HYBRID ATTACKS ON CRITICAL INFRASTRUCTURE

Cyberspace is the latest battlefield for exploiting a supposed enemy or rival's known and, above all, unknown vulnerabilities. Cyber weapons are malicious computer programmes designed to attack an essential cyber-physical system in order to disrupt its normal operation or destroy it. Unlike manufacturing conventional weapons of war, these types of attack on critical infrastructure do not require multi-million dollar investments and their ability to be replicated is highly effective. But how are they produced? Who makes them and how are they distributed? Who do they serve? And how can we defend ourselves?

Manel Medina Llinàs
Director of the Master's in Cybersecurity Management at UPC-School, and Coordinator of the Technical Training Office of the Catalan Cybersecurity Agency

CIDOB REPORT
08- 2022

Some years ago, orbital space joined the traditional battlefields of land, sea and air; more recently, the talk is of cyberspace. In traditional settings, weapons can be seen from planes and satellites, and states and large coalitions like NATO have a good handle on what the other side possesses. But cyberweapons are almost intangible and data networks have removed the need even for a memory chip to cross a border. In the event of a cyber war, this makes establishing an opponent's destructive capacity tricky.

Let's start by establishing what a cyberweapon is. Until less than a decade ago, any malicious computer programme capable of attacking our enemy at any time was considered a cyberweapon. In order to avoid detection and being rendered useless before being deployed, the attack is normally based on one or more methods of exploiting a vulnerability in a programme installed on the victim's computer systems, known as a zero-day vulnerability. Purists would say that for something to be

considered a cyberweapon it must be «destructive», in other words, it must cause material damage to critical infrastructure and/or people. Hidden cyberweapons must therefore be sought out in so-called cyber-physical or internet of things (IoT) apparatus like industrial control systems (ICS), railways, telecommunications, essential utilities (water, electricity, gas) and health infrastructure, among others. Along with the fact that many of these systems are not properly updated, this means they can even be attacked via known vulnerabilities.

An accessible and persistent threat

Many cyberweapons aim to remain hidden and unnoticeable as they await the order to destroy the target. This is what is called an advanced persistent threat (APT). In many cases, it is even difficult to identify the development team. The most powerful include military and government cyber-intelligence units, but, as with their physical equivalents, cyberweapon manufacturers exist – criminal organisations that sell them on more or less hidden markets. The Israeli company NSO, which has recently become more widely known, sells cyberweapons like its Pegasus spyware to states, theoretically to support the fight against terrorism.

To identify cyberweapons, we must look beyond cyber warfare and search in surveillance and biometric identification tools, for example, which can impact the supply chain and potentially collect user and citizen data.

This is an «affordable» type of threat that does not need the multi-million dollar investment required to manufacture war equipment and weapons. Discovering new vulnerabilities and developing tools to exploit them is much cheaper. Above all, these weapons can be replicated hundreds or thousands of times at hardly any additional cost. They can be developed by *grey* organisations, which then market them to governments, openly, and to criminal groups in a more covert way.

But, the catalogue of cyberweapons may also include an apparently less bellicose tool: disinformation, which can also be used to attack critical infrastructure. Using conventional information channels (social networks, media, etc.) disinformation selectively targets people with infrastructure management capacity and may be complemented by cyber-(counter) intelligence. The spy software used by intelligence departments may also be attacked, leading it to generate false information about the enemy and prompting decisions that can lead to a trap that is difficult to escape, blocking the infrastructure or causing control of it to be lost. But the most common use of disinformation as a form of attack in cyber-physical environments is

altering the data provided by physical systems sensors. The aim is to provoke erroneous reaction decisions in infrastructure management systems, such as, for example, attempting to correct a non-existent problem and thereby creating another, inverse, problem that goes undetected. This is what happened in the Stuxnet attack, where a virus (cyberweapon) destroyed Iranian uranium centrifuges, while avoiding detection by changing the revolutions per minute data recorded to show normal levels. There are several ways to achieve this sensor data modification: a) by substituting or introducing a fraudulent sensor; b) by altering the sensor's software to make it give false readings; or, c) by modifying the data stored in a server or cloud. If the data transmission, storage or processing is not adequately protected, it is very easy to alter it without it being noticed, until the damage is irreparable or unavoidable.

Cyber weapons can be hidden anywhere: a chip, a programme, a memory card, or stored in the cloud. A cyberweapon is made up of «bits» that can be hidden in multiple ways and are therefore undetectable. They may remain dormant for years in an energy production plant, a railway or air traffic control centre, or in the office of a government official or manager without anyone noticing. The 2014 Mandiant report warned of this, revealing dozens of organisations that APT1, a Chinese cyber espionage software development team, had targeted and entered, remaining hidden from its victims for an average of 229 days, and in some cases being installed for years (McWhorter, 2021).

CYBER WEAPONS CAN BE HIDDEN ANYWHERE: A CHIP, A PROGRAMME, A MEMORY CARD, OR STORED IN THE CLOUD. A CYBERWEAPON IS MADE UP OF «BITS» THAT CAN BE HIDDEN IN MULTIPLE WAYS AND ARE THEREFORE UNDETECTABLE. THEY MAY REMAIN DORMANT FOR YEARS IN AN ENERGY PRODUCTION PLANT, A RAILWAY OR AIR TRAFFIC CONTROL CENTRE, OR IN THE OFFICE OF A GOVERNMENT OFFICIAL OR MANAGER WITHOUT ANYONE NOTICING.

In a cyber war, the computers or devices that control a country's infrastructure are invaded. But we are unaware of them until someone «presses the button» that wakes up the agents (malicious programmes) asleep in their hideouts, which then begin to act, bringing the infrastructure that keeps the country running to a halt.

