The VISIO JOURNAL

AN INTERDISCIPLINARY JOURNAL OF PUBLIC POLICY ANALYSIS

FUTURE OF EUROPE: SECURITY AND PRIVACY IN CYBERSPACE

Editor
Tanja Porčnik

Authors
Alexandru Georgescu, Andrzej Kozlowski,
Anushka Kaushik, Cosmina Moghior, Gordon Kerr,
Joanna Kulesza and Octavian-Dragomir Jora.

NUMBER 3 • PUBLISHED BY VISIO INSTITUT • 2018

The authors of this publication have worked independently, and opinions expressed by them are, therefore, their own and do not necessarily reflect the views of the supporters or staff of Visio institut. This publication in no way implies that Visio institut or its staff are in favor of, or oppose the passage of, any bill; or that they support or oppose any political alliance, party, or candidate.

Cover design by Milutin Pavićević.
Photos inside the journal by Visio institut.

Cite this publication as:
Title: *The Visio Journal 3*
Publisher: Visio institut
Date of publication: 2018
Digital copy available from <http://www.visio-institut.org/>

Cataloguing Information
The Visio Journal 3 / edited by Tanja Porčnik
Annual.
2018 issue by Alexandru Georgescu, Andrzej Kozlowski, Anushka Kaushik, Cosmina Moghior, Gordon Kerr, Joanna Kulesza and Octavian-Dragomir Jora.

ISSN 2536-1481

The VISIO JOURNAL

AN INTERDISCIPLINARY JOURNAL OF PUBLIC POLICY ANALYSIS

No. 3

Future of Europe: Security and Privacy in Cyberspace

EDITOR'S NOTE

By Tanja Porčnik*

In the highly-digitalized modern world of the 21st century, the citizens, private sector and government alike face a growing challenge of securing cyberspace. Cyber threats and attacks pose as one of the newest and ever-growing security issues. On the one hand, faced with swiftly developing technologies, digitalization of communication and spread of social networks; while on the other, aiming to confront a threat to individual rights by the erosion of security and invasion of privacy being attacked by not only terrorists and criminals but also by state actors. Cyber threats range from the attacks on the integrity of individual information systems and international state-to-state engagement in cyberwarfare to more recently prevalent data breaches and manipulation of expectations and common understandings in the society. These cyber attacks are not reserved to the authoritarian regimes, but they have lately become increasingly associated also with democracies where the rogue actors seem to thrive the most.

In response, governments are putting in place policies to enable active defense and making sure computer technologies they use and the skills of those using them are up to speed on cybersecurity. At the same time, as Mee and Morgan (2017) layout, to become proficient in repelling cyber attacks private sector is engaging in protective steps on its own by quantifying cyber risk concerning capital and earnings at risk; anchoring cyber risk governance through risk appetite; ensure effectiveness of independent cyber risk oversight using specialized skills; mapping and testing controls; and developing and exercising incident management playbooks. Similarly, private individuals are finding ways to become more resilient to cybercrime, mostly by rigorously installing security software on the computers or divides they use as well being knowledgeable about cybersecurity risks and mitigations. Malware and viruses are not putting at risk only individual's financial standing, but also privacy. The latter, once lost, is almost impossible to regain.

This issue of *The Visio Journal* offers papers analyzing the intersection between protection of citizen's rights to both privacy and safety in cyberspace with an aim to offer informed and comprehensive solutions for better protection of citizen's rights. The contributions in the third issue of the journal were presented at the IX. Liberal Colloquium, "The Future of Europe: Security and Privacy in Cyberspace," held in Tallinn, Estonia, November 30 – December 1, 2018. It was a pleasure for Visio institut to partner with the Academy of Liberalism on this conference, which brought together participants from Poland, Romania, the United Kingdom, India, Croatia, Estonia, Germany, Czech Republic, and Slovenia.

Finally, I would like to recognize the generous contribution of the Friedrich-Naumann-Foundation for Freedom for supporting the journal that is before you.

---

* Tanja Porčnik is President of Visio institut. Porčnik is coauthor of the Human Freedom Index.

Mee, Paul, and James Morgan. 2017. "Deploying a Cyber Strategy – Five Moves Beyond Regulatory Compliance." In *MMC Cyber Handbook 2018 – Perspectives on the Next Wave of Cyber*. Marsh & McLennan.

Supported by

Friedrich Naumann
STIFTUNG FÜR DIE FREIHEIT

Pandora's Botnet – Cybercrime as a Persistent Systemic Threat

By Alexandru Georgescu*

The utopian fantasies projected onto the rapidly evolving cyberspace have given way to the realities of the assertion of age-old human instincts, clothed in new technology. New risks, vulnerabilities and threats are manifested in a complex security environment, where cyber-criminals are carving out their ecological niches, catering not only to the profit motive, but also to new ideologies, and frequently staying one step ahead of the capabilities of their victims or the traditional suppliers of security, the state. Their abilities, in a space which is a great multiplier of power, put them on par with groups or even states and their actions serve to undermine not only the consumer web but also the developing infrastructures of e-governance.

Key words: cybersecurity, cybercrime, critical infrastructures, security governance.

Introduction

The boundless optimism of the Information Age, accompanied by irrational exuberance in markets, as well as technologically savvy evangelists preaching a brighter future through technology, have served to accelerate the mass adoption of cyber technologies whose flaws and vulnerabilities present significant opportunities for random as well as deliberate breakdowns.

Regulators and users have a hard time keeping up with the evolving security landscape, made worse by emergent problems deriving from the interplay between complex systems, organizations and behaviours mediated by the communication afforded by cyber capabilities. The race between protectors and malefactors is always geared towards the latter in such a fluid situation, and the impetuousness of mass adoption and the effervescence in the adoption and diversification of the digital is steadily making things worse.

The easiest element to comprehend is the adversarial relations made possible by the cyber environment. Nations may attack each other's militaries or legitimate targets through networks, state and non-state actors may perform acts of terrorism, cybercriminals may steal, disrupt or exploit and random virtuosos may sow chaos for personal gratification and promotion.

The harder elements are those which relate to the changes in our societies wrought from evolving cyber connections. Social networks and hierarchies are remade quickly and threaten the so-

cial fabric that was once limited by geography, transport and cultural barriers. Notions of privacy and intimacy are also steadily subverted, not just as an adaptation to the new possibilities, but also through cynical encouragement from those who see the profit to be made in this way. Law enforcement and protection are outclassed not just by the act of cyber disruption, but also from the way in which the legal realm has remained forty paces behind the reality of these issues. One should especially highlight the cross-border complexities engendered by the irrelevance of geography in cyber security problems. Jurisdictional issues abound, as well as complexities in trying to establish any sort of regulatory environment, with the apparent conclusion that countries may be "condemned to cooperate" at International levels for appropriate governance of these issues. This is easier said than done.

And, finally, we are forging full speed ahead into a situation where the average person may not be able to wash his clothing without an imprint in the digital environment, creating "valuable" data for some company or another, as well as opportunities for mischief. Driverless cars may be on their way, though one should maintain a level of technical and legal scepticism with regards to their mass adoption. Automated transport ships for global production and supply chains are also coming, and they will be easier to implement and possibly even easier to use to cause mass disruption. Vast amounts of data that we unwittingly create serve to generate an online persona that is less protected than our physical selves have ever been. And, more importantly, all of these changes are taking place in an environment so well connected, that one can scarcely imagine the couplings that may propagate an (un)intentional breakdown throughout the entire system-of-systems. Longing for simpler times is going to become more than a saying or a cliché under these conditions.

A Vulnerability Assessment

Our vulnerability to cyber disruptions of all kinds is staggering and increasing daily. Compounding these issues is the understandable lag between the capacity of organizations to formulate and adopt cyber protection and prevention strategies and adapt them to the rapidly changing environment. One must also underline the fact that cyber protection starts in-house, with each user and organization maintaining their first line of defence, both literally and figuratively, through elements of security culture. This is before one may even start to discuss what the state, the judiciary or some third party or the military may do for you, which is generally limited to responding to issues after the fact or proactively addressing a limited number of threats – particular groups, case files, targets, means of assault (embedded and unresolved vulnerabilities) and so on. There is also a significant asymmetry of information between cyber users and would-be cyber protectors. It is not enough to say that the military is using cyber capabilities to protect its country and its allies when actual system architectures are unique and no single organization can centralize expertise in all of these. An actor called upon to actively and passively protect both industrial control systems, administrative databases, communication lines and underlining infrastructure will do neither of those things correctly.

It is not enough to only run through a list of domains which have undergone a cyber transition of the first order and, sometimes, second or third orders (through the underlying cyber vulnerabili-

ties of processes such as financialization, globalization, conglomeration, decentralization). We need to illustrate the boggling realities of cyber issues:

- The first website launched in 1991, while, in 2016, there were 1.2 billion websites (Stevens 2018);
- Microsoft believes that online data volumes will be 50 times higher in 2020 compared to 2016 (Boden 2016);
- Digital content alone will have expanded from 4 Zettabytes annually to 96 Zettabytes, where a Zettabyte is 1,000 billion Gb (Ibid.);
- The Internet of Things will take off, as 2 billion wirelessly communicating smart devices in 2006 will have become 200 billion by 2020, according to Intel Corporation (2017);
- The recent craze in wearable devices for fitness or medicine already amounts to 310 million devices sold yearly in 2017 and 500 million in 2021 (Gartner 2017);
- The hopeful disappearances of passwords in favour of biometrics have been exaggerated – 300 billion passwords will have to be secured in 2020 (Morgan and Carson 2018);
- The 111 billion lines of code added to software each year will make it even more likely that simple human error, unanticipated interactions, planned or unplanned vulnerabilities will increase the risk to networked systems (Kerravala 2017);
- 90% of cars will be connected to the Internet in some way or another by 2020, up from 2% in 2012, and 20 million cars will be sold yearly with integrated cybersecurity defences on-board (Cybersecurity Ventures 2017);
- In 20 years, over 45 trillion sensors will be connected to the World Wide Web, in every imaginable circumstance, from environmental surveillance to social and inside the body of patients or individuals in general;
- Lastly, the area of the Internet which is not indexed by search engines and is as such labelled as "dark" is already 5,000-times larger than the visible Internet (Finklea 2017).

These phenomena have been termed the "expanding attack surface of the cyber environment," which creates new opportunities for mischief and mishaps. Surprisingly, a Cisco study revealed that 40% of manufacturing firms still do not have a strategic approach to cybersecurity (Cybersecurity Ventures 2017).

One must also realize that, as sci-fi author William Gibson said, the future is here, but it is not evenly distributed. Cyber protection issues less penetrate some places or some domains therein. For instance, a less developed country will have found it easier to ensure rapid communications adoption of cyber, while finding it more challenging to upgrade its industrial base so that it may use the latest industrial control systems. This makes it less vulnerable, even as it remains less productive or efficient. At the same time, the lag may very well be recorded in the field of cyber protection, with countries rushing to encourage digitalization without a corresponding awareness of the dangers and the need to invest in security.

Our Brave New Future?

Our growing reliance on the cyber substrate used to coordinate society is also affected by key

trends, some of them new and some old.

The first is the still extant democratization of digital skills and knowledge, combined with the low-cost barrier to take digital action. The rapid innovation in the field was engendered by the possibility that young people working "in garages" with few resources, could be able to generate and sustain disruptive technological change. While the maturing of the Internet era enterprises has reduced the extent to which garage firms are viable players, the possibility that motivated and skilled individuals can punch above their weight remains. This applies to hacking as well, where profit, ideology and daredevilry may inspire individuals or small groups to take on and win against many better-resourced organizations. The profound capacity of the cyber system to permit the proliferation of "weaponry" and other forms of pre-made cyber tools, as evidenced by the Wikileaks revelations of the CIA data breaches which saw its arsenal lost online, also raises the stakes in the field.

The second is the rise of "cloud computing." This is not just the latest buzzword, but also a systemic transformation of staggering proportions, because, in the name of cost and efficiency, it divorces the end user from having to maintain his processing capability or data storage. This centralization makes sense in a world of perfect security, but it compounds the risks associated with the interruption of communication. A computer which is not connected to the Internet may continue to function and be usable. But a simple workstation connected to a centralized processing and data storage hub will be useless in the event of a communications collapse or attack against that critical node. The logic of cyber-attacks also changes, and their scope rises, as the first (and unintentional) cloud computing applications (email services) show, since a single attack may affect, as in the case of the recent Yahoo attacks, over 3 billion users in a single swipe. Any centralization vastly increases the potential payout of an attack or theft, while not necessarily raising its cost, as the consistent and constant revelations of security neglect show.

Thirdly, the ubiquity of cyber raises the number of targets, as well as the number of channels for the propagation of the effects of an attack. It is one thing to fear that one's own devices may be hacked and damaged, or their data were stolen, and it is another entirely even to imagine the second and third order effects of a cyber-attack on a component for a tightly integrated critical infrastructure system physically spread out all over the world. The cascading disruption is difficult to anticipate, and potential victims find it hard to register the risk. For instance, a hacker may attack the control system of an oil pipeline, forcing a reduction in deliveries, thereby generating an energy crisis with the potential to affect numerous consumers.

Fourthly, the deteriorating state of existing infrastructures and systems leads to several possibilities. The first is that some of these systems may become intertwined with cyber issues in a way that mixes different generations of control systems, creating new vulnerabilities. This is especially prevalent in the energy and industrial sectors, where long-lived assets have gone through several upgrades. The second is that pre-digital systems are either neglected, excluded or replaced with the more efficient and productive systems, leaving a capacity gap which a cyber-attack will highlight. We can compare, for instance, the system of road transport as it is now, before the advent of the mass adoption of driverless cars, with the system that may develop in the future. Several economists have claimed that the success of driverless cars will lead to the rapid reduction of actual driving since insurance companies will incentivize the shift to driverless. At every step in the road to full adoption, the disruptive potential of a cyber-attack increases to the point where, from a relatively resilient system, which could even maintain itself

in the context of a breakdown of the traffic light system or GPS navigation, we will have arrived at a totally unworkable system of driverless mass transport.

The Human Factor

Lastly, we must consider the human element of the cyber equation. There is a growing gap between the needs of the cyber security sector and the actual resources, which only a decade-long concerted effort at training, followed by continuing education programs, can cover. The cybersecurity-related employment needs of individual organizations far outweigh the needs of the organizations that create and manage the cyber tools which generate security issues. In the meantime, interesting choices abound for policymakers and various organizations. The tolerance of malicious hackers turned to "whitehats" is one. There is a general debate as to whether captured hackers belong in jail or on the payroll of the organizations they have hacked. Institutions like the military have to reconcile their standards with regards to discipline, indoctrination and leadership culture with the reality of the type of individuals they would have to employ: "The Americans with the best cyber talent may not meet military and appearance standards — they might be out of shape, overweight, have facial tattoos, or some other disqualifying factor" (Barno and Bensahel 2018). It quoted an argument along the lines that "the military needs an entirely new approach to the cyber domain that 'effectively breaks all the personnel rules and shreds all accepted norms of rank, seniority, and deference that currently characterize what it means to be in the military'".

If the military does not find enough talent it can mould according to its standards, and it may come to rely on civilian contractors, then it will be faced with many of the same problems that the intelligence agencies faced by outsourcing key data analysis operations, namely security risks related to security culture, ideology and the lack of control over individual contractors (the famous Edward Snowden, at the time of his data theft, was working as a private contractor). The military has other issues, specifically related to chain of command, the ability to move people around and to integrate with other services since cyber is now a domain of warfare. Putting some hackers in uniform may also be necessary "to legitimately and legally conduct offensive cyber operations — the kind of cyber-attacks whose cascading effects could readily inflict grievous harm and death. These cyber warriors need to be subject to the Uniformed Code of Military Justice, so they are held accountable for their actions and legally protected from liability. Putting them in uniform also clearly identifies them as lawful combatants under the Law of Armed Conflict, and, though it may seem quaint, offers them certain rights under the Geneva Conventions" (Ibid.).

The Burden of Cybercrime

While it may seem appealing to debate the issue of hybrid and asymmetric warfare and what cyber-attacks mean from the standpoint of warfare, the more prosaic field of cybercrime holds some of the best examples of the related dangers. It has been estimated that the cost of cybercrime would total 6 trillion dollars in 2020, up from 3 trillion in 2015, which is a staggering amount compared to a world GDP in 2017 of 78 trillion dollars (Cybersecurity Ventures 2017).

According to Harnish (2017), business falls prey to a cyber-attack every 40 seconds, which will drop 19 seconds by 2020 (). A new and important area of the cybercrime business is ransomware, which is a protection racket for the digital age. Ransom payments have reached 1 billion dollars annually, according to the FBI. Global ransomware costs exceeded 5 billion dollars in 2017, marking a 15-fold increase in just two years (Rosenstein 2017). The fact that 1.4 million phishing websites are created every month is also indicative of the breadth of the business.

