Critical Infrastructure

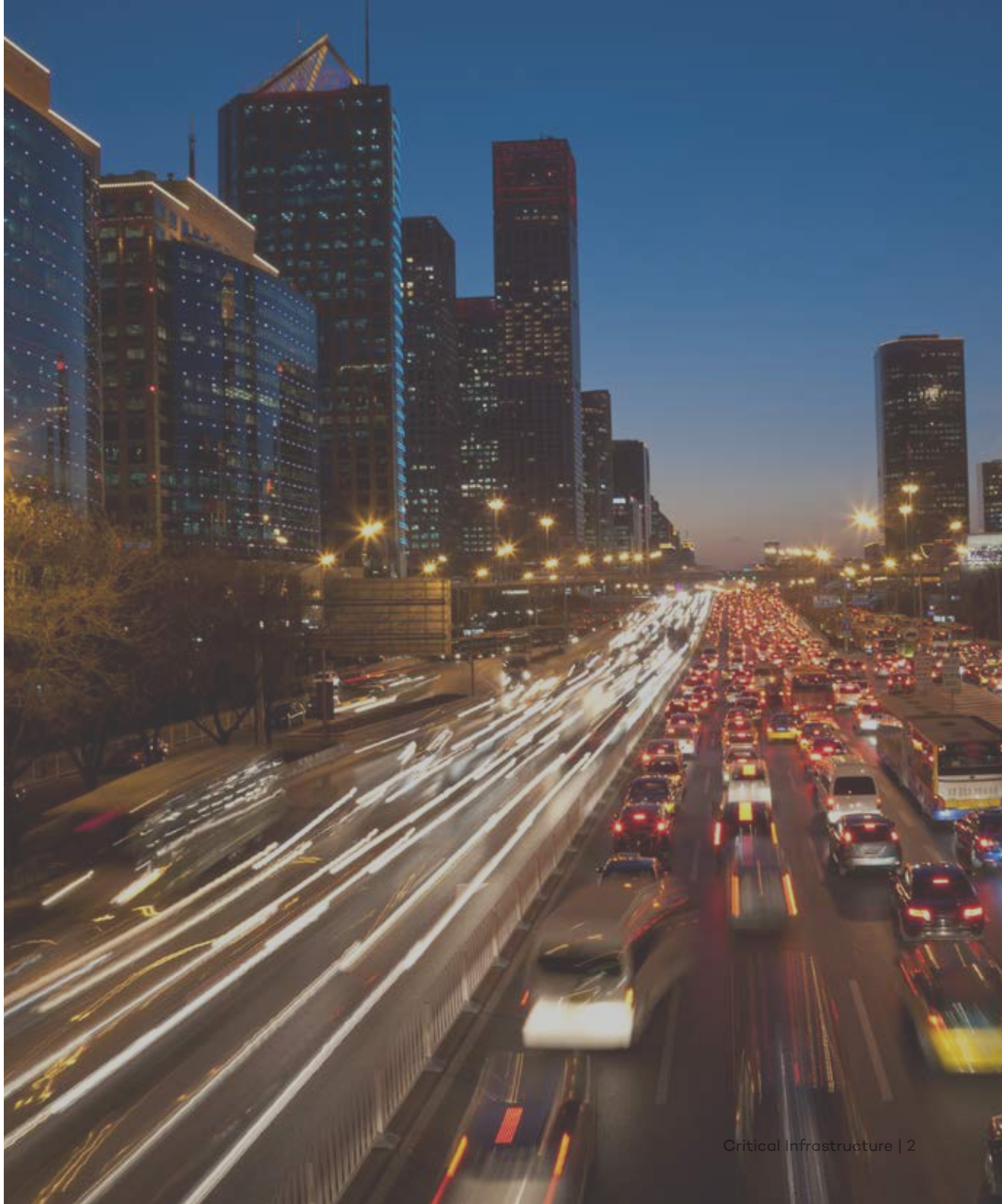
panda

Introduction

One of the great strengths of today's advanced societies is also one of their great weaknesses. In our hyper-connected environment, developed and highly technological societies are heavily dependent on a series of services that have now become essential.

