
mirror object to mirror
mirror_mod.mirror_object
operation == "MIRROR_X":
irror_mod.use_x = True
irror_mod.use_y = False
irror_mod.use_z = False
operation == "MIRROR_Y":
irror_mod.use_x = False
irror_mod.use_y = True
irror_mod.use_z = False
operation == "MIRROR_Z":
irror_mod.use_x = False
irror_mod.use_y = False
irror_mod.use_z = True
selection at the end -add
_ob.select= 1
er_ob.select=1
ntext.scene.objects.acti
("Selected" + str(modifier
irror_ob.select = 0
bpy.context.selected_ob
ata.objects[one.name].se
int("please select exact
OPERATOR CLASSES
types.Operator):
X mirror to the selected
ject.mirror_mirror_x"
rror X"
ntext):
ext.active_object is not

Looking for Space security

BY ANDREA BIRAGHI

Space is a vital framework of the planet's infrastructure, but it is also a potential battleground highlighting the security challenges and dangers it entails. What are the key vulnerabilities and how can the international community guarantee a secure space environment?

Economies and governments around the world are increasingly relying on space-dependent infrastructures; a new frontier for cyber security has therefore now opened.

It seems like a bygone era when we needed to refer to a paper map to orient ourselves in a new city or find the best hiking trails. Today, most of us simply open Google Maps on our smartphone to find our exact location, thanks to the GPS satellites orbiting 20,200 km above our heads. Just a few years ago, connecting to the Internet on an airplane was unheard of. We can now navigate on a transatlantic flight thanks to communications satellites some 35,000 kilometres away.

Most of us take space technology for granted in everyday life. With satellites supporting global communications - not to mention a range of daily economic, government and military functions - it should come as no surprise that it is also a potential target for cybercriminals. As the internet itself extends to the last frontier, potentially to human colonies on Mars, when SpaceX or some other agency or company will manage to create them in the not-so-distant future, it is important to explore the broader implications of cybersecurity in the era of Space.

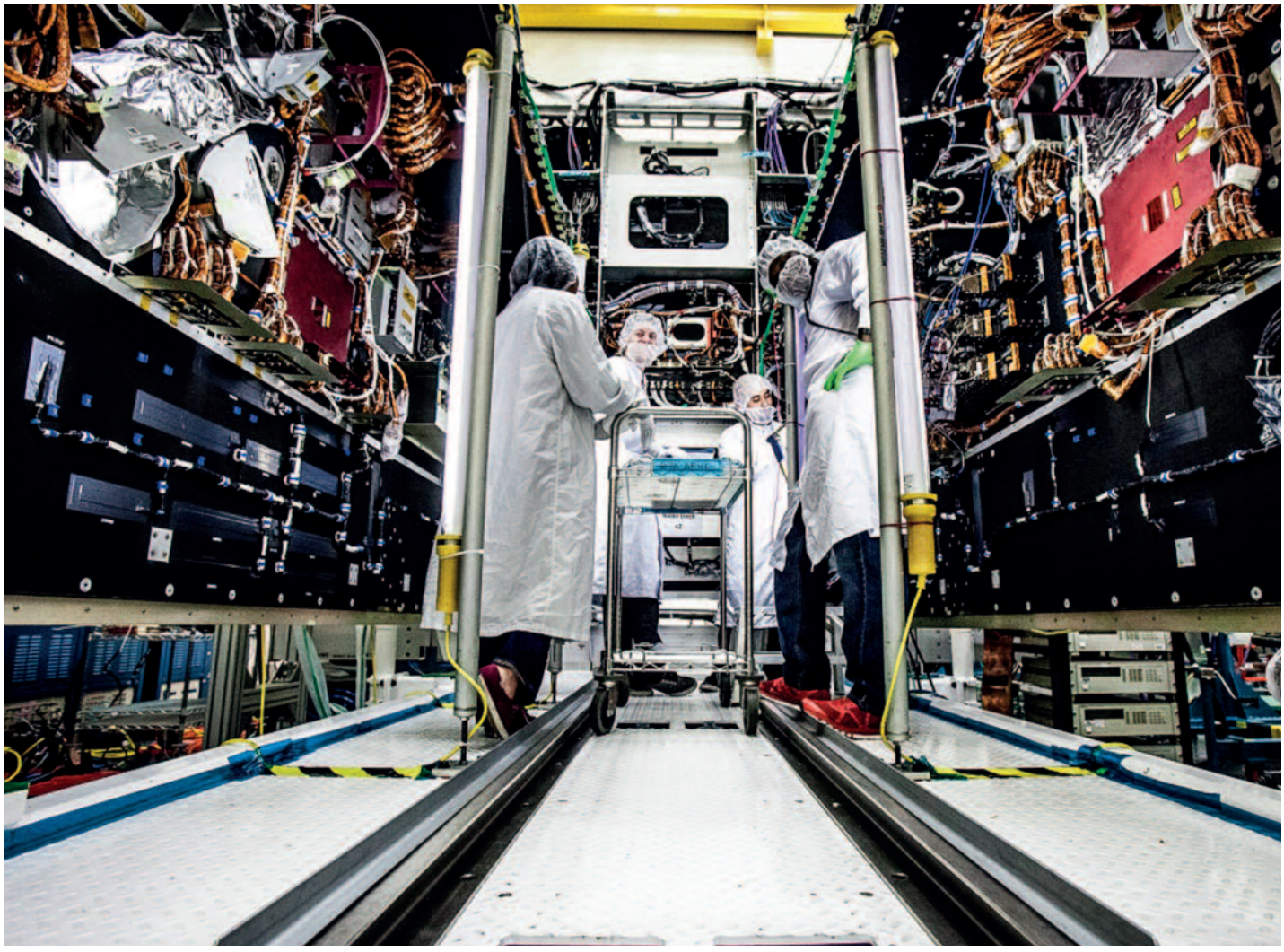
Our overwhelming dependence on Space technology puts us in a precarious position. In industries such as transportation and logistics, location data is regularly recorded in real time by GPS satellites and sent back to offices allowing teams to monitor drivers and assets. Organizations that have remote outposts or ocean-going vessels obviously cannot connect online via a mobile or cable network, they must instead use satellites for communications. Additionally, satellites store sensitive information they collect on their own, which could include images of reserved military installations or critical infrastructure. All of these data are interesting targets for various types of cyber criminals.