Hybrid conflict is warfare with an added layer of remote operations. Unlike conventional warfare, where the invading army can be seen on the streets, preparations for a cyberattack are imperceptible because there are no troop movements across any borders. In cyberspace there are no borders.

The danger of cyberweapon proliferation

Having established the scenario and the weapons, we shall now look at the dangers these new cyber threats pose and the factors that make them attractive and dangerous.

The cyber war is already underway: cyberweapons are being deployed on the internet even if we cannot see them. Weapons more powerful than missile launchers and tanks are being marketed, inadvertently to most citizens and countries because they are just data bits. As with traditional weapons, there are «legal» purchases made by governments and other «illegal» purchases made by individuals or criminal groups with an interest in spying on a commercial or strategic rival in order to supplant them, or to take control of infrastructure or destroy it, as BlackEnergy did on December 23rd 2015, when it shut down and destroyed the control programmes of Ukrainian power plants.

Cyber weapons can be produced by cyber-mafias, by the cyber units of conventional armies or governments, or by companies working on their behalf. Of particular concern to states is that designing and building a cyberweapon is within the reach of any small country or organisation, as the production requires no expensive raw materials. Hybrid warfare is thus preferable to traditional warfare because it is more profitable. Russia and other European countries distribute this type of cyberweapon, which is often produced in public–private collaboration projects. The tools are often produced by governments and large multinational organisations, although the supply chain has not yet been analysed.

In general, when a hybrid cyberattack takes place, we don't know who ordered it, who perpetrated it or when preparation for the attack began. In some cases, however, it is very clear who is responsible. Following the presentation at the 2016 Berlinale of Zero Days, a documentary on the Stuxnet attack, the United States and Israel were condemned for coordinating the cyberattack to destroy Iranian uranium enrichment centrifuges – although neither country accepts responsibility. In other cases, allocating blame is more difficult. The war in Ukraine has also been waged in cyberspace and both sides have accused the other of false flag attacks. For example, in the attacks on Ukrainian government web services in January 2022, the attackers left false leads that framed Ukrainian and Polish dissidents as a way to divert attention from Russia as the attacker. Determining the origin of an attack is therefore essential.

In order to establish the perpetrator of a cyberattack, the cyberweapon's code is analysed for comments or names that may indicate the country or language used by the developer. But the developer may know about

this technique and leave false clues in the target's language in order to simulate a false flag attack. To further complicate matters, the developer may not attempt to hide their identity or ideology, but the actual attacker may be a different entity to the developer if the tool has been sold on the black market. Another technique for detecting the attacker is to examine the origin of the attack. But these clues may not be conclusive either, as intermediate servers can be used to conceal the origin of the attack, such as those on the Tor network. Everything discussed so far opens up a multitude of attack strategies at various levels and requires the deployment of defence strategies based on «mistrusting everything».

Defence strategies against hybrid attacks

Two main types of hybrid attack can be identified: a) those related to (dis) information, which aim to provoke decision-making errors; and b) those that directly affect physical systems.

Analysing public disinformation activities like the fake news that circulates on the internet and influences public perceptions and opinions may lead us to conclude that their success in sowing social destabilisation can be more effective than even attacks on infrastructure control databases. Disinformation can provoke violence, and is another way of starting conflicts or attacks on infrastructure.

HYBRID WARFARE IS PREFERABLE TO TRADITIONAL WARFARE BECAUSE IT IS MORE PROFITABLE.

Disinformation attack strategies are based on the creation and subsequent distribution of news through networks of influential or fake users (social bots) in order to increase their spread among bubbles of like-minded users. In order to defend against this type of attack the distributors of fake news must be identified and blocked; however, social network administrators are not always willing to collaborate, due to the potential advertising revenues associated with these types of dissemination campaigns.

Meanwhile, direct hybrid attacks against critical infrastructure from cyber-space raise the problem of a lack of experience among those responsible for physical security, a lack of collaboration among employees, and managers' lack of conviction about conceiving, planning and implementing appropriate cyber protection measures.

NATO countries declared their readiness to respond to cyberattacks in July 2021, but they are failing to properly take Russia's hybrid attack activities

into consideration. For example, the disruptions to the Colonial Pipeline, the largest fuel pipeline in the US, the 2020 hacking of SolarWinds, the provider of widely used infrastructure system management tools, and widespread ransomware attacks on other NATO countries were all orchestrated by Russia, either directly or through cyber-mercenaries, and yet the Atlantic Alliance has yet to react. One reason may be the European Union's new NIS 2.0 Directive, which describes how to deal with cyberattacks, clearly differentiating between critical and essential services, and emphasising that only the latter should be considered a defence matter.

In short, governments are taking administrative and legal steps to promote cyber protection, above all in relation to essential and critical infrastructure and its providers, and throughout the supply chain of essential components for their service. Those managing this infrastructure must identify which services and assets are most valuable and which are most vulnerable, in order to protect them as efficiently as possible. And, finally, it will also be necessary to plan the operational maintenance of the installed protection mechanisms and properly train all the personnel involved. The proper functioning of states depends on it. Rebuilding after a wide-ranging cyber-attack (cyber war) may be relatively quick, but a hybrid attack can be more difficult to recover from, especially if damage to infrastructure is irreparable and rebuilding requires components that are expensive or hard to find on the market.

Reference

McWhorter, Dan. «APT1: Exposing One of China's Cyber Espionage Units». *The Mandiant Intelligence Center* (2021) (online) https://www.mandiant.com/resources/apt1-exposing-one-of-chinas-cyber-espionage-units