Certain infrastructures underpin the normal operation of fundamental services and production systems of any society, in such a way that any interruption, whether due to natural causes, technical failure or deliberate attack, would have serious consequences for the distribution of vital supplies or the operation of essential services, not to mention the threat to security.

Cyber-crime has been expanding consistently around the globe in recent years. The increasing connectivity and the digital transformation of society represents a double-edged sword, as they offer a channel of opportunity to criminals. Yet what happens when the networks that we see as essential to our very survival become the target of criminal activity?



Sensitive sectors and critical infrastructure

Protection of critical infrastructure is a concern for all countries. The high level of development in modern societies largely depends on a series of basic and essential services delivered to a great extent by the private sector.

Never have infrastructures been so vital to the normal operation of the services and systems that underpin production, such as government, water supply, financial and fiscal systems, energy, space, nuclear energy and transport systems.

What we consider critical infrastructure includes the installations, networks, services and systems which if they were to be interrupted in any way would affect the health, security and general well-being of a country's citizens.

Guaranteeing the delivery of these basic services in the face of new threats is not only the responsibility of public administrations, but also of private operators both nationally and internationally.

Technical characteristics

Certain technical characteristics along with the level of exposure of the data on such networks, means that protecting them is no ordinary task.

The new intrusions targeting the cyber-physical systems of industrial processes running on critical infrastructure have created the need for new strategies to be adopted to detect such threats without interfering with the operation of the infrastructure.

Hybrid Architecture

For one thing, many infrastructures defined as critical are based on a hybrid architecture combining classic IT networks and industrial OT networks which administer the components that interact with physical media (cyber-physical systems).

Isolated from Internet

This point deserves some attention as the increasing tendency towards interconnection of all types of infrastructure this also increases the number of attack vectors available. The control systems for such infrastructures are normally isolated from the Internet and communicate across an internal network.

SCADA

However, there are also Supervisory Control and Data Acquisition (SCADA) systems which are visible and even accessible on the Internet. Most of these systems have no direct relation with those that manage critical infrastructure, yet they could act as a gateway that allowed an attacker to obtain confidential information that could facilitate a more sophisticated attack.

Types of attacks on critical infrastructure

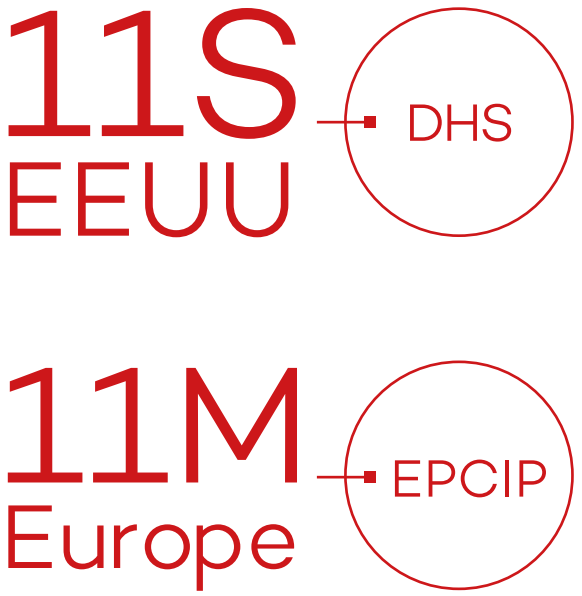
Modern nations face numerous challenges regarding national security. Strategic priorities in this respect include infrastructure that is exposed to a series of threats. To secure this infrastructure, it is essential to draw up a plan that offers prevention and protection against potential threats, both in terms of physical security as well as technology and communications.

Over recent years there has been a series of key events, such as 9/11, that have marked a turning point in global security. Since that date a panorama has been created in which the destruction of certain targets could affect the lives, health and well-being of individuals and entire nations.

