Chapter 5
Critical Infrastructure

Critical infrastructure represents an umbrella term used by governments to group all those resources that are essential for the economic, financial, and social system of a country. The Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience, issued by the President of the United States in 2013, advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure. PPD-21 identifies 16 critical infrastructure sectors: chemical sector; commercial facility sector; communication sector; critical manufacturing sector; dams sector; defense industrial base sector; emergency services sector; energy sector; financial service sector; food and agriculture sector; government facilities sector; health case and public health sector; information technology sector; nuclear reactors, materials, and waste sector; transportation system sector; and water and waste-water system sector [313].

The protection of these resources is crucial, because the destruction (or even the partial or momentary inability) could cause significant harm on the society or, worse, could jeopardize human lives. For example, in desert countries such as Qatar, Saudi Arabia, or the United Arab Emirates, attacking the critical infrastructures essential for the water supply (water desalinization plants) would be tantamount to leaving the entire population without drinking water for the entire duration of the fault. For these reasons, there is great concern among security and government officials about the vulnerabilities of critical infrastructure in their state. The possible threats to critical infrastructures' integrity and functioning are manifold. We can categorize them into three main classes.[1]

- **Natural.** Unpredictable natural disasters, such as earthquakes, floods, volcanic eruptions, hurricanes, and possibly others, can generate serious damage to critical

[1] https://www.securityinfowatch.com/access-identity/access-control/article/12427447/americas-critical-infrastructure-threats-vulnerabilities-and-solutions (Last checked August 2020).

R. Di Pietro et al., *New Dimensions of Information Warfare*, Advances in Information Security 84, https://doi.org/10.1007/978-3-030-60618-3_5

infrastructures. Since such events are normally unpredictable, it is difficult to mitigate the problem. The only countermeasures are to locate infrastructure in areas not subject to such events and to use resilient construction techniques.
- **Human-related.** All man-made events, such as acts of terrorism (explosions, bombing), vandalism (rioting, theft), financial crimes, economic espionage, and possibly others.
- **Accidental or technical.** Events caused by technical errors, such as failures and accidents related to infrastructure and dangerous materials, failures of the power grid, failures of the safety systems, and a series of other catastrophes of omission and/or commission.

According to the Geneva Convention of 1949, It is prohibited to attack, destroy, remove, or render useless objects indispensable to the survival of the civilian population, such as foodstuffs, agricultural areas, crops, livestock, drinking water installations and supplies, and irrigation works, for the specific purpose of denying them for their sustenance value to the civilian population or to the adverse party, whatever the motive, whether in order to starve out the civilians, to cause them to move away, or for any other motive [314]. However, the threat of attacks against these infrastructures remains high, as well as the level of alert by security operators. The malicious actors possibly involved in attacks against critical infrastructures can be identified in six categories, listed below:

1. **Displeased or corrupted employees.** Disgruntled insiders, unqualified employees, and incompetent contractors create the opportunity for outsiders to infiltrate inside the protected environment of critical infrastructure. This category includes unethical employees involved in illegal activities, motivated mostly by earning extra money. They may also be driven by feelings like jealousy, rivalry, or revenge on their superiors or the institutions they work for.
2. **Individual hackers, small groups of hackers, and hacktivists.** People who use their skills, individually or in groups, to support a particular ideology. They could be driven by political views, cultural/religious beliefs, national pride, or even terrorist ideas.
3. **Competing companies.** Companies that work in the same sector that try to steal important information, such as valuable intellectual properties, in order to reuse them on the national/international market.
4. **Cybercriminal organizations.** Criminal organizations that conduct their illegal activities using IT systems. Their only motivation is to make an economic profit.
5. **Terrorists.** Terrorist actions usually arise from multiple causal factors, such as economic, political, religious, and sociological problems, among others.
6. **Foreign governments.** Foreign nations that, driven by different interests, attack the cyber-physical infrastructure of another country.

All these actors, regardless of motivation, have a potential advantage in attacking critical infrastructures. Their goals can be different, ranging from simple demonstration actions to attacks aimed at destroying. Criminal organizations, for example, driven by profit, could take control of a factory's IT system, partially or totally

blocking its production. Then, they can request a ransom to return control to legitimate operators. The main purpose of the terrorists, instead, could be to destroy, disable, or exploit critical infrastructure to threaten national security, causing major casualties, weaken the economy, and reduce public morale and confidence in national institutions.

The list of cyber threats involving critical infrastructures grows exponentially with the increase in hacking-sensitive technologies used within them. The growth of the virtual perimeter attracts more and more malicious actors, whether they are individual, private, or state-sponsored groups. The external exposure of the IT systems used by critical infrastructures is the main threat, as it allows remote attacks carried out without having physical access to the equipment, usually very well protected.

The activities of a critical infrastructure are supported by particular IT systems called Industrial Control System (ICS). These systems are the result of hardware and software integration, capable of controlling and supporting various production activities. ICS technologies include, but are not limited to, Supervisory Control And Data Acquisition (SCADA) systems, Distributed Control Systems (DCS)s, and Programmable Logic Controllers (PLC)s. In several cases, ICS were put into operation decades ago, before the global spread of the Internet. At that time, cybersecurity was not considered of paramount importance, as communication networks were confined to restricted environments and only very few people had access to information. In addition, critical infrastructures were often closed systems, with no connection to the outside world. These types of systems, called air-gapped, make a remote cyberattack very difficult. To control an isolated system, in fact, it is necessary to have some kind of physical access to the target systems. However, the rapid diffusion of new communication technologies, such as Internet of Things (IoT), radically changes this scenario. The convenience of features, like automation and remote control of the key equipment that operates in critical infrastructures, has prevailed over potential security problems, opening new opportunities for malicious actors. In this situation, a modern arms race has developed, with the aim of acquiring techniques, methodologies, and tools that can be used against the IT and ICS systems of rival nations. As a result, cybersecurity has acquired major strategic importance.

🪄 Definitions

Supervisory Control and Data Acquisition (SCADA) It is mainly a software toolkit for implementing ICS. These systems are normally used for remote monitoring and sending commands to valves and switches. For example, they can be found in water facilities and oil pipelines, where they monitor flow rates and pressures. Based on the data provided by these systems, computer programs or the operators of a central control center

(continued)

balance the flow of material using industrial control systems to activate valves and regulators. Normally SCADA systems are used as a means of entering data and exporting commands from a control center. These systems are vulnerable to implantation of faulty data and to remote access via external connections generally used for maintenance.

Distributed Control Systems (DCS) It is a process control system usually deployed in a single production complex. This system generally provides processed information to a control center or supports it in executing commands. A practical example could be identified inside a chemical facility. In this context, a DCS might simultaneously monitor the temperature of a series of reactors and control the rate at which reactants were mixed together. At the same time, it might perform real-time process optimization and reporting the progress of the reaction. An attack targeting DCS might interfere with ongoing production activities, causing extensive damages. However, due to its confined nature, it would be unlikely to affect more than a single infrastructure.

Programmable Logic Controllers (PLCs) They are devices used to automate monitoring and control of industrial plants and are generally used within a manufacturing facility. They tend to provide little external information and do the majority of their data processing internally. Programmable logic controllers can control as little as a single machine to as much as an entire manufacturing facility. An automated assembly line can be comprised of a series of PLCs, with each machine on the assembly line performing a distinct job. An attack targeting PLCs might cause significant turmoil at a single location, but the extent of the damage would depend on both the PLC's size and connectivity.

Air-Gapped System An air-gapped system is an IT system whose components are isolated from unsafe networks.As a result, these systems do not have direct Internet access, and they are not even connected to systems that have it. As a consequence, an air-gapped computer is also physically isolated, which means that data can only enter or leave it using physical media only (for example via USB or other removable media).

In this chapter, we will discuss possible attacks against critical infrastructure related to two major threats in particular: cyberwarfare exploiting vulnerabilities in IT and SCADA systems, especially malware-guided attacks, and a new cyber-physical threat from the sky: commercial drones.

5.1 Scenario: Cyberwarfare Targeting Critical Infrastructures

To better understand the threat of cyberwarfare against critical infrastructures, its different facets, and its potential consequences, it is necessary to know the modern architecture of these structures and the systems that govern them. The ICSs that support the operations of a critical infrastructure are composed of integrated hardware and software resources, interconnected with each other. These systems usually manage the production processes of essential services that underpin modern society and act as the backbone of every nation's economy, safety, and health. These facilities, among other things, produce and transport drinking water and electricity to citizens' homes, supply stores with primary goods, and offer means of transport and communication. To make an example, we can cite the production and distribution of essential goods such as drinking water and electricity, the management of airport facilities, critical manufacturing, and possibly others. Any malfunctioning of the ICSs that manage these infrastructures could lead to serious consequences ranging from slowing down production to a partial or total plant shutdown.

In the context of cyberwarfare, critical infrastructures are very sensitive targets because of the key role they play within a nation. For this reason, critical infrastructures are usually well defended, both physically and virtually, because they are expected to be among the first targets of a possible attack. In this context, the biggest concern is the intrusion, both physical and virtual, of malicious users aimed at interfering with normal operations or exfiltrating sensitive data. Before the spread of the Internet, the defense of critical infrastructures was mainly focused on the physical perimeter. Information systems were often not connected to the outside world. Consequently, the virtual perimeter was nonexistent or very small, which made the likelihood of suffering a cyberattack very low. The advent of new communication technologies has favored the emergence of new network paradigms, such as the Internet of Things, which have pushed the digitalization of production processes. This radical change has created a virtual perimeter that must be defended as, and more than, the physical one.

The defense of the physical perimeter is a need born together with critical infrastructures and is, therefore, a well-known and well-studied problem. On the contrary, the defense of the virtual perimeter is a relatively new need, exacerbated in the last decade following the advent of new communication technologies. The ICS infrastructures are usually composed of a large number of heterogeneous devices developed by different suppliers and often equipped with proprietary software. The lack of homogeneity and standardization considerably increases the costs of research, design, and implementation of cyber defense products and techniques. Furthermore, the privatization and market liberalization policies implemented worldwide in the last period have made the protection of critical infrastructures more difficult for the government. Taking the United States as a reference, the number of critical infrastructures owned and managed by the private sector is around 85%,

according to a report edited by the Department of Homeland Security in 2009.[2] With the private sector so heavily involved, expensive security measures must inevitably run up against several economic considerations. In this scenario, security alone is never a decisive factor, since it must always be considered in relation to the available budget. This situation introduces two critical vulnerabilities: resource disparity and outsourcing complexity.

Cyber and physical security is an expensive task that requires the allocation of significant resources. Resource disparity between private companies of different sizes implies the possibility of coping with security payments in a different way. This could cause under-protection of critical infrastructures managed by small-medium companies, which will, therefore, be more exposed. Modern companies tend to focus on core business processes, outsourcing everything else to third-party organizations. For this reason, very often physical and cybersecurity are also outsourced, making optimized protection more complex and creating opportunities for malicious users.

