved over the past four decades to accelerate decisions, integrate representatives from multiple agencies and ensure information is disseminated transparently. These horizontal coordinating mechanisms do not supplant or replace agency authorities, but create constructs for expeditious whole of government responses. The Presidentially-approved Maritime Operational Threat Response (MOTR) Plan has been used more than 1,000 times over the past six years ago to coordinate the response to maritime threats.[25]

Conclusion

Protecting maritime infrastructure is particularly challenging because threats are not always clear and are often preceded by ambiguous signals, uncertain events and incomplete information. There is no one action, no one activity that can eliminate every threat or the possibility of risk, but the acquisition of fused information, a focus on risk modeling, and a nationally-directed coordination process best positions a government to respond. Significantly, these efforts support the response to potential attacks as well as to floods, wildfires, pandemics, cyber attacks and significant disruptions of the supply chain.

Bibliography

Parfomak, Paul W., and John Frittelli, *Maritime Security: Potential Terrorist Attacks and Protection Priorities* (CRS Report for Congress, May 14, 2007).

Seghetti, Lisa M., Jennifer E. Lake and William H. Robinson, *Border and Transportation Security: Selected Programs and Policies* (Congressional Research Service RL32840, March 29, 2005).

Tomasulo, Gary L., Jr., *Evolution of Interagency Cooperation in the United States Government: The Maritime Operational Threat Response Plan* (June 2010).

United States Government Accountability Office, Cargo Security, Partnership Program Grants Importers Reduced Scrutiny with Limited Assurance of Improved Security (GAO-05-404, March 2005).

United States Government Accountability Office, Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure (GAO-06-91, December 2005).

United States Government Accountability Office, "Maritime Security Responses to Questions for the Record" (GAO-11-140R, October 22, 2010).

Yergin, Daniel, "Ensuring Energy Security," *Foreign Affairs* 85 (March/April 2006).

Security Staff-hosted Maritime Security Interagency Policy Committee, Deputies' Committee and Principal's Committee, among others, serve as national-level venues for addressing maritime security issues.

[25] Maritime Operational Threat Response Plan, October 2006. See also Rear Admiral Brian Salerno, prepared remarks before the Subcommittee on Coast Guard and Maritime Transportation, Committee on Transportation and Infrastructure, U.S. House of Representatives on May 20, 2009, available at http://www.marad.dot.gov/ documents/Testimony-RADM_Brian_M_Salerno-USCG.pdf (last visited Dec. 10, 2012).

This page intentionally left blank

Critical Infrastructure Protection
M. Edwards (Ed.)
IOS Press, 2014

doi: 10.3233/978-1-61499-357-5-93

Planning Methodology for Critical Infrastructures Protection Capabilities

Maria BORDAS[a] and Janos TOMOLYA[b,1]
COE-DAT, Ankara, Turkey

Abstract. The importance of critical infrastructure is seen through its potential to enable the functional continuity of vital societal functions from economic and social perspective. The present state of critical infrastructure protection is related to the creation of a robust security and protection management system, where the effectiveness of this system should be important also in relation to business continuity and disaster recovery. In planning the capabilities for protection of critical infrastructure protection, policymakers and planners need to define and find the balance between four key components: goals, strategy and respective distribution among variety of private and public organizations means or capabilities to implement the strategy and planning risks. The protection of critical infrastructure is just one of the 21st Century security challenges that require a comprehensive approach, plus sound coordination among and, in time, integration of governmental agencies. The planning methodology for critical infrastructures protection capabilities of the kind presented in this article may contribute to finding effective and efficient solutions in the best interest of society.

Keywords. Critical infrastructure protection, CIP programs, CIP planning

Introduction

Every nation has an obligation to protect essential government, financial, energy, transportation, and other critical infrastructure operations against terrorist activities and natural disasters. There is no need to look far back in time in order to recognize the threats to the normal functioning of societies that lead to deliberate attacks, malignant behavior, natural disasters or other types of harmful impact on key elements of the infrastructure. In their attempts to limit possible damage and enhance societal security, governments adhere to one or a mix of two main approaches:

- formulation and application of rules, mandatory for critical infrastructure owners and operators; or
- provision of public funds in order to increase the protection of infrastructure elements.