The traditional way in which the security of such targets has been approached has changed. Until then, security was in the public sphere and was solely the responsibility of public administrations. Yet critical infrastructures are largely in the hands of the private sector, and as such this sector has a responsibility in this area. After 9/11, the USA reacted by creating the **Dept. of Homeland Security (DHS)** along with a series of wide ranging regulations.

In Europe, a similar initiative arose out of another key date, March 11, 2004, the date of the Madrid train bombings. The European commission drew up a global strategy for the protection of critical infrastructure, **'The European Programme for Critical Infrastructure Protection' (EPCIP)**, which includes proposals to improve Europe's prevention, preparation and response to terrorist attacks.

Among other things, the directive sets out that the main and ultimate responsibility for protecting critical infrastructures lies with member states and the operators of such infrastructure, and it urges each nation to implement in national legislation a series of actions and initiatives.



A timeline of attacks

The general public believes that although there may be risks, in reality there have been few cyber-attacks on critical infrastructure. Unfortunately, this is not the case and there have been hundreds of documented cases around the world. Attacks on these networks have been around for decades, and below you can find a timeline of some of them.

Siberian oil pipeline

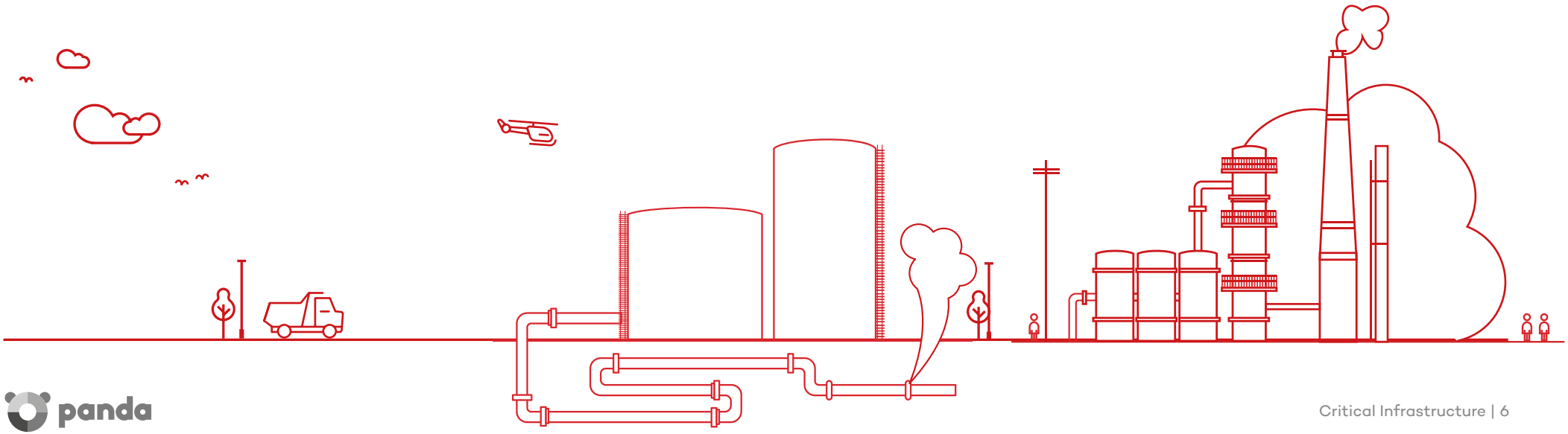
The term Internet springs to mind when thinking of cyber-attacks on critical infrastructure. Yet the first such cyber-attack took place long before the Internet even existed, in **1982**. This was when a group of attackers managed to install a Trojan on the SCADA system that controlled the Siberian oil pipeline, causing a massive explosion. The attack was orchestrated by the CIA, though this wasn't revealed until 2004, when Thomas C. Reed, ex-secretary of the U.S. Defense Department and advisor to Ronald Reagan published the book "At the Abyss: An Insider's History of the Cold War".