The whole area of cybercrime, which easily fits into transborder organized crime and is hard to tackle for many of the same jurisdictional reasons, has been steadily professionalizing, thereby mirroring legitimate businesses (Fortinet 2013). Rather than doing everything by oneself, it is possible to contract with providers for any conceivable cybercrime service, including setting up attacks, creating bespoke attack tools, data theft, crashing systems and so on. There is also an organizational structure of crime-as-a-service, with executives, recruiters, infantry and help wanted ads. Meanwhile, new business models proliferate – pay-per-click, pay-per-install, pay-per-purchase, ransomware. One can rent, buy or lease botnets, remote access, exploit kits, crypters, source code. Finally, the money management side of things is also intertwined with white collar crime, which cybercrime often resembles.

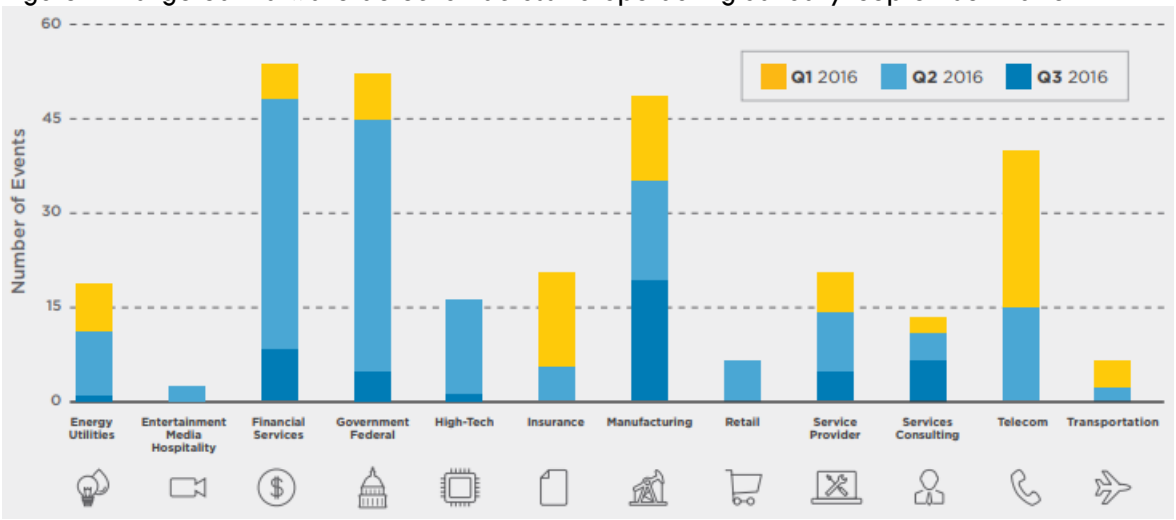
According to the FBI's Internet Crime Complaint Center (IC3), the BEC (Business Email Compromise) scam has seen a 13-fold increase in identified exposed losses, worth 3 billion dollars, between 2015 and 2017, while Cisco reports place losses at 5 billion between 2013 and 2016 - "the average size of distributed denial-of-service (DDoS) attacks is 4X larger than what cybercriminals were launching two years ago — and more than 42 percent of DDoS incidents in 2017 exceed a whopping 50Gbps, up from 10 percent of cases in 2015. Cybersecurity Ventures predicts that newly reported zero-day exploits will rise from one-per-week in 2015 to one-per-day by 2021" (Cybersecurity Ventures 2017, p. 13).

Cybercrime is related to other forms of cybersecurity issues. For one, it provides much of the tools, infrastructure, services and knowledge to conduct cyberterrorism operations or easily denied state cyber-attack operations. Avoiding fingerprints and also being able to perform operations without having to insource much of the work are appealing advantages. At the same time, we should remember that the effect of the crime itself is to undermine organizations by creating and cultivating exploits, whether through corruption or cyber-attacks. There is the possibility that, through anti-fragility, an organization hampered in this way may take the required measures to become more resilient, but we have already established that this should be the exception, not the rule.

The European cybercrime scene mostly targets the most developed economies, especially companies in manufacturing, finance and telecom. According to the report, in Europe, "mean 'dwell time' — the time between compromise and detection — was 469 days, versus a global average of 146 days" (Carpenter and Wyman 2017, p. 13). The links between organizations and government are also not as good – only 12% of intrusions were discovered via notification from a state agency in Europe, as opposed to 53% in the US, which raises the question of whether

the number of intrusions is severely undercounted. Figure 1 illustrates the main patterns of cybercriminals targeting European industries in 2016, to the extent that they had been detected. One can observe the concentration on government, finance, manufacturing and telecom, as well as the shifting interest of organized cybercriminals, moving from telecom in Q1 to finance and government in Q2.

Figure 1: Targeted malware detection across Europe during January-September 2016



Source: Carpenter and Wyman (2017).

Conclusion

It is vitally important that the authorities and other actors, such as the military, become proactive with regards to cyber threats, as concerns issues which only they are authorized to handle, such as prosecution, deterrence, regulations and offensive action, though some companies have been known to contract for retaliatory services.

However, companies themselves must take the first steps in their protection, whose main elements are, from a business perspective (Carpenter and Wyman 2017):

- Seek to quantify cyber risk concerning capital and earnings at risk;
- Anchor all cyber risk governance through risk appetite;
- Ensure effectiveness of independent cyber risk oversight using specialized skills;
- Comprehensively map and test controls, especially for the third-party interactions;
- Develop and exercise incident management playbooks.

The development of cybercrime is a natural outgrowth of the expanding role of cyberspace in our lives and livelihoods. Along the way, the phenomenon has morphed into an enabler for terrorism and asymmetric warfare elements, contributing to their low traceability and high deniability. There is a dynamic at play where enforcement and protection remain one step behind the cybercriminals, sometimes in different jurisdictions as well, and this problem is compounded by the deficiencies of the security culture of the main body of potential victims (individuals, businesses and state entities). So long as the frontier of the emerging cyber environment keeps ex-

panding outward, creating new interactions and multiplying them between stakeholders, as well as opportunities for those who would speculate the latest trends, this dynamic will remain.

---

* Alexandru Georgescu is Research Assistant with the Department of Cybersecurity and Critical Infrastructure Protection of the National Institute for Research and Development in Informatics, Bucharest. Georgescu holds a PhD in Critical Infrastructure Protection (school of Industrial Engineering) from the Polyethnic University of Bucharest, Romania.

References

Barno, David, and Nora Bensahel. 2018. "Strategic Outpost Debates a Cyber Corps." *War on the Rocks. February 20th.* https://warontherocks.com/2018/02/strategic-outpost-debates-cyber-corps.

Boden, Pete. 2016. "The Emerging Era of Cyber Defense and Cybercrime." *Microsoft Secure*, January 10th. https://cloudblogs.microsoft.com/microsoftsecure/2016/01/27/the-emerging-era-of-cyber-defense-and-cybercrime/.

Carpenter, Guy, and Oliver Wyman. 2017. "MMC Cyber Handbook 2018 – Perspectives on the Next Wave of Cyber." *Marsh & McLennan*. https://www.mmc.com/content/dam/mmc-web/Global-Risk-Center/Files/mmc-cyber-handbook-2018.pdf.

Cybersecurity Ventures / Herjavec Group. 2017. "2017 Cybercrime Report." https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf.

Finklea, Kristin. 2017. "Dark Web." *US Congressional Research Service Report*. March 10th. https://fas.org/sgp/crs/misc/R44101.pdf.

Fortinet. 2013. "Cybercriminals Today Mirror Legitimate Business Processes (Fortinet Cybercrime Report 2013)." https://cybersafetyunit.com/download/pdf/Cybercrime_Report.pdf.

Gartner. 2017. "Gartner Says Worldwide Wearable Device Sales to Grow 17 Percent in 2017." Last modified August 24th. https://www.gartner.com/newsroom/id/3790965.

Harnish, Reg. 2017. "What It Means to Have a Culture of Cybersecurity." *Forbes*. September 21st. https://www.forbes.com/sites/forbestechcouncil/2017/09/21/what-it-means-to-have-a-culture-of-cybersecurity/#189651c4efd1.

Intel Corporation. 2017. "A Guide to the Internet of Things Infographic." https://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html.

Kerravala, Zeus. 2017. "Cisco to Network Engineers: Get Comfortable with Software. It's Here to Stay." *Network World*. May 25th. https://www.networkworld.com/article/3198474/lan-wan/cisco-to-network-engineers-get-comfortable-with-software-it-s-here-to-stay.html.

Morgan, Steve, and Joseph Carson. 2018. "The World Will Need to Protect 300 Billion Passwords By 2020." *Cybersecurity Ventures*. July 4th. https://3erczm2x84t2p8xnj226kmxx-wpengine.netdna-ssl.com/wp-content/uploads/sites/4/2018/07/cybersecurity-ventures-thycoti_70778.pdf.

Rosenstein, Rod J. 2017. "Deputy Attorney General Rod J. Rosenstein Delivers Remarks at the Cambridge Cyber Summit (speech)." https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-cambridge-cyber-summit.

Stevens, John. 2018. "Internet Stats and Facts for 2018." *Hosting Facts*. July 10th. https://hostingfacts.com/internet-facts-stats-2016/.

The European Union Effective System of Sanctions Against Cyberattacks

By Andrzej Kozlowski*

Last days the European Union leaders discussed potential sanctions to deter cyberattacks. However, they did not provide any details. The European Union is not the first political organization, which engages in debate on such a topic. Others like the United Kingdom and particularly the United States have used a variety of means to deter cyberattacks and punish the assailants

The paper aims to present the potential tools, which the EU could use to deter cyberaggression and later analyze the potential consequences of using them. What is more, the obstacles organization could meet will be presented and finally the evaluation of the effectiveness of these measures and the probability of using them. This analysis will be done to answer the central question: how to create a system of punishing for a cyberattack. The analysis will be done basing on the experience of other countries, especially the case of the United States. However, the situation with the EU looks different, because it is a political organization, which consists of 28 members.

Key words: cybersecurity, cyberattacks, sanctions, European Union.

Introduction

The growing number of cyberattacks have become a serious security challenge for individuals, enterprises and states in the European Union (Fruhlinger 2018). Increasingly, they are used as a weapon, which is aimed at disrupting critical infrastructure, paralyzing weapon systems, destabilizing the political situation, interfering in the election process, altering significant voting, etc. States such as China, Russia, Iran and North Korea more and more often have used cyberspace as a new arena of conducting a hostile activity. Among the victims were the EU countries such as Germany, the Netherlands or Great Britain but also the EU institutions. In response to this growing threat, the bloc of countries led by the Netherlands and Great Britain proposed to extend sanctions regime to include cyber-attacks (Drozdiak and Chrysoloras 2018). Despite the protests from the Italian government, the EU leaders supported this idea (de Carbonnel and Emmot 2018).

Analysis

Developing an effective system of sanctions against cyberattacks is a daunting challenge for every political actor including the EU. There are several obstacles which need to be addressed like attributing attacks to a certain assailant, the communication policy of presenting proofs

about the source of the attack or influencing member states of the EU to impose sanctions. However, the EU may use examples of the other countries, which have already used some sanctions against the attackers.

The problem of attribution

One of the main problems to retaliate effectively against the authors of cyberattacks is attribution. The architects of global network did not think about security issue when they projected the Internet. Initially, it was created as the tool to establish communication between the military commands in the United States and later also to facilitate the exchange of information between the American academic entities. No one at that time was planning global expansion. Construction's flaws lead to the situation that the cyberspace has become the oasis for the illegal activity (Kaplan 2016, 10-21). Initial cases of hostile activity were dominated by the young teenager's desire to earn extra money.

However, at the beginning of the 21st century more and more advanced, long-time incidents took place and countries, particularly the United States started to treat cyberattacks as the severe threat for national security. Several countries, especially Russia and China were accused of standing behind the attacks, which both of them vehemently denied. Unfortunately, the problem of the identification of the assailant has seemed unresolved until today, mainly due to the architecture of the cyberspace. We are able to trace the IP addresses, which identify the computer in the virtual world, but manipulating them is an extremely simple and available even for beginners. That is a reason that the attack conducted against the members of the European Union from Chinese addresses did not mean that it was orchestrated by Chinese but maybe is the work of Russians or Israelis hackers using the IP located in China.

Despite the difficulty, the American private company Mandiant in 2013 collected data and published reports accusing the Chinese military united 61390 located in Shanghai of conducting a bunch of cyber espionage campaigns against the US. The proofs were solid. It was the first time in history when someone delivered a very detailed and rich report on attacking techniques and tools. It is worth also mentioning how hackers were identified. American IT security experts under the leadership of Mandian Company used the exploit in Chinese hackers' security networks and got access to their systems collecting logs and tracking every move than creating the digital diary. What is even more interesting, it was purely private initiative without the government engagement. However, the Mandiant report was just the beginning (Mandiant 2013). Since that time the United States identified the source of cyberattacks accusing Russia of interfering in the presidential election and breaching the Democratic Committee in 2016. Not only was Russia identified as the source of attack but also China, Iran and North Korea. Unfortunately, in some cases, the American institutions have not always provided persuasive material to support their accusation (Goldsmith 2017).

The EU members have also possessed capabilities to attribute cyberattacks. The Dutch intelligence conducted an effective operation against Russian intelligence assets engaged in hacking United States presidential election. What is more, the United Kingdom accused North Korea of

paralyzing own healthcare system with the use of WannaCry ransomware. Germany was able to identify Russian traces in hacking Bundestag and France detected the Russian false flag operation against Le Monde station. These examples showing the increasing number of technical attributions of the attacks and that the EU members have possessed these capabilities. Likewise, in Skripal case certain countries could share intelligence information with others and in this way supporting the idea of imposing a sanction on the specific attacker. There will be more and more attacks identified on a technical layer.

The Communication Policy

The next problem linked with the attribution is the communication policy. In the case of identifying the assailant, the authorities of the certain country and later the representatives of the EU need to consider the amount of information they intend to reveal. The scarce of technical details can lead to skepticism within the EU members and finish with the lack of any decision. What is more, the other international actors may question the outcome of the inquiry, but also it risks the long-term consequences where states accused other states of cyberattack without presenting evidence. On the other hand, the abundance of the information available to the public may risk intelligence techniques and assets of certain countries and may threaten the next operations. The policymakers in the EU need to find equilibrium between these two options.

Not only, there is a technical attribution of cyberattacks. There are also several theoretical models of attribution of attack based on the social and political background. One of them, Jason Healey's methodology, consisted of 14 factors (see Table 1).

Table 1: The attribution theoretical framework

Analytical Element	Bundestag	National Health Service
Attack Traced to Nation	Many traces to Russia	Many traces to North Korea
Attack Traced to State Organizations	Many Traces	Many Traces
Attack Tools or Coordination in National Language		
State Control over the Internet	High	Very High
Technically Sophisticated Attack	Medium	Medium
Sophisticated Targeting	Yes	No
Popular Anger	Medium	High
Direct Commercial Benefit	Low	Assumed Very High
Direct Support of Hackers	Low	High
Correlation with Public Statements	Moderate	Very High
Lack of State Cooperation	Russia refused to cooperate	North Korea refused to cooperate
Who Benefits?	Russian government	North Korea economy
Correlation with National Policy	High	High
Correlation with Physical Force	Moderate	Moderate

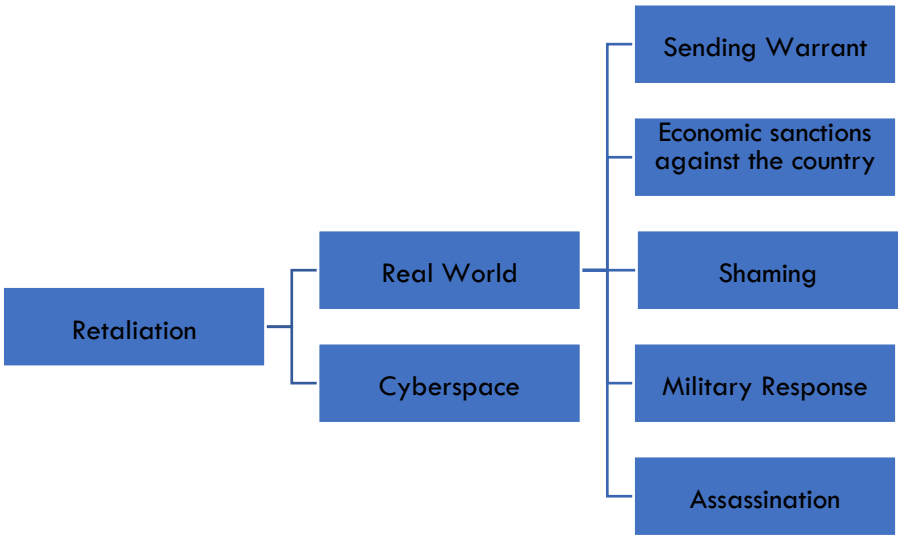
Source: Healey 2013, 265 – 276.

