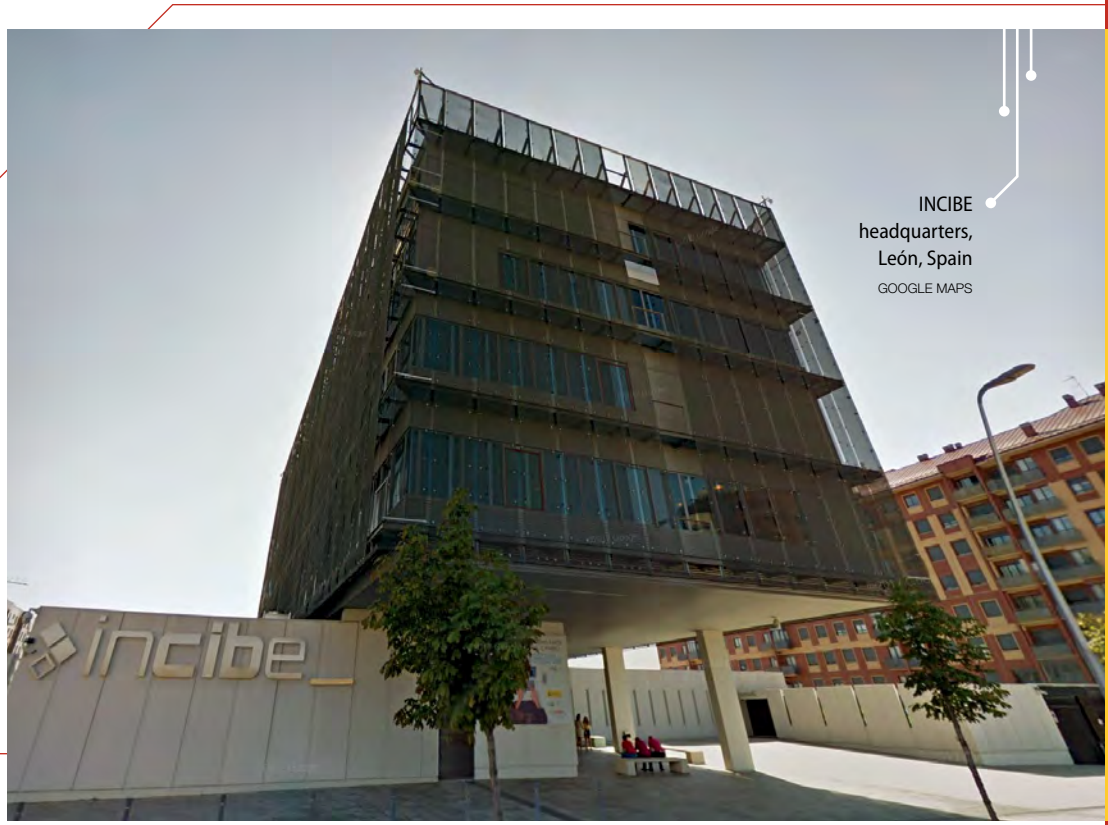
SPAIN'S DIGITAL DEFENSES

Applying Innovative Models to Protect Critical Infrastructure

By **Alberto Hernández**, CEO, National Cybersecurity Institute of Spain (INCIBE)

PER CONCORDIAM ILLUSTRATION



INCIBE headquarters, León, Spain
GOOGLE MAPS

There have been a number of large-scale cyber attacks on critical services and critical infrastructure that have been widely covered in the media. But there have also been attacks with similar impacts that have gone largely unnoticed. These attacks will increase as the connectivity of industrial control systems, communications networks and internet-of-things devices continue to grow. This connectivity has many advantages in operation and management, but introduces new threats related to the internet, or cyberspace, domain. Cyberspace's global scope, low cost of access, anonymity, asymmetry, and its operational time measured in milliseconds are characteristics that hasten the rapid evolution of these new threats.

