

20<sup>th</sup> -21<sup>st</sup> July [Cyber Week](#)

31<sup>st</sup>-5<sup>th</sup> August [blackhat USA](#)

---



## Center for Cyber Security and International Relations Studies

### Cyber Policy, Diplomacy & Legal Framework

- [China to rival US as cyber superpower](#)

Cyber capabilities are now a potent instrument of national power. This fact was dramatized last month when hackers shut down the Colonial Pipeline, which supplies almost half of the motor fuel consumed on the U.S. east coast, for five days.



- [Priorities for critical technology cooperation between India and Australia](#)

Representatives from India and Australia met on June 10 to constitute a Joint Working Group (JWG) to initiate dialogue on cyber security cooperation. The JWG meeting initiated one of the action points from the Comprehensive Strategic Partnership (CSP) that the two countries had signed in June last year.

- [After Geneva Summit, Daunting Diplomacy Ahead for U.S. and Russia](#)

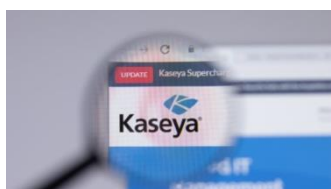
The first summit between Joe Biden and Vladimir Putin eased some of the tension in the fraught U.S.-Russia relationship. It also laid bare the difficult path ahead to resolving differences on many issues, including cybersecurity and human rights.

- [Japan seeks stronger cybersecurity amid China, Russia threats](#)

The Japanese government on July 7<sup>th</sup> compiled a new cybersecurity strategy for the next three years stating for the first time suspected involvement of the Chinese and Russian governments in cyberattacks and calling for enhanced deterrence.

### Cyber Security

- [Kaseya ransomware attack updates: Your questions answered](#)



Kaseya, an IT solutions developer for MSPs and enterprise clients, announced that it had become the victim of a cyberattack on July 2, over the American Independence Day weekend.

- [Cyber attacks in healthcare: the position across Europe](#)

Innovation in digital healthcare will test the measures healthcare providers have in place to protect their systems and data. Growth in telemedicine and other digital



UNIVERSITÀ  
DEGLI STUDI  
FIRENZE

**DSPS**  
Dipartimento di  
Scienze Politiche  
e Sociali



Centro interdipartimentale  
Studi  
Strategici  
Internazionali  
Imprenditoriali

care services has been accelerated as a result of the Covid-19 pandemic and is expected to continue rising.

- [Swedish Coop supermarkets shut due to US ransomware cyber-attack](#)  
Some 500 Coop supermarket stores in Sweden have been forced to close due to an ongoing "colossal" cyber-attack affecting organisations around the world. Coop Sweden says it closed more than half of its 800 stores on Friday after point-of-sale tills and self-service checkouts stopped working.
- ['Cyber-attack' hits Iran's transport ministry and railways](#)  
Websites of Iran's transport and urbanisation ministry went out of service on Saturday after a "cyber-disruption" in computer systems, the official IRNA news agency reported.

## Cyber Warfare, Intelligence and Terrorism

- [NATO Warns That Cyber Attacks on Member States Could Trigger a Coordinated Military Response](#)

NATO could respond to cyber attacks on its member states in similar ways to an armed attack. The alliance's Secretary General Jens Stoltenberg said the military coalition viewed cyber-attacks on its members as armed land, sea, or air assault, which demanded a collective military response.



- [N Korean hackers used VPN flaws to breach S Korean atomic agency](#)  
Korea Atomic Energy Research Institute (KAERI), which is a government-owned organization in South Korea, has disclosed that its internal network was targeted by cybercriminals possibly operating from North Korea. The KAERI is a Seoul-funded research institute established in 1959.
- [Understanding Russia's Cyber Strategy](#)  
The Russian Federation's willingness to engage in offensive cyber operations has caused enormous harm, including massive financial losses, interruptions to the operation of critical infrastructure, and disruptions of crucial software supply chains. The variety and frequency of these operations, as well as the resulting attribution efforts, have offered an unusually vivid picture of Russia's cyber capabilities and tactics.
- [A GRU brute-forcing campaign is reported. Cyberespionage in Central Asia. Inadvertently signed malicious rootkit under investigation.](#)  
NSA and its US and British partners (the UK's NCSC and the US FBI and CISA) on Thursday released an advisory detailing a Russian campaign ("almost certainly ongoing") to brute-force access to cloud and enterprise environments. The campaign is global in scope, NSA says, but focused on American and European targets.