The members of the EU can use this theoretical framework or modify it to combine the political attribution with the technical one. Every one of these two methods possess flaws and problems but together may create a credible and effective attribution mechanism, which would strengthen the possible EU sanctions regime for cyberattacks.

The scenarios of potential sanctions for cyberattacks

Even though the uncertainty linked with the identification process of assailant's state authorities have already prepared a range of tools used to retaliate. A part of them could be observed in certain cases in the past. The others appeared only in doctrines and strategies and had never materialized in the real world. Generally, we can separate the retaliation in the real world and cyberspace. According to the international law, states should use proportionate measures, but it does not always happen.

Figure 5: The possible retaliation measures against cyberattacks



Sanctions in the cyberspace

The most reasonable option should be answered in a virtual world by using similar tools and methods as the opponent. It could be response from single members, groups of members of the EU. In the past, several cases were illustrating the proportional retaliation. In 1999 during Kosovo war Serbian hackers attacked the NATO websites using the Denial Distributed of Service Attacks (DDoS). In response to Western hackers affiliated and sympathized with mission also orchestrated the flooding type attack on the Serbian administration website (Borger 1999). Similar cyber skirmishes happened during 2001 Chinese-American crisis over the crash between the Chinese jet and American spy plane or between the hackers of conflicting sides like Pakistan and India or Israel and Palestinian

There is a slight difference in the Iranian attack on the United States banks in 2012. It was retaliation for the Stuxnet worm, which infiltrated the Natanan uranium enrichment facility and destroyed thousands of centrifuges. This computer program became the first inflicting damages

in the material world (Zetter 2011). However, Iran's abilities were too limited to conduct similar operation against the US and they decided to attack vulnerable sector – American banks (Volz and Finke 2016). This response was not proportional and was far less destructive and limited only to a digital world.

The retaliation in cyberspace is the most popular and probably will remain in the foreseeable future. The easy ways to carry out this kind of operations, the wide range of possible tools and the relatively small consequences in case of the mistake and last but not least the problems with attribution encourage actors to these actions. There are several weaknesses too. In most cases the damage would be minimal, probably the civilians would also be victims and there is also a threat of retaliation in cyberspace.

In the EU it will be hard to conduct such an operation. Firstly, only a small number of countries publicly announced the capabilities to perform the offensive operations. Among them are the Netherlands and Great Britain (Emmot 2018). Secondly, the EU and its members are not eager to use any offensive tools. Finally, it would be difficult to achieve a political agreement within the EU. So, this option could be used only by single countries or a group of countries, but the action from the EU as a whole is rather unimaginable due to the different potentials and willingness to engage in such an activity

Real world

For a long time the response to the cyberattack in the real world has remained only the deterrent tool recorded in different doctrines and strategies. But lastly the situation changed and there were many examples of sanctioning hostile cyber activity by economic sanctions, naming and shaming campaign or sending warrants for persons engaged in the hacking activity. There are several options of retaliation in the real world against cyberattack.

Military response

The strongest and harshest way of response is to conduct the military strike against a country which conducts the hostile operations in cyberspace. This kind of operation never happened in history, but, e.g. the United States officially declared that among retaliatory options they might use military force (Spillius 2011). In Europe, Germany considers this option too (Koch and Riedel 2018). NATO declared officially in the Wales summit declaration that cyberattack could trigger the article V and therefore possible military reaction (NATO 2014).

Considering that the EU has the equivalent of NATO Article V, which is article 42.7 of the treaty of European Union on the EU's mutual defence provision and it was even used after the terrorist attack in Paris in 2015 (Traynor 2015), the EU should consider a similar declaration to NATO. There is no need to provide a precise record of the conditions and situation of executing the military attack. It is commonly recognized as the response to a cyberattack with the magnitude comparable to a conventional attack with the death tolls. This kind of declaration should play a role of a deterrent factor and multiple available options rather than be considered as a feasible tool. There is a little chance that the EU or the EU members would use own armed forces.

First of all, devastating cyberattacks, which bring huge destruction and high death tolls are the part of Hollywood movies, which are far from reality now. What is more, the country that decided to conduct such a strike will change history because the consequences can be unimaginable and extremely politically costly. Furthermore, the EU has not had own armed forces and the armies of its members are relatively weak. Last but not least, there is weak political will for any military operations in the EU. However, it may change in the future with the ambitious plans of German-France tandem to set up European army (Stone 2018). Therefore, such declaration should be announced that EU may answer with a conventional attack against cyberattacks.

Sanctioning individuals

Arresting the cybercriminal was the first method used against persons engaged in hostile activity in cyberspace. In the 90s it was relatively easy because most of the attack was orchestrated from the domestic territory and was covered by national criminal law. In the 21st century, this situation has changed, and pursuing cybercriminals become more and more dangerous. However, the international and bilateral cooperation contributed to catching famous Max "Iceman" Butler and the Dark Market heads and this cooperation is still used and developed, e.g. under the Convention on Cybercrime.

But in 2014 the United States went even further and filed criminal charges against five Chinese military officers for stealing a trade secret. This kind of situation happened the first time in history and obviously could not achieve success, but it presented a determination of the US authorities and also the fact that they are more and more upset with increasing Chinese engagement in cyberspace activities. The government in Beijing rejected the accusations and obviously, the chances that these five persons will be sent to the U.S. are literally none, but it was a signal to the Chinese government to reduce their involvement in cyberespionage campaign and that United States government treats it seriously. It was later repeated against Iranian hackers (Denning 2017).

The members of the EU, but also the EU itself, can conduct similar activities. The Ministries of Justice of General Prosecutors may file criminal charges against officers of the foreign intelligence and issue arrest warrant. What is more, the EU can do the same through the Europol and its European arrest warrant. There are not the only available tools. The EU could also seize assets or ban access to own territory individuals accused or direct or indirect engagement in hacking. Yevgeniy Prigozhin – the head of Internet Research Agency could be banned from entering the EU territory after the next Russian interference in one of the EU countries. The other possible targets are the GRU or FSB commanders. This measure is available to the EU and was used in the past. Dozens of Russian citizens were sanctioned after the Crimean annexation (European External Action Service 2018).

Sanctions against the company

In 2015, just before the last summit between President Obama and Chinese President Xi Jinping, the media speculated that the United States would impose sanctions against the Chinese companies, which gained the largest benefits from the cyberespionage campaign (Davis and

Sanger 2015). Since that time, the Chinese companies Huawei and ZTE were banned from significant projects like building 5G infrastructure in Australia, India and the United States. Other countries like Japan, the United Kingdom, Germany consider these firms as a possible threat to national security (Leonardo 2018). The EU could ban certain companies from the EU market if it detects that they are engaged in espionage activity in the name of foreign intelligence state. There is the EU Air Safety List that includes all airlines banned from operating in Europe (European Commission 2018). It would be a good idea to create a similar list of producers of software and hardware if they threaten the security of the EU. Taking into consideration that the EU market is an attractive business target it could be an effective deterrence factor in the sanction regime.

Economic sanctions against the state

Not only can the certain companies be punished by the economic sanctions but also the states. The first victim of such measures was North Korea, which was accused of a massive cyberattack on Sony and in consequences forced the company to withdraw comedy movie about the North Korean leader from the United States cinemas. Barack Obama's administration decided to impose additional economic sanctions on North Korea and therefore setting precedence (Wroughton 2018). This decision was mostly symbolic as North Korea was imposed with multiple sanctions in the past and remained one of the most isolated countries in the world. But the American decision was more than just to punish Kim Dzong Un regime and should be understood as deterrence action illustrating the possible U.S. response.

The EU sanctions are one of the most dangerous weapons in a toolbox of this organization especially considering the scale of trade volume and investments in the EU. The EU sanctions harm Russia much more severe than the U.S. and Canada together (Rapoza 2017). Taking into account economic sanction, it would be probably the most damaging weapon in EU arsenal against states-sponsor cyberattack.

Implications and Lessons for the Future

Despite the political friction within the EU, the economic sanctions on Russia and travel bans on persons engaged in Crimea operation and a war in Eastern Ukraine have been maintained since 2014. Many pundits were skeptical about the abilities of the EU to first impose sanctions and later prolong them. What is more, these sanctions harm the Russian oligarchs and the Russian economy (Ćwiek-Karpowicz at al. 2015). It shows that the EU sanction regime could be effective and thus play a credible deterrent factor. Cyberattacks being a threat to every state, company and individual, it would be probably easier to persuade authorities of the countries to impose sanctions on hostile actors.

Considering the aforementioned options, it seems that the most probable tools that could be used are the sanctions against individuals both by banning them from entering the EU or by sending European Arrest Warrant. However, in the wake of the Ukraine crisis, the EU has shown determination and has imposed and maintained sanctions on Russian state and companies. This strong presentation of unity and strength has demonstrated the EU as the ambitious international

actor. It means that the sanctions could also be used against the actors engaged in a hostile cyber activity. Considering the military response, which is on this moment is highly unrealistic, but the declaration like NATO should be issued. It gives the next tool in the sanction regime and taking into account the German and France plan to create the EU army, it may be more realistic in the foreseeable future.

Every sanction imposed on other country needs to be supported with credible intelligence. Thus, the EU needs to improve own intelligence capabilities and the exchange of information. There are already countries like the Netherlands, France, Great Britain with significant abilities to detect, identify and attribute cyberattacks. It would be crucial for other EU members to gain such capabilities but there should also be a forum, where countries could exchange details about cyberattacks, techniques and tools of assailants. Similar groups exist and are devoted to the problem of terrorism.

Last but not least, the sanction regime could deter state sponsor or state enabled attacks, but it would be utterly ineffective against non-state actors such as individuals' hackers or group of criminals. The last breach of date in British Airways (Morris 2018) or Facebook breach (O'Flaherty 2018) were done by non-state actors showing the increasing capabilities of such actors. Therefore, alongside with developing the effective regime of sanction, the EU needs to strengthen cyberdefence of its members and institutions.

---

* Andrzej Kozłowski is the editor-in-chief of the biggest portal on cybersecurity and information warfare in Poland: Cyberdefence24.pl. He is also a lecturer at the University of Lodz, Collegium Civitas in Warsaw and European Academy of Diplomacy; and a security expert at the Pulaski Foundation and the Warsaw Institute for Strategic Initiatives.

References

Borger Julian. 1999. "Pentagon kept the lid on cyberwar in Kosovo." *The Guardian*, November 9. https://www.theguardian.com/world/1999/nov/09/balkans.

Davis, Hirschfeld Julie, and David E. Sanger. 2015. "Obama and Xi Jinping of China Agree to Steps on Cybertheft." *New York Times*, September 25. https://www.nytimes.com/2015/09/26/world/asia/xi-jinping-white-house.html.

De Carbonnel, Alissa, and Robin Emmott. 2018. "Fearing election hacking, EU leaders to ready sanctions." *Reuters,* October 18. https://www.reuters.com/article/us-eu-summit-cyber/fearing-election-hacking-eu-leaders-to-ready-sanctions-idUSKCN1MS2N3.

Denning, Dorothy. 2017. "Cyberwar: How Chinese Hackers Became a Major Threat to the U.S." *Newsweek*, October 10. https://www.newsweek.com/chinese-hackers-cyberwar-us-cybersecurity-threat-678378.

Drozdiak, Natalia, and Nikos Chrysoloras. 2018. "U.K., Netherlands Lead EU Push for New Cyber Sanctions." *Bloomberg*, October 11. https://www.bloomberg.com/news/articles/2018-10-11/u-k-netherlands-lead-eu-push-for-new-cyber-sanctions-document.

Emmot, Robin. 2017. "NATO mulls 'offensive defence' with cyber warfare rules." *Reuters*. November 30, https://uk.reuters.com/article/uk-nato-cyber/nato-mulls-offensive-defence-with-cyber-warfare-rules-idUKKBN1DU1GV.

European Commission. 2018. *The EU Air Safety List*. https://ec.europa.eu/transport/modes/air/safety/air-ban_en.

European External Action Service. 2018. *EU sanctions against Russia over Ukraine crisis*. https://europa.eu/newsroom/highlights/special-coverage/eu-sanctions-against-russia-over-ukraine-crisis_en.

Fruhlinger, Josh. 2018. "Top cybersecurity facts, figures and statistics for 2018." *Csoonline*, October 10. https://www.csoonline.com/article/3153707/security/top-cybersecurity-facts-figures-and-statistics.html.

Goldsmith, John. 2017. "The Strange WannaCry Attribution." *The Lawfareblog*, December 21. https://www.lawfareblog.com/strange-wannacry-attribution.

Healey, Jason. 2013. *A Fierce Domain: Conflict in Cyberspace 1986 to 2012, Arlington: Cyber Conflict Studies Association.*

Kaplan, Fred. 2016. *Dark Territory: The Secret History of Cyber War*. New York: Simon&Schuster.

Karpowicz-Ćwiek, Jarosław, at al. 2015. *Sanctions and Russia*. Warsaw: PISM. https://www.pism.pl/publications/books/Sanctions_and_Russia.

Koch, Moritz, and Donata Riedel. 2018. "Germany could dispatch armed forces in response to cyberattacks." *Handelsblatt*, June 6. https://global.handelsblatt.com/politics/germany-soldiers-combat-cyberattacks-931929.

Leonardo, Luigi. 2018. "More countries consider banning Huawei and ZTE." *GadgetMatch,* November 14. https://www.gadgetmatch.com/huawei-zte-5g-ban-australia-japan-uk-germany/.

Mandiant. 2013. *APT1 Exposing One of China's Cyber Espionage Units*. https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

Morris, Hugh. 2018, "British Airways data hack hits 380,000 recent customers." *Telegraph*, September 7. https://www.telegraph.co.uk/travel/news/ba-british-airways-data-hack-compensation/.

NATO. 2014. *Wales Summit Declaration*. Last updated August 30, 2018. https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

O'Flaherty, Kate. 2018. "Facebook Data Breach -- What To Do Next." *Forbes*, September 28. https://www.forbes.com/sites/kateoflahertyuk/2018/09/29/facebook-data-breach-what-to-do-next/#57ba903f2de3.

Rapoza, Kenneth. 2017. "Here's How Europe's Russian Sanctions Differ From Washington's." *Forbes*, June 23. https://www.forbes.com/sites/kenrapoza/2017/06/23/heres-how-europes-russian-sanctions-differ-from-washingtons/#18e79a6a5161.

Spillius, Alex. 2011. "US could respond to cyber-attack with conventional weapons." *Telegraph*, June 1. https://www.telegraph.co.uk/news/worldnews/northamerica/usa/8550642/US-could-respond-to-cyber-attack-with-conventional-weapons.html.

Stone, Jon. 2018. "EU army: Brussels 'delighted' that Angela Merkel and Macron want to create European military force." *The Independent*, November 14. https://www.independent.co.uk/news/world/europe/eu-army-angela-merkel-macron-germany-france-military-european-commission-juncker-a8633196.html.

Traynor, Ian. 2015. "France invokes EU's article 42.7, but what does it mean?" *The Guardian*, November 16. https://www.theguardian.com/world/2015/nov/17/france-invokes-eu-article-427-what-does-it-mean.

Volz, Dustin, and Jim Finkle. 2016. "U.S. indicts Iranians for hacking dozens of banks, New York dam." *Reuters*, March 24, https://www.reuters.com/article/us-usa-iran-cyber/u-s-indicts-iranians-for-hacking-dozens-of-banks-new-york-dam-idUSKCN0WQ1JF.

Wroughton, Lesley. 2018. "U.S. Treasury sanctions North Korean hacker, company for cyber attacks." *Reuters*, September 6. https://www.reuters.com/article/us-cyber-northkorea-sanctions/u-s-treasury-sanctions-north-korean-hacker-company-for-cyber-attacks-idUSKCN1LM2I7.

Zetter, Kim. 2011. "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History." *The Wired*, November 7. https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.

The Encryption Paradox: Examining Bottlenecks in Devising Policy Responses

By Anushka Kaushik*

This paper aims to examine the hindrances to formulating policies on the use of encrypted communication including the fundamental contradiction between the interests of the government and manufacturers or companies aiming to build the most secure software. By using the concept of encryption workarounds, defined by Kerr and Schneier (2017), as lawful efforts undertaken by governments to reveal unencrypted plaintext of a target's data, this paper will highlight the intractable path to developing policy responses at the regional and domestic level. Analysing these bottlenecks that significantly slow down policy formulation will pave the way for a better understanding of the approach that governments should adopt in mitigating technology-driven insecurity. This research effort will be augmented by reflecting on select past examples of governments seeking third-party assistance to decrypt information for the purposes of stemming future criminal or terrorist activity.

Key words: end-to-end encryption, encryption workarounds, cybersecurity, vulnerabilities.

Introduction

According to recent estimates, 22 percent of global communication traffic will be protected via end-to-end encryption by 2019. A significant number of popular messaging applications today boast of securing communication on their platforms in this manner, making the information exchanged both inaccessible and unreadable to a third party (Lewis, Zheng, and Carter 2017) 'End-to-end encryption' refers to the encryption of messages that are in transit from a sender to a receiver, and while it is not as integrated or widely available as endpoint encryption businesses are developing more user-friendly ways to integrate it into their platforms (The Chertoff Group, 2015). This has easily become one of the defining technological trends in today's internet landscape.

