CYBER TERRORISM AND ENERGY SECURITY

A growing threat imperils entire regions

By **Ayhan Gücüyener**, research fellow, NATO Energy Security Centre of Excellence

Imagine being a member of a terrorist organization and wanting to create chaos and fear, but keep your anonymity. A sophisticated cyber weapon and a large power outage would definitely serve the purpose. But, in fact, that scenario doesn't have to be imagined — it already happened.

The website SecurityWeek reported in December 2017 the discovery of a malware variant specifically designed to attack industrial safety systems; it was apparently used to cause an operational outage at a critical infrastructure facility in the Middle East. A state-sponsored actor is suspected of being responsible. Fortunately, SecurityWeek reported, operators safely shut down the plant before any damage could be done.

Despite various doomsday scenarios or popular cyber war theories, if you ask people to define cyber terrorism you can expect various answers. There is neither a consensus nor an international agreement that explains and defines cyber terrorism. In fact, the roots of the concept of cyber terrorism and "electronic Pearl Harbor" theories can be traced to the early 1990s and the boom in internet use with the emergence of the "information society." Despite the gloomy predictions and disaster scenarios, no devastating attack has been recorded.

Still, experts agree that cyber terrorism is not just a theoretical threat today and that it could have a disastrous impact on a targeted nation. But how real is the threat? How much should society and the government worry? In such a context, an overreliance on computers and information systems in every aspect of our lives — banking, e-commerce, business, air travel, law enforcement, etc. — leaves those systems increasingly vulnerable to the threat, and more interconnectivity will spawn even more sophisticated threats.

Because modern societies and economies are highly dependent on the uninterrupted flow of energy, the cyber terrorism threat to critical energy infrastructures deserves a comprehensive assessment. This article explores potential threats against the critical energy infrastructures serving the Middle East and North Africa region.

ENERGY SECURITY AND CYBER TERRORISM

In this era of the internet of things, everything is more interconnected and interdependent. It is estimated that about 1,000 devices were connected to the internet in

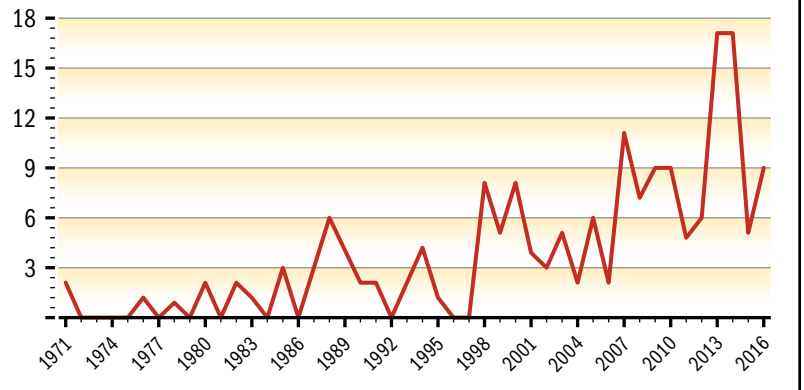
1984; in 2012, about 17 billion devices were connected. Further, technology research firm Gartner Inc. predicts that between 26 billion and 50 billion devices will be connected by 2020.

Among all public and private sectors, perhaps energy is undergoing the most rapid digitalization process. According to the research organization Bloomberg New Energy Finance, digitalization in the energy sector could become a $64 billion market by 2025. Beyond these tremendous investments, it is clear that the digital transformation of energy systems — including smart meters, energy management systems, automated demand responses and smart grids — gives people access to reliable and affordable energy. However, each digital system has its own vulnerability. As an example, the Stuxnet virus was evidently designed and deployed to attack Iran's nuclear power plant in Bushehr in 2010, though no serious damage was reported.

ENERGY IN IRREGULAR WARFARE

Energy infrastructures have long been attractive targets for terrorist groups. In recent decades, terrorists have shown an interest in targeting oil and gas facilities with two main purposes in mind: Undermine the stability of the regimes they are fighting, and economically weaken foreign powers with vested interests in the region. Because of their vulnerability to physical attacks, energy pipelines are considered soft targets that offer strategic advantages for terrorists.

TERRORISM INCIDENTS TARGETING ENERGY INFRASTRUCTURES OVER TIME



Source: Global Terrorism Database, Maryland University

However, as observed during the December 2015 cyber attack on the Ukraine that resulted in an almost nationwide blackout, defending against physical attacks remains a limited and insufficient approach. Cyber attacks can negatively impact daily life and cause lasting damage. They can cause significant damage to the energy company's finances and to the targeted country's economy.

