# Newsletter August 2019

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

## Cyber Policy, Diplomacy & Legal Framework

- [Russia Solidifies Grip on its Cyberspace, via the Sovereign Internet Law](#)
  On May 1, Russian President Vladimir Putin signed the "Sovereign Internet Bill," which would create an intranet which allows Russians to stay connected even though they are cut off from the rest of the world. As a new policy, the Russian government planned to conduct a nationwide test to check its ability to disconnect their Internet infrastructure from the rest of the world.

- [Lawmakers want to block tech giants from offering digital currency](#)
  It's been one month since Facebook (and its partners) announced plans to launch Libra cryptocurrency. Already, US lawmakers are calling for Facebook to pause those plans. Now, some legislators want the company to stop altogether.

- [Cyber-Realpolitik: US Foreign Policy and a Fragmented International System](#)
  When international policymakers are in war rooms around the world, making decisions that could determine the difference between détente or a megadeath, it is not always clear where the directive ends up, who received it, or what will become if it.

- [Australian government, spooks, and industry all on different cyber pages](#)
  Michael Pezzullo, the powerful and ambitious Secretary of the Department of Home Affairs (DHA), wants vast new domestic powers for the Australian Signals Directorate (ASD). But reportedly they're not powers the ASD has asked for.

- [Estonia debuts first-ever cyber diplomacy training](#)
  Dozens of NATO and EU diplomats who focus on cybersecurity issues descended upon Estonia last week for their first-ever "summer school" training on cyber diplomacy.

## Cyber Security

- [North Korea 'stole $2bn for weapons via cyber-attacks'](#)

The confidential report says Pyongyang has targeted banks and crypto-currency exchanges to collect cash. Sources confirmed to the BBC that the UN was investigating 35 cyber-attacks. North Korea launched two missiles on Tuesday, the fourth such launch in less than two weeks.

- Phishing: Watch out for this new version of trojan malware that spreads through malicious Word documents

The Ursnif trojan targets Windows machines and has existed in one form or another since at least 2007 when its code first emerged in the Gozi banking trojan.

- Vectra: Ransomware attacks are spreading to cloud, datacenter, and enterprise infrastructure

Ransomware exploded in 2017, when hackers were breaking into hospital systems and holding patient data ransom in exchange for cryptocurrency. But these types of attacks are now spreading to wider targets, such as cloud, datacenter, and enterprise infrastructure, according to a report by security firm Vectra.

- We keep falling for phishing emails, and Google just revealed why

You should feel cranky about all the phishing emails you get. Because getting your brain in a grumpy gear will elevate the odds of your not getting fooled by the next phony invitation to log into your account.

- Cyber security 101: Protect your privacy from hackers, spies, and the government

Privacy used to be considered generally balanced in many countries -- at least, in the West -- with a few changes to rules and regulations here and there often made only in the name of the common good. Things have changed, and not for the better.

## Cyber Warfare, Intelligence and Terrorism

- Hackers steal personal details of two in three Bulgarians as they mock 'joke' cyber-security Suspected Russian hackers have stolen the personal details of five million people from Bulgaria's national revenue agency, in possible retaliation for the purchase of several US F-16 fighter jets.
- Why cyber warfare represents diplomatic territory

The New York Times reported over the weekend on U.S. military attempts to infiltrate the Russian power grid. The effort represents the latest offensive in an increasingly digital conflict with Russia, whose 2016 election interference is well documented

- The Rise of the Global Cyber War Threat

The prospect of an all-out cyber war involving the United States, Russia, China and a host of other nations sounds like something out of a Hollywood blockbuster movie. Yet, based on the growing sophistication and aggressiveness of state-sponsored cyber attacks around the

world, a cyber war involving attacks on the critical infrastructure of nations can no longer be ruled out.

- Cyber Warfare: Army Deploys 'Social Media Warfare' Division To Fight Russia
  The U.K.'s new special cyber operations unit, 6 Division (6 Div), will move beyond the typical cyber capabilities within the military sphere into full-blown social media "information warfare." And here the primary adversary is Russia
- The 'gamification' of domestic terrorism online
  Hate-filled online posts or "manifestos" have often been purposely left behind by shooters for the public and authorities to find. New York Times opinion writer-at-large Charlie Warzel, who covers information technology, joins to hari Sreenivasan to discuss the 'gamification' and radicalization of white supremacy on online forums.