Explosion in a Siberian pipeline triggered by the CIA

Chevron

The next incident occurred some ten years later, in **1992**, when a worker at the Chevron oil company was fired, having hacked the computers in the company's New York and San Jose offices that were responsible for the warnings systems, and reconfiguring them to crash when the system was started up. This sabotage wasn't discovered until a toxic substance was leaked in Richmond, California, and the system failed to generate the corresponding warning, placing thousands of lives at risk for the ten hours that the system was down.

Leakage of a toxic substance that placed thousands of lives at risk



Salt River Project

In August **1994,** Lane Jarret Davies managed to hack into the Salt River Project network through a modem, accessing information and deleting files from the system responsible for monitoring and supplying water and electricity. He also managed to access personal and financial details of the company's customers and employees.

Deletion of files from the system responsible for monitoring and supplying water and electricity

Worcester Airport

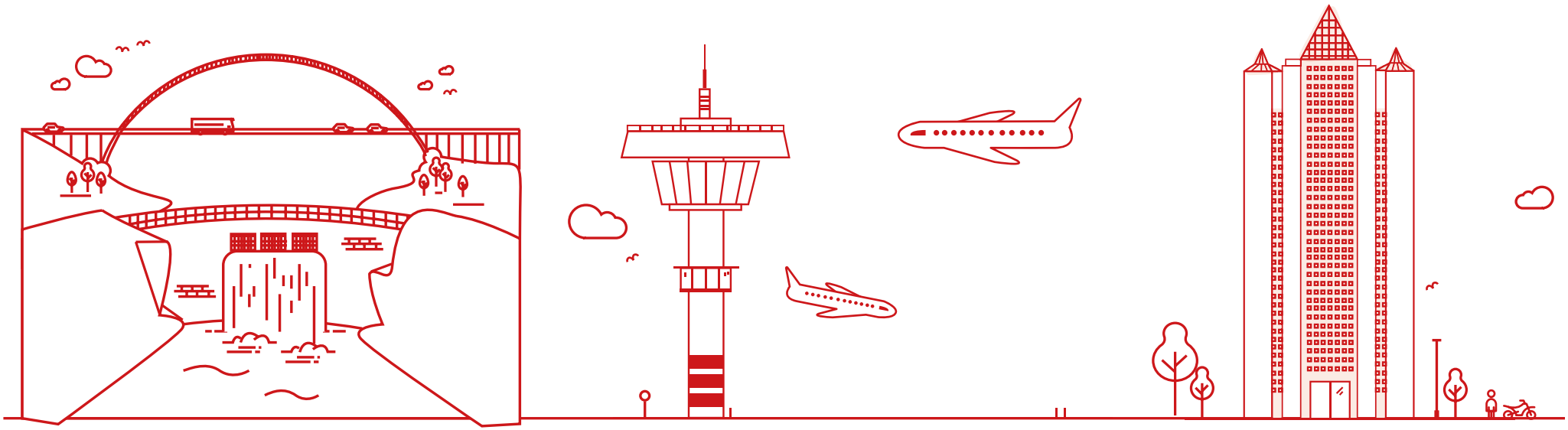
Other key sectors have also suffered targeted attacks. On March 10 **1997**, a hacker got into the control system used for air traffic control communications in Worcester, Massachusetts, causing a system failure that left the phone system down for six hours. It specifically affected the control tower telephone system, the airport fire department and the airline companies based at the airport.

System failure that affected the control tower telephone system, the fire department and the airline companies based at the Worcester airport for 6 hours

Gazprom

In **1999,** a hacker foiled the security systems of Gazprom, the Russian energy giant and – with some inside help- used a Trojan to take control of the SCADA system that controlled the gas flow. Fortunately there were no serious consequences and normal service was restored shortly.

Hackers take control of the Gazprom system that controls gas flow



Maroochy Water System

An ex-employee of the Maroochy Water System ended up with a two-year prison sentence after using stolen material in **2000** to hack the water control system and spill a million liters of waste water into a nearby river, flooding a local hotel too.