The general architecture of the ICS systems, shown in Fig. 5.1, consists of several levels, listed below from the outermost to the innermost, representing the attack surface of a critical infrastructure:

- **External Systems.** This category contains all those systems that are not directly part of the ICS network but are used to interact with it. The corporate network is directly connected to Tier 2, while among the indirectly connected systems, it is worth to mention portable devices, such as USB storage, external users, and, more in general, the Internet.
- **TIER 2.** This level contains those systems which are directly part of the ICS network and are positioned in the outermost layer. Examples include all outward-facing applications that link resources or provide data to external users, such as information servers, historians, or generic web servers.
- **TIER 1.** This layer, also called the supervisory level, is the SCADA network layer. TIER 1 includes all the hardware and software components used to configure, monitor, and control the devices in TIER 0 while feeding data to the upper layers. Typical examples of systems belonging to TIER 1 include HMI, engineering workstations, and application servers.
- **TIER 0.** This category, also known as "production network layer," represents the innermost layer of the ICS architecture and the closest to the physical world. TIER 0 includes all the input/output end-devices, such as sensors, RTUs, and other physical devices that collect data, other systems that directly control physical equipment, such as PLCs, and general Wi-Fi and radio frequency networks.

Any device deployed in the three internal layers (i.e., TIER 0, 1, and 2), may become a potential target in case of attack. In case these devices were directly accessible from the outside, they would increase the attack surface exposed by the infrastructure to the outside world. As shown in Fig. 5.1, the propagation

[2] https://www.gao.gov/new.items/d09654r.pdf (Last checked August 2020).

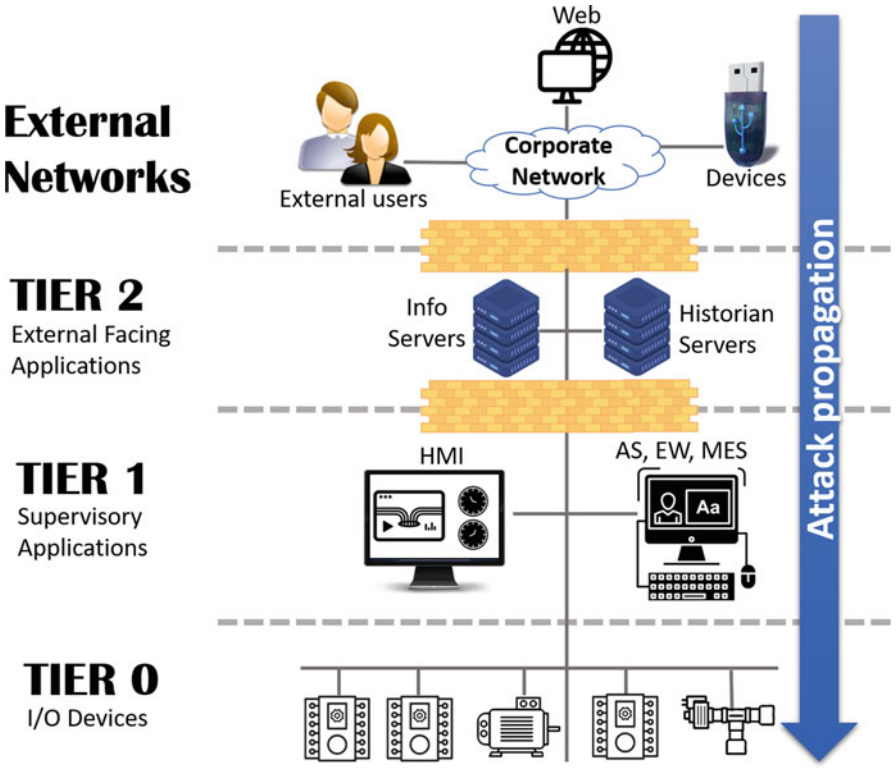

Fig. 5.1 Industrial control systems' common multitier security architecture

of a cyberattack in the ICS architecture occurs from top to bottom, i.e., from external systems to the TIER 0 devices. This is justified by the fact that, in the classic model, each device is reachable only from the layer immediately above. Consequently, the only devices directly accessible from the outside are those belonging to TIER 2. However, the attack surface has dramatically increased with the advent of new network paradigms, such as IoT and cloud computing, which have been integrated into industrial environments. In light of these new technologies, the general architecture of an ICS can be modified according to the specific use cases involved. In some scenarios, both TIER 1 and TIER 0 layers of the ICS architecture could be directly reachable from the Internet, introducing severe security threats. Any digital device operating within a critical infrastructure can be exploited by a mischievous user in different ways. While hardware devices can be physically destroyed, malicious programs can be created to alter the behavior of the software resources. Simple software errors or carefree third-party software executions can lead to external threats, causing the temporary (or definitive) malfunction of the control software, thus leading to the compromise of the protected critical resource. Even worse, instead of causing the control system to be altered or destroyed, an

attacker could take control of it from the outside, deceiving security systems and tampering with the critical resource without triggering security alarms.

This scenario takes into account a critical infrastructure located within a country, which manages a critical resource. The critical infrastructure can be either a complex set of interconnected electrical components, as in the past, or a set of modern IoT communicating devices. In both cases, the critical infrastructure exposes interfaces on the web to receive commands remotely and to show the status of the managed resources. The exposure to the web is necessary, to reduce the amount of dedicated personnel and to real-time monitoring the status of the critical resource from centralized control centers. At the same time, however, exposure to the web could lead to an increase of the attack surface, opening the doors to different attacks such as malware-based attacks and attacks on the SCADA systems, a subset of the ICS widespread in critical infrastructures.

5.1.1 Threat: Malware

In recent years, several security incidents have demonstrated how concrete and potentially destructive the threat of an attack on critical infrastructure can be. Various types of malicious code have been used in these attacks, showing a trend toward the creation of specialized malware targeting ICSs, at least in the past decade. Looking at the examples of attacks that actually took place against critical infrastructures, we can identify two different cases:

- **Specialized malware.** A malware specialized in attacking a particular hardware/software infrastructure, generally a SCADA component, with the specific objective of interfering with its functionality. To design and implement this type of malware, the attacker needs extensive knowledge of the targeted systems. For this reason, this type of malware is usually developed by a highly specialized adversary with access to sensitive information. One of the most famous historical examples of this category of malware is *Stuxnet*, a malware which first appeared in 2010. The *Stuxnet* worm was designed to destroy the motors used in uranium enrichment centrifuges, causing them to spin out of control. Originally used to attack an Iranian nuclear plant, this malware has temporarily disabled around 1000 centrifuges.
- **Generic malware.** A malware designed to hit a generic platform, usually a particular operating system, on a large scale. A malware of this type is normally designed to target as many systems as possible, regardless of their owners and their use, to maximize the creator's profits. These types of malware could attack systems of critical infrastructures even unintentionally. An example of such malware is a ransomware called *WannaCry*, distributed on a large scale by an unidentified group of hackers in May 2017. Once a host is infected, *WannaCry* encrypts all the files inside and locks the system, showing a message with instructions for paying a ransom. Thanks to its ability to infect other hosts on the

same network, the spread was very fast and efficient, also affecting high-profile systems. Among them, the British national health system has recorded numerous infections which, among other things, have caused the partial blocking of several hospitals across the United Kingdom.

Several attack vectors contribute to the spread of malware within critical infrastructures, ranging from software vulnerabilities to human errors. The most common attack vectors for critical infrastructure fall into the following categories:

- **Unpatched vulnerabilities.** An attacker could gain unauthorized privileges by exploiting known vulnerabilities that have not been fixed by security administrators of critical infrastructures yet.
- **Zero-day vulnerabilities.** An attacker could exploit unknown vulnerabilities in both applications and operating systems to get unauthorized privileges, at least since reliable security patches are released.
- **Code injection.** When an application developer does not properly manage the handling of invalid or unexpected input, an attacker could take control of the software execution. In such cases, the introduction of malicious code into the vulnerable application may be possible. Such malicious code would be executed with the same privileges as the victim's application.
- **Social engineering.** A term that refers to all the techniques aimed at obtaining information from an individual and, more generally, to make a person do what he would not otherwise do.
- **Phishing.** Phishing is a particular social engineering technique that aims to obtain sensitive information, such as login credentials. Generally, the attacker impersonates an organization that the victim trusts, such as a bank or government institution, asking for personal data with the most varied reasons. Phishing is one of the most common attack vectors.
- **Misconfiguration.** When there are errors in the configuration of a device or software, such as enabled setup pages, an attacker can obtain information on hidden weaknesses or access systems without authorization.
- **Weak or stolen credential.** The use of weak passwords, i.e., easily guessable through brute force or dictionary attack, as well as the reuse of the same credentials on multiple systems, facilitates the entry and propagation of malware within a protected environment.

Definitions

Attack Vector The method or process followed by an adversary to violate or infiltrate a network/system. Attack vectors allow malicious actors to exploit system vulnerabilities, including the human element.

Among the many countermeasures that can be used to mitigate the attack vectors discussed above, it is worth mentioning some common best practices, valid for any ICT system.

Definitions

Malware The term malware, a contraction of the two words MALicious and softWARE, refers to any piece of software created to run in a system, without authorization, with the intent of stealing data, damaging the system, or generally causing any other harm.

In the literature, malware have been classified in several ways, the two most common are listed in the following:

1. By how the malware infects its victim:
   - **Virus.** A malicious piece of code, unable to work on its own, which must be inserted into a legitimate program. Once infected, the legitimate software is forced to behave maliciously and spread the virus on other software.
   - **Worm.** A standalone malicious code, which reproduces itself via the network.
   - **Trojan.** A malicious code inserted inside an apparently harmless program. Once the user execute such program, the malicious code will be activated, together with its harmful functions.
2. By its behavior on the infected host:
   - **Spyware.** A malware designed to remain silent on the infected computer for the sole purpose of collecting and exfiltrating information from a third party.
   - **Rootkit.** A collection of software used to obtain and maintain unauthorized access to a computer system. Also, this type of malware is able to mask its presence as well as the presence of other malware.
   - **Adware.** A malware that redirects the victim's browser to unwanted advertising or other potentially malicious web content.
   - **Ransomware.** A malware that encrypts all the files contained in the file on the infected host. The victim system is then blocked, displaying a screen with instructions for paying a ransom.
   - **Cryptojacking.** is a malware that uses the resources of the infected system to mine cryptocurrencies without the permission of the system owner.

Proper account management, for example, is certainly a good defense against the problem of weak or stolen credentials. Reducing or banning shared accounts

and password reuse, as well as using advanced techniques such as two-factor authentication, would reduce the attacker's ability to propagate his malicious code within the target system. This simple countermeasure prevents attackers from violating multiple systems with a single stolen credential.