The continuous proliferation of space exploration will only increase the reach of our connected environment. Given the high value of the data stored on satellites and other space systems, they are potentially interesting targets for anyone who wants to exploit this situation to make an illegal profit. Although residing in the vacuum of deep space makes them less vulnerable to physical attacks, space systems are still controlled by computers on the ground. This means that they can be infected just like any other computer system closer to us.

Attackers do not even need to be hackers coming exclusively from nations dealing with or working with Space, just as they do not even need to have direct physical access to control systems belonging to organizations like NASA, ESA or Roscosmos. In such an interconnected world, they really have an easy time.

While satellite navigation systems such as GPS

Advances in digital technology impel satellite manufacturers to provide software-defined solutions that are cheaper and more flexible.



MES

Military satellite program managers are demanding greater on-orbit flexibility to reconfigure payloads based on evolving battlefield requirements.

(USA), GLONASS (Russia) and Beidou (China) may not be the easiest targets to hack, there are dozens of other global communications satellite owners who absolutely do not have the same level of protection. In addition, thousands of other companies lease bandwidth from satellite owners to sell services such as satellite TV, telephone, and the Internet. Then there are hundreds of millions of citizens and businesses around the world who use them. In other words, it is a very large potential attack surface that is directly connected to the Internet.

According to Will Roper of the US Air Force, we still rely on the cybersecurity procedures of the 1990s to protect orbital satellites. This is because Space-based systems are typically built in a closed box environment or (pardon the pun) in a vacuum. The problem is that almost all systems today contain software: the International Space Station is based on the Linux operating system and the Mars Curiosity Rover runs the highly specialized VxWorks on its on-board computers. The criticality with any type of software is that it can contain bugs that cybercriminals could try to exploit. For example, imagine the kind of ransomware that cybercriminals could ask for if they took over a $ 400 million satellite. To demonstrate the risk, in addition to raising public awareness on their bug bounty program, the US Air Force recently challenged hackers to attempt to hijack a satellite in orbit.