In August 2018, the governments of the United States, United Kingdom, Canada, Australia, and New Zealand issued a joint statement on principles of access and encryption. The statement reflected on the increasing use and sophistication of certain encryption designs that present challenges for nations in combating serious crimes and threats to national and global security. While recognising that encryption is vital to the digital economy and a secure cyberspace, the statement emphasised pursuing technological or legislative methods when governments face impedi-

ments to lawful access to information for the protection of their citizens, according to the document published by the Australian Department of Home Affairs. Increasingly, policymakers and legislators around the world are responding to the trend of widespread deployment of encryption in devices in order to take down obstacles to accessing private information. Yet, the joint statement, as well as the broader narrative on encryption around the world is precipitated not only by the increased availability of encryption tools. For example, the recent spate of terror attacks in various European cities has largely influenced the debate in countries like France where an amendment that could require electronic manufacturers to build back doors into their products was debated but ultimately rejected by the National Assembly. With the intention of empowering law enforcement to stem terrorist activities, other member-states of the European Union like Hungary and Poland are issuing new regulations and amendments that increase not only government access to digital data but also the scope of surveillance. In the US, Edward Snowden's revelations about mass surveillance by the government had a profound effect on the availability of strong encryption tools; perhaps owing to the need to distinguish governmental activity from commercial products, device manufacturers have deployed default encryption systems that automatically store data in an encrypted manner (The Chertoff Group, 2015). In August, as Yuthika Bhargava highlighted in her August 23, 2018 The Hindu article, Facebook-owned WhatsApp rejected a demand by the Government of India to find a solution which could trace the origin of a message on its platform. The company argued that traceability would undermine end-to-end encryption and affect the application's privacy protection duties.

The fact that governments want access to private information for achieving broader national security objectives is not new. However, necessitating assistance from manufacturers of encryption products, and the resulting fundamental discord between government objectives and commercial interests, make the policy process more intractable. This article analyses the bottlenecks to policy formulation that significantly slow down policy formulation, in an effort to pave the way for a better understanding of the approach that governments should adopt in mitigating technology-driven insecurity.

What constitutes a 'good' encryption policy?

Encryption policy entails the full array of government activities that guide the development, use, and adoption of encryption technology. It also speaks of a normative judgement on the part of the government about the value of such technology and is underpinned by geopolitical, social, and economic contexts (Budish, Burkert, and Gasser 2018). Therefore, encryption policies can be directly or indirectly used to further certain objectives as they tend to have an impact both domestically and internationally. A country's encryption policy can also have ripple effects: given the massive number of interdependencies between international trade, technological trends, and geopolitics, a decision on encryption at the domestic level can impact another country's public policy, private sector, and regulatory framework. Encryption policy can be implemented via various tools which are not restricted to only legislation and regulation but also include multilateral treaties, standard-setting through cooperation with all stakeholders, exercising hegemonic status and soft power to influence other governments or corporations to follow similar regulation, and compelling private manufacturers to assist in criminal investigation, respectively.

There are numerous examples of states using one or more of such policy instruments to tackle the increasingly grey areas emerging from the widespread use and deployment of encryption tools. The Australian government released a draft of the Assistance and Access Bill in August 2018, which provides security agencies with a new set of powers to respond to the challenges posed by encryption. The explanatory document emphasises that 95 percent of the Australian Security Intelligence Organisation's (ASIO) most dangerous counter-terrorism targets actively use encrypted messages to conceal their communications and therefore, the use of encryption is eroding the ability of law enforcement to access intelligible data. The bill broadens the obligations of domestic and foreign communication providers—which include device manufacturers, application and software providers, and carriage service providers—to allow access to communication. Moreover, it introduces new computer access warrants for law enforcement, enabling them to covertly obtain evidence directly from a device, and strengthens the ability of security authorities to overtly access data through the existing search and seizure warrants, according to the document published by the Australian Department of Home Affairs. The Department of Home Affairs maintains that provisions will only be implemented within caveats like technical feasibility and that providers will not be prevented from fixing existing systemic vulnerabilities. However, there are aspects of the bill that raise significant concerns about transparency, oversight, and accountability structures and processes, as reported by Monique Mann in her August 15, 2018 article in The Conversation. It allows for a relevant government authority to issue a "technical capability notice" that would require a communications provider to build a new capability enabling police access to a device or service. This, coupled with the massive non-compliance fines makes the Australian bill one of the tougher draft legislations to be discussed by a democratic state, stoking worries of a dangerous precedent for other nations.

In the US in August, law enforcement agencies took Facebook to court to obtain access to a suspect's voice conversations on their Messenger app; the police were investigating members of the MS-13 gang, as reported by Dan Levine and Joseph Menn in their August 18, 2018 report on Reuters. Given that Messenger voice calls are encrypted end-to-end, the only way to comply with the government's demand would be to rewrite the code relied upon by all its users to remove encryption, or else, hack the government's target. Similarly, global messaging application WhatsApp, owned by Facebook, has not wavered in its stance against providing traceability to messages, arguing that doing so would rescind one of its key features, i.e., end-to-end encryption, which means the application retains no user data and access to conversations. The Indian government had demanded, among others, traceability of messages following a series of lynchings purportedly caused by the spread of fake news and misinformation through WhatsApp. These incidents are illustrative for two reasons: they indicate the different tools at a government's disposal to shape encryption policy directly or indirectly; and they highlight the perpetual disagreement between, on one hand, software companies wanting the highest levels of privacy, and on the other, state forces mandated to promote security.

What, then, constitutes a good or bad encryption policy? Is there a degree of normativity that can be attached to domestic or international policies on encryption?

At the heart of the policy debate on encryption lays the recurring privacy-security narrative that posits a trade-off between the privacy of citizens and the degree to which the state monitors and intercepts communication for keeping them secure. To a large extent, the diffusion of encryption technology to average users has been largely problematised within this dichotomy and informed by the underlying paradox: less privacy to the individual, better security for the nation. However, in the context of encrypted communications, this poses a problem as there simply is not enough data to indicate the extent to which criminal or terrorist investigations have been hampered by encryption tools. Media reports on the November 2015 Paris terror attacks, for example as highlighted by Evan Perez and Shimon Prokupecz in their December 17, 2015 report in CNN, quote government officials as saying that the suspects had used encrypted messaging applications to communicate with each other. In the US, the Federal Bureau of Investigation (FBI) has taken Apple to court to gain access to the smartphone of one of the suspects in the December 2015 mass shooting in San Bernardino, as reported by Ellen Nakashima in her April 16, 2016 article in The Washington Post. While the ubiquitous nature of encryption will be an impediment to successful law enforcement processes and its use could greatly increase in the future, there is currently a lack of empirical data that shows the magnitude of its impact. Caution must be exercised, therefore, when attributing the role of encrypted technologies in foiling overall national security objectives; any policy framework must reflect such consideration.

Encryption workarounds in the context of policy development

In the context of criminal investigations and the larger question of the impact of encrypted communications, there is another dimension that merits consideration: the existence of encryption workarounds. Defined by Kerr and Schneier (2017) as any lawful government effort to reveal unencrypted plaintext of a target's data that has been concealed by encryption, the use of encryption workarounds raises significant legal and practical hurdles. The most important takeaway, however, is that the existence of workarounds could mean that encryption does not cause as remarkable a shift in law enforcement's investigative powers as thought of. Whenever targets use encryption, governments turn to a set of tools and methods to remove the barrier that denies access to private information. Kerr and Schneier identify six of them—the first three are key-based methods that rely on finding, guessing, or compelling the key which then allows decryption; the latter three focus on government efforts to exploit a flaw in the encryption system, accessing plaintext when the target's device is in use, and locating a copy of the plaintext. Each of these methods brings forth certain tradeoffs and raises questions that need to be addressed by future legal and policy frameworks on encryption. For example, accessing plaintext when the target's device is in use by gaining remote access through technical means, brings with it legal ambiguities on government hacking. There are also substantial privacy and human rights implications associated with this method, including the risk of a paucity of oversight, accountability, and transparency (European Digital Rights 2017). Similarly, governments can exploit a flaw in the encryption scheme as was illustrated in the San Bernardino terrorist attack. After Apple refused to comply with the FBI's request to disable the auto-erase feature on the iPhone, the bureau reportedly sought third-party assistance. This brought forth the question of government stockpiling vulnerabilities and whether the government should have disclosed the vulnerability, so Apple could patch it. Despite the host of ethical, legal, and technical challenges, governments have en-

cryption workarounds at their disposal and they are used, sometimes in combination, to counter encryption barriers.

Security concerns with respect to weakening encryption, in the form of providing exceptional encryption access, for example, have been well-documented and substantiated by security researchers, and recognised—in principle at least—by most governments. 'Exceptional access' is defined as giving an individual or organisation access to readable data someone has encrypted and required that the third party be granted access to the plaintext data associated with encrypted data (Vandenberg 2018). Building on any form of exceptional access would significantly increase system complexity and features to permit such access to law enforcement could be challenging given that their use would be surreptitious (Abelson et al. 2015). Therefore, creating an exceptional access system with encryption accessible to government authorities and law enforcement officials but not to malicious actors, would be technically impossible or complex enough to implement that the overall safety of communications would suffer (The Chertoff Group 2015). Such an exceptional access system would also compel companies to possibly relinquish best practices developed to make the internet and interactions through it more secure. With forward secrecy, for example, a new session key is generated for each session that a user initiates which greatly reduces the exposure of an entity that has been compromised. Since the session keys are discarded after each session, any attacker breaching a network can only gain access to decrypted data from the breach until the breach is discovered, rendering historic data safe (Abelson et al. 2015). Therefore, mandating weaknesses in encrypted systems would not only increase vulnerabilities but also hinder innovation and development of security markets.

Challenges to formulating encryption policies

Given the myriad of technical, legal, practical, and ethical questions regarding the use of encrypted technologies and exceptional access to data, there are a number of obstacles that affect policy development at the domestic, regional, and international level. Owing to the global nature of the internet and involvement of actors across countries in availability and development of interconnected communication platforms, the effects of these bottlenecks cannot be clearly delineated at each level given considerable overlaps.

The first set of challenges arises over the question of jurisdiction. Attempting to develop any international access framework and requiring communication providers to guarantee access to numerous government agencies in countries that do not necessarily have the same legal framework would be extremely complex. Having one set of internationally defined conditions under which lawful access to encrypted communications can be granted would be an immensely arduous undertaking, not least due to the differing approaches of nation-states on freedom of communications, access to the internet, and regulation of cyberspace. There are unanswered questions regarding enforcement and compliance, illustrated in the ongoing discussions between WhatsApp and the Indian government—is it feasible for a government to mandate a feature like traceability across all applications that are used within its jurisdiction? Not only would it be difficult to get companies to comply with such a rule but mandating it would simply spur an increased use in applications like Tor or an increased use of VPNs, providing alternate methods of secure communi-

cation. Any aggressive enforcement would also negatively affect innovation and industry. The Australian Assistance and Access bill is an example of domestic policies having competing regulations to regional ones as certain parts of the bill can compel companies to override the General Data Protection Regulation (GDPR) terms in Europe and hand data over to Australian law enforcement, as reported by Chris Duckett in his September 11, 2018 article on ZDNet. Cross-border regulatory differences, therefore, pose an intractable barrier to developing a universally enforceable and accepted encryption policy.

The fundamental discord between incentives of the private sector—including service providers, vendors, manufactures, and software developers—to enhance the security of communications and the larger national security objectives of the government will continue to be a point of contention. A host of new developments discussed earlier in this paper, represent a technological trend aimed at providing the highest level of privacy and security of communications to the average user. Encryption technology aims to create barriers to third-party access, a property that is in the interests of law enforcement to counter during criminal investigations. The San Bernardino case is a prime example of this and there continue to be more such instances. Therefore, the extent to which third-party assistance can be mandated and necessitated by governments will be crucial. The question of jurisdiction is relevant here as well—can foreign companies be required to fundamentally alter essential features of their application, like default end-to-end encryption for example, depending on where they operate?

The third set of obstacles to encryption policy formulation raises ethical and normative considerations. While this paper has established that moving beyond the privacy-security dichotomy is crucial to developing a comprehensive approach to policy development in this area, encryption policy reflects a normative judgement on the part of the government about the value of such technology. There is a continual strain of thinking on the part of governments to gain access to encrypted communication without breaking encryption or introducing systemic vulnerabilities. Respecting trust, cooperation, and innovation in the internet ecosystem and to all stakeholders forms the benchmark of democratic digital policies. While states have recognised the significance of encryption in ensuring safe and secure communication, the implications of legislation, if it seeks to counter such provisions, on democratic values, would need to be carefully considered.

Conclusion

As businesses develop user-friendly ways to integrate end-to-end encryption and adopt operational systems that change default local encryption setting from ‘off’ to ‘on’, aiming for the highest level of privacy and security for the user, governments face increasing barriers of lawfully accessing citizens’ private information. The recent spate of terrorist attacks in Europe have largely influenced policy discussions, stoking fears that encrypted communications will significantly restrict governments’ abilities to successfully stem terrorist and criminal activities. The misuse of messaging platforms by rapidly spreading misinformation has started to fuel similar conversations in India.

However, lack of sufficient data on the impact of encryption on criminal investigations and the

existence of encryption workarounds at the disposal of the government may point to a less dramatic shift in governments' investigative powers than currently perceived. This also necessitates a move beyond the privacy-versus-security dichotomy that the policy debate on encryption lays within. Security concerns and the detrimental impact on innovation and industry of weakening encryption or enabling exceptional encryption access have been well-documented. These technical, legal, and practical considerations highlight the considerable hindrances to policy development in the field of encryption. There are unresolved issues with respect to jurisdiction and legitimacy of an internationally-enforceable encryption policy framework. The fundamental discord between incentives of the private sector, including service providers, vendors, manufactures, and software developers, to enhance the security of communications and the larger national security objectives of the government will continue to be a point of contention. Encryption policy debates also bring forth ethical concerns and the significance of a normative judgement that a state attaches to the value of such technology, particularly in protecting democratic principles.

The dialogue on encryption, therefore, is part of a much larger debate on security, accountability, and responsibility of internet tools. Developing an encryption policy that recognises the principles of mutual trust and responsibility between all stakeholders and accounts for the commercial interests of private companies, state security objectives, and safe online communications for the individual user will define efforts at the national, regional, and international level.

This paper was originally published in Digital Debates, a journal by the Observer Research Foundation on October 4, 2018.

---

* Anushka Kaushik is Research Fellow, GLOBSEC Policy Institute, Bratislava.

References

Bhargava, Yuthika. 2018. "Whatsapp rejects India's demand to trace origin of message," *The Hindu*, August 23. https://www.thehindu.com/sci-tech/technology/whatsapp-rejects-indias-demand-to-track-origin-of-message/article24761366.ece.

Budish, Ryan., Burkert, Herbert., and Urs Gasser. 2018. *Encryption Policy and its International Impacts: A Framework for Understanding Extraterritorial Ripple Effects*. Hoover Institution. https://www.hoover.org/research/encryption-policy-and-its-international-impacts.

Department of Home Affairs, Government of Australia. 2018. *Assistance and Access Bill 2018*. https://www.homeaffairs.gov.au/consultations/Documents/explanatory-document.pdf.

Department of Home Affairs, Government of Australia. 2018. *Statement of Principles on Access to Evidence and Encryption*. https://www.homeaffairs.gov.au/about/national-security/five-country-ministerial-2018/access-evidence-encryption.

Duckett, Chris. 2018. "Internet Architecture Board warns Australian encryption-busting laws could fragment the internet," *ZDNet,* September 11. https://www.zdnet.com/article/internet-architecture-board-warns-australian-encryption-busting-laws-could-fragment-the-internet/.

Vandenberg, Dustin T. 2018. "Encryption Served Three Ways: Disruptiveness as the Key to Exceptional Access," *Berkeley Technology Journal Law Journal* 32 (4): 531-562. https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2167&context=btlj.

European Digital Rights. 2017. "Encryption Workarounds: A Digital Rights Perspective" https://edri.org/files/encryption/workarounds_edriposition_20170912.pdf.

Abelson, Harold, et al. 2015. "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to all Data and Communications", *MIT Computer Science and Artificial Intelligence Lab*. https://dspace.mit.edu/handle/1721.1/97690.

Kerr, Orin S., and Schneier, Bruce. 2017. "Encryption Workarounds." *Georgetown Law Journal* 106: 989-1019. https://ssrn.com/abstract=2938033.

Lewis, James A., Zheng, Denise E., Carter, and A. William. 2017. *The Effect of Encryption on Lawful Access to Communications and Data*. Washington, D.C.: CSIS and Rowman & Littlefield. https://www.csis.org/analysis/effect-encryption-lawful-access-communications-and-data.