Very often, an attack starts with the exploitation of a known vulnerability, already fixed by the vendors but not yet applied in the system under attack. For this reason, the timely installation of security patches plays a fundamental role in reducing the probability of being attacked by exploiting unpatched vulnerabilities. Furthermore, vulnerability assessments and penetration tests must also be conducted regularly to test deployed defenses and identify any vulnerabilities due to both misconfigurations and zero-day vulnerabilities.

A simple best practice for mitigating the threat coming from social engineering techniques, such as phishing, consists of maintaining security awareness. Knowledgeable employees well trained in cybersecurity threats, in fact, would reduce the risk of opening security breaches due to the human factor, significantly limiting the probability of being attacked. Even if it is not possible to eliminate all possible attack vectors, strict compliance with these guidelines would significantly reduce the attack opportunities available to malicious actors, reinforcing the security perimeter.

In this section, we analyze the threat posed by malware to critical infrastructures. Starting from the most significant examples of attacks that took place in the past, we analyze the effectiveness of the countermeasures currently available to identify the weak points that still persist.

5.1.2 Attacks and Countermeasures

On Friday, May 12, 2017, the *WannaCry* ransomware was detected in several hospitals in the United Kingdom. Some time after, it exploded across the globe, spreading like wildfire, encrypting hundreds of thousands of computers distributed in more than 150 countries in a matter of hours (see Fig. 5.2). The attack affected a wide range of sectors, including health, government, oil and gas production, and telecommunications, in what was later recognized as the biggest ransomware campaign in the history of the Internet. The WannaCry ransomware sets foot on the infected computer in the form of a dropper, which includes the following components:

- An application that encrypts files (i.e., the encrypter)
- An application to decrypt files after a ransom has been paid (i.e., the decrypter)
- A zip file containing a copy of the Tor client
- Several individual files with (hard-coded) encryption keys and configuration information

Fig. 5.2 The spread of the WannaCry malware across the globe in the early days of infection, according to @MalwareTechBlog

Definitions

Dropper A dropper is a vector used as a vehicle to introduce an application, called dropper payload and usually harmful, into another system. If the malicious application is contained in the dropper body in the form of a compressed file (e.g., to avoid being identified by antiviruses), the dropper is called single-stage. If the malicious payload is downloaded from the Internet after activation, the dropper is called two-stage.

The program code of WannaCry is not obfuscated and was relatively easy to analyze by security experts. Once the dropper runs on the victim computer, it extracts the malware components into its working directory. Then, it checks for other malicious programs and the existence of a particular hard-coded URL. If both checks fail, the malware starts the encrypter application. This software starts to encrypt all the files on the disk with common (hard-coded) extensions. Finally, the WannaCry encrypter launches the embedded decrypter, which displays two timers and instructions for sending the ransom. The instructions demand a payment of 300 US dollars worth of bitcoins to a specified (hard-coded) address. If the ransom is not paid before the first timer expires, the ransom price doubles. After the second timer expires, the malware states that the files will be unrecoverable. Since the malware uses the Microsoft Enhanced RSA and AES Cryptographic Provider libraries to perform the encryption, the encrypted files are unrecoverable without the decryption key (Fig. 5.2).[3]

[3] https://logrhythm.com/blog/a-technical-analysis-of-wannacry-ransomware/ (Last checked August 2020).

According to a report by the Department of Health, the WannaCry campaign was devastating for the United Kingdom National Health Service (NHS). Several computers with strategic roles have been blocked by the malware in many hospitals, causing a total loss of about 92 million GBP. Staff from the affected hospitals were forced to return to pen and paper and use their cell phones after the attack hit key systems, including phones. Hospitals and medical clinics in several parts of England were forced to turn patients away and cancel appointments after the infection. People in the affected areas were advised to seek medical assistance only in case of emergency. The hack caused more than 19,000 appointments to be canceled, costing the NHS 20 million GBP between May 12 and May 19, and 72 million GBP in the subsequent cleanup and upgrades to its IT systems.[4] One of the most interesting aspects of WannaCry is the attack vector. In the first phase, it is often delivered via phishing, i.e., sending emails that induce the recipient to open attachments and release malware on their system. Hence, the worm component of the malware spread quickly through the victims' local network using unpatched vulnerabilities. The exploited weakness lies in the Windows implementation of the Server Message Block (SMB), a network protocol that provides shared access to files, printers, and serial ports between nodes on a network. The protocol version developed by Microsoft could be tricked by specifically crafted network packets into arbitrary code execution (vulnerability CVE-2017-0144). This vulnerability is believed to be discovered by the NSA which, instead of reporting it to the IT security community, developed an exploit called EternalBlue. Subsequently, a hacking group, known as the "Shadow Brokers," claimed to have stolen this exploit from the NSA and published an obfuscated version in April 2017. Microsoft discovered the vulnerability and released the corresponding patch a month earlier, but many systems have not been updated.

The rapid spread of WannaCry was stopped by chance by a young British security researcher, Marcus Hutchins, who discovered how the malware attempted to contact a particular URL in the early stages of the infection. Depending on the success of this connection, the malware decided whether to continue its malicious activity or to stop. Given that such a URL was a command and control server, Hutchins realized that the domain was free and decided to register it (for only 10.96 USD). Then, he redirected the traffic to a sinkhole controlled by his company to analyze network packets and produce statistics on the ongoing infection. Later, he realized that the newly registered URL was actually a malware kill switch. The spread of malware stopped suddenly as its new instances, once the domain registered by Hutchins was active, were deactivated without producing malicious effects.

The reason behind the choice of the WannaCry creators to develop such an easily identifiable kill switch is still a mystery. Some security experts speculated that the shutdown mechanism was designed to hinder malware analysis by security engineers. In fact, it is common practice to run malware in a "sandbox" once

[4] https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/ (Last checked August 2020).

discovered. In these protected environments, generally, any URL or IP address will appear as reachable. Probably, by hard-coding an attempt to contact a meaningless URL that was not actually expected to exist, its creators hoped to ensure that the malware did not perform malicious actions while it was under observation.

At first, domain registration helped reduce, although not completely stop, the spread of the malware. This is due to the fact that in a network-restricted environment, with security devices like firewalls and network proxies, the connection was not successful even if the domain was regularly available online.

Definitions

Sandbox A sandbox is a security mechanism used to run untrusted software, usually obtained from third parties, vendors, users, or websites, without risking damaging the host computer or operating system. A sandbox typically provides a tightly controlled set of resources for running the programs under consideration, such as storage space and memory. The access to the network, as well as the ability to inspect the host system, or read from input devices, is prohibited, severely limited, or simulated.

Sinkhole Sinkholing is a technique for manipulating data flow in a network; the network traffic is redirected from its intended destination to another server (the sinkhole). This technique can be used maliciously to drive legitimate traffic away from its destination. However, security professionals more commonly use sinkholing to redirect malicious traffic on a specific server. Once the suspected traffic is isolated in a sinkhole, it can no longer hurt its intended targets. Besides, the traffic can be analyzed to reveal the source of the attack as well as information about the techniques being employed.

In June 2017, ESET researchers discovered a malware, known as "Industroyer" or "Crash Override", that represents the biggest threat to critical infrastructure since Stuxnet. As its name may suggest, Industroyer was designed to disrupt critical industrial processes and is capable of doing significant harm to electric power systems. To make matters worse, there is the opportunity to easily make changes to the malware in order to target other types of critical infrastructures. The 2016 attack on Ukraine's power grid that deprived part of its capital, Kiev, of power for an hour was caused by a cyberattack. ESET researchers have suggested that the Win32/Industroyer malware would be capable of performing such an attack.[5]

Industroyer is a particularly dangerous threat, since it can control electricity substation switches and circuit breakers directly. According to ESET, Industroyer leverages industrial communication protocols used worldwide in power supply

[5] https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/ (Last checked August 2020).

Table 5.1 Most popular malware used to attack critical infrastructure

	Major targeted nations	Start Date	Entry point	Duration of the attack	Known consequencies
Stuxnet	Iran Indonesia India	2010	Infected USBs	Unknown	Temporarily disable 1000 centrifuges used in uranium enrichment process
WannaCry	Over 150 countries	2017	Credential phishing	1 Week	Encrypt data and demand ransom payment
Havex	The United States Europe	2014	Cross-site scripting	Unknown	Information gathering and other malicious code injection
Industroyer	Ukraine	2016	Social Engineering—infected documents	Reconnaissance: several months before the attack Power outage: 1 h Damages: months after the attack	Energy blackout in part of the Ukrainian capital, affecting one-fifth of its electricity needs
Triton	Saudi Arabia	2017	Social Engineering	Unknown	Disable safety instrumented systems, potentially lead to a plant disaster

infrastructures, transportation control systems, and other critical infrastructure facilities (such as water and gas) [315]. Industroyer is described in detail in Sect. 5.1.4 since its main feature is to attack SCADA systems. The most important malware that have affected critical infrastructures are summarized in Table 5.1.

Resources

WannaCry Analysis An extensive analysis of the WannaCry ransomware, including its components and source code, infection and persistence techniques, and propagation mechanisms, can be found here [316].

Modern critical infrastructures are continually exposed to new threats due to the vulnerabilities and architectural weaknesses introduced by the extensive use of Information and Communication Technologies (ICT) solutions. Of particular significance are the vulnerabilities in the communication protocols used in SCADA systems that are commonly employed to control industrial processes. In [317], the authors investigated the impact of malware on SCADA systems, discussing the potential damaging effects. The authors recreated the physical environment of a

power plant in a protected environment, considering its security policies, access policies, maintenance policies, and firewall rules. Later on, they used the source code of four known malware (i.e., Code Red, Nimda, Slammer, and Scalper) to infect the systems included in their test bed, to observe their effects on both ICT and SCADA systems. Results show how malware is capable of damaging the ICT systems that host SCADA servers. The effects observed include system reboots, malicious code propagation throughout the network infecting Windows PCs in the same subnet, and different activities that lead to Denial of Service (DoS) attacks.

Attacks on Modbus, a protocol designed to manage master-slave communications, are among the effects observed on SCADA systems. The main consequences are DoS attacks on system communications and attacks aimed at taking control of the end-devices in the targeted network, by exploiting the lack of authentication and integrity mechanisms in the Modbus protocol.

A similar study was also done in [318], where the authors implemented several attack scenarios within a protected environment. Their experimental test bed consists of a complex electromechanical system composed of several devices, used to physically emulate the different states and the thermodynamical processes of a real power plant. Considering the results obtained, the authors provided a series of countermeasures aimed at decreasing the intrinsic complexity of the ICS systems, which complicates the protection of critical infrastructures. Among the proposed methodologies, it is worth mentioning countermeasures based on standard communication protocols, such as TCP/IP, on SCADA protocols, such as DNP3, AGA 12, and Modbus, and several common security suggestions that regulate the interaction between ICT and SCADA systems.

An investigation into the effectiveness of existing control strategies for SCADA system malware has been provided in [319]. In particular, the authors analyzed the use of antivirus signatures and proposed a new control strategy, which combines the scanning of vulnerabilities with the implementation of security patches.

