Critical Energy Infrastructure: Operators, NATO, and Facing Future Challenges

Dinos Kerigan-Kyrou [*]

Introduction

Critical infrastructure enables modern society. It includes our communications and Internet, our banking systems, the means of safely delivering our supplies of food and water, health systems, defense installations, transportation networks, air traffic control systems, and logistics and port facilities. It also includes our energy and electricity supply. Power generation plants, electricity grids, and diesel, gasoline, oil, and natural gas distribution networks underpin our entire infrastructure. Critical energy infrastructure is the single most important part of the complex web of critical infrastructure. Without energy—particularly the regular supply of gasoline and diesel—no other element of our critical infrastructure can operate. This was clearly seen in the northeastern United States during Hurricane Sandy in 2012. That is why the priorities in the wake of the storm were first to reestablish power, and second to restore transit systems (buses and subways). Governments and relief organizations quickly realized that only then could other infrastructure, such as hospitals, become operational again.

Threats to our energy infrastructure increasingly take different forms. They can arise from environmental hazards (as in the case of Hurricane Sandy, or the March 2011 earthquake and tsunami in Japan); industrial accidents; deliberate sabotage; and "consequential sabotage." The latter two examples are closely connected, and will be explored further below.

The Challenge of Energy Security

This article will highlight a threat to NATO's energy infrastructure that has been a concern for many decades. This threat is energy security. In 1912, the British Royal Navy converted its ships from coal to oil. Winston Churchill, then First Lord of the Admiralty, said "Safety and certainty in oil lie in variety and variety alone." The United States and the U.K., with its oil fields in the Middle East, became the world's oil suppliers. That situation, however, was soon to change, a fact of which U.S. President Franklin Roosevelt was aware. In 1945, Roosevelt met with King Abdul-Aziz Ibn Saud, securing U.S. access to Saudi Arabia's oil output. Today the biggest potential challenge in terms of energy security is supply. There is a vast amount of oil, coal, and natural gas in the world. Each day, however, the world uses approximately 86 million barrels of oil. Daily world production is exactly that figure: 86 million barrels. So even a small 2 percent reduction in output caused by, for example, a crisis in Libya, has an enormous effect on

[*] Dinos Kerigan-Kyrou is an external instructor at the NATO School in Oberammergau, Germany, and a Research Associate of the Dartmouth Strategic Studies Group in the U.K. He holds a Ph.D. from the University of Aberdeen.

the global price of oil. When such problems occur, only Saudi Arabia has the ability to quickly make up the deficit in the supply. The world economy is therefore enormously vulnerable to even a small drop in production.

The security of the oil producing regions is vital to the NATO Alliance. In rural Iraq, it costs USD 15,000 for a family to connect to the electricity grid – an impossibly large amount. These communities, however, see vast oil wealth around them. It is vital that they are not tempted to work with those who want to damage the oil production infrastructure. It is particularly important—for our own security—that the international community help ensure that local communities in oil-rich countries benefit from their national energy resources. These benefits should include schools, hospitals, and infrastructure that oil revenues can bring, as well as help in fighting corruption. Once corruption starts, it is very hard to stop, as Nigeria's government has discovered. Corruption becomes ingrained in the whole system. Improving our energy infrastructure security means ensuring that communities in the Middle East and Africa do not have to turn to terrorist groups such as Boko Haram to feed their children. The Extractive Industries Transparency Initiative (EITI), established by BP's John Browne when he was the company's chief executive, is the ideal way to help ensure that oil money benefits the right people.

Improving our energy security also requires increasing the sources of our oil and the resilience of its transport networks. For example, 20 percent of the world's oil transits the Straits of Hormuz. Saudi Arabia, the United Arab Emirates, and Oman recently opened a pipeline that shifts some of that oil away from the strait. Iran has allegedly threatened that it would wreck an oil tanker, causing an environmental disaster and the closure of the strait, so this new pipeline brings welcome additional oil transit security. Such solutions, however, do not solve our energy supply problems; rather, they take us a step forward in increasing resilience. The key goal is widening the variety of energy sources used and increasing the overall supply of oil.