Spillage of a million liters of waste water into a river

Gas processing plant

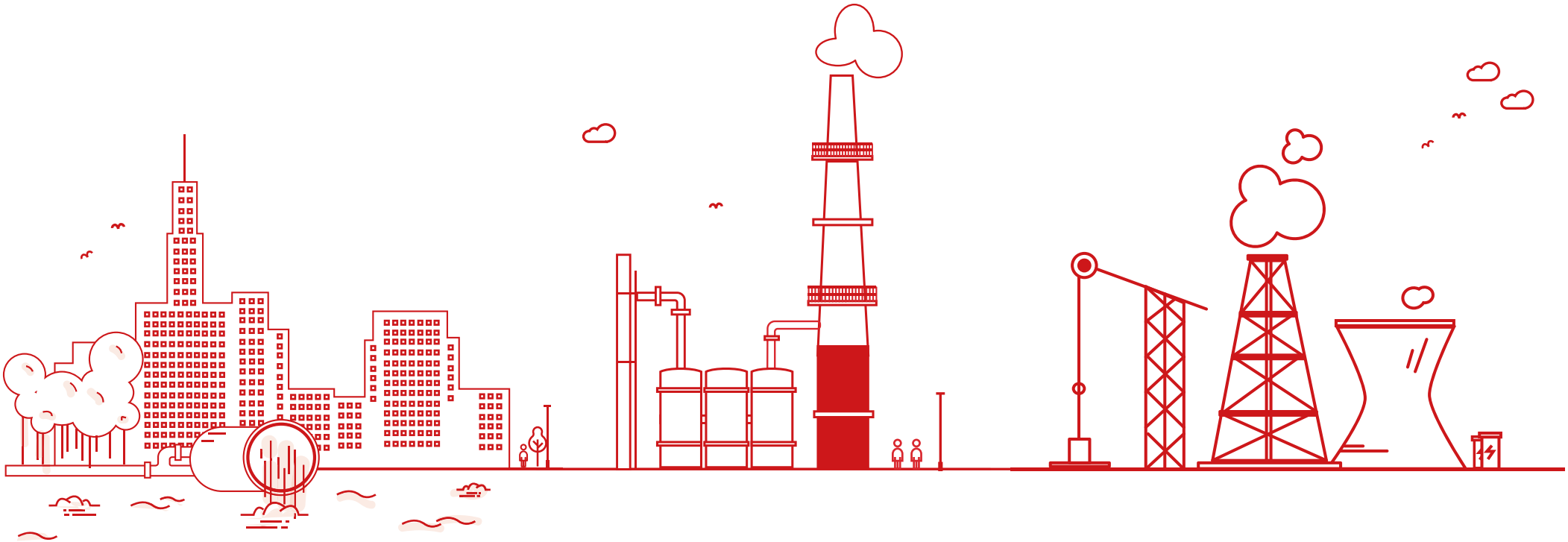
A gas processing plant run by a US oil company also suffered an attack in **2001**. After a six-month investigation, it was determined that it had been the work of one of the suppliers who, in order to cover up an error they had caused on a computer, had created a distraction by hacking three of the company's computers and causing a service outage to homes and businesses in a European country.

Cyber-attack leads to gas service outage to homes and businesses in a European country

PDVSA

In December **2002**, the Venezuelan oil company PDVSA was hit by an attack that reduced production from 3 million barrels a day to 370,000. The attack involved the hacking of several of the company's computers and took place while company staff were on strike, suggesting it may have been carried out by employees.

Attack reduces oil production from 3 million barrels a day to 370,000



Los Angeles city's traffic lights

In **2006,** two traffic engineers from Los Angeles hacked the city's traffic lights during an industrial protest. They managed to change the programming of some strategically placed signals in order to keep lights set on red and cause major traffic jams.

