

16th Nov [European Cyber Week](#)

23rd-24th Nov [Benelux Cyber Security](#)

[Summit](#)



**Center for Cyber Security and
International Relations Studies**

Cyber Policy, Diplomacy & Legal Framework

- [USA signs internet freedom and no-hack pact it's ignored since 2018](#)

The United States has signed up for The Paris Call for Trust and Security in Cyberspace – an international effort to ensure the internet remains free and open, and an agreement to put critical infrastructure off limits to electronic attack by sovereign states and other actors.



- [Why the time has come to embrace the Zero-Trust model of cybersecurity](#)

The concept of Zero-Trust has been around for a while. While this model has been widely recognized as an effective approach to prevent data breaches and mitigate the risk of supply chain attacks, its adoption across the private and public sectors has been slow and inconsistent. This is about to change.

- [China May Seek Cyber Check for HK Listings of Firms Holding Data](#)

China may require a cybersecurity review for companies holding data that plan to go public in Hong Kong, if it's decided that the listing will potentially have an impact on its national security

Cyber Security

- [FBI probes cyber-attack emails sent from internal server](#)



The FBI has launched an investigation after thousands of fake email messages were sent from one of its servers warning of a possible cyber-attack. The messages purported to be from the US Department of Homeland Security.

- [BotenaGo botnet malware targeting millions of IoT devices](#)

The IT security researchers at AT&T Alien Labs have tracked down malware utilizing over 30 different exploits to compromise routers and Internet of Things (IoT) devices.



UNIVERSITÀ
DEGLI STUDI
FIRENZE

DSPS
Dipartimento di
Scienze Politiche
e Sociali



Centro interdipartimentale
Studi
Strategici
Internazionali
Imprenditoriali

According to their analysis, the malware is an early beta version linked with the infamous Mirai botnet. They opined that this malware is difficult to detect and can exploit millions of internet-connected devices.

- [Ransomware attacks are getting more complex and even harder to prevent](#)
Ransomware attackers are probing known common vulnerabilities and exposures (CVEs) for weaknesses and quickly capitalizing on them, launching attacks faster than vendor teams can patch them. Unfortunately, ransomware attackers are also making attacks more complex, costly, and challenging to identify and stop, acting on potential targets' weaknesses faster than enterprises can react.

Cyber Warfare, Intelligence and Terrorism

- [Iran Suffered A Cyber Attack Shutting Down Smart Gas Stations With Hacked Electronic Signs Allegedly Mocking The Supreme Leader](#)

Iran's President Ebrahim Raisi acknowledged a massive cyber-attack that disrupted gas stations across the country, blaming it on an unnamed country allegedly seeking to create disorder and disruption.



- [North Korean Lazarus Hacking Group Leverages Supply Chain Attacks To Distribute Malware for Cyber Espionage](#)

North Korean threat actor Lazarus group has resorted to supply chain attacks similar to SolarWinds and Kaseya to compromise the regime's targets, according to cybersecurity firm Kaspersky. Kaspersky's Q3 2021 APT Trends report says that "Lazarus developed an infection chain that stemmed from legitimate South Korean security software deploying a malicious payload."

- [The cyber battlefield against China and Russia is constantly shifting. Here's how the NSA is trying to stay on top.](#)

In the battle over cyberspace, adversaries to the United States are continually switching up their methods to hack U.S. systems, a senior National Security Agency official said Wednesday. That means the U.S. must in turn keep shifting the tools and techniques it uses to counter hackers from nations like China, Russia, Iran and North Korea — and team up with the private sector to do so

Cyber Opportunities: Economy, Research & Innovation



- [IBM creates largest ever superconducting quantum computer](#)

IBM has created the world's largest superconducting quantum computer, surpassing the size of state-of-the-art machines from Google and from Chinese researchers. Previous devices have demonstrated up

to 60 superconducting qubits, or quantum bits, working together to solve problems, but IBM's new Eagle processor more than doubles that by stringing together 127.

- [Sure, there's hype. But blockchain has concrete space applications](#)

Since it burst onto the scene with Bitcoin, blockchain has been linked with other cryptocurrencies, digital artwork and extraordinary energy consumption. The heart of blockchain, though, is a distributed ledger with important applications for the space sector.

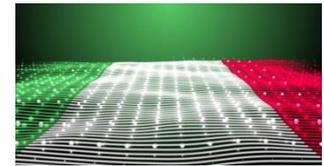
- ['Yeah, we're spooked': AI starting to have big real-world impact, says expert](#)

A scientist who wrote a leading textbook on artificial intelligence has said experts are "spooked" by their own success in the field, comparing the advance of AI to the development of the atom bomb.

Italian Focus

- [To manage cyberspace. Draghi's new strategy](#)

An Italian government document produced by the Farnesina and Palazzo Chigi sets out a road map for the governance of cyber space. From human rights to the defense of sovereignty up to aggression by foreign states.



- [Italy and Europe under attack; the risk of the healthcare system](#)

From the discovery of the fake Green Passes, the latest that of Bettino Craxi, to the alleged compromise of the systems of the Ministry of Health, there are many elements that confirm that the healthcare system of Italy and Europe is under cyber attack.

- [Attack against SIAE, phishing and ransomware are the number one threat for enterprises](#)

After the attack on the SIAE, Proofpoint confirms that in 2020, ransomware affected 66% of companies. While phishing costs companies \$ 14.8 million a year. The SIAE was hit by cybercriminals who entered its systems thanks to a phishing attack that allowed them to access a large amount of sensitive data.

European Focus

- [Can Europe compete in the quantum 'space race'?](#)



Quantum information science has long languished in an academic corner of the tech sector. But recent advances mean that the sector has taken on geopolitical significance. With several nations rushing to develop their own quantum systems, the quantum competition has started to resemble a new "space race."

- [Spain adopts EU copyright law, paving way for Google News to return](#)

Spain has adopted a European Union copyright directive that allows third-party online news platforms to negotiate directly with content providers, the government said on Tuesday, setting the stage for Alphabet's Google News to return to the country.

- [French AI strategy: Tech sector to receive over €2 bln in next 5 years](#)

A total of more than €2 billion in public and private funding will be poured into French tech over the next five years to create future champions at the national and European levels, according to phase two of the national AI strategy presented by government ministers.