In the first approach, the main responsibility for the normal functioning of the infrastructure elements is transferred from the state to other entities, primarily private actors. In such cases, the companies will add to the price of their product the costs arising from the fulfillment of security-related obligations. Thus, the infrastructure

[1] Prof Dr. Maria BORDAS, PhD, is academic adviser of COE-DAT; Colonel Tomolya, PhD, is the Chief of Capabilities at COE-DAT.

protection measures will be paid indirectly by the customers, e.g. by the population. Another disadvantage of this approach relates to the process of globalization of businesses. If overregulated, the national economy may lose its competitive advantages and thus the business environment in the country may deteriorate considerably, leading extreme bankrupts and unemployment.

In the second approach, central and local governments will carry the financial burden of measures to decrease the vulnerability of infrastructure elements. While enhancing security, such investment of public funds may have an unintended side effect of enhancing the competitiveness of particular companies. While state authorities try to increase the security for the citizens, such effects might be unavoidable but their impacts should be clearly understood and limited to the extent possible. Therefore, for a state with market economy and democratic governance, it is crucial to ensure due decision-making procedures – a process which is transparent, where the rules are fair and where the public is well informed on the relevant criteria. This process should be monitored by an independent body and subject to audits when necessary.

This article presents such a process. First, it looks at how a decision on the 'criticality' of certain infrastructure elements is made. Next, it presents a framework process for planning and developing capabilities and measures for protection of critical infrastructures. The final part presents major methodological organizational challenges, emphasizing for much greater coordination amongst governmental organizations, security services, owners and operators of critical infrastructure. In the conclusion, the applicability of the approach to other security-related issues is briefly addressed.

1. Defining the Criticality of Infrastructure Elements

Structures typically included under the heading of critical infrastructure are highways, airports and aircraft, trains and railways, bus lines, shipping and boat lines, transport, trucking systems, and supply networks for basic goods, electric power plants and lines, along with oil and gas lines and utilities of all kinds, including water and sewer systems, land and cell phone systems, computer networks, television, and radio (not only that which is publicly accessible, but that controlled by private or government entities in special networks or on special frequencies), banks and other financial institutions, and security, fire, hospital, and emergency services. Each element of critical infrastructure is so vital that if it were removed from the equation, even temporarily, the entire nation would experience monumental repercussions. Even when the infrastructure of a particular area is threatened, the results can be disastrous. To this day, people alive at the time remember the northeastern electrical blackout of 1965, or the New York City blackout of 1977. Today, the critical systems that run the engine of America are far more interlinked than they were even in the 1970s; this interdependence carries with it new vulnerabilities.

Although logical, this definition does not provide for a comparative evaluation of criticality of particular elements of infrastructure. It is not even sufficient to determine whether a particular asset, system or service can be examined as potentially 'critical' or not. Therefore, the definition cannot be in the process of identifying and analyzing the effectiveness of measures for protection of infrastructure; it cannot be used for setting priorities ether. Generally speaking, the current legislation does not provide a proper

basis for a reasonable distribution of public and private resources in order to enhance the security of critical infrastructures. The approach outlined in this article does provide such a basis. It also entails a model of decisionmaking on private and public investment in security-related measures, thus enabling the achievement of highest possible impact within limited resources.

The applicable European Union (EU) regulation, EU Directive 2008/114/EC,[2] defines critical infrastructure as follows: "'critical infrastructure' includes in particular those physical resources, services, information technology facilities, networks and infrastructure assets which, if disrupted or destroyed, would have a serious impact on the critical societal functions, including the supply chain, health, safety, security, economic or social well-being of people or of the functioning of the Community or its Member States."[3]

In November 2005, the Commission adopted a Green Paper on a European Programme for Critical Infrastructure Protection (EPCIP) which provided policy options on how the Commission could establish EPCIP and the Critical Infrastructure Warning Information Network (CIWIN).