Environmental Threats to Energy Security

Among developed nations, Japan has long been particularly reliant on nuclear power. Indeed, the 2011 earthquake and tsunami is the prime example of an environmental challenge to critical energy infrastructure. The Fukushima nuclear power station was resilient to the earthquake, the most powerful ever to occur. The plant immediately shut down, as it was designed to do. The problem came an hour later, when the protective seawall surrounding the plant was surmounted by a fourteen-meter tsunami. A nuclear power station needs power even after it is shut down in order to cool the uranium fuel rods. The equipment, control systems, and diesel backup generators, however, were underwater, and the cooling water pipes were damaged. The uranium fuel rod storage tanks, which have to be continuously cooled, had no power. The "fail safe" was a heat exchange condensation system, but this lasted only a few hours. Backup generators rushed to the site did not have the right connections. The Tokyo Electric Power Company (TEPCO) thought a total power loss was impossible, and this is understandable.

There were multiple backup power generating systems, but these all failed, one by one. It is very difficult for an organization to plan for situations that it cannot foresee.

The main threat facing nuclear power stations, as Fukushima demonstrated, is flooding. In October 2012 during Hurricane Sandy, Indian Point and Oyster Creek nuclear power stations, in New York and New Jersey, remained resilient as they avoided getting flooded. Oyster Creek was offline, but still had spent radioactive fuel rods that needed to be kept cool. Likewise, the 2011 tornadoes that swept across the southern United States killed over 300 people, but an even greater tragedy was averted due to the resilience of the Browns Ferry nuclear power station on the Tennessee River in Alabama. The winds wrecked part of the station, and it lost internal power. Browns Ferry, however, managed to perform a "cold shutdown," thereby avoiding a reactor core meltdown. Nuclear power stations can be safe even if there is a hurricane, tornado, or earthquake.

The Fukushima disaster was obviously not caused by climate change – an earthquake was the cause of the tsunami. But extreme weather events are continuing to occur. This has been seen in the United States over the past couple of years, but also in Russia, China, and Europe. It does not matter what is actually causing this increase in weather catastrophes, although global warming is obviously an issue of grave concern. What is important is that the number of extreme weather events is increasing, and the NATO Alliance needs to be resilient to these new challenges.

When problems occur that cannot be foreseen, however, such as Fukushima, then substantial challenges will occur. This matters, because the number of such "asymmetric" emergencies is growing. Indeed, Hurricane Sandy demonstrated a fundamental point about our energy infrastructure's resilience. Power outages occurred across New York, New Jersey, and Pennsylvania. Most were caused by a problem at the system's weakest point – the individual power line, not the power station. A tree falling on an electricity pylon or the flooding of one substation would knock out power for thousands of people. The lack of electricity meant that oil refineries could not get back online. The Bayway refinery in Linden, New Jersey, which typically produces 238,000 barrels per day, was particularly damaged by salt water. Refineries that were not flooded, such as that in Reading, New Jersey, could not get back online quickly due to the lack of electricity. New York Harbor needed to ensure that high priority cargoes, particularly refined gasoline, could be delivered quickly. (Indeed, there were plenty of oil tankers lining up to get into New York, but they could not be docked or unloaded.)

Additional Challenges to Energy Infrastructure

Our infrastructure is increasingly interconnected. It does not, however, require a major event such as Hurricane Sandy to affect it. In 2003 a tree fell on a single pylon near the French–Italian border. This incident cut off electricity across much of Italy. Energy resilience is only as good as the system's weakest point. The fear is that terrorists or extremist protesters may know this. Indeed, it is known that terrorists can sabotage our energy infrastructure. Emergencies can also be caused by what can be called "consequential sabotage," brought about by groups that can be referred to as "reckless protesters."

Their actions may produce results as catastrophic as a terrorist attack. In the U.K., there have been power station occupations and vehicle attacks, such as on trains transporting coal to power stations. Indeed, the recent Greenpeace occupation of the Leiv Eriksson oil rig, in transit from Turkey to Greenland, is a further example. A few weeks later off Greenland, Greenpeace occupied the oil platform again. The Royal Danish Navy removed the protesters for their own safety, the oil workers' safety, and to protect the environment. A protest on an oil rig or in a power station could produce a disaster. At airports, protesters have infiltrated active airfields. If one was to run across a live runway it could result in catastrophe. Energy and aviation infrastructures face many of the same threats from reckless protesters. It is important that aviation and energy companies work together, sharing information, to prevent such challenges from occurring.