Mann, Monique. 2018. "The devil is in the detail of government bill to enable access to communications data." *The Conversation*, August 15. https://theconversation.com/the-devil-is-in-the-detail-of-government-bill-to-enable-access-to-communications-data-96909

Nakashima, Ellen. 2016. "FBI paid professional hackers one-time fee to crack San Bernardino iPhone." *The Washington Post*, April 12. https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html.

Perez, Evan, and Shimon Prokupecz. 2015. "Paris attacker likely used encrypted apps, officials say," *CNN*, 17 December. http://www.cnn.com/2015/12/17/politics/paris-attacks-terrorists-encryption.

The Chertoff Group. 2015. *The Ground Truth About Encryption*. https://www.chertoffgroup.com/files/238024-282765.groundtruth.pdf.

The Political Culture in The Cyberspace. Profiling the Cyber Security

By Cosmina Moghior*

Concepts like cyberspace, cyber security, and cyber war are increasingly raised either in media, public discourses or in everyday life. The main reason is likely the high interconnection of cyberspace with the physical space, our daily life. We live a double life, one in the virtual space and the other in the physical one. What is the role of the state in this constellation? Are the characteristics of a state influencing the level of cyber security? This article aims to identify some of the factors impacting the cyberspace, present the approaches on cyberspace in the selected countries, effectuate the preliminary analyses of the selected data, and provide the individual interpretation of the results, correlations, and graphics.

Key words: cyberspace, cyber security, political culture, personal freedom, democracy, ICT.

Introduction

The cyber domain is evolving, and along with the opportunities, we are witnessing the emergence of new security challenges from the cyberspace. The cyber-attacks can inflict grave risks, spanning from information leaks to actual physical damage. The importance of cyberspace had been recognized by a great number of states, recognizing it as the fourth operational domain. But what is the meaning of cyberspace and what are the factors contributing to cyber security? The present comparative research seeks answers to these questions, using various statistical analyses on the People's Republic of China, Netherlands and Russian Federation.

The first section of the research focuses on depicting the main characteristics of the cyber security strategies of the states, chosen as a reference for the study, while the second section emphasises the methodology used. The third section discusses the initial interpretation of the results for each country. Finally, the last section compares the results and verifies if there is a general factor that influences the cyber security of the selected states. The conclusion confronts the hypothesis set of the study with the results.

1. The Cyber Security Strategies

The term cyberspace is often defined with cyber security, cyber-terrorism and cyber-attacks. Guiora (2017, 17) made a clear distinction between cyber-attacks and cyber security. The first refers to the action of harming the state's critical infrastructure, while the former illustrates the

states' contractual duty to protect the individuals from any attacks. If we are posing the question 'Cyber security for whom?' Guiora's answer would be civilians, public infrastructure and overseas assets, public and private.

Many states have recognized the strategic importance of the cyberspace. Thus, they formulated a cyber-security strategy which varies depending on their security culture and threat perception (Yarger 2008, 43-49). As an example, the Chinese government evokes sovereignty, as stated in the UN Charter: the states have equal sovereignty and the right to choose their path of development without foreign intervention in the internal affairs. China stands for the regulation of the cyberspace, in a form agreed by all the states, to protect the individuals' rights and interests and to promote the digital economy and the cultural exchange (Shaohui, 2017). China believes that the arms race in the cyberspace is one of the main threats for the international security and stability, contradicting the principle of peaceful use of cyberspace. To defend itself from these threats, China introduced a backup force for the cyberspace (China Copyright and Media, 2016).

The strategy of the Dutch government is concentrated the most on the military dimensions of the cyber security, where the Dutch Ministry of Defence is tasked to eliminate the cyber threats and the cyberspace offers an opportunity to increase national security by using the cyber instruments for enhancing military and intelligence capabilities. The Defence Cyber Expertise Centre (DCEC) was created to foster the knowledge development of the cyberspace in cooperation with research institutions and businesses (Dutch Ministry of Defence 2012, 8-16). The civilian dimension of the strategy was designed on a triangle model, involving the individuals, the government and the private sector. The second strategy clarifies the roles and the relations between the actors involved in the cyberspace and the methods used for assuring the cyber security (National Coordinator for Security and Counterterrorism 2013, 18).

In the case of the Russian Federation, there is a terminological dissonance involved, as the concept of cyberspace is too narrow to cover all the aspects of cyber security. Thus, the concept of information space is employed, which deals with all the technical communication: the internet and other telecommunication networks. Also, because of its trans-national nature, Russia believes that the cyberspace regulation is almost impossible. The priority in the Russian strategy is to create the necessary mechanisms to deter cybercrime with the support of the private parties. Other priorities are the critical information infrastructure protection, development of the public-private partnership, the increase in the citizens' digital literacy and strengthening of the international cooperation to formulate a global system of cyber security (Federation Council (Russia), 2014).

2. Methodology

The quest of this research is challenging, but it might help to understand better certain aspects of the cyberspace. This section will unpack research questions, select the variables and set the research hypothesis.

2.1. The Theoretical Framework of the Research

Aiming to identify the factors which are influencing the cyber security in the People's Republic of China, Netherlands and Russian Federation, the Personal Freedom Index, the Democracy Index and the ICT Development Index (IDI) are used as independent variables. To illustrate the cyber security, the risk of malware infection is used as the dependent variable. The selected states have different national and foreign policies, levels of technology development and organizations responsible for the cyber security. They have different perspectives on cyberspace. To identify the factor of cyber security, the following hypotheses are tested:

A. The relation between Personal Freedom and the risk of malware infection:

H0: There is no relation between Personal Freedom and the risk of malware infection.
H1: The highest the Personal Freedom is, the highest is the risk of malware infection.
H2: The highest the Personal Freedom is, the lowest it the risk of malware infection.

B. The relation between the democracy index and the risk of malware infection:

H0: There is no relation between the democracy index and the risk of malware infection.
H1: The highest the democracy index is, the highest is the risk of malware infection.
H2: The highest the democracy index is, the lowest it the risk of malware infection.

C. The relation between the ICT Development Index and the risk of malware infection:

H0: There is no relation between the ICT Development Index and the risk of malware infection.
H1: The highest the ICT Development Index is, the highest is the risk of malware infection.
H2: The highest the ICT Development Index is, the lowest it the risk of malware infection.

Malware is a software which has malicious intent or effect. The malware family includes threats like Trojan horses, viruses, worms, adware, backdoor, spyware and others (Aycock 2006, 2). This article focuses only on the web-based attacks (online threats). The figures used to reflect the risk of online threats resulted from the frequency of encountered detection verdicts on users' machines in each country, by the Kaspersky Lab's web antivirus. The value illustrates the percentage of users from a particular country who experienced a malware infection (Garnaeva at al., 2015). The risk of malware infection is the dependent variable.

The Personal Freedom Index measures the degree in which individuals enjoy the civil liberties (freedom of speech, religion, and association and assembly). The freedom of expression, which includes control over the Internet Access, is one of the components of the Personal Freedom Index. The use of internet has tremendous importance as it is one of the main instruments to inform, express and interact with other individuals (Vásquez and Porčnik 2017, 9-14).

The Democracy Index measures citizens' fundamental political freedoms and liberties, the government functioning efficiency, independent media and judiciary system and isolated anomalies (The Economist Intelligence Unit 2017, 52).

The ICT Development Index (IDI) is combining 11 indicators for monitoring the level, the progress, the differences and the development potential of the information and communication technolo-

gies (ICTs) in different countries. There are three factors of information and communication technologies development: access, use and skills. Combining these variables, creates an outcome, or an impact, which is the level of ICT development level in a country. The values resulted from combining those indicators reflect the stage of development of the information society (United Nations - ITU 2014, 36-37).

2.2. Data Processing, Corroboration and Analysis

We have selected secondary data, gathered through desk-based research from various sources. *The Personal Freedom Index* was collected from the *Human Freedom Index 2018* (Vásquez and Porčnik 2018, 121-301) a report co-published by the Cato Institute, the Fraser Institute, and the the Friedrich Naumann Foundation for Freedom. *The Democracy Index* was collected from the report issued by the Economist Intelligence Unit (2017, 25-27). The *ICT Development Index* was collected from different reports for 2011 (ITU 2012, 21), 2012-2013 (ITU 2014, 42), 2014-2015 (ITU 2016, 13) and 2016 (ITU 2017, 31) by the United Nations International Telecommunication Union. Finally, the *Risk of Malware Infection* was collected from the annual statistics issued by Kaspersky Lab at the for 2011 (Namestnikov, 2012), 2012 (Namestnikov and Maslennikov, 2012), 2013 (Funk and Garnaeva, 2013), 2014 (Garnaeva at al., 2014), 2015 (Garnaeva at al., 2015) and 2016 (Garnaeva at al., 2016) (see Table 1).

Table1: The People's Republic of China, the Netherlands and the Russian Federation

	Year	Personal Freedom	Democracy index	ICT Development Index	The risk of malware infection
CHINA	2011	5.74	3.14	3.88	41.4
	2012	5.64	3	4.39	38.4
	2013	5.74	3	4.64	32.2
	2014	5.52	3	4.8	30.1
	2015	5.37	3.14	5.19	33.12
	2016	5.35	3.14	5.17	36.53
THE NETHERLANDS	2011	9.22	8.99	8.34	37.1
	2012	9.16	8.99	8.95	23.9
	2013	9.19	8.84	8.93	27.3
	2014	9.21	8.92	8.36	26.4
	2015	9.37	8.92	8.46	18.7
	2016	9.4	8.8	8.4	14.5
THE RUSSIAN FEDERATION	2011	6.38	3.92	6	55.9
	2012	6.3	3.74	6.48	58.6
	2013	6.27	3.59	6.7	54.5
	2014	5.97	3.39	6.79	53.81
	2015	5.69	3.31	6.95	48.9
	2016	5.71	3.24	5.91	42.15

Next, the article provides the radiography based on the statistical distribution of the indicators. This model indicates the type of relationship between the variables (see Table 2). China's cyber security level is the lowest among the selected countries. With a low statistical deviation of σ= 3.87, the level of cyber security in China is relatively constant in comparison with the other countries, the aspect which is also illustrated by the quartiles. Also, the mean of Me= 34.83 shows that the risk of malware infection has a tendency towards high values, which implies mostly low levels of cyber security. The high statistical deviation of σ= 7.12 shows that the Netherlands fluctuant level of cyber security and the mean of Me= 22.15 shows that the Risk of Malware Infection tends to oscillate from a relatively low level of cyber security (37,1 in 2011) to a high level of cyber security (18,7 in 2015). As a result, the interquartile range is the highest among the selected countries. The situation is different in the case of the Russian Federation, where we can identify a low level of cyber security, as the indicators show high levels in the Risk of Malware Infection with a mean of Me= 54.16. The value of the statistic deviation σ= 5.39 mid-range in comparison with the other two countries, which shows that although there have been registered some changes in this respect, they are not significant ones.

Table 2: Statistical Analysis of the Indicators

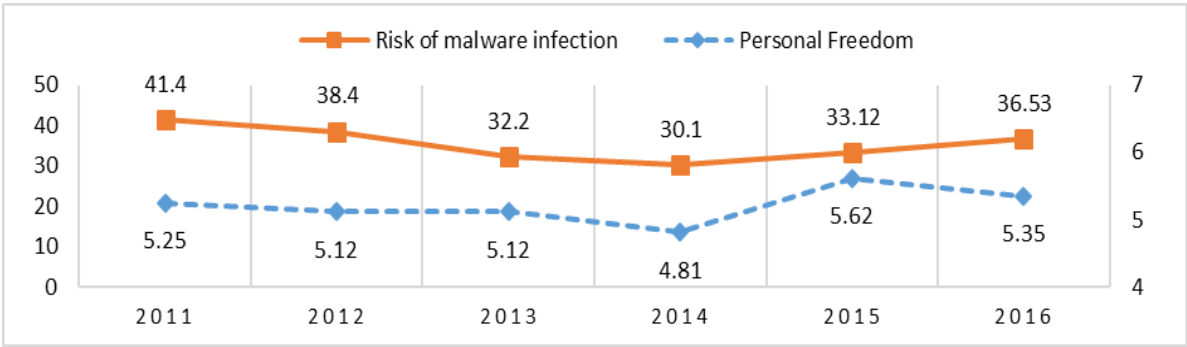
	Variable	$\bar{X}$	Me	M0	Q1	Q2	Q3	A	Aiq	σ2	σ	CV
CHINA	Personal Freedom	5.35	5.58	5.12	5.37	5.58	5.74	-0.15	0.38	0.03	0.16	2.98
	Democracy index	3.14	3.07	3.14	3	3.07	3.14	0.14	0.14	0.006	0.07	2.23
	ICT Development Index	5.17	4.72	0	4.26	4.72	5.18	1.31	0.913	0.25	0.45	8.79
	The risk of malware infection	36.53	34.83	0	31.68	34.83	39.15	11.3	7.48	17.95	3.87	10.57
THE NETHERLANDS	Personal Freedom	9.26	9.22	0	9.18	9.22	9.38	-0.01	0.20	0.01	0.09	0.99
	Democracy index	8.91	8.92	8.99	8.83	8.92	8.99	-0.19	0.16	0.01	0.07	0.79
	ICT Development Index	8.57	8.43	0	8.36	8.43	8.94	0.12	0.58	0.08	0.26	3.06
	The risk of malware infection	24.65	25.15	0	17.65	25.15	29.75	10.70	12.10	60.82	7.12	28.88
THE RUSSIAN FEDERATION	Personal Freedom	6.05	6.12	6.06	5.71	6.12	6.32	0.26	0.62	0.09	0.28	4.63
	Democracy Index	3.53	3.49	0	3.29	3.49	3.79	0.07	0.49	0.07	0.24	6.86
	ICT Development Index	6.64	6.75	0	6.36	6.75	6.92	0.95	0.56	0.13	0.32	4.88
	The risk of malware infection	52.31	54.16	0	47.21	54.16	56.58	16.45	9.36	34.87	5.39	10.31

3. Interpretation of Measurement Indicators

China, the Netherlands and Russia have different cyber profiles, due to their political culture, security perceptions and objectives in cyberspace. In each case, the correlation of three variables (Personal Freedom, Democracy Index and ICT Development Index) is tested. This study aims to identify the factors that influence the risk of malware infection.

For China, the relation between Personal Freedom (independent variable - I. V.) and Risk of Malware Infection (dependent variable - D. V.) shows a weak positive correlation, with a value for Pearson coefficient of R= 0.31. The influence between those variables is seen in Figure 1, where we observe a decrease in the Risk of Malware Infection when Personal Freedom is decreasing between 2011-2014 and a reverse phenomenon between 2014-2016.

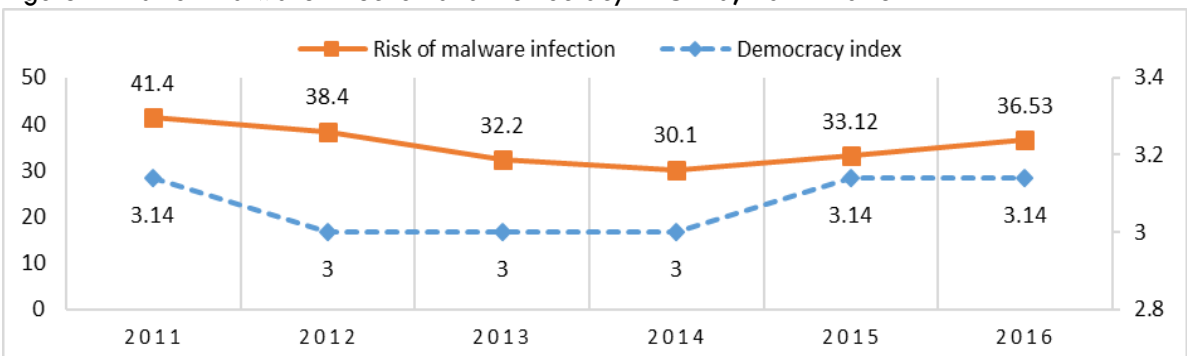
Figure 1: Risk of Malware Infection and Personal Freedom in China, 2011-2016



Sources: Kaspersky Lab; Vásquez and Porčnik, *The Human Freedom Index 2018*.

The second set of variables, the Democracy Index (I. V.) and the Risk of Malware Infection (D. V.) are correlated positively as well, with the Pearson coefficient of R= 0.45. The correlation graphic (see Figure 2) shows that the decrease/stagnation of the Democracy Index for the period 2012-2014 leads to a lower Risk of Malware Infection. With the increase of the Democracy Index between 2014-2016, the Risk of Malware Infection also increased.

