Preparing for physical and cyber security convergence

BY ANDREA BIRAGHI

A comprehensive security strategy in today's threat environment calls for solutions that take both physical and cyber-security into account, because cyber threats are physical threats too. By thinking of cyber-physical security in a unified way, leaders can invest in advanced digital technology making their network and facilities safer.

The physical, real world is becoming more and more saturated with objects that have a computational capacity and that communicate with the network, with each other or with users / citizens. Virtually everything, in the near future, will be interconnected and will have to collect information, make autonomous decisions and respond to predefined stirrings.

In this technology-rich scenario, the components of the real world interact with the cyberspace through sensors, computers, communication systems, quickly leading us towards what has been called the Cyber-Physical World (CPW) convergence.

Flows of information are continuously exchanged between the physical and cyber world, adapting this converged world to human behavior and social dynamics. Eventually, humans remain at the center of this world, since information relating to the context in which they operate is the key element in adapting CPW applications and services. On the other hand, a wave of (human) social networks and structures are now the protagonists of a new way of communicating and computing paradigms.

Concerning this limitless world and linked scenarios, it is important to delve deeper into some of the security issues, challenges and opportunities, because physical security is increasingly looped to cyber security.

By 2020 There will be more than 230 billion active intelligent objects (known as IoT - Internet of Things), 24.4 billion of them will be directly connected to the network; each of us is already completely immersed in a technological landscape on which we depend for many elementary actions during the day: for example the car navigator system to move around, the mobile phone or applications to order online shopping and so on.

However, people hardly stop to reflect on the fact that there are also many other elements of their life that absolutely depend on the cyber world. Just to give a few examples in the world of transport, almost all the newly built subways, high-speed trains, aircraft landings in conditions of poor visibility, are all governed by computers that manage the systems to which they are dedicated in an absolutely "human less" way. The subways are therefore "driver less", the train driver is present only to manage emergencies, in the airplanes the landing with fog is managed by a ground-based automatic system that communicates with the control systems of the plane allowing it to land even without seeing the runway.

We can therefore easily understand the tricky correlation between cyber and physical security of passengers. If someone had the ability to violate any of these systems it could cause damage to human life, thus instantly short-circuiting the cyber and physical world.It is only a first example of how the two realities have now collapsed into a new single universe.

Now shift your attention to healthcare, which by technological advances, has allowed us to increase av-

PLANET LABS

The possible outcome of the Israeli cyber attack on the Iranian nuclear facility as seen by satellite.

erage life expectancy all over the world, not only thanks to drugs but also to electronic devices. Pacemakers and implanted defibrillators that inform doctors in real time about the behavior of your heart and that react to every problem by stimulating the muscle to restart or change pace, all these devices communicate continuously from inside your body with a small box on the outside, in turn connected with the doctor who is treating you. These networked medical devices and other mobile health (mHealth) technologies are a double-edged sword: they have the potential to play a transformational role in health care but at the same time they can become a vehicle that exposes patients and health care providers to safety and cybersecurity risks such as being hacked, being infected with malware and being vulnerable to unauthorized access.

Patient safety issues – injury or death – related to networked medical device security vulnerabilities are a critical concern; compromised medical devices also could be used to attack other portions of an organization's network.

As a further risk scenario for citizens, it is worth analyzing the so-called "essential services" such as water, electricity, gas, which are vital for daily life. All networks that allow your home to receive its own water, electricity and gas, are automatic systems, consisting of sensors, actuators and computers that allow to manage and regulate the flow, pressure, voltage to give everyone an efficient and continuous service. However, the fact that these networks are spread throughout the territory and therefore are so extensive, exposes them to possible attacks that have the purpose of interrupting the public service. The temporary lack of light isn't just a "nuisance" it could involve a real risk to human life. The lack of home heating gas in a northern European nation could easily entail a real risk of hypothermia.

As there is a history of cyber security and virtual warfare becoming real war, with real impact on human life, it may be interesting to report some examples of

© PH

Copenhagen's driverless light railway.

what really happened (and continues to happen) in the world of critical infrastructures.

In 2005, with the attack, allegedly performed by the United States and Israel, on Iranian nuclear power plants, on centrifuges aimed to enrich uranium in order to develop an atomic bomb, we discovered that even infrastructure considered unassailable from the point of view of cyber security, namely nuclear power plants, were absolutely exposed to attacks. This sabotage took place through a malware called Stuxnet and it has been the most advanced used on nuclear infrastructure so far. The malware infected the systems that run the spinning machines and modified the rotation of speed of centrifuges continuously. This compromised the enrichment process and caused severe damage to the plant, with the centrifuges spinning at enormous speed and suddenly slamming on the brakes. The primary intention of the attackers was to slow down Tehran's nuclear program by destroying the plant, possibly to gain time to complete diplomatic negotiations. The attackers decided to limit the hit only to the centrifuges, but potentially they could have decided to raise the level of the attack to the total destruction of the nuclear plant.