Deliberate attacks on our energy infrastructure are therefore obviously of particular concern. Such attacks can sometimes be a necessary part of conflict. In 1943, a Royal Air Force (RAF) squadron attacked three dams in the Ruhr Valley in Germany: the Mohne, Edersee, and Sorpe. This action was called Operation Chastise, but the airmen eventually became informally known as the "Dambusters." The dams were key parts of Nazi Germany's energy infrastructure. Two particularly interesting things can be learned from this operation. First, attacks on critical infrastructure often require ingenious and highly unusual methods – with the Dambusters, it was the development of a "bouncing bomb," which was designed to skip across the water and then detonate underwater next to the dam. Second, how critical infrastructure is built makes all the difference to its resilience. The Mohne and Edersee dams, built of concrete, were indeed breached. But the Sorpe dam suffered only minor damage; its core was covered in earth, making it much more resilient to attack. Breaching the Sorpe dam proved impossible. Not enough Lancaster bombers could get through German air defenses to launch the highly complex attack pattern—an attack that had to be even more complex than those on the Mohne and Edersee dams. (Those attacks required dropping the bouncing bombs at sixty feet above the water, at a precise point at 280 miles per hour, while under anti-aircraft fire.)

Seventy years later we can learn two particularly important lessons about our energy infrastructure resilience. Operation Chastise demonstrates the importance of innovation for an attack (using a bouncing bomb), and resilience—as the Sorpe dam proved—in defending infrastructure. Innovation and resilience were as important in World War II as they are today in protecting critical infrastructure from advanced cyber attack. Indeed, cyber methods are particularly useful for the group mentioned earlier in this essay, the "reckless protesters," sometimes called "hacktivists," after activists who hack computer systems. Extreme elements within environmental groups may use cyber methods against energy companies they disapprove of. Such strategies are also, of course, ideal for terrorists. Indeed, cyber attacks may soon begin to resemble the actual physical attacks that have occurred over the last few years.

In 1996, the Irish Republican Army (IRA), attempted to attack four electricity substations near London. This would have crippled electricity supplies for many months, potentially crashing the U.K.'s economy. The plan failed, but proved how vulnerable the energy infrastructure is to such challenges. In 2002, Al Qaeda attacked the oil tanker

Limburg with a suicide boat near Somalia. Indeed, documents seized from Osama Bin Laden's house in Pakistan indicate that oil tankers would continue to be targets for Al Qaeda attacks. In Saudi Arabia and Iraq, Al Qaeda terrorists have attacked oil refineries and energy facilities, causing many casualties and damaging infrastructure. Such damage to energy producing infrastructure, wherever in the world it happens to be, affects all countries of the NATO Alliance. As was mentioned above, the world uses 86 million barrels of oil each day, precisely the amount that is produced. Any disruption to this supply of oil anywhere in the world has substantial consequences for the NATO Alliance.

Technology-Based Attacks on Energy Infrastructure

Physical attacks against our critical energy infrastructure can increasingly be caused by communications technology, even if the person or organization responsible is on the other side of the world. Control systems are vulnerable to hacking, manipulation, and viruses that can remain undetected for months, even years. Such a cyber attack could take place against almost any aspect of our critical infrastructure. U.S. Secretary of Defense Leon Panetta has warned of the potential of a cyber "Pearl Harbor." In November 2011, U.S. Homeland Security and FBI officials were alerted to an apparent cyber intrusion at a water treatment facility in Illinois. Hackers caused a water pump to burn out of control by accessing its Supervisory Control and Data Acquisition (SCADA) software.

Power stations are a particularly vulnerable target of this increasingly worrying phenomenon. Each one has equipment that issues commands, controls turbine speeds and steam production water control valves. In the U.S., power stations and grids are regionally divided, providing increased separational security. However, 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. Such a virus can be spread accidentally by engineers with USB drives, or deliberately over the network. A sustained electricity blackout on the East Coast of the U.S. could cause food shortages across the nation in just a week. Moreover, by the time authorities have ascertained what is causing the problem in New York, the virus could have been encrypted and hidden on other systems across the country. A new attack could be launched days, weeks, or even months later.[1] It is very hard to totally insulate a critical infrastructure system from the Internet, USB devices, or emails; indeed, I would argue that it is impossible. Such an attack does not even need a commander with a phone or remote control – the attack can simply be launched when the virus identifies a specific control process, causing a turbine to spin 100 times faster than normal, wrecking the entire plant.

