

December 11

[WISPT](#)

December 2

[Black hat Europe](#)



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

Cyber Policy, Diplomacy & Legal Framework

- [China's New Encryption Law Highlights Cryptography as a Strategic Priority](#)

The so-called “cryptography law” will regulate the role of encryption in both the public and private sector, as well as set forth guidelines for how cryptography should be used to help safeguard national security.

- [BRICS member nations propose creating a cryptocurrency for payment settlements](#)

BRICS, a group of five major emerging nations - Brazil, Russia, India, China and South Africa, has proposed creating a cryptocurrency for settling payment transactions between the countries.

- [Iran shuts down country's internet in the wake of fuel protests](#)

Iran, one of the countries most strongly identified with the rise cyber terrorism and malicious hacking, appears now to be using an iron fist to turn on its own. The country has reportedly shut down nearly all internet access in the country in retaliation to escalating protests that were originally ignited by a rise in fuel prices.

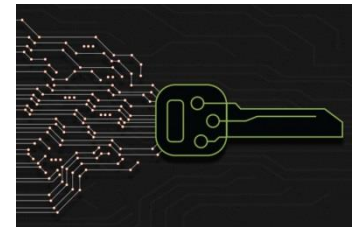
- [Swedish Police Given Green Light For Spyware](#)

At an October 22 press conference, Swedish Interior Minister Mikael Damberg announced a sweeping new 34-point plan from the Swedish government to upgrade law enforcement powers of the Swedish police, with a particular focus on cracking down on violent crime

- [Supreme Court to consider Oracle's copyright clash with Google](#)

The Supreme Court on Friday said it would take up Oracle's long-running dispute with Google over Google's use of Java APIs to build the Android mobile operating system. By taking up the case, the high court will by July of next year put to rest an epic legal battle with billions of dollars at stake, as well as the future of software development.

- [Could norms be the answer to policing cyberspace?](#)



UNIVERSITÀ
DEGLI STUDI
FIRENZE

DSPS
Dipartimento di
Scienze Politiche
e Sociali



Centro interdipartimentale
Studi
Strategici
Internazionali
Imprenditoriali

Most states across sub-Saharan Africa have resisted ratifying treaties that seek to police cyberspace. A handful of governments have signed the AU Convention on Cybersecurity and Personal Data Protection (2014) and the Council of Europe Convention on Cybercrime, while cherry-picking the bits that seem most applicable to them.

- [Facing Down the Surveillance State](#)

The use of facial recognition technology, which scans faces for the purposes of identifying individuals, has been increasingly used by local, state and federal law enforcement across the country. But the technology is not just being used to catch criminals.

Cyber Security

- [Malware attacks on hospitals are rising fast, and the problem is about to get a lot worse](#)

Trojan malware attacks targeting hospitals and the healthcare industry have risen

significantly over the course of this year as hackers increasingly look to exploit a sector that is often viewed as an easy target by those with the aim of stealing sensitive personal data.



- [Cost of Cyber Attack on Asia-Pacific Ports Could Reach \\$110 Billion](#)

In a globally interconnected world, in which supply chains extend across both countries and continents, it only makes sense to consider the potential risks to those supply chains from a massive cyber attack. What happens, for example, if malicious threat actors decide to launch a cyber attack against the maritime ports of the Asia-Pacific region, which is home to 9 of the world's top 10 container ports?

- [As 5G rolls out, troubling new security flaws emerge](#)

Researchers have identified 11 new vulnerabilities in 5G. It's not yet prime time for 5G networks, which still face logistical and technical hurdles, but they're increasingly coming online in major cities worldwide.

- [146 new vulnerabilities all come preinstalled on Android phones](#)

The dozens of flaws across 29 Android smartphone makers show just how insecure the devices can be, even brand new. In fact, when you buy an Android smartphone, it is rarely pure Android.

- [Android malware disguises as ad blocker, but then pesters users with ads](#)

Security researchers have discovered a new Android malware strain that's currently being distributed as an ad blocker for Android users, but, ironically, once installed, it pesters victims with ads through multiple methods at every couple of minutes.

- [Breaking News: Huawei position paper on cyber security](#)

Today Huawei released its position paper on cyber security. This paper sets out the company's philosophies and policies on cyber security. It also provides Huawei's view on the

issues and suggested solutions. This paper aims to help governments, the industry, and other stakeholders correctly analyze the issues and find effective solutions.

Cyber Warfare, Intelligence and Terrorism



- [Massive Web Defacement Attack in Georgia Raises New Concerns About Politically Motivated Cyber Attacks](#)

On October 28, an unknown cyber attacker brought a significant amount of Internet traffic in the country of Georgia to a standstill for much of the day with a massive web defacement attack. Hackers defaced nearly 15,000 websites and forced nearly 2,000 websites offline for a period of time.

- [Malware Attack on Administrative Systems at India's Kudankulam Nuclear Power Plant Thought to Be Connected to North Korea](#)

A malware attack on India's largest nuclear power plant appears to have been perpetrated by a North Korean state-sponsored hacking group. The attack took place at the Kudankulam Nuclear Power Plant (KKNPP) on September 4, 2019, but was not publicly acknowledged until nearly the end of October.