The legislative framework for the EPCIP consists of the following:

- a procedure for identifying and designating European critical infrastructure and a common approach to assessing the need to improve the protection of such infrastructure. This will be implemented by means of a directive;
- measures designed to facilitate the implementation of EPCIP, including an EPCIP action plan, the Critical Infrastructure Warning Information Network (CIWIN), the setting up of Critical Infrastructure Protection (CIP) expert groups at EU level, CIP information sharing processes, and the identification and analysis of interdependencies;
- support for EU countries regarding National Critical Infrastructures (NCIs) that may optionally be used by a particular EU country, and contingency planning;
- an external dimension;
- accompanying financial measures, and in particular the specific EU programme on the "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" for the period 2007-13, which will provide funding opportunities for CIP related measures.

The ECPIP action plan has three main work streams:

- the first relates to the strategic aspects of EPCIP and the development of measures horizontally applicable to all CIP work;

[2] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

[3] Euratom, "Council Decision of 12 February 2007 Establishing for the Period 2007 to 2013, as Part of General Programme on Security and Safeguarding Liberties, the Specific Programme Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks (2007/124/EC), Article 2, Definitions para (c).

- the second concerns the protection of European critical infrastructures and aims to reduce their vulnerability;
- the third is a national framework to assist EU countries in the protection of their NCIs.

The Critical Infrastructure Warning Information Network (CIWIN) as a warning network will be set up by a specific Commission proposal for the purposes of exchanging best practices and providing an optional platform for the exchange of rapid alerts linked to the Commission's ARGUS system. The abovementioned 'Green Paper' from 2005 further delineates the critical infrastructure sectors into eleven sectors:

- energy;
- nuclear industry;
- information and communication technologies;
- water;
- food;
- health;
- financial;
- transport;
- chemical industry;
- space; and
- research facilities;[4]

In US the Department of Homeland Security defines the critical infrastructure sectors as follows:

- Food and Agriculture
- Banking and Finance
- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Government Facilities
- Healthcare and Public Health
- Information Technology
- National Monuments and Icons
- Nuclear Reactors and Materials
- Postal and Shipping
- Transportation Systems
- Water[5]

In Germany, subject matter experts list the following sectors as critical infrastructure:[6]

[4] European Commission, "Green Paper on a European Programme for Critical Infrastructure Protection" (Brussels, 17 November 2005), Annex 2, p. 24.
[5] John Moteff and Paul Parfomak, "Critical Infrastructure and Key Assets: Definition and Identification" (Congressional Research Service, RL32631, October 1, 2004), p. 5.
[6] Christoph Riegel, "Risk Assessment and Critical Infrastructure Protection in Health Care Facilities: Reducing Social Vulnerability" (German Federal Service of Interior 2008), p. 5.

