



Upcoming Events

April 17

[Cyber Crime Conference](#)

April 22

[The International Conference on Codes, Cryptology And Information Security](#)

April 25

[AI&Big Data EXPO](#)



Cyber Policy, Diplomacy & Legal Framework

- [Trump's homeland security purge worries cybersecurity experts](#)

Former Customs and Border Protection commissioner was appointed acting secretary of the Department of Homeland Security, leaving to wonder what will happen to the rest of DHS' many essential responsibilities, including cybersecurity.

- [Huawei admit Chinese law obliges companies to work with government, under conditions](#)

Chinese State Security Law forces companies based in the country to "provide assistance with work relating to state security," a senior Huawei official in Brussels has said, adding however that the company "has never been requested to implement backdoors in its equipment."

- [UK Government moves to implement new 'Duty of care' tech policy](#)

Propositioned last May, the UK government intends to put forward a 'duty of care mandate' for all technology/digital incumbents ensuring consumer safety and audience protections from 'harmful content'.

- [Pakistan: Cyber security policy to be launched soon](#)

Dr Khalid Maqbool Siddiqui, Pakistani Minister for Information Technology and Telecommunications, on Wednesday said a comprehensive cyber security policy would be introduced soon.

- [5G, here's US plan to win the race with Beijing](#)

The United States have announced a series of measures and initiatives to promote and develop new mobile networks, especially wireless systems and 5G technology.

Cyber Security

- [Forget Russia, China and Iran, up to 80% of cybersecurity threats are closer to home](#)



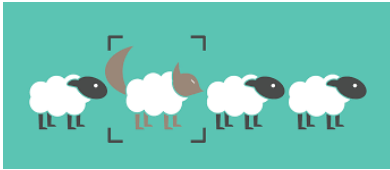
UNIVERSITÀ
DEGLI STUDI
FIRENZE

DSPS
Dipartimento di
Scienze Politiche
e Sociali



Centro interdipartimentale
Studi
Strategici
Internazionali
Imprenditoriali

When we think of cybersecurity, we think of hackers hidden in online shadows, we think of nation-state bad actors. However, one in five cyber-attacks and data breaches come directly from insiders with companies and organizations.



- [IBM says automation is the next big step in cyber security](#)

Despite widespread acknowledgement that a strong cyber security response plan can save companies significant damages in the wake of an attack, the study shows that many organisations still do not have an incident response plan in place.

- [The Cybersecurity 202: Hydro hack shows even low-level criminals can cause major disruptions](#)

A digital attack that spread from the U.S. to Norway is a stark reminder that even simple digital attacks from low-level hackers can produce major disruptions to people's daily lives and international commerce.

- [Triton, one of the most dangerous malware, is back in action](#)

Two years ago Triton was employed to attack an oil facility in Saudi Arabia, now another Saudi facility has become the target of the same malware.

- [Julian Assange's cyber-sins seem quaint in comparison to those of big tech](#)

Assange saw himself as a warrior for truth across the boundless paradise of the web, where people could make their own rules. Now he finds himself badly in need of a secure border, a friendly judge and legal protections.

Cyber Warfare, Intelligence and Terrorism



- [The Russians are screwing with the GPS system to send bogus navigation data to thousands of ships](#)

All critical national infrastructures rely on global navigation satellite system (GNSS) to some extent. The Russians have started hacking into the it on a mass scale in order to confuse thousands of ships and airplanes.

- [Australian cyber spooks hacked Islamic State comms before major battle](#)

The Australian Signals Directorate was "firing highly targeted bits and bytes into cyberspace" in close support of the Coalition's battlefield operations, says director-general Mike Burgess.

- [International collaboration on cyber warfare: an essential plan, but is it realistic?](#)

The French president has launched an initiative to tackle malicious actors in cyberspace, backed by some 50 nations. International collaboration is essential for cybersecurity, but how realistic is it?

- [Cyber terrorists threaten Nigeria, experts proffer solutions](#)

Nigeria as a country is at risk of cyber terrorism and needs urgent framework including laws to stave off premeditated, politically motivated attacks against government, institutions, information and computer systems in the country.

Cyber Opportunities: Economy, Research & Innovation

- [IMF and World Bank Launch Quasi-Cryptocurrency in Exploration of Blockchain Tech](#)
The International Monetary Fund (IMF) and the World Bank have jointly launched a private blockchain and a so-dubbed quasi-cryptocurrency, named 'Learning Coin'. It will be accessible only within IMF and World Bank and used only to test blockchain.
- [Google has opened its first Africa Artificial Intelligence lab in Ghana](#)
When people think of Artificial Intelligence, they most likely think of scenes from science fiction movies, but in reality, it applies to everyday life. Google now wants to position itself as an "AI first" company.
- [Building a data pipeline to defend New York from cyber threats](#)
Given the scale and federation of New York City's IT infrastructure, the New York City Cyber Command decided to build its own open-source data pipeline.
- [New Study: The Internet of Things \(IoT\) Security Market Will Radically Change Globally in Next Eighth Years](#)
Advancement in technologies and increasing use of 2G, 3G, and 4G Long-Term Evolution (LTE) wireless networks have made IoT increasingly susceptible to cyber-attacks.
- [Pet Stablecoins: Why Some Banks Issue Their Own Digital Tokens, While Others Don't](#)
While quite a few financial institutions seem ready to go blockchain and create tokens in a bid to streamline cross-border payments, some still choose to set the technology aside.



Italian Focus

- [A powerful spyware app now targets iPhone owners](#)
Researchers linked a surveillance app designed for Android to the makers of a previously discovered Android app, developed by the same Italian surveillance app maker Connexa, known to be in use by the Italian authorities.



- [Digitalisation of the Italian PA, the 3 Cs strategy](#)
Citizens, Accounting and Centralisation (Cittadini, Contabilità, Centralizzazione) are the three main points of the new strategy to boost the digitalisation of the Italian Public Administration.
- [Electromagnetic limits put at risk 5G in Italy: here's why they should be adjusted to the European one](#)

Limits for emission in Italy are so high that the development of 5G technology can be endangered, a study of the CNR and Polytechnic of Milan revealed.

- [Blockchain, Italy will invest 100 million Euros in two years](#)
Italy is following the European trend in the development of blockchain technology. Despite this change in attitude, the main investors in the EU remain Germany, Austria and France.
- [Cyber Security: cybercrime hits the Sport sector in Italy through BEC](#)
Italian Table Tennis Federation (FITET) and other participants to the international championship were defrauded through Business Email Compromise, losing more than 30.000 euros.

European Focus

- [ESA To Build Quantum Communication Satellites For European Quantum Communications Network](#)
An agreement forged today between the European Commission (EC) and the European Space Agency (ESA) marks the first steps towards creating a highly secure, pan-European quantum communication infrastructure.
- [E-terrorism, social media will be given one hour to delate any sign](#)
The EU Parliament will approve a law to stop terrorist contents on the Internet by forcing digital platforms to delate them, as quickly as possible.
- [Ethics guidelines for trustworthy AI](#)
On April 8th, the High-Level Expert Group on AI presented their ethics guidelines for trustworthy artificial intelligence, following the guidelines' first draft in December 2018.
- [EU law enforcement agencies prepare for major cyber attacks](#)
Large-scale cyber attacks with serious repercussions in the physical world, such as crippling an entire sector or society, are no longer unthinkable, according to Europol.
- [EU tests cyber resilience ahead of May elections](#)
EU institutions have put their cyber systems to the test in a bid to assess the efficiency of responses to attacks against critical network infrastructure, ahead of European elections in May.