Like many technologies we have come to rely on, Space systems are largely the result of national security objectives and military advancement. The Space race itself was a competition between the United States and the Soviet Union. Fortunately, nations have come together to ban weapons of mass destruction from Space and promote the peaceful use of the last frontier. Unfortunately, the world's greatest powers are not doing as good a job of keeping Space a peaceful environment for all and have begun to put pressure on each

LOCKHEED MARTIN

The Global Positioning System, better known as GPS, marked its 25th year of operation on 27 April 2020. GPS III is pictured through an artist's rendition.

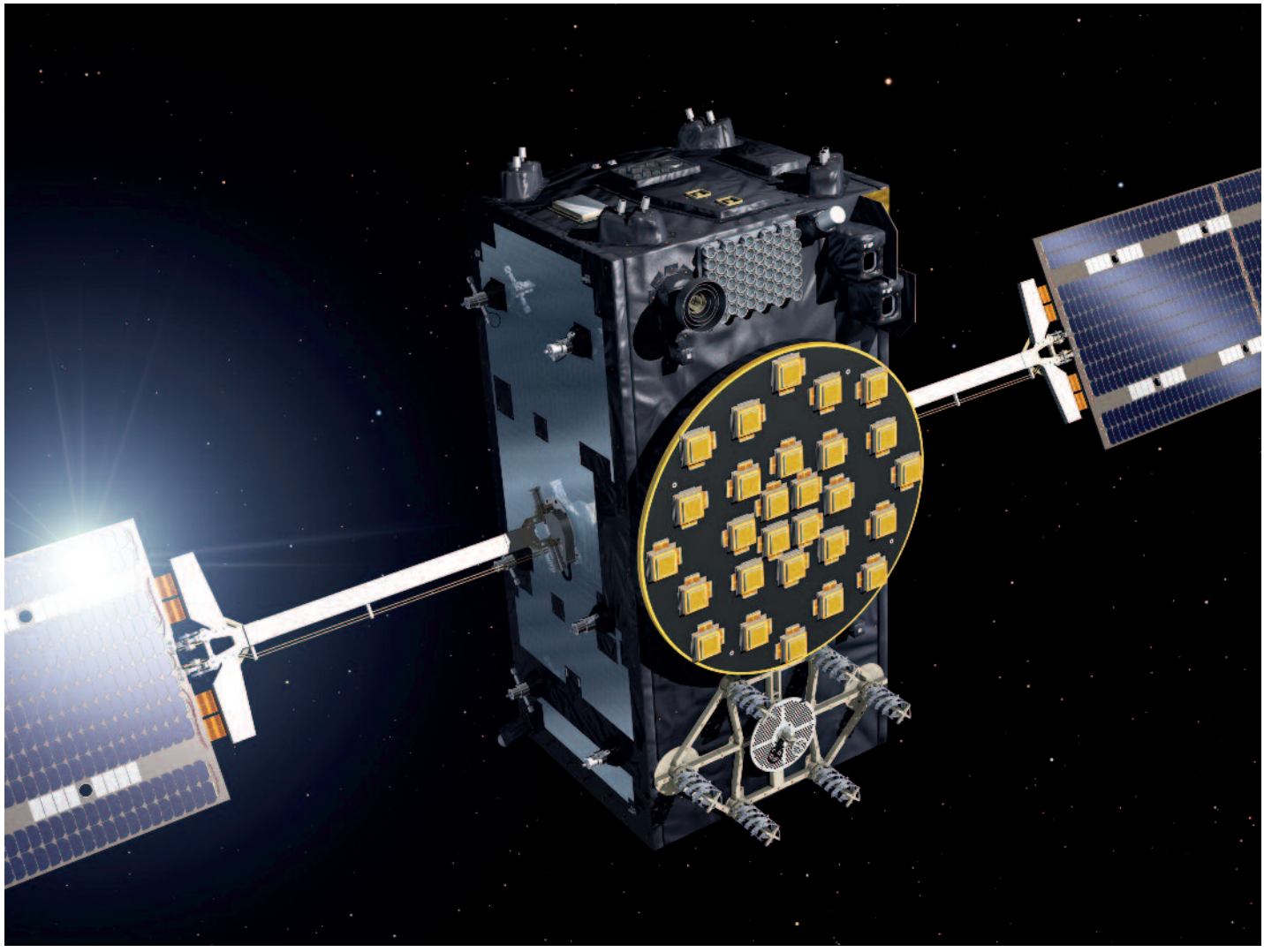
other by testing controversial new capabilities.

