Newsletter February 2020

Center for Cyber Security and International Relations Studies

Upcoming Events

March 4

The European Cybersecurity Summit

March 17

Security Summit

Cyber Policy, Diplomacy & Legal Framework

- Brazil launches cybersecurity strategy
  The Brazilian government has created a national cybersecurity strategy with the core objectives of increasing the country's digital trustworthiness and resilience against cyber threats. There are good initiatives currently in place in Brazil around cybersecurity, but they are "fragmented" and introduced on ad-hoc basis, which "hinders the convergence of efforts in the sector," said the presidential decree that created the strategy.

an

- Macron calls for attribution, cybersanctions to stop Russian election meddling
  French President Emmanuel Macron Saturday said the EU should be more assertive in slapping sanctions on countries trying to interfere with elections in Europe. Calling out Russia, Macron said it "will remain a country that tries to intervene" in European elections through the use of deep fakes and manipulation techniques.
- Global digital tax talks: All you need to know
  The digital tax fight passes through Paris Thursday (1/28th), when 135 countries wrap up two days of talks to hammer out a deal on how to tax the likes of Google and Facebook. The talks — overseen by OECD — follow a public spat between France and the United States over the former's domestic digital tax plans, which led to threats of retaliatory tariffs.
- On data protection, the UK says it will go it alone. It probably won't.
- The Prime Minister listed data protection as an area that the UK could legislate on following Brexit - but diverging from European Union rules on privacy would only complicate things. The UK may have finally left the European Union, but the now the wrangling over key aspects of the country's future relationship with Europe – including data flows – really begins.
- The Biometric Threat
  As with so many other convenient technologies, the world is underestimating the risks associated with biometric identification systems. India has learned about those risks the hard

way – and should serve as a cautionary tale to the governments and corporations seeking to expand the use of these technologies.

Cyber Security

- Coronavirus outbreak used by hackers to spread malware

One sophisticated attack method takes advantage of the trusted World Health Organization name to distribute an attachment that will install the AgentTesla Keylogger.

- Hacking brain-computer interfaces

Brain-computer interfaces (BCI) are still in their infancy, yet they've already been hacked. As well as the machine learning models they're built on, For once, can we build in security from the ground up, rather than trying to duct tape it on later? What, and overthrow decades of poor security practice? Not likely

- The US Fears Huawei Because It Knows How Tempting Backdoors Are
  After publicly pressuring its allies to ban Huawei equipment in their 5G networks, US officials are now publicly accusing the Chinese telecom giant of being able to spy on mobile data. The allegations, reported by the Wall Street Journal on Tuesday, represent the first specific concern the US has articulated about Huawei after months of conceptual arguments.
- Redcar cyber-attack: Watchdog probes council 'ransomware'
  A watchdog is probing a cyber-attack on a council which is still unable to provide any online services more than a week after its systems were crippled. Redcar and Cleveland Borough Council's website and all computers at the authority were attacked last Saturday, affecting 135,000 residents.
- Over 500 Chrome Extensions Secretly Uploaded Private Data
  More than 500 browser extensions downloaded millions of times from Google's Chrome Web Store surreptitiously uploaded private browsing data to attacker-controlled servers, researchers said on Thursday.

Cyber Warfare, Intelligence and Terrorism

- Top UN official: It's not too late to curb AI-powered weapons
  There's still time to stop the march of killer robots. That's the view of the U.N.'s disarmament chief, who argues that a key forum trying to agree on banning or restricting autonomous weapons powered by artificial intelligence is making progress and deserves more time.
- Facebook says it dismantles Russian intelligence operation targeting Ukraine

Facebook on Wednesday (12 February) said it had suspended a network of accounts used by Russian military intelligence to seed false narratives online targeting Ukraine and other countries in Eastern Europe.