## Cyber Opportunities: Economy, Research & Innovation

- [Programming languages: Python could soon overtake C and Java as most popular](#)



C and Java remain the most popular languages in the Tiobe community index, but Python is stalking them and will likely take top spot in the future. According to Tiobe's July 2021 index, the three most popular programming languages are C, Java and Python.

- [Why Data Privacy Is a People-Centric Problem](#)

Attitudes about data privacy are changing. For one thing, consumers are increasingly vocal about how their data is used. For another, organizations are beginning to recognize that data privacy actually expands business opportunities.

- [Microsoft Emergency Patch Fails to Fix Exploitation of PrintNightmare Zero-Day Vulnerability](#)

The Microsoft emergency patch update could not combat the exploitation of PrintNightmare Zero-Day Vulnerability, which means that attacks could still happen. On Tuesday, June 6, the IT giant launched an emergency patch update to fix PrintNightmare Zero-Day Vulnerability. However, Microsoft's solution to the flaw failed to deliver its promise.

- [How quantum networking could transform the internet](#)

Quantum computing (QC) and quantum networking (QN) are related, though independent, industries. Both leverage the same unexplained phenomenon in quantum physics: the entanglement between particles that enables them to share states -- or in the digital sense, information -- in apparent violation of relativity theory. But as services, they fulfill separate functions.

## Italian Focus

- [Italian government strengthens cybersecurity measures](#)

The Italian government has decided to expand the actors included in the national cybersecurity perimeter to include public and private companies will have the obligation to promptly report attacks or incidents detected, as well as to adapt the protection measures of their networks to defined standards if they want to continue operating.



- [Italy breaks up fake EU COVID pass schemes](#)

Italian police said on July 3<sup>rd</sup> they had broken up a number of online schemes offering to sell fake European Union digital COVID-19 status certificates or purported coronavirus vaccines.

- [Italy ratifies the renewed Convention 108+, for a more modern data protection](#)

Italy has ratified [Convention 108+](#), adding a new and important step in the management of personal data with third countries in order to ensure better overall protection.

- [Zero Trust Network Access: what is it and why is it essential for corporate security](#)

Change or die. The sentence is as effective to describe the state of nature as to depict the nature of cybersecurity in the current context of digitalization and transformation of IT architectures. In this context a major role is played by the concept of Zero Trust Network Access.

## European Focus

- [UK gets data flows deal from EU, for now](#)



The U.K.'s digital businesses can breathe a sigh of relief today as the European Commission has officially signed off on data adequacy for the (now) third country, post-Brexit.

- [Commission proposes 'operational arm' of European Cyber Shield](#)

The Joint Cyber Unit will serve as a platform for cooperation for cybersecurity communities across the EU, enabling them to draw on each other's support and to create a cybersecurity shield to detect cyberthreats before they can cause damage.

- [EU to impose stricter export controls on cyber-surveillance items](#)

Following the Council of the European Union's (Council) adoption of an updated regulation on May 10, 2021 (Updated Regulation), the European Union (EU) is set to expand its Dual-Use Regulation (Council Regulation (EC) No 428/2009, as amended) to authorize restrictions on exports of items that could be used to support human rights abuses, with a focus on "cyber-surveillance items," among other changes.

- [EU Parliament lets companies look for child abuse on their platforms, with reservations](#)

The European Parliament on Tuesday approved a controversial law that would allow digital companies to detect and report child sexual abuse on their platforms for the next three years.