Indeed, there have been cyber attacks on elements of energy infrastructure in the Middle East. In August 2012, 30,000 computers at Saudi Aramco, the world's biggest oil company, and at Qatar's RasGas, which produces the world's largest output of

[1] Joseph Menn, "U.S. Power Plants Vulnerable to Cyberattack," *Financial Times* (11 October 2011); available at http://www.ft.com/cms/s/0/00148d60-c795-11e0-a03f-00144feabdc0.html#axzz2e4TzZDvB.

liquefied natural gas, were infiltrated. The virus, called "Shamoon," and possibly a second, known as "Mini-Flame," were re-engineered versions of Stuxnet. It is possible that Iran, or a group acting for Iran going by the name "Cutting Sword of Justice," was behind this cyber attack in retaliation for Qatar and Saudi Arabia's support for the Free Syrian Army. Cyber methods provide the perfect cover for Syria and Iran, as they are easily deniable. The attack itself can be launched from anywhere. However, these incidents affect the global oil supply, and therefore all of the economies within NATO.

Managing Unforeseen Challenges

How asymmetric challenges are managed is of crucial importance to our critical energy infrastructure; indeed, it is becoming ever more important. Of particular concern are emergencies that cannot be planned for – the famous "unknown unknowns," in Donald Rumsfeld's parlance. They will increase over coming years. The Australian government produced very useful research into how such events can be managed. Their Critical Infrastructure Resilience Strategy states:

> 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.[2]

The Australians have summarized NATO's challenge perfectly. What does this mean in practice? The key is developing methods and exercises to enhance surprise-response capacities.[3] Emergency plans to respond to contingencies that can be imagined will always be required. However, in addition to these arrangements for predictable events, "at the ready" institutional capacities must be established to counter catastrophic surprises that could overwhelm our conventional capabilities. In other words, NATO must prepare itself to deal with emergencies that cannot possibly be foreseen.

With this matter of resilient behavior in mind, I will now turn to the issue of how NATO is making progress on this important issue. NATO's currently developing policies on critical infrastructure protection largely took shape in the wake of 9/11. Just a week after the terrorist attacks on New York and Washington, NATO defense ministers asked for a military concept for defense against terrorism. The concept was formally adopted at the 2002 Prague Summit. It enables NATO to take the lead in providing support to counterterrorism and anti-terrorism efforts, including sharing intelligence and

---

[2] Australian Government, *Critical Infrastructure Resilience Strategy* (Canberra: Commonwealth of Australia, 2010), 5; available at www.tisn.gov.au/Documents/Australian+Government+s+Critical+Infrastructure+Resilience+Strategy.pdf.

[3] For further information, see Arjen Boin and Allan McConnell, "Preparing for Critical Infrastructure Breakdowns – The Limits of Crisis Management and the Need for Resilience"; and T. R. LaPorte, "Critical Infrastructure in the Face of a Predatory Future—Preparing for Untoward Surprise," both articles in *Journal of Contingencies and Crisis Management* 15:1 (February 2007): 173–80 and 60–64.

lessons learned; an emphasis on deterring attacks to prevent dealing with the aftermath of attacks; and providing assistance to civilian authorities, so that the actions of emergency services—and increasingly operators of critical infrastructure—will become more coordinated.

At the NATO Summit in Lisbon in 2010, the Alliance adopted the New Strategic Concept (NSC). The NSC highlights the protection of critical infrastructure from cyber attacks and the importance of energy security. A new, more integrated Counterterrorism and Anti-terrorism Policy was agreed at the May 2012 Summit in Chicago. Critical infrastructure protection is now a key part of this policy. Moreover, the 2002 Military Concept for the Defense Against Terrorism will need to be reviewed in light of the new policy.

In addition to these changes, NATO has established on-the-ground implementation of resources that bear on critical infrastructure protection. The Center of Excellence—Defense Against Terrorism in Ankara and the International Security Assistance Force (ISAF) are clear examples. Other examples include Operation Active Endeavour, NATO's developing cyber protection measures, work to counter improvised explosive devices, energy security (note the recent establishment of the Center of Excellence—Energy Security in Vilnius), and the Euro-Atlantic Disaster Response Coordination Centre (EADRCC). Of particular relevance to critical infrastructure protection is the Terrorism Threat Intelligence Unit (now integrated and fully part of the Emerging Security Challenges Division at NATO headquarters), which is specifically intended to help share knowledge and information.

The Defense Against Terrorism Program (DAT) began in 2004 to add more structure to these efforts. DAT was approved at the Istanbul Summit, and was of particular relevance to critical infrastructure protection, as critical infrastructure is one of the program's ten key areas of work. The DAT Program is now a key part of the Emerging Security Challenges Division at NATO.