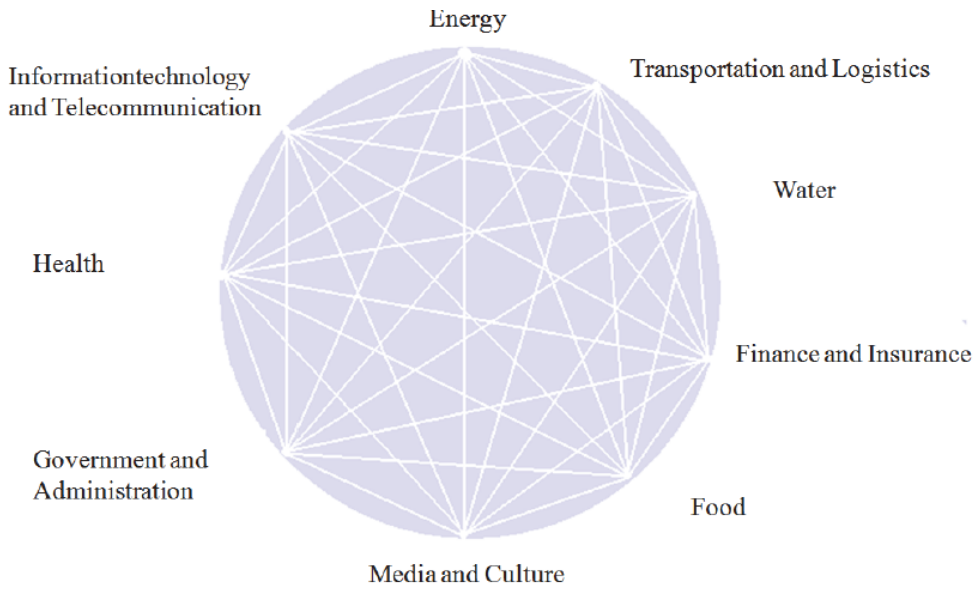

Figure 1. German Definition of Critical Infrastructure

The lessons learned from 9/11, along with some outcomes from the ongoing European debate and discussions on national levels on what type of infrastructure can be considered a candidate for critical and thus subject to public investment for higher degree of protection, and our analysis identifies three additional candidate types of critical infrastructure:

- waste and waste management,
- public crisis management service and their key assets, and
- national symbols

Shared understanding and decision on what are the sectors of critical infrastructure is a necessary condition for the elaboration of transparent process of defining criticality of particular infrastructures and elements. Such process incorporates the following assessments:

1. Sector analysis: Identification of main sectors, sub-sectors and assets of critical infrastructure and determination of most critical among them. Criticality is measured by the anticipated negative impact from failure or impediment of an asset. The most severe impact, the most critical is the asset. Among the criteria for assessing the potential magnitude of an incident are the:

a. so-called "public impact" (e.g. number of citizens affected: loss of life, injuries or illness that requires long-term treatment evacuation);

b. economic impact (effect on GDP, economic loss, degradation of products and services);

c. environmental impact; and

d. political and psychological impact, e.g., the confidence in the ability of government to cope with the incident. In addition, the time aspect of the impact should be accounted for i.e. the immediate one or two days, one week over long term.[7]

2. Identification, description (characterization) and evaluation threats to the critical infrastructure. These threats can arise from the deliberate attack, natural disaster or human error. In the course of a threat assessment, we need to consider the capabilities of possible intruders to carry out a successful attack, as well their intention, accounting for existing vulnerabilities of critical infrastructures. The exploitation of the vulnerabilities could aim at incurring damage to the economy, defense or other aspects of national security.

3. Vulnerability assessment for the main sectors of the critical infrastructure with respect to specific threat. Vulnerability can be defined as a weak point, exposed to malignant actions, performed in order to destroy or damage certain assets of critical infrastructure.

4. Assessment of interdependencies among subsystems and infrastructures, with a focus on identifying those that potentially lead to cascading effects or other similar processes. Interdependencies may play a crucial role in deciding on measures to protect since often damage to one sector has a derivative, sometimes even more destructive, impact on other sectors dependent on the first one.

5. Risk assessment (the consequences to be expected of certain attack against particular sectors accounting all types of negative impact: loss of human life, economic losses over time, etc.) The risk estimate is integral, i.e. across threats and accounts for the likelihood of related incidents. The results of these assessments are then are used to identify and prioritize risk mitigation strategies and measures:

6. Elaboration of critical infrastructure strategy. Normally it is would be a strategies for risk mitigating and risk management.

7. Elaboration of set of measures and capabilities for protection of critical infrastructure protection and risk mitigation in the framework of strategy.

The activities in the course of analysis and planning of critical infrastructure protection shall be performed step by step in the framework of an integrated process as shown in Figure 2, which involves a number of feedback loops. The critical infrastructure protection policymaking involves decisions on the scope of critical infrastructure, setting objectives, indentifying and prioritizing measures, and allocating resources for critical infrastructure protection. Thus, it both informs the implementation of the seven steps outlined above and feeds on their results in an interactive manner.