Don't make the mistake of thinking that this is something that could have only happened in the past, assuming that today's cyber security systems allow to fully guarantee the functioning and protection of networks. The reality is that while on one hand the level of cyber protection is now much higher, on the other hand, the refinement of the attacks has also grown exponentially, forcing a security escalation that seems to never end.

Today, for example, Israel turns out to be one of the most attacked nations. By attacking Israeli critical infrastructures, cyber terrorism wants to strike at Jewish citizens and therefore through cyber attacks to threaten real, physical life using this as a lever for geopolitical reasons. Israel is attacked 1,000 times a minute by cyber-terrorists who are largely targeting the coun-

AP

Self-driving shuttles are already being used to ferry people in retirement communities, industrial complexes, shopping centers and airports.

try's infrastructure: water, electricity, communications, and other important services. While the hackers have so far failed to mount a meaningful attack on major systems that might leave Israelis without power, there's no guarantee it can't happen in the future.

In fact, the odds are with the cyber-terrorists, at least as far as the Israeli Electric Company (IEC) is concerned, because the company is subject to between 10,000 and 20,000 cyber-attacks each day.

The IEC is treating these attacks as a security emergency, with a 24/7 deployment of top security staff, military-style strategies to outwit, thwart, or fight back against attackers, in order to ensure that attacks do not disable the IEC's ability to keep the energy flowing.

A cyber-war can inflict the same type of damage as a conventional war. If you want to hit a country severely you hit its power and water supplies. Cyber technology can do this without firing a single bullet. Cyber-security in this case, is not about saving information or data, it's about securing the different life systems regulated by computers. It is useful, here, to recall that NATO itself between 2014 and 2016 brought the domains of operations from 4 (land, air, sea, space) to 5, adding the cyber battlefield. It is proof that today cyber-protection cannot be ignored in the safeguard of nations because of the repercussions for the health and safety of citizens.

NATO also reached this decision following the campaign of attacks in Estonia, when in April and May 2007, it became the target of several coordinated cyber attacks. Over a three-week period, government and parliamentary portals, ministries, news outlets, internet service providers, major banks, and small businesses were all targeted, predominantly by a Distributed Denial of Service (DDoS). The offensive coincided with the Estonian government's decision to relocate the 'Bronze Soldier Memorial' in Tallinn, which led to significant civil disturbance in both Estonia and Russia. The vast majority of malicious network traffic was of Russian-language origin and seemed politically motivated. The Russian government denied any involvement, however, the cyber attacks were accompanied by

SIEMENS

Siemens Smart Infrastructure and NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) have signed an MoU to continue cooperation on cybersecurity of critical infrastructure.

hostile political rhetoric by Russian officials, unfriendly economic measures, and refusal to cooperate with the Estonian investigation in the aftermath of the attacks, all of which likely to have encouraged the perpetrators. The attacks caused some disruption and economic cost to Estonia, but more importantly, they exposed Estonia's vulnerabilities, and demonstrated the potential of cyber war to cause lasting damage if intended.

Following these attacks, Jaap de Hoop Scheffer, NATO Secretary General (2004-2009), declared:

"These cyber attacks have a security dimension without any doubt and that is the reason that NATO expertise was sent to Estonia to see what can and should be done. […] Does this have a security implication? Yes, it does have a security implication. Is it relevant for NATO? Yes, it is relevant for NATO. It is a subject which I am afraid will stay on the political agenda in the times to come."

We can only confirm that the Secretary General was absolutely right and today more than ever the issue of cyber security is one of the top priorities for every government, not only for the economic aspects related to financial fraud or the theft of intellectual property that impoverishes a state, but above all because the digitalization of all critical infrastructures and the ubiquitous diffusion of objects connected to the network exponentially increases the potential surface exposed to cyber attacks that can easily have repercussions and impact on the very life of their citizens.

To conclude, we are much more interconnected, we have many more services and "comforts" thanks to the spread of digital technology, but at the same time we are much less safe.

ANDREA BIRAGHI *is Cyber Security and Digital Transformation advisor, and former Chairman of European Organisation for Security.*