Just as important as how the Alliance handles asymmetric emergencies is its ability to avoid such situations in the first place. This is the ability to identify a problem when it is a minor issue and deal with it early, before it becomes a major issue. This requires changing NATO's working culture. An example: in 2011 some employees at Norway's Statoil noticed some strange emails. They immediately voiced their concerns. Statoil reported the emails to NorCERT, the Norwegian security authority. NorCERT discovered well-hidden viruses that could have affected oil and gas production. The problem was effectively dealt with early on, well before it became a serious issue. Why was this? The most important part of this story was the excellent immediate action taken by Statoil's staff when they suspected a problem. The investigation aimed to discover what was causing the problem, rather than who had made an error or who was to blame in the company. In other words, a "no-blame" working culture encourages the early identification of problems. Unfortunately, such a no-blame working culture is very unusual in the countries of the NATO Alliance. Most operators of critical infrastructure do not encourage the early identification of problems, despite their claims to the contrary. Indeed, this is not surprising. Operators of critical infrastructure elements, and especially critical en-

ergy infrastructure, are regulated and operate under a license administered by the country in which they operate. The operators are terrified, quite literally, of losing their license to operate. Therefore, problems are very often swept under the rug as the operator is extremely worried that their national regulator will become aware of the problems they have encountered. The "no-blame" culture, which is at its best in Norway, needs to be copied across NATO – not only within the operating companies, but also in the relationship between the operator and the national regulator.

Operators of critical energy infrastructure, and their national regulators, need to change their thinking about security, especially cyber security. This does not happen quickly, especially in hierarchical organizations. This is not a technical issue – it is a management and organizational issue. Doing this will help achieve what I call "pushing threats away," or identifying threats long before they become major issues. Connected to this is the matter of effective knowledge management across hierarchies and divisions, and between competing companies. A knowledge-sharing culture able to identify threats early on is vital. The U.S. 9/11 Commission's inquiry highlighted the "human—or systemic—resistance to sharing information."[4] It identified the problems of "compartmentalizing" information, basing access on a "need to know" basis. The Commission found that systems for information sharing should be decentralized and network based.[5] Its recommendations can apply to very different situations, such as that in Fukushima. Indeed, the International Atomic Energy Agency reported that inadequate information and compartmentalized decision making contributed to the accident.[6] There is a significant similarity between the lessons learned about information sharing in the 9/11 inquiry and what we need to do to protect our energy infrastructure from emerging threats.

It is crucial that knowledge is managed in such a way that lessons are learned and new ways of thinking and adapting can be followed. Knowledge needs to be shared across companies and NATO Allies. Indeed, knowledge management and continual learning is key to reconstruction and recovery.

Conclusion

Threats to NATO's critical energy infrastructure will evolve and change over the coming years. The next event will not be like the last. Like the "Dambusters" raid of seventy years ago, challenges to our critical energy infrastructure will be increasingly innovative. Resilience is vital, requiring new ways of dealing with challenges. These new methods require operators to prepare to deal with unusual events that cannot necessarily be spe-

---

4 National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report* (Washington, D.C.: Government Printing Office, 2004); available at http://govinfo.library.unt.edu/911/report/index.htm.

5 Chapter 13, "How to Do It? A Different Way of Organizing the Government," in *The 9/11 Commission Report*.

6 See Conclusion 6, IAEA *Mission Report: The Great East Japan Earthquake Expert Mission* (Vienna: IAEA, 16 June 2011), 51; available at http://www-pub.iaea.org/mtcd/meetings/pdfplus/2011/cn200/documentation/cn200_final-fukushima-mission_report.pdf.

cifically planned for. Resilience also requires new methods to avoid these challenges in the first place. It is imperative that problems and challenges are dealt with when they are minor, before they become serious. Doing this requires changing how we evaluate challenges, and above all, how we work within organizations and companies that manage our critical energy infrastructure.

Bibliography

Boin, Arjen, 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, no. 1 (2007): 173-80.

Government, Australian. *Critical Infrastructure Resilience Strategy*. Canberra: Commonwealth of Australia, 2010.

IAEA Mission Report: The Great East Japan Earthquake Expert Mission. Vienna: IAEA, 2011.

LaPorte, T. R.. "Critical Infrastructure in the Face of a Predatory Future—Preparing for Untoward Surprise." *Journal of Contingencies and Crisis Management* 15, no. 1 (2007): 60-64.

Menn, Joseph. "U.S. Power Plants Vulnerable to Cyberattack." *Financial Times* (2011).

States, National Commission. *The 9/11 Commission Report*. Washington, D.C.: Government Printing Office, 2004.