[7] Myriam Dunn and Victor Mauer, *International Critical Information Structure Protection Handbook* (Vol I, Center for Security Studies, Zurich, 2006) p. 367.

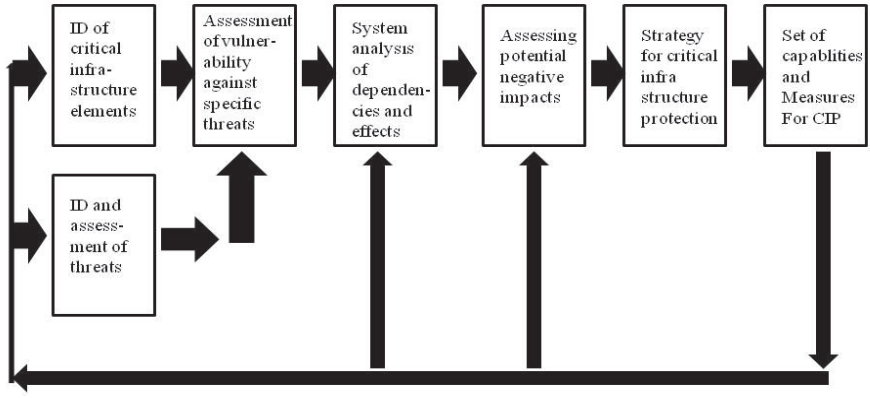

Figure 2. Policy Development for Critical Infrastructure Protection

2. Framework Process for Planning Critical Infrastructure Protection

In planning the capabilities for protection of critical infrastructure protection, policy makers and planners need to define and find the balance among four key components: goals, strategy and respective distribution among variety of private and public organizations means or capabilities to implement the strategy and planning risks.[8] The term of capability here is defined as "the capacity provided by set of resources and abilities, to achieve a measurable result in performing a task under specific conditions and to specific performance standards."[9] Therefore, in addition to the four main components, a more detailed 'top-down' part of the planning process requires defining a set of plausible conditions, as well as the set of tasks to be performed in these conditions. Thus a rigorous planning process links the:

- objectives in the area of the critical infrastructure protection;
- goals in terms of protection of critical infrastructures;
- strategy for achieving the objectives and respective roles of public and private organizations engaged in critical infrastructure protection;
- scenarios describing plausible risks and threats to critical infrastructure; tasks to be performed in preventing and responding to the plausible risks and threats and to be managed consequences of an incident;
- measures and capabilities required to perform the tasks for protection of critical infrastructures; and

[8] Henry Bartlett, G. Paul Holman and Timothy E. Sommes, *The Art of Strategy and Force Planning* (Naval War College Press, 2004), pp. 17-33.
[9] US Department of Homeland Security, *Critical Infrastructure and Key Resources (CIKR) Protection Capabilities* (2008), p. 13.

- ways to provide these capabilities (coordination of the development of the variety of capability components - human, material, training, etc. - within a selected capability model often described through programs) within resource constraints.

The framework accounts also for the various horizons of the planning process, the possibility to act simultaneously to protect critical infrastructure across a number of scenarios, the centralized nature of capability planning, and decentralized budgeting and execution tasks, as well as programs the distribution of decision-making authority for planning and implementation oversight in addition to a number feedback loops.

The next figure (Figure 3) presents this framework with the assumption that a country applies output-oriented (e.g. program-based) management of resources for the protection of critical infrastructures and equivalently program-based implementation of measures and development of respective capabilities.

3. Methodological and Organizational Challenges

Our expectation is that, in the foreseeable future, all EU member states will develop an official methodology for guiding the assessment of criticality of infrastructure assets, the planning of protective measures and capabilities, as well as the allocation of public and private resources. In all probability, it will be based on a risk management strategy from the EU.