- US Cyber Command, DHS, and FBI expose new North Korean malware
  US Cyber Command, the Department of Homeland Security, and the Federal Bureau of Investigations have exposed today a new North Korean hacking operation. Authorities have published security advisories detailing six new malware families that are currently being used by North Korean hackers. According to the Twitter account of the Cyber National Mission Force (CNMF), a subordinate unit of US Cyber Command, the malware is being distributed via a North Korean phishing campaign
- Israeli soldiers tricked into installing malware by Hamas agents posing as women
  Members of the Hamas Palestinian militant group have posed as young teenage girls to lure Israeli soldiers into installing malware-infected apps on their phones, a spokesperson for the Israeli Defence Force (IDF) said today.Some soldiers fell for the scam, but IDF said they detected the infections, tracked down the malware, and then took down Hamas' hacking infrastructure.
- Iranian hackers have been hacking VPN servers to plant backdoors in companies around the world
  2019 will be remembered as the year when major security bugs were disclosed in a large number of enterprise VPN servers, such as those sold by Pulse Secure, Palo Alto Networks, Fortinet, and Citrix. A new report published today reveals that Iran's government-backed hacking units have made a top priority last year to exploit VPN bugs as soon as they became public in order to infiltrate and plant backdoors in companies all over the world.

Cyber Opportunities: Economy, Research & Innovation

- We Need to Talk About 'Cloud Neutrality'

We spent a lot of years talking about net neutrality—the idea that the companies that provide access to the internet shouldn't unfairly block, slow down, or otherwise interfere with traffic even if that traffic competes with their services. But there's an even bigger issue brewing, and it's time to start talking about it: cloud neutrality.

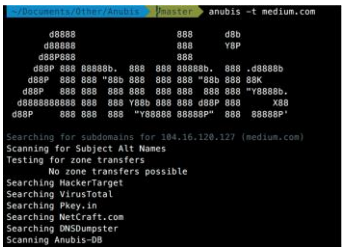
- Tired of packed trains? Here's how smart cities can make your commute less painful

It might be hard to believe – when you're waiting for a bus that finally arrives so full, you'd have been better off walking – that we are any closer to the smart cities that have been pitched to us for years. The daily commutes in the world's largest cities easily run into millions, and managing those travel flows remains a major task for the authorities as they work towards smarter networks.

- [IOTA cryptocurrency shuts down entire network after wallet hack]
  IOTA Foundation, the nonprofit organization behind the IOTA cryptocurrency, has shut down its entire network this week after hackers exploited a vulnerability in the official IOTA wallet app to steal user funds. The attack happened this week, Wednesday, on February 12, 2020, according to a message the foundation posted on its official Twitter account.
- [Mastercard announces first European Cyber Resilience Centre]
  The state-of-the-art centre for cyber resilience is the first establishment of its kind that Mastercard has invested in outside of North America.

Italian Focus

- [Anubis, Android malware which steals data and locks the devices: details and hints to avoid attacks]
  Infostealer, keylogger and ransomware: these are the three components of Anubis, the mixed malware which allows to hack Android devices, steal information, register conversations and lock victims' files.



- [It's all about the Supply Chain!]
  In the lead up to Europe's most prestigious and impactful Security Conference in Munich, we headed to the Bavarian capital to speak with Natalia Oropeza, Global Chief Cyber Security Officer, Siemens
- [Sixth Millennium brings Italian investors to startup nation]
  The investment instrument launched a crowdfunding campaign to raise up to 500 thousand euros in order to support the first steps of the association on the Israeli market. Here's the detail.
- [Informatic worm, the self-replicating malware: here's the details]
  The informatic worm is capable of self-replicate itself from a single computer, spreading to others connected through LANs. Here's the best known ways of diffusion and the most dangerous types.

European Focus

- [Automated facial recognition breaches GDPR, says EU digital chief]

The EU's digital and competition chief has said that automated facial recognition breaches GDPR, as the technology fails to meet the regulation's requirement for consent.

- [MEP Axel Voss publishes EU digital manifesto, warns of EU's 'digital dependency']

Conservative German MEP Axel Voss, also known as the father of the controversial copyright reform, has published a manifesto on European digital policy in which he warns that Europe should not become a "digital colony" of other powers

- LEAK: Commission outlines plan to create single EU data space by 2030
  The EU wants to create by the end of the decade a genuine single market for data that corresponds to its economic power, prioritising nine "strategic sectors" including health, climate, agriculture and energy, and dedicating up to €6 billion to investment in data centres, according to the Commission's data strategy draft
- Azimo gets loan from European Investment Bank to build cross-border payments infrastructure in EU
  Part of the money will be spent on software engineers as the company evolves its product, particularly with European Union (EU)-based customers in mind.