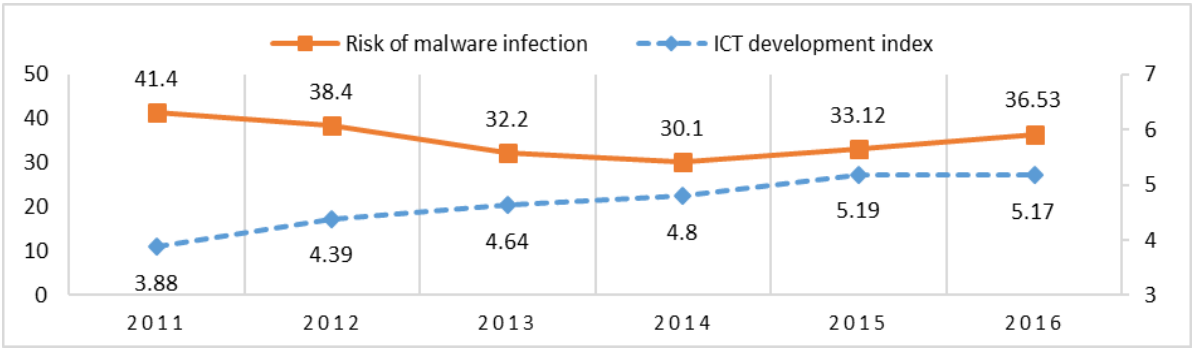
Figure 2: Risk of Malware Infection and Democracy in China, 2011-2016



Sources: Kaspersky Lab; Economist Intelligence Unit.

The last set of variables, the ICT Development Index (I. V.) and the Risk of Malware Infection (D. V.) have a strong and negative correlation of R= -0.64 (see Figure 3). One of the reasons why these two variables might not correlate is because the ICT Development Index has a constant growth, while the Risk of Malware Infection tends to variate.

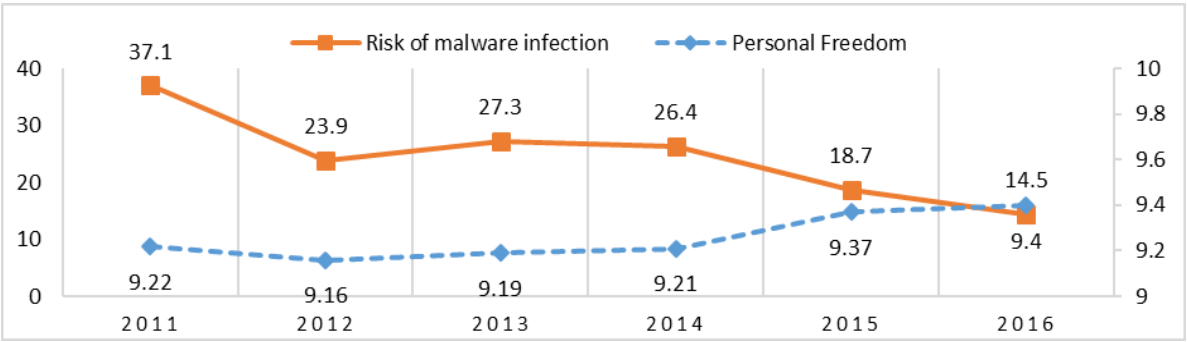
Figure 3: Risk of Malware Infection and ICTs in China, 2011-2016



Sources: Kaspersky Lab; United Nations International Telecommunication Union.

For the Netherlands, the first set of variables, the Personal Freedom (I. V.) and the Risk of Malware Infection (D. V.) indicates a strong and negative correlation of R= 0.-71. Figure 4 indicates a constant growth of the Personal Freedom, while the of Malware Infection has the tendency to decrease, with the exception of 2013, where it shows a growth.

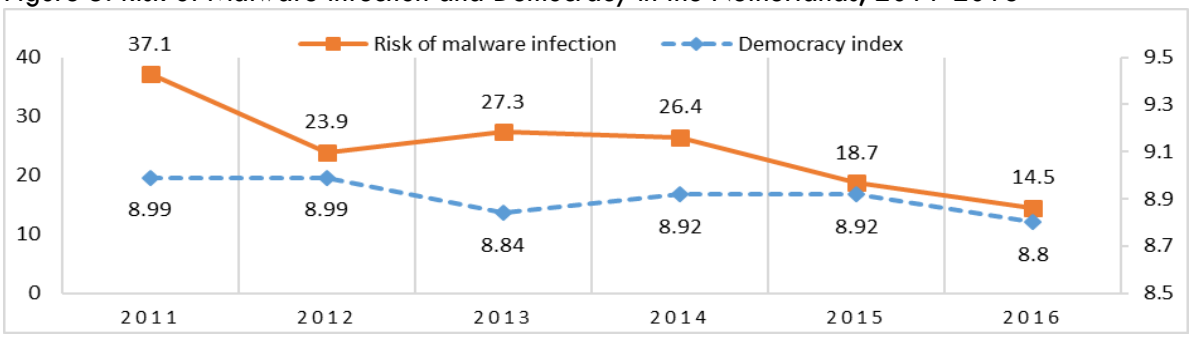
Figure 4: Risk of Malware Infection and Personal Freedom in the Netherlands, 2011-2016



Sources: Kaspersky Lab; Vásquez and Porčnik, *The Human Freedom Index 2018*.

The relation between the Democracy Index (I. V.) and the Risk of Malware Infection (D. V.) shows a strong and positive correlation of R= 0.6. Figure 5 indicates that the Democracy Index is either oscillating or stagnating. The stagnating periods of the Democracy Index between 2011-2012 and 2014-2015 are correlated with the decrease of the Risk of Malware Infection. The value of the Pearson coefficient indicates that the decrease of the Democracy Index is correlated with the decrease of the Risk of Malware Infection.

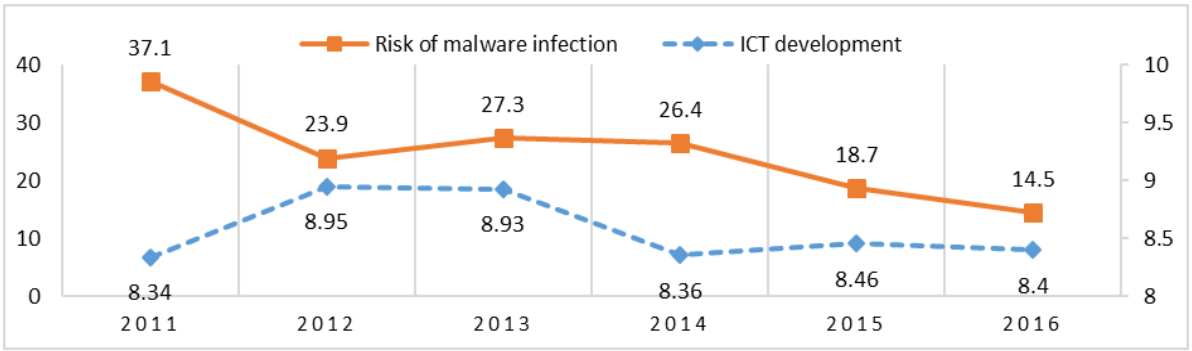
Figure 5: Risk of Malware Infection and Democracy in the Netherlands, 2011-2016



Sources: Kaspersky Lab; Economist Intelligence Unit.

The ICT Development Index (I. V.) and the Risk of Malware Infection (D. V.) are close to a null correlation of R= 0.02. Figure 6 shows that the Risk of Malware Infection has is oscillating, while the ICT Development Index has a relatively constant growth.

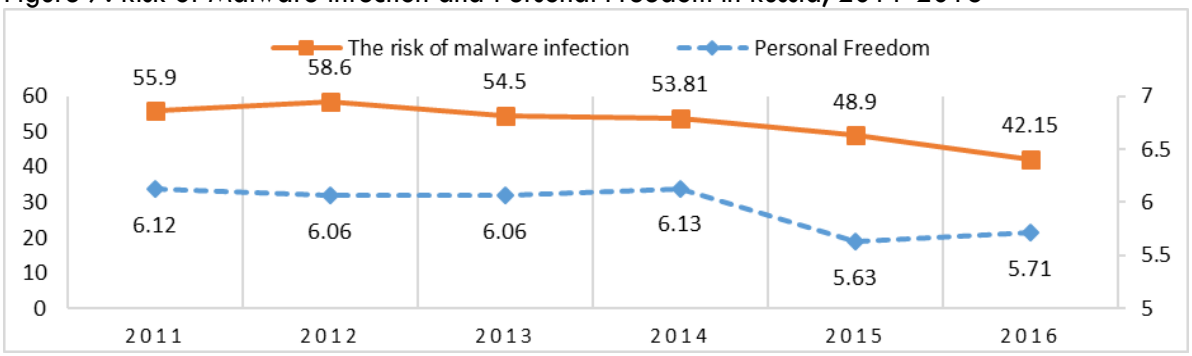
Figure 6: Risk of Malware Infection and ICTs in the Netherlands, 2011-2016



Sources: Kaspersky Lab; United Nations International Telecommunication Union.

In Russia, the strongest correlation is between the Personal Freedom (I. V.) and the Risk of Malware Infection (D. V.) with R= 0.86. Figure 7 indicates that the decrease of the Personal Freedom Index is correlated with a decrease of the Risk of Malware Infection.

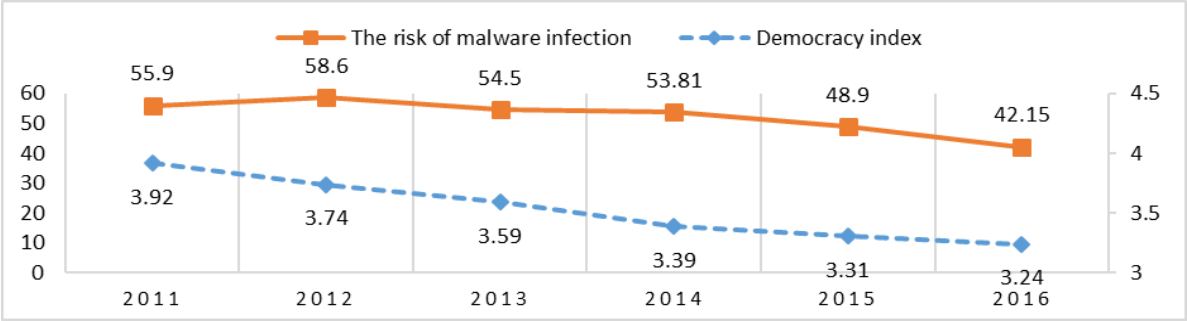
Figure 7: Risk of Malware Infection and Personal Freedom in Russia, 2011-2016



Sources: Kaspersky Lab; Vásquez and Porčnik, *The Human Freedom Index 2018*.

The correlation with the Democracy Index is strong and positive with R= 0.81. Figure 8 shows a continuous decrease of the Democracy Index correlated with a decrease of the Risk of Malware Infection. This indicates that the decrease of the democratic performance leads to higher cyber security.

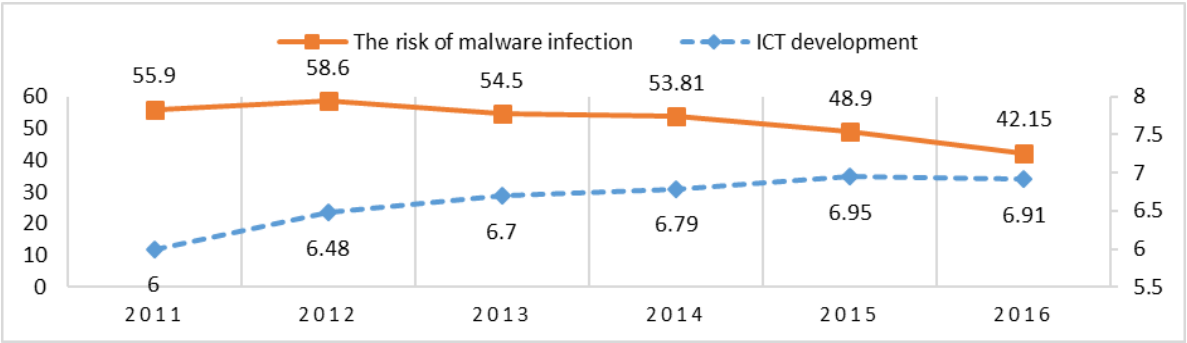
Figure 8: Risk of Malware Infection and Democracy in Russia, 2011-2016



Sources: Kaspersky Lab; Economist Intelligence Unit.

The last set of variables, ICT Development Index (I. V.) and the Risk of Malware Infection (D. V.) feature a strong and negative correlation with R= -0.64. The relation between the two variables is mixed (see Figure 9). In general, the increase of the ICT Development Index leads to the decrease of the Risk of Malware Infection, with an anomaly in 2012, where we observe that the Risk of Malware Infection increased, although the ICT Development Index increased.

Figure 9: Risk of Malware Infection and ICTs in Russia, 2011-2016



Sources: Kaspersky Lab; United Nations International Telecommunication Union.

4. Further Considerations

Even though it is being advocated that it transcends the national borders and the state's expertise, cyberspace bears tremendous importance for national security and is such influenced by the political culture. The design of the security strategy in the traditional operational domains (air, sea, land) is highly influenced by political culture and this research shows that this aspect is also valid for cyber security. The selected states are contrasting in the manner they frame the aspects of cyber security. Thus, culture is so powerful that managed to influence even an inherently technical aspect.

The correlation between the Personal Freedom and the Risk of Malware Infection is quite eye-opening as it indicates the impact that the political culture has on the cybersecurity. For China and the Russian Federation, the decrease of Personal Freedom leads to a decrease of the Risk of Malware Infection. This confirms the hypothesis 'the highest the Personal Freedom is, the highest is the Risk of Malware Infection' (A. H1). On the other hand, in the Netherlands the trend is reversed, namely 'the highest the Personal Freedom is, the lowest is the Risk of Malware Infection' (A. H2). Although the cyberspace was built on self-governing basis, it quickly became necessary to adopt security and controlling measures. The states have a different view on what constitutes the cyberspace, thus they manifest a different strategy to secure it. Notably, this is often seen on the level of control imposed by states on the access and the activity on the internet through regulation and monitoring activities (Eriksson and Giacomello 2009, 209). Personal Freedom is only an element of the state control constellation in the cyberspace. Many states, both democratic and totalitarian are already "controlling what their citizens can and cannot do on the Internet" (Cavelty 2014, 8). This study showed that for China and the Russian Federation, the control over the internet does not serve only to consolidate the state power, but it also used to increase the cybersecurity. On the other hand, in the case of the Netherlands higher freedom leads to stronger cybersecurity.

There was a strong and positive correlation of the Democracy Index for China and Russia, which confirms the hypothesis 'the highest the democracy index is, the highest is the risk of malware infection' (B.H1). In the case of the Netherlands there was also a positive correlation, which also confirms the hypothesis B.H1, which probably is resulted from the lack of constancy of the Democracy Index. Anyhow, the result is quite worrying as it indicates that the cybersecurity is built upon a weaker democracy. In the case of Netherlands, this result is contradictory with the previous one, aspect which shall be further analysed.

The interesting correlation is related to the ICT Development Index, which has a strong and negative correlation for China and Russia and close to null for the Netherlands. The negative correlation for China and Russia indicates that 'the highest the ICT Development Index is, the lowest is the risk of malware infection' (B.H1). For the Netherlands on the other hand, there is no correlation between the two variables (B.H0). Still, it would be a major error to draw hasty conclusions in this case, reason why further research is needed.

Conclusion

The results lead to the conclusion that a factor which influences the cyber-security is the political culture. All the states selected in the study have a different cultural background. The Netherlands features a stable Western democracy and the citizens are enjoying Western values. Russia has the Soviet Union and Slavic heritage. China is still influenced by its ancient Chinese culture, along with its present communist regime. On top of that, each country views the cyberspace from a different perspective. Therefore, like the other security sectors, cyber security reflects a country's political culture. Each country has a unique profile which matches the needs and the interests of that nation.

* Cosmina Moghior holds a master's degree in Security and Diplomacy from the National University of Political Studies and Public Administration, Romania.

References

Aycock, J. 2006. *Computer Viruses and Malware*. Springer.

Cavelty, M. D. 2014. *Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities*. Center for Security Studies: 701–715.

China Copyright and Media. 2016. *National Cyberspace Security Strategy*. Consulté le November 20, 2018, sur https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/

Dutch Ministry of Defence. 2012. *The Defence Cyberstrategy*.

Eriksson, J., and G. Giacomello. 2009. Who Constrols What, and Under What Conditions? *International Studies Review*, 206-210.

Federation Council (Russia). 2014. *КОНЦЕПЦИЯ СТРАТЕГИИ КИБЕРБЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ" ["The Strategic Concept of Cyber Security of Russian Federation"]*.

Funk, C., and M. Garnaeva. 2013. *Kaspersky Security Bulletin 2013. Overall Statistics for 2013*, https://securelist.com/analysis/kaspersky-security-bulletin/58265/kaspersky-security-bulletin-2013-overall-statistics-for-2013/#04.

Garnaeva, M., at al. 2014. *Kaspersky Security Bulletin 2014. Overall statistics for 2014*, https://securelist.com/analysis/kaspersky-security-bulletin/68010/kaspersky-security-bulletin-2014-overall-statistics-for-2014/.