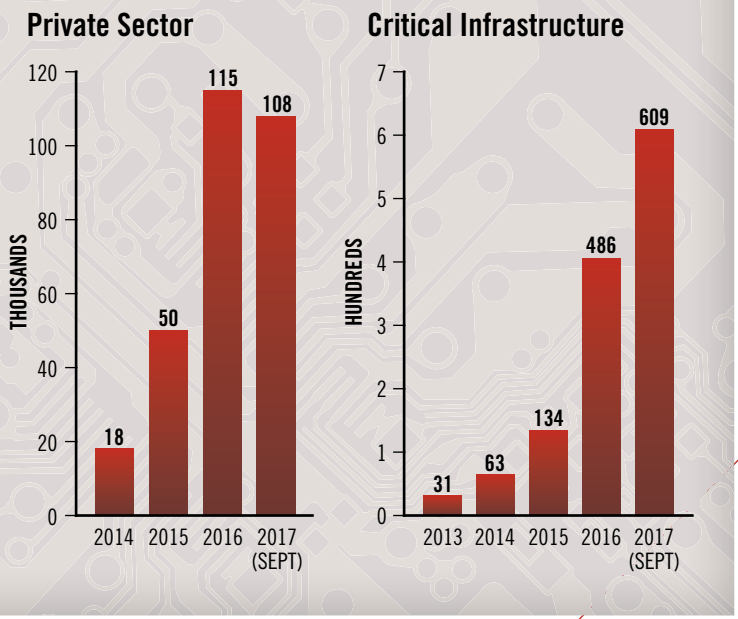
Attacks can vary in impact. In 2000, more than 2 million liters of untreated water was dumped into rivers and parks in Maroochy, Australia, as a result of several remote cyber attacks by a disgruntled worker. In 2008 in Lodz, Poland, four trains were derailed and several people were injured because a 14-year-old turned his television remote control into a device able to change the switch rails of the tracks. In June 2010, Stuxnet was discovered. This was the first known malware designed to spy and reprogram industrial control systems affecting critical infrastructure such as nuclear power plants. More recently, in 2015 in Ukraine, several power outages in the electrical distribution network left 1.5 million people without electricity for several hours. These cyber attacks show that the threats to essential services and critical infrastructure are real and that it is necessary to define and develop strategies to reduce and manage the associated risks.

In Spain, the number of cyber security incidents affecting citizens and the private sector is increasing, from about 18,000 in 2014 to 50,000 in 2015, and from over 115,000 in 2016 to 108,000 through September 2017. Regarding critical infrastructure, the number of incidents has also grown during the past four years, from 31 in 2013 to 63 in 2014, 134 in 2015, 486 in 2016, and to 609 through September 2017. Response to these incidents is managed by the Security and Industry Computer Emergency Readiness Team (CERTSI) operated by the National Cybersecurity Institute of Spain (INCIBE) and the National Centre for Critical Infrastructure Protection (CNPIC). This growth in the number of managed cyber security incidents may be due to three causes: an increase in cyber attacks, the improvement of CERTSI detection capabilities, and greater trust between CERTSI and strategic operators. This is evidence of the need to establish a strategy for critical infrastructure protection that can help organizations improve cyber security.

INCIBE's Strategy

In 2007, the Spanish Ministry of the Interior created CNPIC with the objective of protecting national critical infrastructure, including in the cybernetic domain. With the approval that year of a law protecting critical infrastructure, Spain

CYBER SECURITY INCIDENTS IN SPAIN



Source: CERTSI

established the appropriate strategies and structures to direct and coordinate the actions of the different public agencies involved in protecting critical infrastructure, with cyber security considered a key factor in all sectors.

To facilitate regulatory compliance and implement the most recognized practices for the improvement of cyber security, INCIBE, in collaboration with CNPIC, developed a comprehensive and specific strategy for critical infrastructure covering aspects such as prevention, protection and reaction in the event of a security incident. This strategy includes the following lines of action:

A. **ENSI:** The national cyber security framework is known as the National Scheme on Industrial Security (ENSI). It features common methodologies and tools for improving capabilities, minimizing the risks to which essential services are exposed, and establishing methodologies and measures to mitigate the risks applicable to industrial organizations.

High-voltage power lines are repaired near Slavyansk, Ukraine. In 2015, cyber attacks on the power distribution network left 1.5 million people without electricity.

AFP/GETTY IMAGES

ENSI is composed of a general policy and three units: cyber resilience improvement measures (IMC), a value chain cyber security capability building model (C4V), and lightweight risk management in integral security (ARLI-SI).

- **IMC:** The IMC model defines a set of indicators for improving cyber resilience as an instrument to diagnose and measure the ability to withstand and overcome disasters and disturbances emanating from the digital field.

  The question at this point is not whether an organization and its systems, including those related to essential services, are going to be attacked, but whether it will be sufficiently prepared to resist it, prevent essential services from being interrupted, and be able to recover in the briefest time possible. In short, is the organization cyber resilient?

  In the cyber world, the concept of cyber resilience rests on the need for organizations to be capable and ready to respond quickly to attacks, keeping the services they provide free of interruption while strengthening their capacity to identify, detect, prevent, contain, recover from, and cooperate and continuously improve against cyber threats.