The number of cyber incidents targeting energy infrastructure has significantly increased in recent years. According to the U.S. National Security Agency, 41 percent of cyber attacks target energy enterprises, particularly oil and gas. With respect to the growing and sophisticated threat landscape worldwide, greater efforts are being made by policymakers and regulators to combat the attacks. For instance, the U.S. recently created an office dedicated to protecting energy infrastructure, the Office of Cybersecurity, Energy Security, and Emergency Response. Furthermore, according to the U.S. Cyber Emergency Response Team, the energy, government facilities, transportation systems and wastewater sectors are assessed for cyber safety more frequently than other sectors, accounting for 75 percent of all assessments.

VULNERABILITY OF CONTROL SYSTEMS

Traditionally, companies operating in the critical services sectors (energy, finance, health) have been concerned about protecting their critical and confidential business/customer data or defending against cyber espionage activities. However, another crucial point has been ignored for too long: the security of industrial control systems (ICS). These systems are an integral part of power, oil, water and transportation systems, providing control over the safe shutdowns of these facilities. The best-known ICS systems are: DCS (distributed control systems), PLC (programmable logic controller) and SCADA (supervisory control and data acquisition).

They monitor and control physical processes in real time. However, they were not designed with security in mind, and the consequences could be catastrophic if a terrorist group gained control of the system; they could control and command the system, threatening regional and national security.

Experts are alerting the energy industry and governments of the significant difference between the security philosophies of general information technology (IT) and ICS security frameworks. While, generally speaking, IT officers are trying to defend data residing in their servers from cyber attacks, the purpose of ICS security is to protect the facility's ability to operate in a safe and secure environment. Moreover, the systems have different designs and are operated by different teams and professionals from different backgrounds. Despite the progressive improvements in IT security, there are few ICS-specific cyber security technologies, training programs and policies.

CYBER TERRORISM AND ENERGY INFRASTRUCTURES

The emerging literature on defining and regulating cyber terrorism mostly assumes that the vulnerability of computer networks and the vulnerabilities of critical

infrastructures are the same, putting national security at significant risk, according to a report by James A. Lewis published by the Center for Strategic and International Studies.

The context should be taken into consideration when making a differentiation between cyber terrorism and cyber crime, though similar techniques, tactics and procedures could be used by attackers. Some experts argue that terrorism should be discussed only when physical damage is caused and the perpetrators are motivated by politics or ideology. Nevertheless, there are differing nuances and variations on this concept because a one-size-fits-all approach cannot fully cover all the scenarios considered under the umbrella of cyber terrorism.

The United Nations Office on Drugs and Crime describes three major ways that terrorists can make use of computer systems: indirect support of a group, operational support of terrorist activities, and targeting systems for destruction and disruption. In such scenarios, targeting any energy infrastructure for disruption or destruction by cyber weapons would have devastating effects.

Two important questions come to the forefront when cyber warfare and cyber terrorism scenarios are discussed. In the near future, should we expect an act of cyber terror against national critical infrastructures? And is it possible to assess the risk of cyber terrorism? Experts have diverging and mostly pessimistic opinions for the near future.

Finally, the "Global Terrorism Index 2017," released by the Institute for Economics and Peace, found that terrorism "is offering terrorist groups greater strategic and operational freedom and new types of 'leaderless attacks.'… In the future, sophisticated forms of technology, the IoT (internet of things) self-driving cars and smart cities will create even greater cyber vulnerabilities that terrorists can exploit." Based on these statements and given the abundance of realistic scenarios, it is reasonable to predict that energy infrastructures could be targeted by cyber weapons in a politically or ideologically motivated way with the aim of causing massive physical damage.

But how can the cyber terrorism risks be assessed to take the proper counter measures? At the assessment point, a risk management framework developed by the Rand Corp. can help to define the risk based on the interaction of three variables: Threat, vulnerability and consequences as it relates to risk. Even within that framework, it remains difficult to assess with certainty the risks posed by cyber terrorism, especially for those risks associated with energy infrastructures. Even though terrorist groups today are limited to launching simple cyber attacks and exploiting existing vulnerabilities, future cyber terrorism may manifest itself by applying offensive tactics to damage ICS and spread fear, which could threaten the integrity of critical energy infrastructures, undermine the public's faith in government and in