———. 2015. *Kaspersky Security Bulletin 2015. Overall statistics for 2015*, https://securelist.com/analysis/kaspersky-security-bulletin/73038/kaspersky-security-bulletin-2015-overall-statistics-for-2015/.

———. 2016. *Kaspersky Security Bulletin: Overall statistics for 2016*.

Guinora, A. N. 2017. *Cybersecurity. Geopolitics, law, and policy*. London and New York: Routledge.

United Nations - International Telecommunication Union (ITU). 2012. *Measuring the Information Society*. Geneva: International Telecommunication Union.

———. 2014. *Measuring the Information Society*. Geneva: International Telecommunication Union.

———. 2016. *Measuring the Information Society Report*. Geneva: International Telecommunication Union.

———. 2017. *Measuring the Information Society Report*. Geneva: International Telecommunication Union.

Namestnikov, Y. 2012. *Kaspersky Security Bulletin. Statistics 2011*, https://securelist.com/analysis/kaspersky-security-bulletin/36344/kaspersky-security-bulletin-statistics-2011/.

Namestnikov, Y., and D. Maslennikov. 2012. *Kaspersky Security Bulletin 2012. The overall statistics for 2012*, https://securelist.com/analysis/kaspersky-security-bulletin/36703/kaspersky-security-bulletin-2012-the-overall-statistics-for-2012/.

National Coordinator for Security and Counterterrorism. 2013. *National Cyber Security Strategy 2: From*

awareness to capability.

Shaohui, T. 2017. *International Strategy of Cooperation on Cyberspace*, http://news.xinhuanet.com/english/china/2017-03/01/c_136094371.htm

The Economist Intelligence Unit. 2017. *Democracy Index 2016. Revenge of the 'deplorables'*. London, New York and Hong Kong: The Economist.

Vásquez, I., and T. Porčnik. 2018. *The Human Freedom Index 2018. A Global Measurement of Personal, Civil, and Economic Freedom*. Washington, D.C: Cato Institute, Fraser Institute and Friedrich Naumann Foundation for Freedom.

Yarger, H. 2008. "Towards A Theory of Strategy: Art Lykke and the Army War College Strategy Model." In *The U.S. Army War College Guide to National Security Issues, Volume I: Theory of War and Strategy,* edited by J. R. Cerami and J. F. Holcomb, Jr., 43-49. Carlisle: Strategic Institute Studies.

Cybersecurity in Banking and Payments in the United Kingdom

By Gordon Kerr*

Despite the banking industry's excellent level of cybersecurity protections for itself, the UK public, media and Parliament appear unaware of the security weaknesses in the UK's payments architecture which has encouraged a new push button fraud trend. Banks claim that solutions are imminent, but meanwhile do little to protect customers. Manned help desks could easily be provided.

A combination of factors has resulted in this state of affairs. On one level this is a variant on the too big to manage diagnosis of root problems of the global financial crisis – banks are giant businesses often comprised of an array of legacy systems which are not well understood by regulators or even their managers. At another level, there is the cost issue. Better to suppress the concerns in public today whilst a huge and publicly funded overhaul of the architecture takes place than risk making interim changes to systems and protocols which could saddle banks with liability for fraud losses which they are presently successfully imposing on innocent retail customers.

Statements made by banks and their regulators on all aspects of this security issue are unreliable. How has this come to pass? The relationships between the key stakeholders and the regulator are simply too close and stakeholder banks are in control of all aspects.

Key words: banking, United Kingdom, cybersecurity, GDPR, data breach, payment fraud.

Introduction

This paper will focus on payment security in the UK and likely consequences for Europe in the context of cybersecurity. The banking industry is highly advanced in terms of cybersecurity. Especially in the recent decade, banks have striven to show themselves alive to these risks and conservative in their approaches. Banks are keen to be seen to be co-operating closely with authorities.

A new cybersecurity concern is the planned overhaul of the UK's non-card payments architecture ostensibly to facilitate new technological developments in payments, part of the "Fintech" branch of new technology, and to comply with new European data rules, as explained in next section. However, these changes will phase out traditional slow payment methods – cheques and credit transfers, to be replaced with online initiated, relatively instant, payments. The effect will be to

encourage greater use by customers of precisely the type of push button online payment mechanism at the core of the fastest growing area of retail banking fraud in the UK today.

Banks in the guise of the Payments Service Providers (PSPs) - and the UK's Payment Services Regulator (PSR) are aware of this and claim that planned new protections will address this problem, but unfortunately, such claims are hopelessly optimistic. Meanwhile, the small cartel of banks tasked with managing the overhaul is more focused on the careful design of new customer reimbursement rules likely to leave the bulk of losses from these frauds with retail and small business customers.[1]

2018 – GDPR, Open Banking, and Embarrassing UK Bank Data Breaches

Two major legislative initiatives imposed on banks this year, GDPR[2] an EU law passed in 2016, and Open Banking[3], have been designed to give bank customers greater control of their data and obtain hopefully better terms from their banks.

GDPR rules aim to "protect…natural persons with regard to the processing of personal data and on the free movement of such data". Open Banking aims to expose established banks to competition from new Fintech enterprises primarily in the area of mobile and online payments. The UK has sought to lead Europe and from early in 2018 the nine largest banks[4] have been required to share data in standardised formats, provided that customers consent.

Despite the intense focus on cybersecurity in the context of new GDPR and Open Banking rules, UK banks continue to experience mass data breaches. These are management issues rather than technological weaknesses.

As Emma Rumney and Lawrence White mentioned in their September 21, 2018 *Reuters* article, UK banks have since 2014 experienced a raft of embarrassing and well-publicised security breaches ranging from outages/ shutdowns at RBS, Barclays and Co-Operative Bank to April's botched migration of customer data by TSB to its new system. This resulted in the mass exposure of its customers' data and account details. TSB was switching from a system operated by TSB's former owner, Lloyds Banking Group, to one operated by its 2017 buyer – Sabadell of Spain. It

[1] I am indebted to Bob Lyddon of Lyddon Consulting (www.lyddonconsulting.com) for his detailed research work on the efforts of the Payment Systems Regulator to tackle payments fraud, and on the development of the "Confirmation of Payee" service aimed at mitigating Authorised Push Payments Fraud, and on the "Contingent Reimbursement Model" code for compensating victims of such frauds in certain circumstances.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[3] Open Banking Europe is an initiative developed by PRETA, EBA Clearing's subsidiary created in 2013 to develop and innovate market competitive services in digital payment and identity solutions, https://www.openbankingeurope.eu.

[4] Allied Irish Bank, Bank of Ireland, Barclays, Danske, HSBC, Lloyds Banking Group, Nationwide, RBS Group and Santander.

seems obvious that the system was not properly tested, that a pilot – say 5% - of customers should have been migrated first, but this did not happen, and chaos ensued. Many customers who logged in online found themselves in a different customer's account. One third of customer's accounts were affected. Customers were unable to make or receive payments for up to six weeks, many saw sums being taken out of their accounts. 370 received letters saying they were dead. Frustratingly few could get through on the phone, many waiting for up to nine hours in queues. Unsurprisingly this situation was exploited by fraudsters who pretended to be TSB employees and robbed at least 1,300 customers.

Criminals managed to drain the accounts of 1300 innocent customers during this meltdown by exploiting new automated communication methods, as admitted by TSB chief executive Pester to the UK Parliament Treasury Select Committee. One method used was spoof text messages. Because TSB's data blunder revealed swathes of customer phone numbers, multiple groups of criminals sent texts purporting to be from the bank. Because of the way that modern smartphones group text messages, and the criminals' ability to copy the format and style of genuine bank texts, the spoof text would be grouped along with genuine ones. Typically, the message would falsely state that a third-party payment of say GBP 1,000 was about to be made and invite the customer to call a number if she had not in fact authorised this payment. In this way, the customer was tricked into calling the fraudster who, pretending to be TSB, sought to identify the customer by asking for her user ID, full name and date of birth. With this information, the fraudster would reset the password and empty the account. Seventy times the usual level of frauds occurred during this turbulent period and the Bank of England's conduct unit is expected to issue a damning report within a few months.

The TSB story implies a failure of technology. However, even with some of the best cybersecurity technology in place – which TSB clearly possessed - this disaster still happened. This case is best thought of as a data breach rather than a fundamental failure of cybersecurity, but here is the point at which the lines become blurred and customers *think* that the bank's cybersecurity has failed, whereas the problems really stem from business management. Sadly, in the area of online and mobile payments, we anticipate a rising tide of such problems, because the direction of travel in the payments industry, fully encouraged by the regulators, is to encourage users to migrate away from old-fashioned cheque and card payments in favour of eBanking: online and mobile payments. But eBanking is a nirvana for fraudsters because of a fundamental flaw in the payments architecture which has opened wide the door to a new type of fraud – Automated Push Payments.

Automated Push Payment Fraud and Online Banking

Just as the dust began to settle on the TSB story there was a renewed focus in the UK media and Parliament on a relatively new, but rapidly growing, type of fraud – Automated Push Payment (APP). Data published by two trade associations *UK Finance*, and Financial Fraud Action UK, showed that APP fraud in H1 2018 was £145 million, up 44% on H12017. Although these gross numbers are small, the average loss per customer (GBP 4,000) is much larger than for card fraud (GBP 300).

There are many APP variants. A common example is where the criminal induces the bank customer to send a typically quite large payment—for example, a deposit to purchase an apartment—to a bank account controlled by the criminal. Property purchase deposits are a typical use case. The customer is excited about buying his home, there is time pressure, he has not previously made an online payment to his solicitor (many solicitors are today provided *free* by mortgage lenders) so when he receives an email purporting to emanate from the lawyer in identical font and format to what he is used to, correctly identifying the apartment, the date the payment is due and stating the correct amount he is easily persuaded to press the button on a transfer of say GBP 25,000.

Consumer groups are worried, particularly because unlike card fraud, where the loss is usually borne by the bank, the significance of this rapidly growing APP fraud is that the loss is typically not reimbursed to the customer. Bob Lyddon (2018a) provides the latest detailed evidence. When a customer disclaims liability for a card transaction in the UK and most of Europe, the bank must demonstrate on the balance of probabilities that the customer has been reckless with his PIN number and stewardship of the card. If it cannot, the bank bears the loss. However, the cybersecurity measures and rules which banks have established regarding online payments concentrate on the physical hardware. As a result, if a device (laptop/ phone) which has been accredited by the customer as his own is used during an APP scam or spoof, the customer will usually bear the loss.

Easy Solution to APP Fraud - Confirmation of Payee

The central flaw in the present online payment system is the lack of a name check in the messaging system which is at the heart of the UK's online payments system known as Faster Payments.[5] How was this allowed to happen? This absence can be viewed as a side door to the system which was opened when the present Europewide Point of Sale (PoS) payments architecture was established some 20 years ago. For PoS to work, the payments system had to generate a fast and accurate response from the purchasing customer's bank as to whether a) she had enough funds in her account to pay for the item; b) whether the debit / credit card was valid and not reported lost or stolen. Authentication was initially based on a visual check of the signature strip which later was replaced by Personal Identification Numbers. These cards based PoS purchases were the first payment processes requiring the payer's bank to receive a message and respond to it within a few seconds. The payee's identification information was never required to be captured by such a messaging system since that information was contained in the PoS device which initiated the message/ payment request.

As each new iteration of payments technology was adopted, the payments architecture was further constructed, but around this side door flaw. Today the Faster Payments architecture uses the IS08583 data protocol, the same as for card payments, throughout Europe. In Europe, and a few

[5] APP fraud can also occur in one of the UK's other main payments system called BACS. This supports cheque clearing and customer-initiated payments over the slower, paper form-based system called CHAPS. For brevity we will consider only Faster Payments here.

countries beyond Europe's borders, a similar fast payments architecture is in place, known as SEPA INST. This is an instant credit transfer system, in any major currency, which can be conducted using just an IBAN number, so again the payee's name is not required and the side door to APP fraud is wide open.

The obvious solution to APP fraud is for the system not to make the payment unless the payee's account details match the payee's name which the customer types into her tablet or another device. The payments industry has been talking about implementing such Confirmation of Payee (CoP) protection for years, and in January 2018 the UK's regulator (The Payment Systems Regulator Limited - PSR) assured the UK Parliament's Treasury Select Committee that CoP would likely be *in place* by the end of 2018. This was a remarkable assertion given that there is little chance of a working CoP protocol being established before 2023-25, if at all because the UK is at the start of a project to completely overhaul the non-card payments infrastructure. The project is labelled the New Payments Architecture (NPA) and aims to rip out and replace this infrastructure. The new architecture will facilitate the replacement of the old, slow, costly (to banks) payment methods such as cheques and encourage retail customers to make greater use of irreversible online payment tools which are beloved of APP fraudsters.

New Payments Architecture and likely Confirmation of Payee Protection Delays

The NPA project is to be overseen by an entity called Pay.UK. This entity is the merger of the three underlying UK payments systems: Bankers Automated Clearing Services (BACS) - a typical method of making regular payments such as utility bills; Cheque and Credit - the ordinary system for manually signed paper cheques; and Faster Payments, the main online/ ebanking payments protocol discussed above.

All these three payment systems are owned by more or less the same group of major UK banks. Pay.UK was formed in July 2017 for the purpose of *procuring* the NPA, as announced on its *We are Pay.UK* website. Pay.UK is formally under the supervision of the Bank of England, but in practice, the PSR provides its main oversight.

Because the Confirmation of Payee (CoP) protection function has always been presented as *overlaying* on this new architecture, it was inconceivable that it could have been up and running this calendar year. But the subject is pithy, technical, and riddled with computer language and the Parliamentary Committee were easily fobbed off in January.

There are two reasons why the NPA project is likely to take a long time to implement. Firstly, the banks behind Pay.UK have little financial incentive; the banks are comfortable with the present payments architecture. The regulator's NPA vision is to open retail banking to further Fintech competition, but this runs counter to banks' incentives. Secondly, the procurement model envisages the NPA tendering companies swallowing substantial costs to be recouped, together with hoped for profits, only when the NPA is deployed and then over five years. This is called a Cost Recovery Model. Of course, bank customers (the public) will ultimately foot the bill. But the costs to be

absorbed by successful tenderers will likely run into the hundreds of millions, so high in fact that only giant US companies such as Amazon, IBM and Microsoft are expected to tender.

A tendering process was begun in 2017 by the Faster Payments scheme company, which was envisaged as involving the building of NPA, but that process has been stopped by Pay.UK after Pay.UK's assessment of the NPA Blueprint, as explained on the *We Are Pay.UK* website (2018b). Now Pay.UK will start a new tendering process and from square one. Latest versions show a scope creep, the danger that the project grows beyond providing the basic system rails to incorporating features, ownership of which payment services providers would wish to retain. The Bank of England is known to be concerned that the project's design is likely to entrust the bulk of the work and financing to US technology giants. For all the above reasons, implementation by 2023–5 appears optimistic.

Pay.UK is now very careful with the language of its assurances as to NPA timing but is under political pressure for a CoP solution now. For this to happen, the Faster Payments messaging system will need to be reprogrammed to enable the individual payment service providers to communicate such information between each other. The banks (Payment Service Providers – PSPs) using Faster Payments appear disinclined to spend the estimated GBP 200 million on this work, and as a result Pay.UK has redefined its role into that of a rule designer and publisher of standards and protocols, and seeks to pass responsibility for implementation back to the PSPs themselves. A CoP launch event took place in October, and the APP Scams Steering Group - a creature of the PSR - has duly published the resulting proposed customer compensation rules for consultation and feedback. These rules set out the conditions for customers to be compensated when they avail themselves of the putative CoP. Payments expert Bob Lyddon (2018b) has reviewed the documentation and observes:

> "*The result is a carte blanche for the banks to give the victims the brush-off. Victims have to have taken numerous steps, show they have educated themselves, and in the process become semi-experts on matters for which the bank has a duty of care to them and not the other way round. The banks are allowed to be judge and jury on the matter and are permitted to apply numerous tests of reasonableness about their own behavior*."

One remarkable exclusion from the scope of compensation is SMEs. Of the non-personal users, only charities and micro entities will qualify for compensation. To recap, the subtext is rather concerning. Insiders know that CoP is highly unlikely to be deployed on the existing architecture. However, Pay.UK and the regulator (PSR) maintain the pretence that it might, whilst their main focus is on designing customer compensation rules which heavily favour the banks in their guise as PSPs. Meanwhile, the PSR has published a consultation on the proposed Confirmation of Payee service.

Not only does the regulator appear to condone this abnegation of responsibility by PSPs, but such concerns are compounded by the regulator appearing to ignore that every instance of APP fraud involves two major breaches of key banking laws. Firstly, there has been a failure of bank due diligence in every case where a criminal has managed to open and maintain the account

into which the stolen funds are transferred; secondly, by permitting the fraudster to draw down the funds, each bank in every case is offending Europe wide laws proscribing the facilitation of the handling of the proceeds of crime. Nor does the regulator demand a relatively simple and quick solution to APP Fraud – the establishment of manned telephone help desks, which could assure the customer that the name and account details of the payee match the proposed push button details and are valid.

