



Cyber Policy, Diplomacy & Legal Framework

- [The UN Struggles to Make Progress on Securing Cyberspace](#)

The stability of global financial, healthcare, and security systems is increasingly at risk from cyber threats. As more critical infrastructure and industrial control systems are connected to the internet, a growing number of state and nonstate actors have developed, purchased, and deployed tools, weapons, and strategies to deter and disrupt cyberspace.



- [The Emerging Biden Administration Cyber Strategy](#)

The recent surge in high profile cyber-attacks has correlated with a similar surge in cybersecurity policies and announcements from the Biden Administration. These actions are a mix of explicit requirements for federal agencies, federal contractors, and critical industry entities, and broader recommendations for industry and the public-at-large.

- [Brazil-Portugal undersea link goes live](#)

A new submarine cable linking Brazil and Portugal has gone live as part of efforts around improving connectivity in the South American country. The undersea link is 6.200 kilometers long and connects the Brazilian city of Fortaleza to Sines, in Portugal and allows data traffic at a speed of 100 terabits per second, with response time of 60 milliseconds

- [So Far, Yet So Close: Japanese and Estonian Cybersecurity Policy Perspectives and Cooperation](#)

Estonia and Japan are among the leaders in cyber diplomacy and cybersecurity on the global stage, Japan also being a key strategic partner for the EU and NATO. They have many similarities in their approaches to cybersecurity and state behaviour in cyberspace, which has established solid ground for closer bilateral ties.

fastly

Cyber Security

- [Fastly internet outage explained: How one customer broke Amazon, Reddit and half the web](#)



UNIVERSITÀ
DEGLI STUDI
FIRENZE

DSPS
Dipartimento di
Scienze Politiche
e Sociali



Centro interdipartimentale
Studi
Strategici
Internazionali
Imprenditoriali

The internet was brought to its knees by a massive outage on Tuesday (8th June). Now we know exactly what the cause was, and how the problem was fixed.

- [How an app to decrypt criminal messages was born 'over a few beers' with the FBI](#)
Australian and U.S. law enforcement officials on Tuesday announced they'd sprung a trap three years in the making, catching major international crime figures using an encrypted app.
- [The EU's Response to SolarWinds](#)
While EU's issuance of the declaration of solidarity in response to the SolarWinds cyber campaign is a sign of progress, it fails to provide clarification on what, if any, further actions can be expected from Brussels.
- [A Mystery Malware Stole 26 Million Passwords From Windows PCs](#)
Researchers have discovered yet another massive trove of sensitive data, a dizzying 1.2 TB database containing login credentials, browser cookies, autofill data, and payment information extracted by malware that has yet to be identified.

Cyber Warfare, Intelligence and Terrorism

- [Ransomware: Russia told to tackle cyber criminals operating from within its borders](#)
The United States and other G7 countries have warned countries that allow ransomware groups to operate from within their borders, and don't make any efforts to deter their actions, that they will be held accountable for their lack of action.
- [Pros and cons of the cognitive war](#)
The advantage in cognitive warfare, which represents a mixture of cyberwarfare and psychological warfare, goes to those who manage to move first and adequately choose the time, place and means of the offensive.
- [REvil ransomware gang claims breaching US nuclear weapons contractor](#)
Sol Oriens, a US-based nuclear weapons contractor, has become a cyberattack from the REvil ransomware gang. Hackers have said that they will auction the data that was stolen during the attack.
- [Dominant companies a fat target for hackers and cyberwarfare](#)
The recent ransomware attacks that temporarily crippled major U.S. suppliers of beef and fuel offer a frightening glimpse of the chaos cyberwarfare could sow, especially if the perpetrators were more focused on damaging critical infrastructure than reaping a financial bounty.



Emerging Technologies



- [Researchers create an 'un-hackable' quantum network over hundreds of kilometers using optical fiber](#)

Researchers from Toshiba have successfully sent quantum information over 600-kilometer-long optical fibers, creating a new distance record and paving the way for large-scale quantum networks that could be used to exchange information securely between cities and even countries.

- [Tanzania Considers Crypto—And Boosts Bitcoin—As Nations Line Up Behind El Salvador To Embrace Decentralized Finance](#)

Tanzania became the latest country to signal its support for digital assets this weekend as its president instructed financial authorities to prepare for widespread use of cryptocurrencies, elevating bitcoin prices further after El Salvador became the first country to make bitcoin legal tender last week and Elon Musk outlined plans for Tesla to resume accepting bitcoin as a form of payment.

- [What are the key concerns around artificial intelligence and the right to privacy?](#)

In its submission to the UN report on AI and the right to privacy, Privacy International highlights concerns about facial recognition technology and argues for effective laws accompanied by safeguards to ensure AI applications comply with human rights.

Italian Focus

- [More than just a new Agency; the main point of the new cyber decree](#)

The reform of cyber governance, announced by Gabrielli on his debut at the helm of the Services, is about to become a reality. A passage of great political importance, with a timing that is anything but casual.

- [Italy unveils plans for cybersecurity agency to aid its cloud strategy](#)

Italy plans to set up a national agency tasked with combating cyber attacks as it continues work on its unified cloud infrastructure. The country is one of many European nations attempting to enhance their cybersecurity capabilities. Many aspects of Italy's digital security, which are dispersed among various Ministers and state bodies, are to be brought together under the authority of the Prime Minister.

[Leonardo, Microsoft team up to help digitalize Italy's public system](#)

Italian defence group Leonardo (LDOF.MI) and U.S. tech giant Microsoft (MSFT.O) have teamed up to boost the digital transformation of Italy's public administration and critical national infrastructures, the two companies said in a statement.

- [Data of seven million vaccinated Italians for sale](#)



There are 6,583,199 (89%) email addresses and 5,324,895 (72%) passwords in an online database for sale. A good part would appear to come from one or more regional booking portals, the largest one being the Campanian. Investigations are ongoing, here's what we've seen so far

European Focus



- [European Parliament amps up pressure on EU-US data flows and GDPR enforcement](#)

European Union lawmakers are facing further pressure to step in and do something about lackadaisical enforcement of the bloc's flagship data

protection regime after the European Parliament voted yesterday to back a call urging the Commission to start an infringement proceeding against Ireland's Data Protection Commission (DPC) for not "properly enforcing" the regulation.

- [EU security strategy a 'step up' on cyber leadership, says Brussels](#)

The European Union (EU) has published details of its new EU Cybersecurity Strategy, intended to bolster Europe's collective resilience against cyber threats and ensure citizens and businesses can benefit from trustworthy and reliable digital services. The bloc hopes the move will enable it to step up its leadership on international cyber security norms and standards, and strengthen international collaboration.

- [Eu lawmakers call for stronger cyber security measures](#)

Cybersecurity is one of the biggest challenges in the digital age. Because of this, MEPs have demanded that the EU improves its security against cyber threats. In a resolution on the bloc's Cyber Security Strategy, which is also known as EUCSS, lawmakers have called for new strategies to deal with new and evolving threats, that are becoming increasingly sophisticated and often include a geopolitical dimension.

- [Reported Amazon fine \(\\$425M\) 'biggest test' of GDPR enforcement yet](#)

The online retailer—whose European headquarters are based in Luxembourg—could be fined more than \$425 million (€350 million) under the EU's General Data Protection Regulation (GDPR) over the way it collects personal data and uses it for marketing purposes, according to the Wall Street Journal.



UNIVERSITÀ
DEGLI STUDI
FIRENZE

DSPS
Dipartimento di
Scienze Politiche
e Sociali



Centro interdipartimentale
Studi
Strategici
Internazionali
Imprenditoriali