

January 19

[TeissOnline](#)

January 28

[Women in Cloud Summit](#)



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

Cyber Policy, Diplomacy & Legal Framework

- [State Department creates bureau to reduce 'likelihood of cyber conflicts'](#)

Secretary of State Mike Pompeo announced on Thursday the creation of a new bureau inside the US Department of State dedicated to addressing cybersecurity as part of the US' foreign policy and diplomatic efforts. The new bureau will be named the Bureau of Cyberspace Security and Emerging Technologies (CSET).



- [2020 Shows the Danger of a Decapitated Cyber Regime](#)

On almost every significant cybersecurity issue of the past year, President Trump has appeared to be either AWOL or at war with his own federal agencies. But cybersecurity observers on both sides of the political divide say the results of that disconnect have been a surprisingly mixed bag:

- [Spanish government to prepare a list of 'safe' 5G mobile providers](#)

The Spanish government will draft a list of "safe" mobile technology suppliers for the future local 5G mobile network, assessing their level of risk and allowing the government to avoid issuing an explicit ban against Chinese giant Huawei or any other mobile operator, EFE reported.

- [From mobile money to blockchain: How this UN agency's tech stops people starving](#)

In October, the Nobel Peace Prize for 2020 was awarded to the UN's World Food Programme (WFP). Founded in 1961, the Programme supported around 100 million hungry people around the world last year. Tech plays a key role in its work.

Cyber Security

- [SolarWinds hack exploited weaknesses we continue to tolerate](#)



The cyber attack still unfolding in the US may turn out to be the most serious nation-state espionage campaign in history. Assessing the possible



UNIVERSITÀ
DEGLI STUDI
FIRENZE

DSPS
Dipartimento di
Scienze Politiche
e Sociali




Centro interdipartimentale
Studi
Strategici
Internazionali
Imprenditoriali

damage and clearing up the infection will take many months and will extend to the thousands of government departments and companies in many countries that used SolarWinds Orion for managing their networks

- [Anti-Secrecy Activists Publish a Trove of Ransomware Victims' Data](#)
For years, radical transparency-focused activists like WikiLeaks have blurred the line between whistle-blowing and hacking. Often, they've published any data they consider to be of public interest, no matter how questionable the source. But now one leak-focused group is mining a controversial new vein of secrets: the massive caches of data stolen by ransomware crews and dumped online when victims refuse to pay.
- [Nissan source code leaked after it used "admin" as username, password](#)
Nissan's source code was leaked because of a misconfigured Git server of the company. The company secures the server with the default access credentials (username and password) of admin/admin.
- [Windows zero-day with bad patch gets new public exploit code](#)
Back in June, Microsoft released a fix for a vulnerability in the Windows operating system that enabled attackers to increase their permissions to kernel level on a compromised machine. The patch did not stick. The issue, which advanced hackers exploited as a zero-day in May, is still exploitable but by a different method as security researchers demonstrate with publicly available proof-of-concept code.

Cyber Warfare, Intelligence and Terrorism

- ['Hashtags come to life': How online extremists fueled Wednesday's Capitol Hill insurrection](#)
As Americans began to process the horrors of Wednesday's assault on Capitol Hill, many far-right groups exulted in what they saw as a triumph, using the deadly riot to push an extremist agenda of sedition, conspiracy theories and overthrowing the government.
- 
- [Intelligence Agencies: Russia Likely Origin of Federal Hack](#)
U.S. intelligence agencies and the FBI said a major hack of the federal government and some corporations was likely undertaken by Russia -- contradicting President Donald Trump's efforts to suggest China might be responsible -- and "will require a sustained and dedicated effort to remediate."
 - [Five Russian hacks that transformed US cyber-security](#)
For more than three decades, hackers linked to Moscow are believed to have tried to steal US secrets online. Those breaches of US systems have done much to define how America sees cyber-space, and how it defends itself. And they have learnt it is not always possible to predict, or stop, Moscow's efforts.
 - [Twin-seat variation & domestic engine-equipped version of J-20 make official appearances](#)

The twin-seat variation of the J-20 could be used for electronic warfare, command of wingman drones or bombing, and the domestic engine means the J-20 is no longer reliant on Russian engines, analysts said on Sunday.

Emerging Technologies



- [Experts: Closing the Digital Divide Will Take More than Satellites](#)

Although satellite Internet technology has advanced far beyond its initial capabilities, some experts have advised that the emerging broadband solution still has limitations that local and state stakeholders should consider.

- [IBM is using light, instead of electricity, to create ultra-fast computing](#)

To quench algorithms' seemingly limitless thirst for processing power, IBM researchers have unveiled a new approach that could mean big changes for deep-learning applications: processors that perform computations entirely with light, rather than electricity.

- [Internet, the quantum revolution and national security.](#)

A recent experiment illustrated a new, safe and significant step towards the creation of a quantum Internet, whose potential in terms of communication and information exchange becomes more and more evident.

- [Energy Blockchain Can Boost Smart Energy Communities](#)

Blockchain technology still finds itself in a situation of unclear utility—similar to the internet when it was relatively new. As a cryptographic, peer-to-peer ledger system for the reliable recording of information without centralized authority, blockchain holds promise for sectors like energy that are trending toward decentralization.

Italian Focus

- [Covid, seven hacker attacks on AstraZeneca's servers](#)

Rome's prosecutors have opened an investigation after the hacker attacks on the Irbm of Pomezia, the Italian company that is collaborating with the University of Oxford in the development of the anti-Covid vaccine produced by the multinational AstraZeneca.



- [Cryptocurrencies, identified the hacker who defrauded 230 thousand savers: 120 million euros missing](#)

It was the largest cyber-financial attack in Italy and one of the most serious one in the cryptocurrency sector at the international level, according to the Italian Police.

- [Italy's Ho-Mobile database with 2.5m accounts allegedly stolen, sold](#)



UNIVERSITÀ
DEGLI STUDI
FIRENZE

DSPS
Dipartimento di
Scienze Politiche
e Sociali



Centro interdipartimentale
Studi
Strategici
Internazionali
Imprenditoriali

What sounds like a nightmare for a company? Waking up to the news that the data of their customers is being sold online. That's exactly what has happened to Ho-Mobile, an Italian phone service provider owned by Vodafone Italy.

- [The integration needed for national cyber security; an analysis](#)

The cyber threat landscape is very broad, complex and constantly evolving. In recent months many Italian companies have been the object of attention by those adversaries of the "structured cyber crime" type that culminate their offensives by generating a block of IT systems.

European Focus

- [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.

- [Thousands of EU domains registered to UK users 'suspended' after Brexit](#)

Over 80,000 internet domain names assigned to UK registrants have been suspended by the EU registry, EURid, following the end of the Brexit transition period at the close of 2020. The registry has informed EURACTIV that "a few minutes" into the new year, thousands of .eu domains belonging to UK users had been downgraded to a so-called "suspended" status.

- [Data can still flow freely between Europe and the UK. But for how much longer?](#)

After years of negotiation, the UK and the EU have finally signed their long-awaited trade deal on Brexit, but that is not to say that every sticking point has been resolved – and among the issues that are yet to be agreed on, is the transfer of personal data from the continent to the UK.

- [International sting shuts down 'favorite' VPN of cybercriminals](#)

The latest international action against cybercrime infrastructure involves the takedown of a virtual private network (VPN) used to hide the activities of ransomware gangs and other illegal operations. The FBI and European police announced the sting against the Safe-Inet service Tuesday (22nd December) morning.