Hack attack leads to major traffic jams

Tram network in the city of Lodz

In **2008,** a 14-year-old student hacked the systems of the tram network in the city of Lodz in Poland, resulting in four derailed trams, and injuries to 12 people. The student had built an infrared remote control, similar to a TV remote control, with which he managed to control the track crossings.

Cyber-attack results in four derailed trams and injuries to 12 people

Saudi Aramco

In **2012,** the world's largest oil company, Saudi Aramco, became the victim of a targeted attack on its headquarters. The attackers had gained access to the network through an attack on one of its employees, and from there they gained access to 30,000 of the company's computers. At one point the attackers managed to delete the contents of all computers while the screen displayed a burning American flag. A group calling itself the "Cutting Sword of Justice" claimed responsibility for the attack.

Deletion of the contents of every computer in a company while the screen displays a burning American flag

RasGas

Just two weeks after the Saudi Aramco attack, the Qatari company RasGas, the world's second largest producer of liquefied natural gas, was attacked with the same malware used against the Saudi oil company. For several days both the company's internal network and its website were inoperative.

Hack attack crashes a company's internal network and its website

Metallurgical plant in Germany

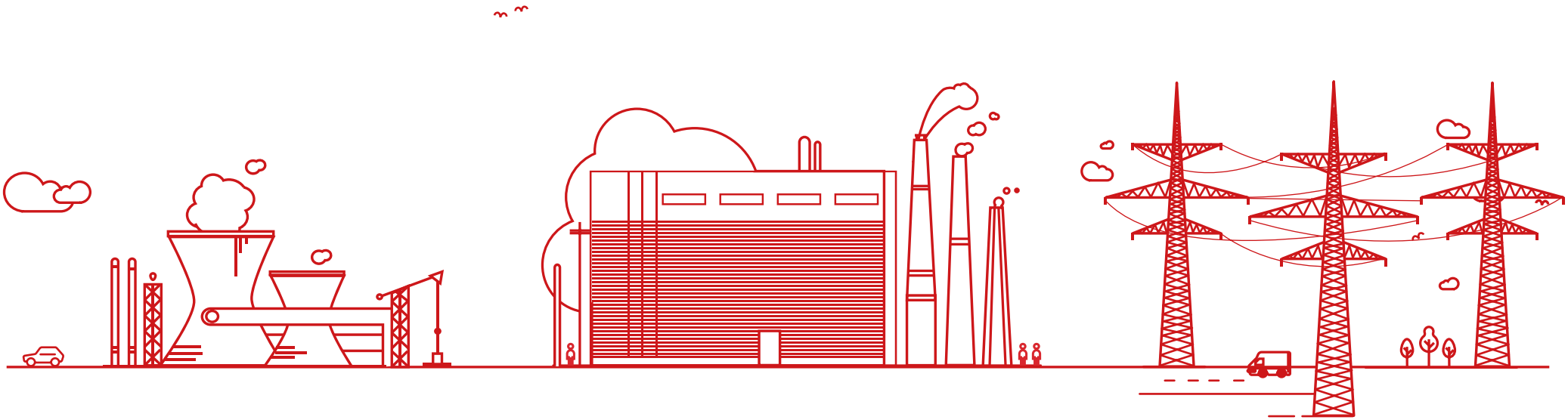
In **2014**, a metallurgical plant in Germany was also the victim of an attack. By employing social engineering, attackers were able to access an employee's computer, and from there they gained access to the internal network of the control system. As a result of this, it became impossible to shut down one of the blast furnaces, which caused massive damage to the plant.

Cyber-attack causes massive damage to metallurgical plant

Electricity grid of Ukraine

In late **2015,** Ukraine suffered a cyber-attack on its electricity national grid that left more than 600,000 homes without energy.

Cyber-attack leaves the homes of 600,000 Ukrainian citizens without energy



The first cyber-attack in history against the Internet infrastructure

Despite this long list of incidents, the first cyber-attack in history against the Internet infrastructure in any country didn't take place until April 27, **2007, when a series of attacks in Estonia brought down numerous websites belonging to many organizations**, including the parliament, government ministries, banks, newspapers and other media, etc.