Several methods for assessing risks and vulnerabilities in ICS networks have been proposed in [320]. The authors first introduced basic information on industrial network protocols, their design, and their architecture. Then, they implemented security and access control mechanisms, as well as exceptions, anomalies, and threat detection methodologies. These contributions are very important to help security operators prepare against increasingly sophisticated ICS-targeted malware.

The aforementioned studies, along with many others in the literature, helped to raise the problem of malware attacks against ICS systems, also providing valuable information for the development of new, effective countermeasures.

In addition to ransomware, cryptojacking is another category of generic malware that is very dangerous for critical infrastructures. This type of malware is characterized by the use of the victim's computational power for mining activities. If installed on systems of critical infrastructures, they may no longer be able to perform their functions, causing risks of different types, depending on the criticality of the system concerned. Furthermore, this type of security incident could easily be perpetrated by insiders, attracted by easy profits, making it much more difficult to detect and block this harmful activity. Security incidents of this type have already occurred

in very sensitive critical infrastructures, such as nuclear power plants,[6] research centers,[7] and even in the US federal reserve.[8] Since it is more prevalent as a browser-based threat, all existing countermeasures are mainly host-based, designed to protect ordinary users. Defending corporate networks and critical infrastructure from this threat, however, requires a different approach. In [321], for example, the authors profiled the network traffic generated by the mining software, managing to identify cryptojacking activities in a local network even if the malicious traffic is encrypted. The network-based approach makes the countermeasure suitable for the defense of corporate networks, as well as critical infrastructures, even if the attacker is an insider.

5.1.3 Threat: SCADA System Vulnerabilities

Many of today's ICSs derive from the application of IT methods into existing physical systems, often replacing or integrating physical control mechanisms. For example, the built-in digital controls replaced the analog mechanical controls in rotating machines and motors. Both the cost and the performance improvements have encouraged this evolution, resulting in the introduction of many of today's "smart" technologies such as smart grids, smart transportation, smart buildings, and smart manufacturing. While on the one hand, this evolution increases the connectivity and criticality of these systems, on the other hand, it creates a greater need for their adaptability, resilience, security, and protection. Engineering models are evolving to address these emerging properties including safety, protection, privacy, and interdependencies on the environmental impact. However, the full understanding of SCADA systems, their structure, as well as their functionality is fundamental for the management of their security. SCADA systems are essential components of the production processes used in several sectors, from the control of machinery in nuclear power plants to the management of traffic lights and cameras in cities. Since SCADA systems are involved in very critical processes, any kind of vulnerability, if exploited, could have serious repercussions not only within the critical infrastructures themselves but also across the whole region. The introduction of IT capabilities into physical systems involves a change in the structure and behavior of those systems, with implications for their security. These systems are constantly evolving, acquiring new functionalities in response to the new requirements of an increasingly connected world. In this section, we analyze the possible consequences of attacks against SCADA systems, discuss the state of

[6] https://www.bbc.com/news/world-europe-43003740 (Last checked August 2020).

[7] https://bitcoinmagazine.com/articles/government-bans-professor-mining-bitcoin-supercomputer-1402002877/ (Last checked August 2020).

[8] https://dealbreaker.com/2017/01/bitcoin-federal-reserve-scandal/ (Last checked August 2020).

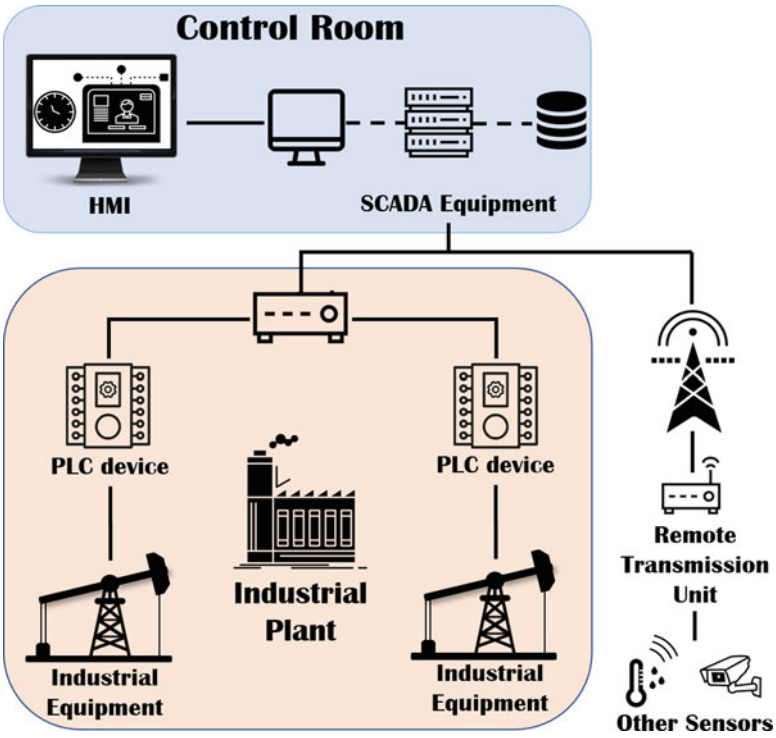

Fig. 5.3 SCADA systems components and common architecture

the art of existing countermeasures, and highlight the problems that are still open, which would jeopardize the protection of critical infrastructures.

SCADA systems are a particular category of ICSs that provide specific supervision-level control over industrial machinery and production processes that cover a vast geographical area (such as electricity production and distribution plants). The SCADA systems architecture, depicted in Fig. 5.3,[9] includes supervision and data acquisition systems and other devices that participate in the local management of more specific sub-processes, such as PLC and Remote Transmission Units (RTU). Both PLCs and RTUs have sensors and actuators that receive commands and send information to other components of the SCADA system. In particular, PLCs and RTUs are microcomputers that communicate with an array of objects, such as factory machines, sensors, and other end-devices. From these objects, they route the information to other computers equipped with supervisory control and data acquisition software. This information supports supervisors in making critical decisions based on real-time data. Administrators only need to

[9] https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/one-flaw-too-many-vulnerabilities-in-scada-systems (Last checked August 2020).

examine Human Machine Interface (HMI), where the different functions and data elements of SCADA systems are presented for human review, interaction, and control. Thanks to their versatility and the critical role they play, SCADA systems are widespread in all types of industrial contexts and infrastructures.

Some of the sectors and infrastructures that use SCADA systems for the management and control of their processes are as follows:

- Energy production and distribution
- Oil and gas
- General manufacturing
- Food production
- Drinking water treatment plants
- Wastewater treatment and distribution
- Smart buildings
- Smart cities and transportation network

SCADA systems are crucial for industrial organizations since they help to maintain efficiency, process data for smarter decisions, and communicate system issues to help mitigate downtime. In particular, they allow organizations to:

- Control industrial processes locally or remotely in specialized control rooms.
- Monitor, gather, and process real-time data.
- Directly interact with devices such as sensors, valves, pumps, and motors.
- Record and display events through HMI software.

The current market of SCADA systems indicates that industries continue to appreciate the advantages that this technology offers to its production processes. However, the vulnerabilities they suffer from and the evolving threats affecting them pose a critical challenge for its users. These vulnerabilities could lead to potential financial losses in the case of private industries, as well as to possibly cascading effects down the supply chain. Furthermore, in the case of critical infrastructure, they can also easily translate into devastating effects for the population. The exposure to the network provides the attackers with a wide range of possibilities. When compromised, SCADA systems could be used by malicious users to gather a lot of information, such as the facility's layout, machinery details, critical safety thresholds, and possibly others.

A careful analysis of where vulnerabilities could be found in SCADA systems can help manufacturers and administrators understand how and where to apply mitigation against exploitation to promptly prevent and neutralize attacks. Unfortunately, SCADA systems control a large number of heterogeneous devices, sensors, and software that greatly increase the attack surface. The main classes of components where it is more likely to find vulnerabilities, and on which protection efforts must be concentrated, are the following:

- **HMI.** Human machine interfaces display data from various sensors and machines connected to a SCADA system to help administrators make and implement decisions using the same interface. Because of its capabilities and role in SCADA

systems, HMIs can be a key target for potential malicious actors who aim to gain control over processes or steal critical information.

- **Mobile applications and web interfaces.** Following the spread of the IoT, several functions of the ICS systems, such as logging, monitoring, and even control functions, have been moved to the cloud. As a result, mobile applications and web interfaces have also become an integral part of SCADA systems. Mobile applications can be grouped into two classes: local applications, installed on devices directly connected to ICS devices in the field or process layers, and remote applications, which allow engineers to communicate with ICS servers using remote channels. These interfaces are subject to different types of attacks, including unauthorized physical or "virtual" access to the device data, compromised communication channel (Man-in-the-middle (MITM) attack), and compromised applications.
- **Communication protocols.** Communication protocols such as Modbus and Profinet help to manage and control the data flows generated by the various mechanisms supervised by SCADA systems. These protocols are generally dated, or, in some cases, they derive from updating old protocols. For this reason, there is a lack of security capabilities to defend against the new threats that endanger SCADA systems. Through vulnerabilities in communication protocols, malicious actors can damage ICS systems or lead to malfunctions of a SCADA component should they change the data sent by PLC and RTU or tamper with the firmware.
- **Other components.** There are countless technologies to make individual parts of SCADA systems stay connected, dynamic, and work in real time. Some of these components may be poorly equipped for threats currently faced by different sectors. These components are not necessarily used exclusively in SCADA systems but are fundamental for other technologies and systems. This large variety of systems and use cases makes very difficult the standardization of a defensive strategy, causing SCADA systems to be vulnerable to remote attacks.

Resources

SCADA And Mobile Security In The Internet Of Things Era A thorough discussion of how the security landscape of SCADA systems has evolved in recent years, with an assessment of the security of SCADA systems and mobile applications in the Industrial Internet of Things (IIoT) era [322].

Previous attacks against critical infrastructures, described in Sect. 5.1.1, give us an idea of what are the possible impacts of attacks on SCADA systems. Potential damages could range from production delays, with possibly cascading effects along the supply chain, to damage to equipment and critical risks for human safety. These are devastating consequences for the organizations and governments that control critical infrastructures and consequently are a primary target for any cybercriminal

groups. For this reason, the urgency to correct vulnerabilities in SCADA systems increases, to prevent future cyberattacks from being successful with similar, if not more serious, consequences than those that occurred in the past.

5.1.4 Attacks and Countermeasures

According to the Ukrainian President, Petro Poroshenko, several Ukrainian institutions have been subjected to about 6500 cyberattacks in the last 2 months of 2016. Part of the attacks targeted key elements of the government, such as the ministry of finance, the ministry of defense, and the state treasury that allocates money to other government institutions. In addition, a cyberattack also wiped out part of the Kiev's electricity grid, causing a blackout in part of the city.[10] According to the Ukrainian president, part of the incidents show that Russian security services were waging a cyberwar against the country, following the collapse of relations between the two nations due to Russia's annexation of Crimea in 2014. The attribution of a single incident, or an entire campaign of cyberattacks, to a specific entity is always difficult and controversial. However, whoever was responsible, this event has shown the tendency toward a cyberwar, proving its effectiveness and efficiency.