Indeed, reconnaissance satellites have been deployed in Space since the 1950s, and all the superpowers in the world now depend on them to make strategic military decisions. Whether it is detecting missile launches or intercepting stray radio waves, these machines regularly handle some of the most sensitive data of all - the kind of information that could cause a war if it gets into the wrong hands. Of course, this increases the incentives for state-sponsored attackers to hack their rivals in the same way that commercialization of Space makes communications satellites attractive targets for cybercriminals.

State-sponsored attacks against Space assets could manifest themselves in various ways: the disturbance of the GPS signal could render missile guidance systems useless. Access to unencrypted satellite links could allow hackers to hijack satellite communications. Civilian and military operations could also be directly affected if the United States were to turn off the GPS that is wholly owned by the US government while being used around the world.

Precisely to deal with such an eventuality, in 2003, Europe started the Galileo project, to create a new positioning system. This project was born from the need to avoid the US commercial monopoly on the positioning service, which until then was the only one available. For a long time, in fact, the only existing systems were GPS and GLONASS, the Russian version, but the latter remained inefficient for a long time. For this reason, the exclusive use of the American positioning service was established worldwide, as it is the only one available globally.

The idea was born, not only to avoid a commercial monopoly, but also (and above all) for the desire to be immune from the possibility that the American government could decide the fate of the world positioning system, given that the US reserves to themselves the



ESA

Scale model of the Galileo GPS satellite.

right to be able to decrease the accuracy of the service or even to turn it off completely. An event not only theoretical, but which took place during the Gulf War.

Officially launched in 2003, the European Galileo project required an agreement between the European Union and ESA (European Space Agency); unlike GPS, the Galileo positioning system guarantees the highest possible accuracy, reliability and exactness at all times, and continuity of service. It is aimed at the global system and is characterized by high coverage, designed for not only military but also mainly civil use. In fact, it provides for an improvement in positioning accuracy, reducing the probability of error, and a prompt response to any emergencies.

Born much later than GPS, it was natively equipped with security systems to avoid cyber-attacks and/or jamming. In particular the Galileo Programme incorporates in its service baseline a Navigation Message Authentication service, which consists of the digital signature of the navigation data of the Open Service (OS), to ensure the data authenticity, and a Commercial Authentication Service (CAS), which consists of the encryption of one of the Galileo signals to protect against signal replay attacks.

This is a clear and tangible demonstration of how seriously the cyber security risk is correlated to the Space technology.

Returning to the broader context, the biggest challenge facing Space age cybersecurity then is the fact that so few organizations, all hugely dependent on funding from a handful of governments, ultimately have control over all Space assets. Almost all of the world's launch facilities are owned by the governments of the United States, Russia, China, France, Japan, and South Korea. Further down the hierarchy, there are dozens more companies that own satellites and many

AXIOM

companies that own data collection systems on the earth's surface.

This depicts a rather poor picture for the data democratization of information: the ability for end users to access digital information. With the power to ensure access and management of digital assets in Space in the hands of so few, the risk of attacks is lower, but such systems are also high-value targets for state-sponsored attackers.

We also take into account that things are gradually changing with the democratization of Space and data. Private companies already promise to offer faster and cheaper ways to access Space. Some companies are even working to put data storage in the cloud where it is safest from data breaches that rely on physical interaction: in Space. However, if someone has digital access, it is all it takes to compromise the system, even if they reside thousands of miles away from the earth. At the same time, it is difficult to argue that Space is democratic when it is an exclusive frontier only for the richest individuals, businesses and governments in the world.

This will undoubtedly change, but we may have to wait a few centuries before that will happen, in the meantime we will witness a silent war between great powers that will also move the dispute over data, that is now a daily occurence here on earth, up into Space.

In an era in which privileged individuals search constantly for the next experience to obsess over and post about on social media, space truly remains the final frontier, a luxury that only the one percent of the one percent can afford.

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