However, the attack also targeted certain addresses that were not known publicly, including the country's system for processing financial orders and its telecommunications services. Urmas Paet, the Estonian foreign minister, publicly accused the Russian government of being behind the attacks, though he was unable to provide evidence to substantiate the allegation.

The most infamous cases of cyber-attacks on critical infrastructures in history: Stuxnet

In **2008** we witnessed one of the most infamous cases of cyber-attacks on critical infrastructures in history: **Stuxnet. It is now known that this was a coordinated attack between the Israeli and US intelligence services, aimed at sabotaging Iran's nuclear program**.

They created a worm which, by infecting the computers that controlled the uranium centrifuges at the Iranian plant at Natanz, caused them to operate at full speed while manipulating data displays to make the engineers think that everything was normal. This caused physical damage to all the uranium centrifuges in the plant and the case became the catalyst that made the general public aware of these types of threats.

The types of attacks previously mentioned also happen in these installations

In addition to the attacks aimed specifically at sabotaging the aforementioned type of infrastructure, similar attacks have also afflicted the following installations; and the consequences have, sometimes, been just as serious. **These types of problems largely began at the start of the last decade, as network worms began to propagate by themselves across a network.**

One example happened at a leading food factory in the US after a virus infection that cost thousands of dollars. One of its employees logged in remotely from home, and his computer was infected with the Nimda virus so, as soon as it entered the company's network, the worm spread through all control systems.

In 2003, an American oil company suffered the effects of the SQLSlammer worm when it entered the company's intranet. Although it didn't cause production to shutdown, it did affect internal communications and it took several days to completely remove it from the network and to update systems to prevent further attacks. This worm has in fact been one of the most historically disruptive to businesses globally.

In order to spread, it exploited a vulnerability in SQL database servers (a common tool in corporate environments). The vulnerability was patched by Microsoft in January 2003, and as such, another US oil company began updating all its installations as soon as the patch was available, in order to keep the worm at bay. However, to finish installing it, it was necessary to restart the servers on which it had been applied, and as several of them were on oil platforms without dedicated IT personnel, the operation had to be supervised by specialized personnel flown in by helicopter. While they were in the process, the worm infiltrated some of the company's systems and those that had not been restarted were infected.

In 2003, one of the largest carmakers in the United States also suffered an SQLSlammer attack, which spread rapidly and affected 17 of its manufacturing plants. The total cost to the company was $150 Million. Although the patch had been available for six months, the company's IT managers had not applied it.

In the same year, a malware infection (the malware that was responsible for the incident was not made public) affected an Air Canada's computer responsible for flight information, fuel loading, etc. As a result of the infection, 200 flights were delayed or canceled.

In 2005, in Japan, an employee of Mitsubishi Electric was infected with malware, which resulted in the leaking of confidential inspection documents from two nuclear power plants owned by the company.

In 2006, two computers in a UK hospital that were responsible for managing the application of radiotherapy treatment to cancer patients were infected with malware. The treatment of 80 patients had to be delayed. A couple of years later, three other UK hospitals were infected with a variant of the Mytob worm which led to them having to disconnect all the computers for 24 hours in order to resolve the incident.

In 2013, 200 computers at the Cook County Department of Highway and Transportation were infected. These systems were responsible for the maintenance of hundreds of miles of freeways in the Chicago area. As a result of the attack the network had to be shut down for nine days in order to disinfect all the computers.

This list of incidents shows that the danger of cyber-attacks on critical infrastructures is real, and today all governments are aware of the risks involved.

Advanced protection for essential infrastructure

The reality we have seen and in which we are living means that it is necessary to regulate the protection of critical infrastructure in order to provide a greater level of protection against all types of threats.

In May 2016, after a meeting of G7 energy ministers, a joint declaration was published in which, among other points, there was an insistence on the importance of achieving resilient energy systems –including gas, electricity and oil- in order to respond effectively to emerging cyber-threats and maintain critical services.