One of the most interesting things about the Ukrainian case is certainly the type of attack used to damage the national electricity grid. The Ukrainian power grid has undergone two different attacks, both malware enabled, directed to SCADA equipment. The first attack, which took place in December 2015, caused a power outage to around 225,000 customers, lasting up to 6 h. The second one, which took place in December 2016, is characterized by the use of much more sophisticated malware. Although different from each other, these two attacks marked a precedent that changed the international cyberwarfare scenario. In both of them, the attackers demonstrated the ability to plan, coordinate, and use malware for remote access and manipulation of particular SCADA systems, causing malicious changes to the distribution electricity infrastructure. Consequently, the implicit message behind these attacks has been far more worrying than the damage produced: attackers are now able and willing to invest time and resources to develop software specially designed to manipulate electricity network operations. For many years the possibility of attacking critical infrastructures, such as power grids, has been feared, and now Europe has direct experience. Given the particularity and their importance, the two attacks on the Ukrainian power grid are described in detail below.

December 2015: A Coordinated Attack on the Ukrainian Power Grid
On December 23, 2015, Kyivoblenergo, a Ukrainian electricity distribution company, reported a power outage to its customers. At around 3 pm, about 30 electrical substations were switched off for several hours, leaving around 80,000 users without

[10] https://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN14I1QC (Last checked August 2020).

electricity. Subsequently, 3 other companies suffered the same attack, causing several other outages that left without power about 225,000 users, distributed across different areas of the country. A subsequent investigation, using information made available by interested power companies, researchers, and media, concluded that the power outages were the result of a coordinated cyberattack. Cybercriminals managed to remotely access the IT system of the distribution companies and their ICSs. Then, they manually changed the SCADA controllers' settings to disconnect several substations across the country. According to what emerged from the investigations, the cyberattacks were synchronized and coordinated, probably following a large reconnaissance phase of the victim networks, performed months before the main attack. According to the employees interviewed, the companies involved in the incident suffered the attacks within 30 min of each other. During the cyberattack, which affected several infrastructures at central and regional levels, malicious remote operations were conducted by multiple external humans to manipulate the state of circuit breakers. The attackers used remote administration tools already existing in the operating system and the ICSs client software, connected through Virtual Private Network (VPN) software. When the attack began, several workers noticed how their computer's cursor suddenly started moving on its own, running on the screen out of their control. Employees could only watch helplessly as the cursor intentionally moved over the buttons that control circuit breakers in a substation in the region, finally clicking to open the switches and take the substation offline. Even though they knew that such an action would have left an entire region without electricity, the workers had no way to prevent what happened or to restore proper operation. The system was not responding to their commands, logged them out of the control panel, and prevented them from logging in. The attackers continued to act undisturbed for several minutes, shutting down about 30 substations and disabling the backup power supplies for two of the three distribution centers in the region, leaving the operators themselves in the dark. The attackers proved to be skilled and stealthy. Their assault was carefully planned for many months, first making a reconnaissance to study the networks and discover credentials of the target systems and then launching a synchronized assault in a well-choreographed dance. The greatest ability shown by the attackers was not their skills or their choice of tools, but their capability of performing long-term reconnaissance operations necessary to learn the environment and perform a multistage, highly synchronized, and distributed attack. The attackers used a complex methodology, consisting of several technical components, listed below in chronological order of execution [323]:

- A phishing campaign aimed at targeting the attacked distribution companies
- The use of BlackEnergy 3 malware to gain access to the local network of attacked distribution companies
- Theft of the system's credentials of the impacted companies
- The use of VPNs to access the ICS network of the exposed companies
- The use of legitimate remote access tools, already installed inside the environment

- Compromise of serial-to-Ethernet communication devices at the firmware level using unpatched vulnerabilities
- The use of a modified malware, known as KillDisk, to clear the master boot record of the affected systems and delete some specific logs
- Denial of Service attack on the call centers of the companies involved, to delay the reporting of the energy blackout by customers

Definitions

BlackEnergy BlackEnergy is a Trojan that is mainly used to compromise energy companies worldwide by attacking their ICS infrastructure. This malware is commonly delivered via phishing emails that include malicious Microsoft Office attachments and generally used as an initial access vector to acquire legitimate credentials, as well as for cyber recognition and installation of additional malware and backdoors.

KillDisk A family of malware used to sabotage computers by deleting and rewriting files, often associated with cyber espionage and cyber sabotage operations.

Power outages were caused by the manual use of ICS and SCADA systems and their software by the adversary. All other automatic tools and technologies, such as the BlackEnergy 3 and KillDisk malware, have been used to enable and support the attack, as well as to delay recovery efforts. The blackout did not last long. In all the affected areas, the electricity power was, in fact, restored in a period between 1 and 6 h. Despite this, 2 months after the accident, the control centers of the affected infrastructures still had not resumed full operation. This is because, as reported by Ukrainian and American investigative sources, the attackers have deleted or overwritten the firmware of several critical SCADA devices inside the affected substations. In this state, the tampered equipment had become useless and unresponsive to any remote control attempt by the operators. As a result, the electricity was restored, but the operators of the affected substations had to manually control the equipment for months.

December 2016: Win32/Industroyer: A Powerful Malware Against the Ukrainian Power Grid

In December 2016, Ukraine experienced a second attack on its electricity infrastructure. This time the target was an electrical transmission station located north of the city of Kiev, hit by new cyberattacks that left in the dark a part of the Ukrainian capital, equivalent to one-fifth of its electricity needs. The blackout lasted for about 1 h, causing several problems for the population. Security researchers did not take long to understand that this incident was also caused by a cyberattack, finding traces of what immediately seemed like a very powerful malware, called “Industroyer” or

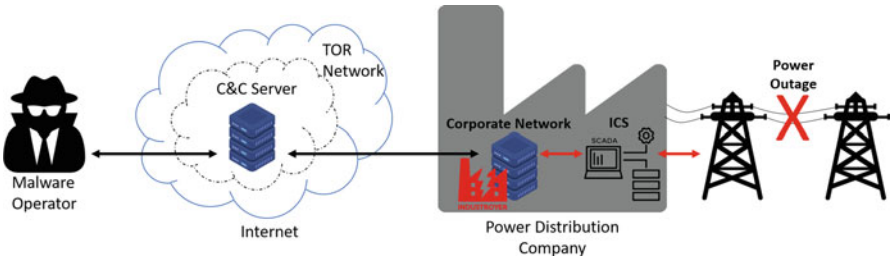

Fig. 5.4 Industroyer malware architecture

"Crash Override". It is not clear how the malware infected the victim's network yet. However, the attackers likely used phishing emails, the same technique employed in the 2015 attack. Unlike what happened in December 2015, however, the malware not only allowed the attackers to access the victim's systems but also directly caused the blackout, without any human interaction.

Industroyer is a highly sophisticated malware designed to interfere with the working processes of ICS systems using specific protocols that control the electrical equipment of substations. The developers of this malware have a thorough knowledge of these systems. In fact, it seems unlikely that malware of this type could be developed and tested without having available the specialized equipment used within the targeted industrial environment.

Industroyer's architecture is distributed on several levels, as shown in Fig. 5.4. Once it has infiltrated the network of the victim distribution company, it automatically maps the control systems and identifies the target equipment. The program also records network logs and sends information to its operators who, through a Command and Control (C&C) server, collect information about the target environment and decide where and when to hit.

The creators of the malware developed several payloads capable of directly interacting with different SCADA components active in the targeted substations, with support for several specific protocols, listed below:

- IEC 60870-5-101 (aka IEC 101)
- IEC 60870-5-104 (aka IEC 104)
- IEC 61850
- OLE for Process Control Data Access (OPC DA)

In addition, the malware authors developed a tool that exploits some vulnerabilities of a particular family of protection relays, the Siemens SIPROTEC range, implementing several attacks against them, such as Denial of Service (DoS).

The component of the malware, shown in Fig. 5.5, are described individually below.

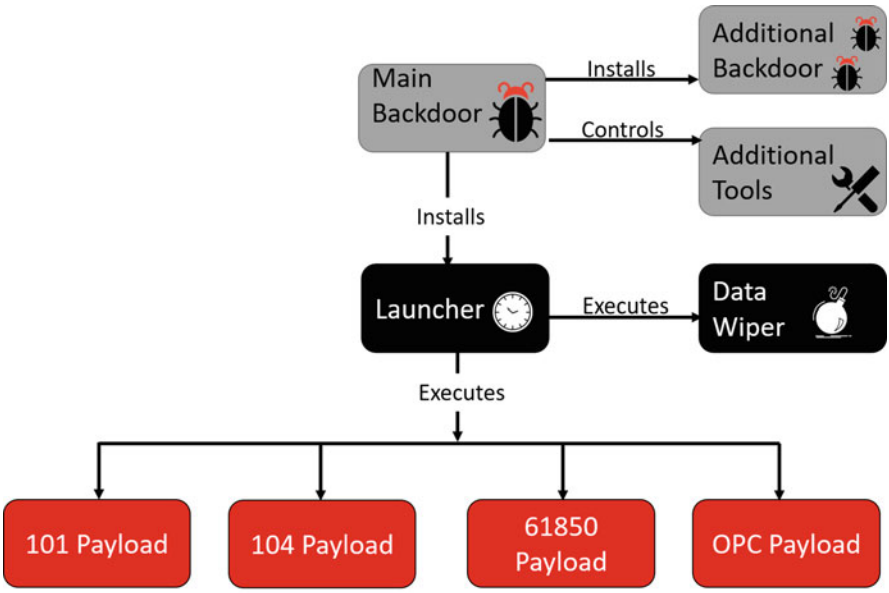

Fig. 5.5 Simplified scheme of industroyer components [324]

- *Main Backdoor.* The core component of Industroyer, used by the attackers to control all the other components of the malware. Once installed, this component communicates with a C&C server, sending the acquired data and receiving commands to be executed in the network under attack.
- *Additional Backdoor.* This component is a backup system that allows attackers to regain control of the compromised machine if the main backdoor is discovered and removed. This malicious application is a weaponized version of the Windows Notepad software. Once replaced with the malicious version, Windows Notepad works as expected, even if connected in the background with a C&C server, different than the one used by the main backdoor.
- *Launcher.* This element is an independent executable responsible for starting other components, such as payloads and data wiper applications.
- *101 payload component.* This component partially implements the protocol described in the IEC 101 standard, used for communications between ICS and RTU transmitted on a serial connection. Once launched, this payload terminates active connections between the victim host and the connected RTU devices. Then, it establishes a new connection to the RTU devices, maintaining their control and changing their state at will.
- *104 payload.* This payload has the same functions as payload 101, with the difference that it works using the IEC 104 standard, which is an extension of the IEC 101 protocol over TCP/IP networks.
- *61850 payload.* This component implements the IEC 61850 standard, used for multivendor communication between devices that perform protection, automa-

tion, measurement, monitoring, and control of electrical substation automation systems. Once executed, this payload tries to connect to known devices or tries to independently discover the devices available in the same subnet of the victim host.