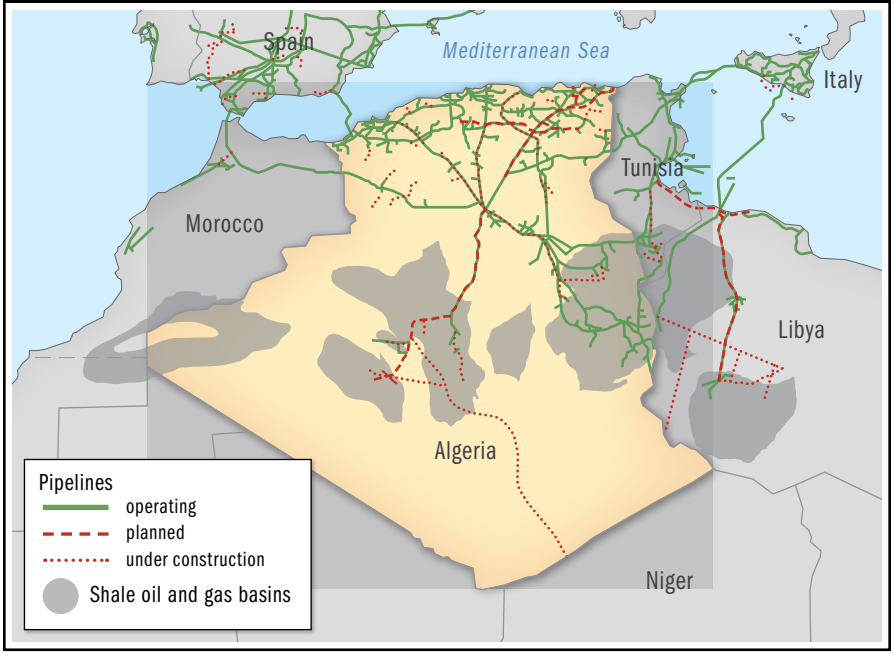
Algerian soldiers guard a gas plant in Amenas, Algeria, after an attack by militants in 2013. THE ASSOCIATED PRESS

the security of the nation's critical infrastructure, according to *Infosecurity* magazine.

REGIONAL ENERGY SECURITY

Considering the interdependent nature of critical energy infrastructures (other than nuclear) — pipelines, distribution/transmission lines and production facilities — the threat gains an international character that might require regional cooperation and a simultaneous response.

PIPELINE ROUTES FROM ALGERIA TO SPAIN AND ITALY



Source: Energy Intelligence Agency

With cross-border electrical transmission lines, oil and natural gas pipelines passing across borders into neighboring countries and operated by numerous companies, a well-targeted cyber attack could affect many countries and actors. In such a case, a country that doesn't have domestic energy resources would concern itself with securing and sustaining its energy supplies (for meeting domestic demand) in contrast with a country that holds energy reserves and would fear a loss of profits and credibility in its investors' and customers' eyes.

The Middle East and North Africa region is particularly crucial to the world economy because of the large volumes of oil and gas that flow from and through it. A major concern is that the region still suffers from traditional terrorism acts. For instance, the high-profile terror attack in 2013 against a gas production facility near Amenas, Algeria, resulted in the loss of lives and a disruption in production.

The same scenario could be projected for a successful cyber attack that could damage a country's energy production and threaten the supply for consumers across the region. In fact, even though officials claimed the 2012 Shamoon virus attack against Saudi Aramco in Saudi Arabia did not affect its production capacity — oil production is controlled through a different network and the attack did not target ICS systems — it forced the company to shut down its internal network for more than a week.

What would be the consequences of a cyber terrorism incident that targeted regional pipelines? For example, an attack affecting the pipeline routes from a producer country such as Algeria to energy consuming countries such as Spain and Italy would threaten the four A's of energy security: accessibility, availability, affordability and acceptability. In other words, such a large-scale and well-planned attack would disrupt regional energy security and affect oil or gas supplies for both producer and consumer.

Cyber terrorism could also undermine a country's investor-friendly environment and damage its reputation as a safe and reliable trade partner. In addition, such attacks would carry diplomatic, economic and social costs. Also, there is no doubt that operating in a high-risk environment creates discouraging burdens for private companies.

While traditional cyber weapons such as basic viruses and worms continue to be deployed, the most popular cyber threats being deployed today are advanced persistent threats.

CONCLUSION

Defining a commonly accepted approach to cyber terrorism may be the most important step in countering the threat. In addition to individual efforts by companies and/or states, an international and coordinated response will strengthen multinational investigations, information sharing and monitoring. Finally, as NATO's Cooperative Cyber Defence Centre of Excellence's text states, international counterattack exercises should be held to improve each nation's ability to defeat cyber terrorism. □

Ayhan Gücüyener is a research fellow at the NATO Energy Security Centre of Excellence in Lithuania and regional director of the International Association of Critical Infrastructure Protection Professionals. Her expertise focuses on energy security, strategic cyber security and international politics. She is also a former researcher for the Center on Foreign Policy and Security, a Turkish think tank. She is co-author of the handbook, *Critical Energy Infrastructure Security*, and has been acting regional director of the Industrial Cyber Security Center (CCI) since October 2017.