## Cyber Opportunities: Economy, Research & Innovation

- Battery Research Advances Quantum Computing Capabilities
  Scientists from IBM and Mitsubishi Chemical have simulated the initial steps of the reaction mechanism between lithium and oxygen in lithium-air (Li-air) batteries. It's the first research of its kind to have been simulated on a quantum computer and it lays the groundwork for modeling the entire lithium-oxygen reaction on a quantum computer.
- Consumer watchdog calls for new measures to combat Facebook and Google's digital dominance
  The Australian Competition and Consumer Commission (ACCC) has called for "holistic, dynamic reforms" to address the online dominance of digital behemoths such as Google and Facebook.
  - Exploring Internet of Things connectivity solutions via satellite
    New satellite constellations are being launched to improve the connectivity options for the Internet of Things (IoT) market. Many application segments will benefit from these new constellations due to the larger range of coverage they offer when compared to terrestrial communication networks.
- Smart Cities or Surveillance? Huawei in Central Asia
  Since 2014, about 500 cities in China have launched transformative efforts toward becoming cyber-connected "smart" cities, and now Chinese tech giant Huawei is moving to export its systems to Central Asia.
- IBM Recently Registers a Patent for Blockchain-Based Web Browser for the Peer-to-Peer Framework
  IBM is as of now spearheading enterprise-level blockchain solutions, which includes blockchain as a service, supply chain management and a program called as Oracle which uses third party information to execute smart contracts. IBM states that tokens will confirm a clients browser session actions as they are encased into blocks for the Peer-to-Peer framework.

- [As Protests In Hong Kong Surge, So Does Demand For Cryptocurrency](#)
  Cryptocurrencies and Bitcoin were built to address several of the most pressing points in the Hong Kong protests, which are at the forefront of what it means to protest against a state equipped with all of the sophisticated technologies of the 21st century and the unrestrained ability to weaponize those capabilities against its citizenry.

## Italian Focus

- [Cyberspace: threats, risks and opportunities for Italy](#)
  The Italian Intelligence Apparatus has highlighted, in a recent annual report, the risks that the cyber threats represent for the Italian economic, military and scientific interests. Moreover, the attacks are now sophisticated enough to threaten the whole PA apparatus.
- [How a national security perimeter will enforce the Italian cyber defence](#)
  On 19th July, the Italian Parliament passed a law to develop the concept of national security perimeter, which should encompass a series of technical and organizational dispositions, aiming at increasing the security of the country.
- [5G and Golden Power? Ahead without hesitation](#)
  A conversation with the Lega deputy on the necessity to develop a new digital identity for the country and to enforce the digitalization of our economy
- [Digital transformation: Italian CEOs are still not ready](#)
  Digital transformation has caught unprepared not only the PA, but also the private sector, In Italy, we still lack a new digital leadership capable of creating new strategy and deploying financial resources to change the digital business models.

## European Focus

- [How Europe's 'Digital Tax' Plans Will Hit U.S. Tech Companies](#)
  France and Britain are hatching plans to tax the revenue, rather than the profit, of companies such as Facebook Inc. and Alphabet Inc.'s Google that make their sales primarily in cyberspace. They're the first of potentially several countries in Europe implementing "digital taxes".
  - [Infosys launches cyber defence centre in Bucharest](#)
  Infosys, a global leader in next-generation digital services and consulting, announced on July 29 the launch of a state-of-the-art cyber defence centre in Bucharest, Romania. The defence centre is an expansion of services delivered through the Infosys digital innovation centre which opened in Bucharest earlier this year.
- [How Brexit Impacts the Future of Europe's Cybersecurity Posture](#)

The British parliament has been unable to agree the exit package from the European Union. With the possibility of a "no deal" departure looming, EU leaders have granted a six-month extension to Brexit day. But the uncertainty that still lingers with regards to Britain's future, creates various opportunities which cyber criminals could try to exploit.

- [A federal Cloud for the European sovereignty in the technological field: a plan.](#)
European Union has to implement in order to avoid dependency from foreign corporations and governments. The new plan for a digital Union wants to achieve this objective, starting with the development of a federal Cloud among member states.