In order to improve prevention and response to logical attacks, governments are implementing a series of measures on a global level. Measures aimed at setting up centers to record all relevant information to improve protection of critical infrastructures. As a result, a comprehensive strategy has been developed to tackle the problem, and this must be incorporated into national legislation.

It is not easy to answer the question of whether the security of critical infrastructures is currently adequate, since the information or techniques that might be used by cyber-criminals is not known, so it is impossible to be 100% secure. What can be improved is the protection against known attacks, and these can be avoided by adopting a series of good practices, such as:

Good Practices

1. **Checking systems for vulnerabilities, especially those with security holes that have been reported and known for some time.**
2. **The networks used to control these infrastructures should be adequately monitored and where necessary, isolated from external connections. This will enable the detection of external attacks and prevent access to systems controlled from an internal network.**
3. **Control of removable drives is essential on any infrastructure and not just because it has been the attack vector for attacks as notorious as Stuxnet. When protecting such critical infrastructure, it is essential to ensure that malware doesn't enter the internal network through pen drives or that they are not used to steal confidential information.**
4. **Monitoring PCs to which programmable logic controllers (or PLCs) are connected. These Internet-connected devices are the most sensitive, as they can give an attacker access to sensitive control systems. Moreover, even if they don't manage to take control of a system, they can obtain valuable information for other attack vectors.**

The solution

The solution consists of protection against advanced threats and targeted attacks, and that can even detect unusual or suspicious behavior. A system that can safeguard data confidentiality, information privacy, and the assets and reputation of a company.

An intelligent platform that can help security personnel on critical networks react rapidly to threats and guarantee that they have the information they need to formulate an adequate response.

This is Adaptive Defense 360, the only advanced cyber-security system to combine latest generation protection and the latest detection and remediation technology with the ability to classify 100% of running processes.

Adaptive Defense 360 classifies absolutely all active processes on endpoints, guaranteeing protection against known malware as well as zero-day attacks, advanced persistent threats and targeted attacks.

The platform uses contextual logic to reveal malicious behavior patterns and generate advanced cyber-defense actions against known and unknown threats.

It analyzes, categorizes and correlates all the data gathered on cyber-threats, in order to carry out Prevention, Detection, Response and Remediation tasks.

It determines how data has been accessed and by whom and controls data leakage, whether due to malware or employees.

It discovers and resolves system vulnerabilities and those on installed programs and prevents the use of unwanted applications (toolbars, adware, add-ons, etc.).

More information at:

BENELUX
+32 15 45 12 80
belgium@pandasecurity.com

BRAZIL
+55 11 3054-1722
brazil@pandasecurity.com

FRANCE
+33 (0) 1 46842 000
commercial@fr.pandasecurity.com

GERMANY (& AUSTRIA)
+49 (0) 2065 961-0
sales@de.pandasecurity.com

HUNGARY
+36 1 224 03 16
hungary@pandasecurity.com

ITALY
+39 02 24 20 22 08
italy@pandasecurity.com

MEXICO
+52 55 8000 2381
mexico@pandasecurity.com

NORWAY
+47 93 409 300
norway@pandasecurity.com

PORTUGAL
+351 210 414 400
geral@pt.pandasecurity.com

SOUTH AFRICA
+27 21 683 3899
sales@za.pandasecurity.com

SPAIN
+34 900 90 70 80
comercialpanda@pandasecurity.com

SWEDEN (FINLAND & DENMARK)
+46 0850 553 200
sweden@pandasecurity.com

SWITZERLAND
+41 22 994 89 40
info@ch.pandasecurity.com

UNITED KINGDOM
+44(0) 800 368 9158
sales@uk.pandasecurity.com

USA (& CANADA)
+1 877 263 3881
sales@us.pandasecurity.com

Adaptive Defense 360

Limitless Visibility, Absolute Control

pandasecurity.com

panda