- *OPC DA payload* This component implements the OLE for Process Control (OPC) protocol, which allows real-time data exchange between distributed components, based on a client-server model. As previous payloads, this software can discover compatible devices, establish a connection with them, and change their state.

The two attacks in Ukraine are the only confirmed cases of blackouts caused by a cyberattack in history. But while the first of those attacks received more public attention than what followed, some evidence about the malware used in the latter shows that it was much more than just a repetition. In December 2015, in fact, the attackers manually turned off the affected substations after illegally obtaining access to the systems of the electricity distribution company.The 2016 attack, instead, was carried out completely automatically. The used malware, Industroyer, has been programmed with the ability to communicate directly with SCADA components. This ability allowed Industroyer to send commands directly to the equipment, using the protocol employed to regulate the flows of electric current in the power grid. This means that malicious users are now able to attack an electrical distribution network faster, with little preparation and minimum human control.

Resources

Analysis of the Cyberattack on the Ukrainian Power Grid A technical report that consolidates open-source information on the attack against the Ukrainian power grid in December 2015. The document clarifies important details surrounding the incident, offers important lessons learned, and recommends new strategies to help the ICS community avoid similar attacks [323].

Industroyer A whitepaper released by security researchers at ESET with a detailed analysis of the malware known as Industroyer or Crash Override. The report includes a description of all the software components that compose the malware, including their goal and behavior [324].

A subsequent investigation showed that the attack that caused the blackout might have been just a dry run. From the evidence and testimonies collected, it appears that the attackers tested the most advanced sample of grid-sabotage malware ever detected. When it was discovered, Industroyer was only the second-ever known case of malware designed specifically to interact with SCADA systems and destroy their physical components. The only other malware known at the time capable of conducting such an attack, known as Stuxnet, was allegedly used to destroy centrifuges in an Iranian nuclear enrichment facility in 2009.

The two cyberattacks in Ukraine described above are the first publicly acknowledged incidents to result in power outages. Control systems in affected Ukraine power plants were surprisingly more secure than those operated by other nations. Indeed, their ICS networks were well segmented by the corporate networks using robust firewalls. But in the end, these security measures were not enough, paving the way for the attackers. For example, one of the safest authentication methodologies, the two-factor authentication, was not deployed for workers who remotely accessed the SCADA network at the time of the first attack. This neglect allowed attackers to easily hijack the credentials of legitimate employees, gaining crucial access to the systems that controlled critical end-devices, such as switches. A first stream of thought has speculated that these events are both of little relevance for concerns related to hacking electricity grids in the rest of the world, since the Ukraine case occurred under very particular technological and political conditions, difficult to apply elsewhere [325]. However, what happened in Ukraine holds many lessons for every critical infrastructure in the rest of the world. Researchers who studied Industroyer said this malware can automatize attacks on a state's electrical infrastructure to generate mass power outages. Its highly customizable nature, which includes interchangeable plug-in components, allows attackers to easily reuse its malicious code, adapt the malware to different infrastructures, and launch simultaneous attacks on multiple destinations. These capabilities suggest that Industroyer could cause much more serious disruptions than the Kiev blackout, with a much larger extension of the affected area, and significantly longer duration. Furthermore, the adaptability of the malware means that the tool potentially poses a threat to all the world's electricity networks, not just Ukraine's one, as claimed after the 2015 attack.

Furthermore, another consideration makes the threat observed in Ukraine extensible to the rest of the world. Both the cyberattacks of 2015 and 2016 impacted nationwide different portions of the Ukrainian electricity distribution network. This has led operators to switch from automatic control of the distribution network, governed by ICS systems, to a "manual mode." Indeed, the electricity companies involved in tech incident intervened by sending their technical staff to the disconnected substations. They manually close the switches to power the system and change the management mode from automatic to manual. The plan worked and all services were restored within 3–6 h. This operation allowed a quick resolution of the problem, bringing the electric current back to the homes of Ukrainian users after a few hours from the attack. However, the distribution network was managed without the aid of SCADA systems for the entire period of the infection, which lasted several months after the attacks, according to statements by the operators of the affected substations and local media. This scenario introduces several risk components that are impossible to ignore for any utility worldwide. First of all, the operation of a power grid without the advantages offered by ICS systems is very risky. Being a very complex system, both its monitoring and management operated by an automated control center are fundamental for the safety of the production and distribution processes of the electric current. Furthermore, utilities that depend heavily on this automation may not be able to restore large parts of their system, as happened in Ukraine. Generally, it is possible to lose the functionality of multiple SCADA

devices for a considerable time without this resulting in outages, as happens, for example, during scheduled maintenance operations. However, such an event, when massive and unexpected, considerably exacerbates the risk of accidents. Without the advantage of SCADA systems, in fact, in the event of voltage overloads or other malfunctions, the system will continue to supply energy. This will potentially cause damages to infrastructure components, unless timely human intervention, which is, however, difficult to guarantee in any situation. It has been verified that the adversaries have developed knowledge and skills to create malware capable of taking over the ICT and ICS infrastructure of the targeted utilities, deploying a command and control server, and facilitating the planning of an attack by providing network access and necessary information. Besides, during the attack, some tools were used to delete system files and the firmware of some devices, in an attempt to deny the use of the SCADA system for recovery purposes to amplify the effects of the attack and possibly to delay the restoration. This procedure greatly complicates the full restore of ICSs, making attack mitigation very difficult. In these cases, in fact, if the attacked distribution infrastructures do not have manual backup functionalities, as often happens in different countries, it could be much harder for workers to restore power and outages could last much longer.

Academic research centers, after surveyed most important cybersecurity problems on SCADA systems, are focusing on forward-looking security solutions for these important control networks. In [326], the authors analyzed several cybersecurity incidents involving critical infrastructures and SCADA systems. They classified these incidents based on source sector, method of operations, impact, and target sector. Using this standardized taxonomy, is it possible to compare and counteract to current and future SCADA incidents? In [327], the authors surveyed ongoing research and provide a coherent overview of the threats, risks, and mitigation strategies in the area of SCADA security. The research done in this area looks more toward providing long-term solutions and applying both industry and academic work to the problem. As such, these institutes remain very connected and interact regularly with industry to make sure the research is gauged to provide a positive impact on the national infrastructure. Several open-source projects have been created for various efforts in the SCADA space as well, including items ranging from snort signatures to protocol-specific firewalls and encryption overlays. Some studies have been released in the attack vector space as well, such as SCADA protocol scanners, and information-gathering tools [328].

5.1.5 Open Issues and Future Directions

Ukraine's power grid attack demonstrated that malicious actors seem to have extensive knowledge about ICS hardware and protocols used in critical infrastructures. This knowledge could stem from employees involved in the development or management of ICS components. These highly skilled operators could transfer information to cybercriminals, or they could even actively participate in the design

of malware. Alternatively, malicious actors could learn in the field the architecture of ICS components by gaining illicit access to corporate networks connected with them. Once done, attackers are free to explore systems and interact with ICS devices until the intrusion is discovered. This eventuality highlights the importance of discovering an attack as soon as possible, in order to minimize the time available for attackers to gather information about the system. According to Symantec researchers [329], zero-day attacks last on average more than 1 year before the vulnerability is discovered and corrected. During this time, cybercriminals are free to use the same vulnerability several times, on multiple systems, with low probabilities of being discovered. Since the possibility of being attacked and compromised cannot be excluded, a defense strategy must be developed to detect the attack as quickly as possible and, in the meantime, to prevent the attacker from doing any significant damage.

Cyber deception is one of the most promising technologies that aim to build such a defense methodology. The basic idea is to deploy traps or deception decoys along the virtual perimeter, designed to mimic the legitimate resources [330]. In this way, a possible attacker who obtains illegal access to the network will not be able to distinguish the real resources from the decoys, spending time to exfiltrate fake information or to compromise simulated devices. The feasibility of this defensive methodology has been investigated by several contributions in the literature, relating to multiple assets. In [331], for example, the authors proposed a system that protects devices connected to the network from malicious scans used by attackers to discover vulnerabilities. When a network scan is detected, the system responds with a mix of true and false information to confuse the attacker. If he believes that the answers are all true, he will be deceived. While if he realizes that some are false, he would have to spend time figuring out which ones are true. The same principle can be applied to other assets, such as digital documents. Indeed, the possibility to automatically create believable, hard-to-comprehend fake documents generated from real ones was demonstrated in [332]. The application of this methodology considerably improves cyber deception systems by creating fake documents that are credible and difficult to understand, to help defense mechanisms in misleading cyberattackers. Cyber deception techniques, although supported by several scientific studies, are still little used in production environments. However, this technology is among the most promising in the cyber defense landscape. For this reason, more research and development efforts are needed to enable and promote the use of these innovative techniques in real-world scenarios.

To mitigate the risk of ICS attacks, first, critical infrastructure administrators need to manage their system following the most simple and important best practices. Paul Edon, director at Tripwire, suggests that “security best practice includes selecting suitable frameworks such as NIST, ISO, CIS, ITIL to help direct, manage and drive security programs. It also means ensuring that the strategy includes all three pillars of security; People, Process, and Technology. Protection should apply at all levels; Perimeter, Network, and End Point. Finally, select the foundational controls that best suit your environment. There is a wealth of choice—Firewalls, IDS/IPS, Encryption, Dual Factor Authentication, System Integrity Monitoring,

Change Management, Off-line Backup, Vulnerability Management, and Configuration Management to name but a few".[11]

The examples described in Sect. 5.1.1 show that malware poses a real, pressing, and extremely dangerous threat to critical infrastructures. Whether specifically designed to attack a particular ICS or to accidentally attack critical infrastructures, any type of malware can generate severe consequences on public health, safety, and prosperity. The lessons learned from the attacks of recent years make us understand how the approach to the cyber defense of critical infrastructures is not fully adequate to the threat of malware. The main reason is the current defensive strategy that is not specifically designed for ICS but derives from the experience of protecting generic IT systems. On the one hand, this mitigates some common aspects shared between critical infrastructure and generic IT systems. However, on the other hand, it limits the countermeasures deployed, making them often inadequate for the protection of critical infrastructure. These observations reveal the need to adopt a holistic approach to information security that incorporates processes, technologies, and people. This new approach should be contextualized and used for the protection of all critical infrastructures, even those that are generally less protected, such as ships [333].