- [The zero-day war? How cyber is reshaping the future of the most combustible conflicts](#)

Conventional wisdom would suggest that scaled-up capabilities, growing competition, and the proliferation of malware across cyberspace presents a legitimate risk of escalation in state conflict, transcending the cyber domain toward the kinetic. However, recent history has shown that states have more often availed themselves of their offensive cyber arsenals to achieve surprisingly de-escalatory effects.

- [U.K. political parties targeted by large-scale pre-election cyberattacks](#)

Both the U.K. Conservative and Labour parties were targets of large-scale cyberattacks on their digital platforms Tuesday just weeks before a national election. The source said both attacks were "very unsophisticated" distributed denial-of-service (DDoS) attacks, which try to take down target websites by flooding them with malicious traffic.

Cyber Opportunities: Economy, Research & Innovation



- [Every Tech Company Wants to Be a Bank—Someday, At Least](#)

The US tech firms need only look to Asia for a lesson in how a push into banking can accelerate their growth. There, tech firms plowed into finance years ago and largely won out. In Beijing, it's embarrassing to pull out a credit card rather than a QR code that links to your WeChat account.

- [Google finishes the install of its private Curie cable, announces Panama branch](#)

Google today announced that it has finished the install and test of its private Curie cable. When it was announced, Curie, which connects the U.S. to Chile, was the company's third private cable. Since then, it has announced two more, Dunant and Equiano, which will connect the U.S. to Europe and Portugal to South Africa.

- [Google: As Go programming language turns 10, here are the big names using it](#)
Google launched Go exactly 10 years ago, in November 2009, offering developers a new programming language that was optimized for multicore processors and which could exploit multithreading.
- [19 useful metrics for measuring blockchain progress](#)
Blockchain proponents need to pinpoint key areas of the business where progress can be measured and documented. The survey's authors, Sheila Warren of WEF and David Treat of Accenture, have a few suggestions as to where they can start, and cite examples of key metrics that may fit
- [Automating Segregation](#)
As more companies seek higher profits through automation, artificial intelligence, and other digital innovations, we should consider what is lost when we replace humans with machines. The fact is that we need other humans in our lives to avoid despair, and we need encounters with those unlike ourselves to sustain our diverse democracies.
- [BRICS member nations propose creating a cryptocurrency for payment settlements](#)
BRICS, a group of five major emerging nations - Brazil, Russia, India, China and South Africa, has proposed creating a cryptocurrency for settling payment transactions between the countries.

Italian Focus

- [Italian Bank UniCredit Suffers New Data Breach Impacting 3 Million Customers](#)
In recent years, global financial services companies have too often become victims of carefully planned cyber attacks designed to steal personal information and banking account details of customers. The latest financial services giant to suffer a data breach is Italian banking giant UniCredit.
- [A dangerous backdoor for Windows is hiding among Word documents: how to defend](#)
A string of malspam attacks is aiming at Italian business companies, thanks to Word documents that can download many malicious items on the victims' desktop, included the dangerous Maze ransomware.
- [Data protection by design and by default: the operational and managerial implications for business companies](#)
The concepts of data protection by design and data protection by have many consequences of the managements. It is therefore capital to organise it following the principles of data protection. Here's some advice.
- [Maze, the ransomware hidden behind communications from Agenzia delle Entrate](#)



In this hours, the Maze ransomware is attacking Italian business companies and PAs, pretending to be the Agenzia delle Entrate. In the article, the characteristics to recognise an ongoing attack.

- [Italy offers Qatar full range of cyber, defence protection assistance](#)

Italy, which is among the most important players in the world cyber market, can provide Qatar with a full range of cyber and defence protection, in addition to the expertise by leading Italian companies in the field of cybersecurity, Angelo Tofalo, Italian Undersecretary of the Minister of Defense has said yesterday.

European Focus

- [European cloud network to start in late 2020](#)



The "Gaia-X Project" is due to be established in the spring of 2020, according to a paper published on Tuesday by the Ministry of Economic Affairs. The live operation should then start in late 2020 with initial providers and users. "Our goal is to develop the next generation of European data infrastructure for Europe, its states, its businesses and its citizens," says the paper.

- [Hungary's emergency infrastructure hardware built by Huawei](#)

Devices provided by the Chinese telecommunications firm Huawei play a core role in the operation of Hungarian state infrastructure, including in the country's emergency services, an in-depth investigative report by Direkt36 shows. The US responded to the news by reaffirming the fact that they have "strong concerns" about the company.

- [EU institution staff 'unaware' of Microsoft data misuse, EU data chief says](#)

Members of staff working across the EU institutions are "not aware" of the extent to which the US tech firm Microsoft collects and stores their data as part of the use of their products and services, the EU's data protection watchdog has told EURACTIV.

- [EU unveils new cooperation projects in training, cyber operations, naval warfare](#)

The European Union has unveiled the latest batch of projects under its flagship defense-cooperation scheme, boosting the areas of training, cyber operations and naval warfare.