This strategy will be implemented through a set of measures and capabilities for critical infrastructure protection. However, it is not recommended to create respective plans independent of other security-related requirements. Since a considerable number of the organizations contributing to the protection of critical infrastructures maintain a wide spectrum of capabilities, many of which are 'multipurpose,' our recommendation is to set the planning process in the context of 'protection of population against terrorist threats, natural disasters industrial accidents and catastrophes.' It is possible but not advisable at this stage to use an even border context, such as:

- Critical infrastructure protection capability planning in the context of protection of the population and the national economy against terrorist attacks, natural disasters, industrial accidents and catastrophes;
- Critical infrastructure protection capability planning in the context of capability planning for the national security sector (which in addition needs to account for the NATO and EU planning requirements.)

From the analytical point of view in further development and implementation of methods tools and analyzes techniques it is recommended that:

1. Critical infrastructure protection should be treated as a very complex adaptive system. All typical features of this type of system are to be taken into account, including inherent uncertainty and rather limited predictability within such a system.

2. The most promising and competing methodologies for exploration of complex adaptive system are based on the creation of two very different critical infrastructure models: an architectural model (tools for and object-oriented modeling can be integrated in the course of its elaboration) or an agent-based model.

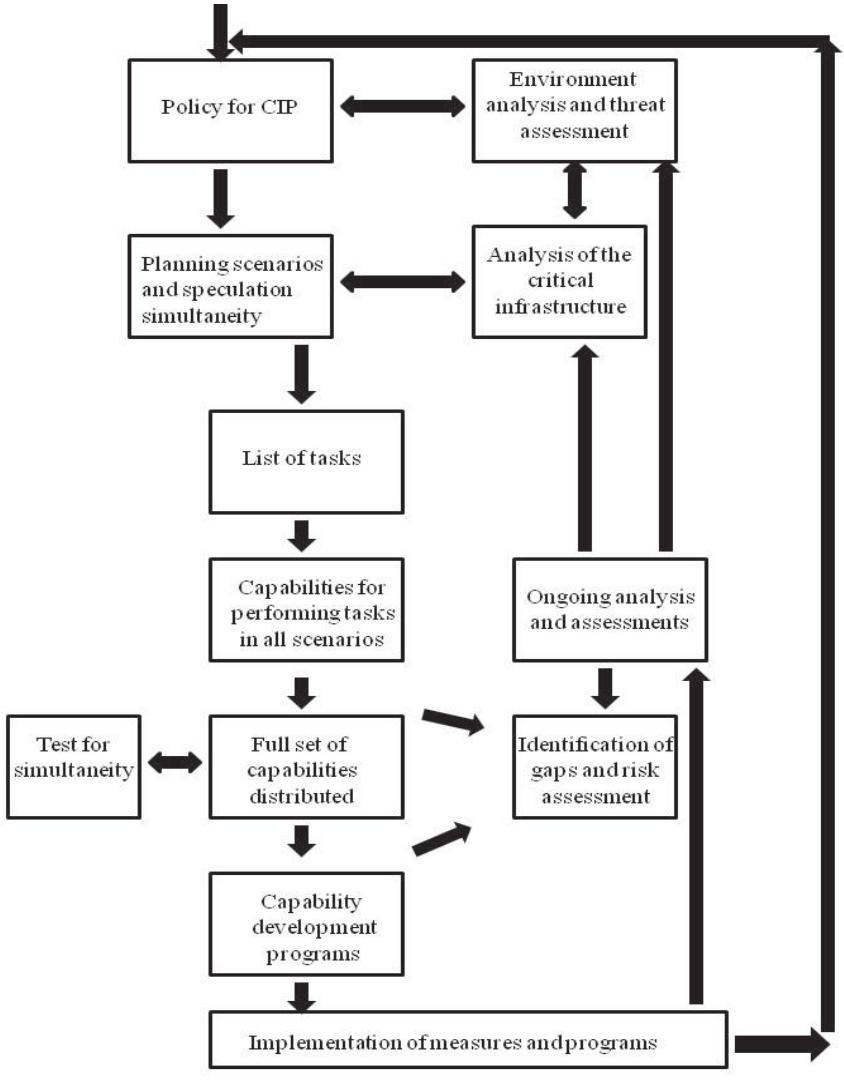

Figure 3. Development of CIP Measures and Programs

3. The implementation of these models shall be complemented by integration of expert assessment, for example, in defining integral criteria, defining objectives and ambition levels (in the course of the development of a critical infrastructure protection policy) in generating and assessing alternative solutions, etc.
4. In certain cases, as expert estimates, we can consider group decisions, i.e. ones made by participants in computer-assisted exercises and simulations.
5. A broad variety of methods and approaches is available to support the performance of specific tasks. It is important however to integrate the latter in the overall planning framework for critical infrastructure protection.

From the organizational point of view, the key challenge is the break down organizational stovepipes. Otherwise the state administration will not be able to get the whole picture, i.e. to assess interdependencies, and respectively, impact of infrastructure-related incidents to seek cost-efficient distribution of critical infrastructure protection among the organizations involved. That was one of the reasons for the creation of the Department of Homeland Security in the US.

Conclusion

The dependence of business government and societal services on critical elements of infrastructure creates vulnerabilities that can cause considerable losses from malevolent behavior, terrorist attack, human error, or extreme forces of nature. Societies are determining the value of vulnerabilities and resulting losses when they decide how much to invest in particular measures and for the protection of critical infrastructure.