One of the key aspects of this new strategy should focus on understanding the differences between a generic IT system and an ICS. ICS technology is becoming increasingly accessible, with threat vectors now extending from centralized systems to individual atomic components, such as smart sensors. Designing the cyber defense strategy by having in mind a generic IT approach is no longer acceptable in this new reality. Operational constraints in industrial sectors such as energy, production, healthcare, and transportation require an approach to cybersecurity that safeguards ICS. The primary goal of IT systems is the management of data and its ability to flow freely and securely among users. IT systems and techniques exist in the virtual world, where data is stored, recovered, transmitted, and manipulated. A typical IT system is composed by many moving parts and gateways. This makes it highly vulnerable and liable to a large surface area for a wide array of ever-changing threats. Defending against attacks means safeguarding each level by identifying (and continuously correcting) the weak points to maintain the flow of data secure and consistent. ICS, on the contrary, belongs to the physical world. Its main goal is to guarantee the correct execution of all the actions undertaken during a production process. While IT must safeguard every level of the system, ICS aims to control physical systems that can be turned on or off, closed, or opened. ICS aims to guarantee the security and control of what were usually closed systems in the past. Everything in ICS is geared to physically move and control devices and processes to keep systems functioning as expected, with a primary focus on security and greater efficiency. With the advent of the IIoT and the integration of physical machines with sensors and software on the network, the dividing line between IT and ICS, well

[11] https://www.informationsecuritybuzz.com/expert-comments/industroyer-biggest-threat-critical-infrastructure-since-stuxnet-discovered/ (Last checked August 2020).

defined in the past, is moving. With the increase of objects connected to the Internet, there has been an increase in the number of potential targets for cybercriminals. Each connected device also represents a new gateway for private IT infrastructures that malicious actors are ready to exploit. Another important aspect is the placement of cybersecurity techniques in the software life cycle. In many cases, companies worry about the security of their software only after implementation. For a decrease in cyberattacks, it is essential to consider security threats during the initial design and development phase, rather than to integrate cyber resilience from the beginning of the life cycle.[12] This approach is fundamental in the development of information systems for critical infrastructures that use new technologies, such as edge and fog computing [334].

The WannaCry malware campaign that the world experienced in 2017 contains several lessons useful to understand how to avoid the repetition of such a dangerous event. Brad Smith, president of Microsoft, has identified several measures that, if implemented by public and private companies, could establish a protective barrier against cyberattacks. First of all, this attack demonstrated how cybersecurity has become a shared responsibility among tech companies, governments, and customers. The vulnerability exploited by attackers has persisted in several systems 2 months after the release of the security patch. This fact highlights how the basic rules of cybersecurity, like keeping computers updated, are not followed. However, the most important lesson is about the malicious code used as an attack vector. As confirmed by several sources, the exploit was stolen from a government agency and then used to start the attack. For this reason, Microsoft itself has asked for a world government's commitment to issue a digital version of the Geneva Convention that applies in cyberspace the same rules applied to weapons in the physical world. This convention should include a new requirement for governments to report vulnerabilities to vendors, rather than stockpile, sell, or exploit them.[13]

In order to plan an effective attack on SCADA systems, the malware developer should know at least the high-level details of the system architecture he wants to target and the protocols used. This knowledge, combined with the ability to send commands to end-devices, allows malware to take control of a SCADA system. According to [317], "generic" intrusion detection systems are not effective in protecting SCADA systems from unauthorized intrusions. This is because all commands sent by malware are legitimate commands. Consequently, one of the main future research directions is based on the design and development of intrusion detection systems that are aware of the SCADA protocols, traffic models, and operational context.

[12] https://iecetech.org/index.php/Technology-Focus/2019-02/Cyber-attacks-targeting-critical-infrastructure (Last checked August 2020).

[13] https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/#sm.0000mpb068eggcqczh61fx32wtiui (Last checked August 2020).

5.2 Scenario: A New Cyber-Physical Threat from the Sky

As discussed in the previous sections, the defense strategy of a modern critical infrastructure takes into account both the physical and the cybernetic dimensions. The main goal is to avoid unauthorized intrusions, both in the real and virtual space. Unlike the virtual perimeter, which is a relatively new concept, the defense of the physical border of a state, as well as of its critical infrastructures, is a requirement that dates back to ancient times. In the absence of digital technologies, surveillance of the security perimeter was committed to lookouts posted in special watchtowers, serving 24 h a day. With the advent of technology, however, the surveillance of a perimeter is performed using cameras, sensors, and other digital alarm systems, often combined and automated.

The human component is still fundamental for the identification of a possible threat, but the support of IT systems has made the task easier and more accurate. Sophisticated equipment, such as high-definition cameras, radar, and sonar, allow the identification of unauthorized people or objects approaching the protected perimeter from anywhere: land, air, and sea. However, these countermeasures are geared toward identifying the classic threats affecting the infrastructure to be protected. The sensitivity of these devices allows the detection of medium/large objects, such as unauthorized people, vehicles (on land, air, and sea), and other fast objects (such as missiles and torpedoes). For example, the defense of an airport perimeter consists of several heterogeneous devices. First, its land border is closed by a fence, heavily guarded, and under constant surveillance. CCTV cameras monitor the perimeter to prevent unauthorized access of men and vehicles, possibly with the aid of motion sensors. Then, its airspace is monitored by several radars, capable of determining the distance and speed of approaching aircraft, even more than 100 km away. These defense systems are quite standard, and their technological evolution over time has affected their performance rather than the ability to identify new threats. The radar system, for example, detects the position of an aircraft by analyzing the signals that, previously emitted by a powerful antenna, have returned after being reflected by the target. This technology has evolved by increasing its coverage area, but its basic functioning, as well as the objects it can recognize, has remained the same. The slow evolution of the physical perimeter surveillance systems matched the static nature of the threats, which remained unchanged for a long time. In the IoT era, attention has shifted to cyber threats, which, on the contrary, are continuously evolving and characterized by an ever-increasing danger. The physical defense has therefore slowed down its evolution, becoming dangerously weak in some sectors.

In this section, we analyze how the advent of medium/small commercial drones brought a new threat to the physical security of critical infrastructures, for which defense systems are still not ready. Through the analysis of attacks that occurred in the real world, we highlight how the detection systems have been caught unprepared by this new threat. This resulted in the helplessness of security personnel during an attack, leaving the closure of critical infrastructure under attack as the only countermeasure to ward off possible harmful consequences.

5.2.1 Threat: Drones

The drone sector is a universe in constant evolution characterized by a continuous extension of use cases that advances hand in hand with technology. Throughout the years, the applications that these small aircraft find in the most disparate contexts are increasingly widespread. The range of activities related to drones is truly endless. For example, the use of drones in agriculture is very widespread, as well as for professional aerial shots that concern sectors of all kinds: from tourism to construction and from mining to aerial surveillance. The use of drones for environmental purposes is also frequent. In fact, the monitoring of geographical areas from the sky enables several activities, such as the detection of dangerous illegal landfills or the prevention of devastating forest fire outbreaks. The birth of the first drone is linked to the military world and dates back to the First World War, when the first prototypes of aircraft controlled via radio waves were developed.

Definitions

Unmanned Vehicle With Unmanned Vehicles (UV) we refer to a type of vehicle that is able to operate without a human pilot onboard. Most of these vehicles were developed in the military sector; however, there have been numerous developments for civil purposes available in the public markets. There are two major types of unmanned vehicles:

- *Unmanned Underwater Vehicles:* UVs that are able to operate underwater without a human pilot onboard. There are two main categories of Unmanned Underwater Vehicles (UUV)s: Autonomous Underwater Vehicles (AUV)s, and Remotely Operated underwater Vehicles (ROV)s. The former is able to operate independently and can be thought of as a robot, and the latter, instead, is controlled remotely by a human operator.
- *Unmanned Aerial Vehicles:* Unmanned Aerial Vehicles (UAV) are aircraft that are able to operate in airspace without a human pilot onboard. UAVs, together with a ground-based controller and a system of communication, compose the Unmanned Aircraft System (UAS). As UUVs, the UAVs can operate both under the remote control of a human operator and autonomously, by relying on an onboard computer.

From that moment on, the military world kept developing and using drones for war purposes, with research and development programs still in progress. Being a technology born within the military world, it took several years before the drones expanded their borders, also embracing civilian use. A driving force toward the success of these aircraft can be placed around the mid-2000s, with technological advancement that has increased reliability and lowered production costs.

The use of drones can be due to many different reasons: professional, commercial, security and defense purposes, or even for recreational uses. However, drones are increasingly used for illicit purposes, whether they are carried out with the will of the operator or as a consequence of the negligent use of the device. In fact, the advent of drones has introduced a whole new system of attacks aimed at mobile and nonmobile targets. In addition to the innocent fun related to making it fly to take breathtaking shots, there are some disturbing ways to use drones. Several news events, for example, have shown how significant the trouble created by the intrusion of a small drone in airport areas are and how they can harm air traffic, the safety of people, and also the economy of both the public and private sectors. It is therefore not difficult to imagine what the implications of a drone attack, carried out against the critical infrastructures of a nation, could be. Thanks to the technological advancement and miniaturization of drone components, they are a good way to perform an asymmetrical attack or complete stealth missions. With relatively low costs, it is possible to reach slightly high technical performances from devices so small that they can lift off almost anywhere. Furthermore, the use of inertial and odometric navigation systems, as well as the integration of new technologies such as 5G or artificial intelligence, increases the possible malicious applications of drones. Also, thanks to additive manufacturing, the drone can be highly customized to adapt to unconventional uses. In fact, an attacker could use a 3D printer to create components designed to maximize the negative effects of an attack.

Definitions

Asymmetrical Attack The nature of modern conflicts has changed from traditional conflicts between states, often due to territorial expansion, to conflicts between states and non-state actors with a huge disparity of means and with purposes other than expanding their borders. Asymmetric warfare is an undeclared conflict, with a significant disparity in military or financial resources and the status of the two opponents. In these conflicts, the militarily and economically strongest contender is often at a disadvantage because he has to defend himself against an opponent that is difficult to identify. In this context, an asymmetric attack is therefore carried out by one of the two parties involved in an asymmetric war. A classic example is the 9/11 attack.

UVs can be categorized according to different aspects, such as their dimensions, capabilities, and costs. These categorizations allow different actors, such as developers and legislators, to understand the variety of existing devices and consequently calibrate national regulations, commercial products, and also defense strategies. In fact, classifying UV devices is essential for understanding the type of threat on which to customize the countermeasures of a sensible area. One of the most important categorizations of UV is based on the role played by a human operator during his mission:

Table 5.2 UAVs classification according to the US department of defense

Category	Size	Maximum gross takeoff weight	Normal operating altitude (ft)	Airspeed (knots)
Group 1	Small	0–20	<1200 (Above ground level)	<100
Group 2	Medium	21–55	<3500	<250
Group 3	Large	<1320	<18,000 (Mean sea level)	<250
Group 4	Large	<1320	<18,000 (mean sea level)	Any
Group 5	Largest	<1320	<18,000	Any

- **Human in the loop.** Remote-controlled systems that perform functions selected by a human operator in real time. These systems are generally controlled by radio frequencies, typically in the 2.4 and 5.8 GHz frequencies. This type of UV cannot perform any operation in real time without a command activated by the pilot.
- **Human on the loop.** Semiautonomous systems capable of selecting a target and attacking it independently. However, the activity as a whole remains constantly subordinated to the supervision of a human operator, who can intervene in each phase of the mission and decide whether to carry out the attack.
- **Human out of the loop.** Fully automated systems which, once activated, can select, engage, and attack targets without the further intervention of a human operator.