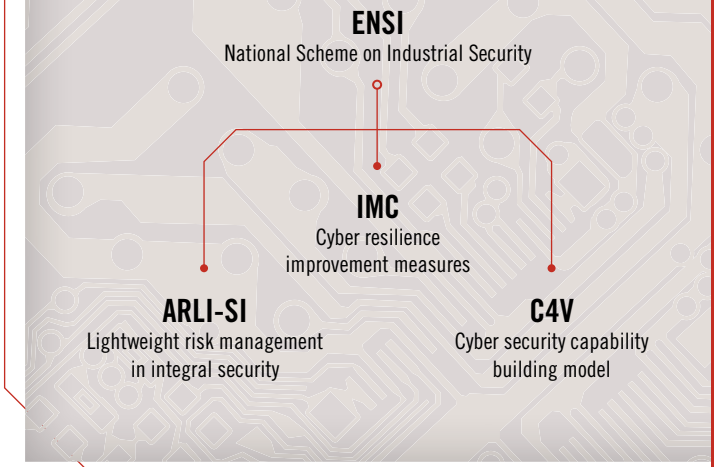
  INCIBE developed this comprehensive framework for measuring an organization's cyber-resilience indicators after conducting an international review of the National Cyber-Security Strategies, which are the main cyber security standards, metrics and indicators. The IMC model includes 46 metrics covering four main goals of cyber resilience: anticipate, resist, recover and evolve.

IMC GOALS

- **ARLI-SI:** The ARLI-SI methodology is a lightweight, risk-management methodology that is intended as a practical and simple risk-assessment model. It is centered on industrial control systems as the starting point and is a cornerstone of the safety improvement process.

  After a normal audit process, critical operators are provided with an initial diagnosis of the security of their systems. However, it is essential that they get additional information about steps needed to improve security and what is considered an adequate cyber security level.

SPAIN'S NATIONAL SECURITY FRAMEWORK



- **C4V:** INCIBE developed the C4V to give operators an understanding of the degree of maturity and robustness of the protection measures implemented in critical infrastructure systems. The C4V pays special attention to the dependence of essential services and to risk management in the information and communication technology supply chain.

  One advantage of this model is that, in cases where third-party service providers affect the capacity level, the organization responsible for the service must establish mechanisms to ensure that such third parties meet capability requirements. The third parties should also have monitoring procedures to ensure that this level is maintained throughout the service life cycle.

B. The Spanish platform for sharing cyber security threats, known as the ICARO system, is a tool to help identify threats. Early alerts are necessary to adequately prevent and respond to cyber attacks. To facilitate information sharing about threats and cyber attacks, INCIBE designed and deployed ICARO, which is based on a malware information sharing platform (MISP) used to share indicators of compromise caused by cyber threats. Using ICARO, Spanish critical operators have a channel that facilitates the anonymization of shared information and access to CERTSI information. This platform also can be federated with other MISPs worldwide.

C. The National Network of Industrial Laboratories (RNLI) is a search platform for information on industrial laboratories with the capacity to experiment and research national industrial infrastructure security solutions. RNLI pursues the dual objectives of promoting innovation in industrial cyber security through collaboration and facilitating the development of solutions that improve the competitiveness of domestic industry.

A tram pulls away from the station in Lodz, Poland. A cyber attack by a teenager caused four trams to derail in 2008.

AFP/GETTY IMAGES

INCIBE is one of the organizers of CyberEx, an annual competition providing different scenarios to test cyber resilience.
INCIBE

EARLY ALERTS ARE NECESSARY TO ADEQUATELY PREVENT AND RESPOND TO CYBER ATTACKS.

RNLI allows operators to find information on national infrastructures and create a point of union between the supply of, and demand for, security in these environments. Other benefits include promoting collaboration and cooperation among all actors involved and facilitating the exchange of expert knowledge within the community.

D. INCIBE collaborates with manufacturers, cyber security companies, laboratories and critical infrastructure operators to develop innovative tools for the improvement of the critical infrastructure's cyber security and CERTSI's detection capabilities.

With these tools, INCIBE and CERTSI can provide new services, such as generating alerts to those operators with vulnerable industrial control devices. Once INCIBE receives an alert from a manufacturer about a specific device, INCIBE identifies those operators that have this type of device and sends them an alert with all of the information required for self-protection.

Other complementary tools allow the detection of industrial control systems that are accessible from the internet, allowing INCIBE to improve its alert services.

E. As the final element of the strategy, national cyber security exercises in Spain allow for the testing and improvement of the cyber security capabilities of critical infrastructure operators. As part of this initiative, named National CyberEx, several exercises have been carried out. After centering on the banking sector in 2015, the 2016 edition was developed to assess and improve several sectors' resilience to attack, giving participants tangible benefits for their security teams' operations.

Across these exercises, involving all professional roles on the operators' teams, participants improve their response capabilities and strengthen coordination between entities.

Conclusions

The global perspective and nature of the challenges of cyber security in critical infrastructure protection require a comprehensive approach, where a variety of actions are necessary. These actions should cover state-of-the-art technology and manufacturers, current regulations, users and the human factor. Vitally, it also requires perfect coordination among all stakeholders along with a continued commitment to innovation and evolution. □