That means transparency - clear rules and decisions on which assets are critical, what could be done to increase the robustness of these assets, which measures to implement within resource constraints, what would be overall impact of one measure or another. This paper outlines a methodological approach to assuring such transparency. With all methodological, procedural and analytical challenges in place, the major obstacle to effectiveness and efficiency is the culture of centralized decisionmaking within strict hierarchies that limit interagency cooperation, coordination, and often even the communication as well. Being a relatively novel challenge of EU that enjoys the highest interest on the EU's agenda, critical infrastructure protection has the chance to turn into a 'Trojan Horse,' breaking organizational stovepipes; enhancing transparency of decisionmaking and accountability of central and local governments of the EU's member states; and to provide a new much higher level of coordination and cooperation among governmental organizations, security services owners and operators of critical infrastructure. The utmost challenge itself, the protection of critical infrastructure, is just one of the 21st Century security challenges that requires a comprehensive approach, plus sound coordination among and, in time, integration of governmental agencies. Countering the terrorist threats and their origins conducting stabilization operations and dealing with pandemics, catastrophic or mass-casualties terrorism, and major disasters are other missions that require such comprehensive approach. A methodology of the kind presented herein may contribute to finding effective and efficient solutions in the best interest of society.

Bibliography

Bartlett, Henry, G. Paul Holman and Timothy E. Sommes, *The Art of Strategy and Force Planning* (Naval War College Press, 2004).

Dunn, Myriam, and Victor Mauer, *International Critical Information Structure Protection Handbook* (Vol I, Center for Security Studies, Zurich, 2006).

Euratom, "Council Decision of 12 February 2007 Establishing for the Period 2007 to 2013, as Part of General Programme on Security and Safeguarding Liberties, the Specific Programme Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks (2007/124/EC).

European Commission, „Green Paper on a European Programme for Critical Infrastructure Protection" (Brussels, 17 November 2005).

Moteff, John, and Paul Parfomak, "Critical Infrastructure and Key Assets: Definition and Identification" (Congressional Research Service, RL32631, October 1, 2004).

Riegel, Christoph, "Risk Assessment and Critical Infrastructure Protection in Health Care Facilities: Reducing Social Vulnerability" (German Federal Service of Interior 2008).

US Department of Homeland Security, *Critical Infrastructure and Key Resources (CIKR) Protection Capabilities* (2008).

This page intentionally left blank

Critical Infrastructure Protection
M. Edwards (Ed.)
IOS Press, 2014

Subject Index

This page intentionally left blank

Critical Infrastructure Protection
M. Edwards (Ed.)
IOS Press, 2014

Author Index

This page intentionally left blank