The US Department of Defense classifies UAVs into five categories, considering technical capabilities such as the maximum gross takeoff weight, the altitude, and the speed that a drone can reach, as showed in Table 5.2.

Resources

Other UAVs Classifications Several UAV classification schemes have been proposed to help differentiate existing systems based on their operational characteristics and capabilities. A correct categorization is of fundamental importance for several reasons, including the development of adequate countermeasures, the design of standards, and commercial purposes. Furthermore, some of these categorizations are of regulatory importance since the metrics used by the legislator are often directly related to the risk of impact on the ground or of accidents in midair. This contribution provides several characteristic UAV classifications from a variety of sources, both civil and military cite [335].

A drone, in the hands of terrorists or malicious users, would make it easier to attack any target, causing massive damages. Strengthened by the fact that its limited size makes it extremely difficult to detect, the drone could be used for different purposes, involving both passive and active attacks:

- **Aerial surveillance.** A drone can easily be equipped with a high-definition camera, infrared sensors, thermal sensors, and any other device useful for aerial surveillance. With this type of equipment, a drone can be used for reconnaissance missions to acquire information on a future target, such as critical infrastructures. In this way, the attacker can accurately map the targeted site, identifying security systems in use such as alarm sensors and video surveillance. This will enable the identification of any weaknesses in the defense systems, crucial to elaborate a detailed attack plan.
- **Active Attacks.** A drone could also be used to actively attack a target by releasing objects or crashing on it. Low-cost drones easily available on the market, in fact, have a load capacity of several kilos, which can be used to carry explosives on and release them on the target. A drone could also carry other equipment to be used for malicious purposes. For example, a jammer could be carried by a drone near a critical infrastructure to disturb the wireless communication links used by workers, security personnel, and SCADA equipment. Another type of attack could be carried out using commercial drones capable of vaporizing substances in the air, typically used in agriculture, to spread chemical/bacteriological weapons in urban areas.

Definitions

Jammer A Jammer is a sophisticated electronic device capable of producing and transmitting high-frequency signals that interfere with normal communications. These signals are set precisely in the frequencies used by a wide range of equipment, in order to occupy all the available bandwidth and prevent legitimate devices from sending or receiving data. A specially configured jammer can disturb any communication channel, such as GSM telephone transmissions, GPS, WIFI, satellite communications, and possibly others.

In the last decades, several episodes across the world have helped to raise awareness of the threat of UAVs against national institutions. A nonexhaustive list of the main demonstration actions carried out with the help of drones is shown below.

- **Germany.** In 2013, a drone controlled by an extremist political party managed to land near the German chancellor Angela Merkel, violating the security perimeter set by the authorities, during a sporting event in Dresden.

- **Japan.** In April 2015, a drone controlled by activists and carrying radioactive sand from the Fukushima nuclear power plant managed to land on the roof of the presidential palace in Tokyo, where the Japanese Prime Minister works.
- **USA.** In 2015, a small UAV have crashed into the White House lawn. This event, although it may seem of little importance, has demonstrated the difficulties of the Secret Services in protecting the White House from a new and unexpected type of threat.
- **Venezuela.** In 2018, two drones exploded near a military parade attended by Nicolas Maduro, the President of Venezuela.
- **Italy.** In July 2019, during a drone competition called "Drone Race," the drones in the race were subtracted from the control of their respective pilots remaining in flight without a guide for about 15 min. Thanks to the safety nets and the pilots' skills, there were no consequences for the health of the onlookers or the integrity of the drones involved.

In light of these and other incidents, it is not surprising that drones have been banned in several countries, such as Egypt, North Korea, and Iran, and limited in others, such as Russia, the United States and, Belgium. Features such as ease of use, availability on the market at low costs, and high performance make UVs a very dangerous weapon to use against critical infrastructures. In fact, these devices represent a new potentially destructive cyber-physical threat that cannot be underestimated. All types of attacks, both active and passive, which can be performed with the help of a drone are made even more dangerous by the physical characteristics of these devices. Thanks to their dimensions, often contained, and to their ability to fly at low altitude and in a relatively silent way, UVs are very difficult to detect and possibly neutralize. The perimeter defenses of critical infrastructures are normally calibrated on the profiles of typical objects that can intrude without authorization in protected areas. Some examples can be humans, identifiable with security cameras and alarm sensors, vehicles of any type, detectable with radar/sonar, missiles, and possibly others. The profile of a drone does not typically fall within these, making classic countermeasures almost useless. In fact, depending on the size, UVs have a very small radar trace, making their detection and tracking very difficult. Small drones that fly at low altitudes can travel completely unnoticed, be confused with birds, or be spotted late. Furthermore, once sighted, they are still difficult to neutralize using automatic systems.

The next section describes in detail the use of drones to attack the critical infrastructures of a country. We discuss several real cases of security incidents, such as the attack of armed drones at the Russian military base in Syria, and different episodes of UVs that flew over airports paralyzing air traffic for several hours.

5.2.2 Attacks and Countermeasures

In the last few years, several episodes have helped to raise awareness among the institutions of the threat of UAVs against critical infrastructures. In December 2014, France revealed that unauthorized and unidentified UAS had breached the restricted airspace over 13 of the country's 19 nuclear plants during the preceding 3 months. These UAS were described as highly sophisticated civilian devices, and the flights over nuclear facilities appeared to be coordinated, with most of the violations occurring at night. In light of the increasing security concerns in Europe following terrorist attacks in France and Belgium, there is concern over the possible motivations. There have been many notable incidents also in the United States. In early July 2016, the US Department of Energy revealed that its Savannah River Site, which processes and stores nuclear materials, had experienced eight unauthorized flyovers in the span of 2 weeks. There have been unauthorized flyovers of a US Navy nuclear submarine base, major sporting events, large public gatherings, and national monuments. UAVs have crashed into the White House lawn and the New York Capitol, and there has been widespread documentation that they are being used to deliver smuggled goods to prisons [336].

Although these incidents have demonstrated the real extent of the problem and the inability of current defense systems, there are no known consequences to people or things. Conversely, some attacks on critical infrastructures, carried out with the help of drones, have caused significant economic damage.

The first example took place in December 2018, when the air traffic at London Gatwick airport was interrupted due to the intrusion of an unspecified number of small UAVs, which entered the airport's security perimeter. Following the incident, the British authorities decided to block the airport's operations for security reasons. The blockade of air traffic lasted about 36 h, highlighting the substantial unpreparedness of the security systems of critical infrastructures to face this new type of threat. The incident was initially handled by the police force, which deployed several teams of specialized agents. After failing to locate and identify the aircraft, police forces called for army intervention. The military approach to the problem was immediately based on the physical shooting down of hostile aircraft, using specialized personnel, such as snipers. After a brief evaluation, however, the hypothesis of shooting down the aircraft was shelved. The collateral risks deriving from the use of firearms near the populated area located close to the airport were considered too high, as well as the possible fall of the drone, which could have also transported explosives. The intervention of the security forces ended the day after the beginning of the attack with the reopening of air traffic. However, still today, the UAVs, their pilots, and the reasons behind this malicious action have not been identified. Subsequent investigative activities have excluded that the air space violation was due to a simple human error, describing the incident as a deliberate act of disruption. The intrusions within Gatwick's airspace, which occurred several times over the same day, caused the paralysis of one of the most important airports in England for almost 2 days. There were over 800 flight cancellations, forcing more

than 140,000 passengers to land, for an estimated total economic damage of around 25 million US dollars.

Three weeks later, in January 2019, the same type of attack occurred at Heathrow airport, following the same dynamic. After the sighting of an unidentified UAV, air traffic in the first airport of the United Kingdom was blocked for about an hour. In this circumstance, the British police used some of their own remotely piloted aircraft for reconnaissance and identification operations. However, this strategy only contributed to create further confusion, hindering the operations of mitigation of the attack. Also on this occasion, the investigative activities did not bring any results. The attackers have not been identified, and their motivations remain unknown.

The two incidents in England represent an important precedent, not only for the British authorities but for the whole world. The adjustment of public security systems to the continuous evolution of threats, both internal and external, represents an open problem for every nation. UAVs, especially those of group 1 (as defined in the table), are a very recent threat to critical infrastructures, and for this, there are no direct experiences. The attacks that took place in airports, therefore, represent an important case study, with fundamental lessons to be considered for the design and implementation of new generation cyber-physical defense systems. First of all, the simplicity with which the attacks were carried out, as well as the enormous damage suffered, highlighted the urgent need to develop legislation, both nationally and internationally, capable of regulating UVs and contrasting their illicit and malicious use. Furthermore, the uncoordinated and ineffective action of the police forces in handling the emergencies of Gatwick and Heathrow highlights the need to develop a specific contrasting strategy, which coordinates the work not only of the police but also of the private security systems of any critical infrastructure.

Since their introduction to the retail market, public opinion, as well as the research community, wondered about the actual danger of drones, opening the debate on what the threats and the benefits of this technology are. In [337], the author investigated drones' benefits, risks, and legal considerations. In [338], the authors, considering the significant number of non-military UAVs that can be purchased to operate in unregulated air space and the range of such devices test a specific UAV, the Parrot AR Drone version 2, and present a forensic analysis of tests used to deactivate or render the device inoperative. They found that these devices are open to attack, which means they could be controlled by a third party.

5.2.3 Open Issues and Future Directions

Most traditional radar cannot detect small, low-flying UAVs, so this trend is particularly troubling. The majority of previously discussed documented flyovers were only discovered because of human detection—often by vigilant security personnel with keen eyesight. There have been efforts to improve upon the available technology, and many companies are marketing drone detection security systems. However, even when they are detected, there are complications intercepting them and identifying

the operators [336]. A possible solution is the design and implementation of anti-drone systems based on jamming technologies. However, such countermeasures may not always be efficient. In [339], for example, the authors used the signal emitted by a jammer as a navigation system for the drone under attack.

Recognizing and implementing security practices that meet states' regulatory requirements are key to successfully managing potential security incidents associated with UVs. Although no single solution will fully mitigate this risk, several measures can be taken to address UVs-related security challenges [340]:

- Research and implement legally approved counter-UV technology.
- Know the air domain around the facility and who has the authority to take action to enhance security.
- Update emergency/incident action plans to include UV security and response strategies.
- Build federal, state, and local partnerships for adaptation of best practices and information sharing.
- Sensitize citizens and institutions to the problem, inviting anyone to report potential UVs threats to local law enforcement agencies.