Our Explanation; New APP Fraud Rules and Payments Standards are a *Thin Political Market*

Both the APP fraud resolution effort and the NPA project are essentially political markets which banks appear to have easily captured. Each envisages protocols, standards and new rules. Karthik Ramanna (2015) has analysed how US banks captured various aspects of bank accounting standards in a similar way. He coins the phrase *thin political market* to explain how. Political markets are distinguished from political processes. In the latter, for example, national public healthcare systems and the financing thereof, the general public is incentivised to participate. However, for accounting rules or payment standards and protocols, in contrast, the general public feels no such incentive. Further, in thin political markets, the required expertise can only be obtained *experientially*, by being a practitioner, an insider. Outsiders are dismissed as obviously incompetent. In thin political markets, there is no role for *independent* experts. Here, independence correlates with a lack of the required experience. The term political applies because the results of the rules will encourage certain behaviour which will benefit certain classes of society at the expense of others.

Ramanna defines a thin political market as one in which an area of rule-making or regulation where corporate managers succeed in capturing the standard setting, system changing or rule-making process. Three characteristics are observable in a thin political market (Ibid., 20):

a) The managers clearly possess the technical expertise necessary for assuming the role of rule designers;
b) They have strong economic vested interests in the outcome of the rule(s);
c) They face little political opposition from the general public or general interest.

Further, as with the NPA project where the banks stand to gain little benefit, Pay.UK (2018c) presents itself as performing a charitable and noble public service duty, as technocratic rather than an unelected policymaker:

> "*We will do this by driving more participation and involvement in payments, so payment service providers are competing and innovating solutions which respond to customer needs, driving better service and value for end users. Our goal is to be the leading retail payments authority by delivering best in class infrastructure and standards for the benefit of people everywhere. We will be the guardians and pioneers of payments, modernising the payments ecosystem and ensuring that companies and individuals participate in payments according to the standards and rules which we will set.*"

Implications and Lessons for the Future

At the wholesale level, bank cybersecurity is so effective that banks are almost immune to the risk of hacks and data thefts. Interbank payments rarely if ever go astray. Banks could quite easily fund the messaging upgrades to the Faster Payments protocol required to provide a Confirmation of Payee (CoP) layer of protection. Rather than do so, they produce (via Pay.UK) unrealistic estimates of when such protection will be in place and focus their efforts on designing a compensation regime (Contingent Reimbursement Model) which will minimise losses imposed on banks and maximise those suffered by retail and business customers.

How is it possible that banks with such strong cybersecurity can expose their customers to growing levels of payment fraud? We conclude that cybersecurity should not be seen principally as a technical matter but rather as a business management one, and the usual incentives apply. We set out concerns that the regulator is neither sufficiently independent from the PSP cartels nor seemingly knowledgeable enough about how deep the problems lie. Perhaps the pithy, detailed, and frankly rather boring complexity underlying the existing payments architecture and the planned enormous overhaul, is too tough or turgid for the scrutineers. This has in effect deterred the PSR and other public bodies from delivering on their January promise to Parliament to take any effective action to address APP fraud.

How should policymakers adjust their supervision of matters such as payments systems mergers to protect the public good element of such services? The 2018 focus on security with the onset of GDPR and Open Banking, has made it easy for the incumbents to seize control of these processes. By implication, nobody else is capable. A good place to start would be to address the factors contributing to such thin political markets.

Regulators could start by imposing simple and logical rules; for example, victims of APP fraud should be treated in the same way as victims of card fraud; unless the bank (PSP) can demonstrate gross negligence on the part of the customer, banks should bear the loss. Were this rule implemented, it is likely that the cartel of large UK banks would quickly agree to share the estimated GBP 200 million costs of the necessary upgrade to the Faster Payments messaging system. In addition, regulators should enforce anti-money laundering and due diligence (account set up) laws.

---

* Gordon Alexander Kerr is an investment banker, financial markets expert and founder of the British financial think tank Cobden Partners.

References

Lyddon, Robert. 2018a. *Our response to the PSR consultation on their Contingent Reimbursement Model draft code, aimed at Authorised Push Payments Fraud*. http://www.lyddonconsulting.com/our-response-to-the-psr-consultation-on-their-contingent-reimbursement-model-draft-code-aimed-at-authorised-push-payments-fraud/.

———. 2018b. *Vendorcom Event Deck*. http://www.lyddonconsulting.com/wp-content/uploads/2018/11/Vendorcom-event-deck-08nov18.pd.

Ramanna, Karthik. 2015. *Political Standards*. University of Chicago Press.

Rumney, Emma, and Lawrence White. 2018. "MPs criticise RBS and Barclays for online banking outages." *Reuters*, September 21. https://uk.reuters.com/article/uk-natwest-outages/mps-criticise-rbs-and-barclays-for-online-banking-outages-idUKKCN1M10NN.

The Payment Systems Regulator Limited (PSR). 2018. "Consultation on the proposed Confirmation of Payee Service". https://www.psr.org.uk/psr-publications/consultations/cp-18-4-consultation-general-directions-implementing-cop.

UK Finance. 2018. *Criminals steal £500m through fraud and scams in the first half of 2018*. http://www.ukfinance.org.uk/criminals-steal-500m-through-fraud-and-scams-in-the-first-half-of-2018/.

UK Parliament Treasury Select Committee. 2018. *Oral evidence: Service Disruption at TSB, HC 1009*. http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/treasury-committee/service-disruption-at-tsb/oral/84824.pdf.

Pay.UK. 2018a. *Introducing the New Payments Architecture*. https://www.wearepay.uk/what-we-do/.

———. 2018b. *NPA – Procuring the Core Infrastructure*. https://www.wearepay.uk/new-payments-architecture-core/.

———. 2018c. *Who We Are*. https://www.wearepay.uk/who-we-are/.

Dr. Joanna Kulesza. Foto: Visio institut.

Balancing Privacy and Security in a Multistakeholder Environment. ICANN, WHOIS and GDPR

By Joanna Kulesza*

The chapter covers the perplexities of the internet governance multistakeholder model, its meaning and implications. While relying on the well-established reference to three principal groups of stakeholders (states, business, civil society), the chapter includes discussion on different approaches to internet governance and reflects on arguments against the current model of setting standards and norms for cyberspace. It contrasts the existing model of governance with challenges posed by international cybersecurity and protecting human rights online. The case study example focuses on the most recent challenges posed to the multistakeholder model by the European Union's General Data Protection Regulation (GDPR) and its implementation by non-European legal persons operating on Europeans' data. The analysis is focused on the Internet Corporation for Assigned Names and Numbers (ICANN) – a non-profit based in California, managing core internet resources, including the Internet Protocol (IP) and the Domain Name System (DNS). It concludes with a summary of perspectives for future development of multistakeholderism, referring to contemporary trends in meta-governance.

Key words: cybersecurity, multistakeholderism, international law, cybernorms, internet governance.

Introduction

Internet governance relies on multistakeholderism – a distributed policy making model based on voluntary cooperation of key actors, usually identified as states, business and civil society, operating "in their respective roles" (WSIS 2005) through "rough consensus and running code" (Clark 1992; Huizer and Crocker 1994). This approach, although neither new or unique to cyberspace, significantly differs from national lawmaking or international norm development. While in both of those scenarios it is states who play a key role, internet governance grants national governments and institutions only a complementary function in setting and enforcing "principles, norms, rules, decision making procedures and programs" for the global network (Drake 2009,8). While a similar, supporting rather than leading, role for states can be witnessed in many other areas of international law and relations, just to mention environmental protection, oil transportation, production of pharmaceuticals or banking, where much is left to good business practice, civil society input and/or consumer choice, the interplay of governments, companies and individuals is no-

where more complex, abundant and transnational than online. Likely due to three factors: 1) the complexity and scale of online interactions, with 3,6 million Internet users worldwide in 2017 (ITU 2018) 2) the global monopoly of few U.S. based companies (often referred to as "GAFA": Google, Amazon, Facebook and Apple) and 3) the gross value of the online market (estimated at 2.304 trillion USD in online transactions globally in 2017) (eMarketer 2018, online) the lines between the roles of stakeholder groups are nowhere more controversial and disputed than in the online environment. While many still praise the network's unique governance model as key to Internet's boom and rapid development since the early 1990s that lead to shifts in the global economy and fundamental political changes across the world, existing multistakeholder model is far from ideal. Not only does it fail to identify particular rights and obligations of individual actors effectively, but, most significantly at the time of the global war on terror and increasing terrorist uses of the network, it strongly disables state institutions in performing their original roles as lawmakers and enforcers. Much is being said about an alleged "lex Facebook" – a company policy that serves as a global law for billions of its users - particularly in the light of the recent (2018) Cambridge Analytica scandal, disclosing ways to effectively influence individual political choices by personal data profiling with the use of advanced advertising algorithms. The lawmaking power is dramatically shifting away from states, who are desperate to regain it at a time of political and economic insecurity. In their attempts to do so, either in the domain of online security or global trade, they must consider the networks' specifics: its architecture, design and, most significantly, the particular traits of its current multistakeholder model of governance, as discussed below.

Analysis

Governance – a term often used in reference to the unique Internet ecosystem - is neither new or unique to the global communication network. A recent, comprehensive anthology by Levi-Faur offers a versatile review of the rich array of contemporary policy areas subject to "governance". They range from state reform and its democratic institutions to international organisations, global economic relations, labor relations, public health management, banking, risk management and environmental protection (Levi-Faur 2012). In this context, Dutton refers to the Internet and its governance as "a Fifth Estate" describing how the Internet "is being used (…) in ways that support social accountability across many sectors" (Dutton 2012, 585). He refers to the power Internet holds over social relationships and political decisions, reflecting the eighteenth-century concept of Fourth Estate created by the press, now, as he alleges, substituted by the unique impact the Internet has on the global society. While nearing on "a fuzzy term (that) can be applied to almost anything and (…) explains nothing" (Bygrave 2015, 12), Dutton's take of governance focuses on the actual challenge Internet poses to existing regulatory mechanisms and reflects the versatility of its process and actors. Yet as Bygrave rightfully notes, the "nebulous and broad" concept of governance has been defined with other references, like those to "processes influencing other actors" or "the sum of the many ways in that individuals and institutions public and private manage their common affairs" (Bygrave 2015, 11-17). While "governance" is often perceived as contrary to "government", Bygrave views it as one of many methods of regulation. He sides with a "decentered" definition of the latter, covering more than just the activities of governments and state actors" (Bygrave 2015, 13). Drake, on the other hand, offers an "action-

oriented" approach to global governance, relying on its steering mechanisms or institutions rather than the actors behind them. He defines global governance as "the development and application of shared principles, norms, rules, decision-making procedures, and programs intended to shape actor's expectations and practices and to enhance their collective management capabilities in world affair" (Drake 2009, 9). This definition offers a good reflection of the complexity of actions and institutions behind contemporary global governance processes and seems best suited for the following discussion on Internet governance.

Distributed governance, operating on consensus among various groups of stakeholders is, as already said, not unique to the Internet model. As noted by Weber and Weber, particular analogies are to be drawn with environmental law, where individual rights, including the right to information and freedom of speech, in particular, the right to protest, are granted by international treaties, most notably by the Aarhus Convention (Weber and Weber 2009, 9). Using this analogy, the authors suggest a "Memorandum of Understanding" between Internet governance bodies and civil society to ensure their equal participation in the existing governance model. Other popular analogies include references to international trade law where self-regulation, good business practice and political lobbying have always played a major role in shaping global and local policies (Haufler 2013, 31 ff.). Much like the greatly disputed lex Facebook, international companies, particularly within the baking sector, have long used their dominant position to influence policies and adapted to popular consumer demands even if there was no specific law requiring them to do so. Haufler refers to specific examples that include labour standards abroad, information privacy and environmental protection where the private sector takes the lead on policy making and leaves states to only later repeat those within local and international laws (Haufler 2013, 31). Also, international food safety regulations, most notably the Codex Alimentarius and its implementing norms within the World Health Organization (WHO), are often referred to as a case of "private law making" (Henson and Humphrey 2011, 42). As Henson and Humphrey note these private standards have become a "prevalent part" of global food governance, relying on standards for food safety and quality developed by "private firms and standards setting coalitions, including companies and NGOs" (Henson and Humphrey 2011, 42). While developed by FAO and WHO, the document remains a classic example of soft-law and although non-binding to states, serves as a set of globally adopted fundamental safety standards among food suppliers.

These bottom-up processes of international standard setting and lawmaking have not gone unnoticed by international law scholars, who have coined the term "Global Administrative Law" (GAL) to frame them. While GAL remains disputed as to its methodology and application, it offers a comprehensive and insightful look at global governance. The authors see global governance processes aligned along five categories, all based on "global administrative regulation". Kingsbury, Krisch and Stewart include Internet governance with its multistakeholder model as one of those key types, referred to as "Hybrid Administration". They view it as a "hybrid intergovernmental-private arrangement" and directly point to the Internet Corporation for Assigned Names and Numbers (ICANN), discussed further herein, as a unique example (Kingsbury, Krisch and Stewart 2005, 15). Other four types include: 1) "International Administration" by formal interna-

tional organizations, e.g. the United Nations Security Council; 2) "Network Administration" relying on "collective action by transnational networks of cooperative arrangements between national regulatory officials" with the work of and round the Basel Committee and the banking sector; 3) "Distributed Administration" of national regulators implementing international "treaty, network, or other cooperative regimes" and 4) "Private Administration" done by private bodies, such as the International Standardization Organization (ISO).

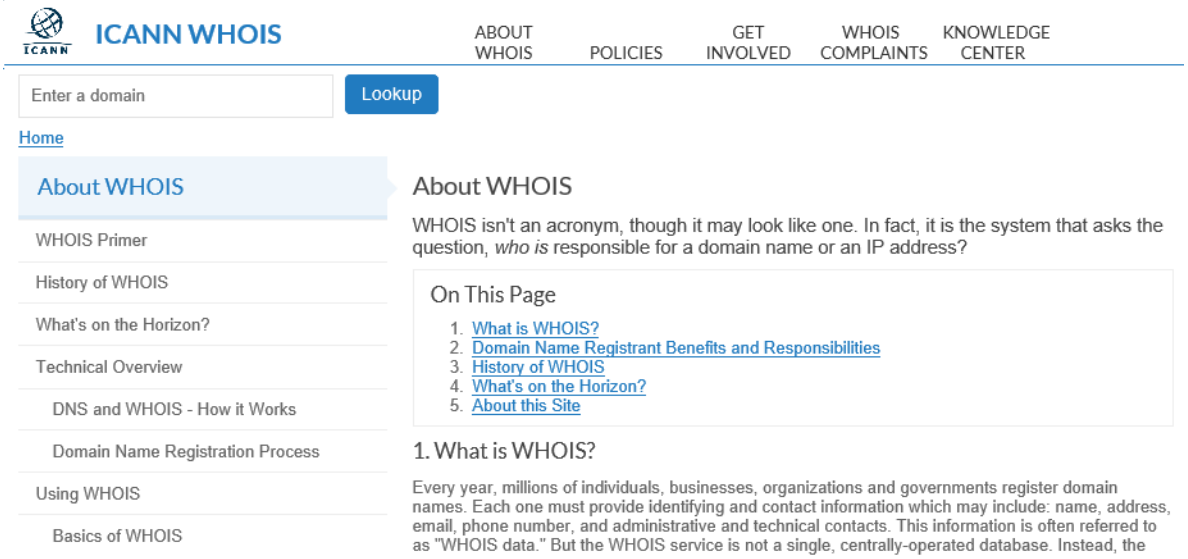
Once the U.S. National Science Foundation, shepherd of the US academic network, allowed for its commercial use in the early 1990s, the commercial potential and rapid economic growth of online market stunned the White House officials. They attempted to resist the lobbying from both: local business and international governments, opting for a novel, non-commercial model of supervising critical technical resources of the network. A new, unique solution was offered in 1998 with the setting up of ICANN – a non-profit corporation operating from California. As per ICANN Bylaws, its mission is to "ensure the stable and secure operation of the Internet's unique identifier systems" (ICANN 2018, online). In particular, ICANN coordinates the allocation and assignment of names in the root zone of the Domain Name System ("DNS") and coordinates the development and implementation of policies concerning the registration of second-level domain names in generic top-level domains ("gTLDs"); 2) facilitates the coordination of the operation and evolution of the DNS root name server system; as well as 3) coordinates the allocation and assignment at the top-most level of Internet Protocol numbers and Autonomous System numbers (ICANN 2018, online). ICANN offers "registration services and open access for global number registries", working closely with the Internet Engineering Task Force (IETF) and Regional Internet Registries (RIRs) (ICANN 2018, online). Its Bylaws explicitly state that "ICANN shall not act outside its Mission", as defined above, and in particular it is not to "regulate (i.e., impose rules and restrictions on) services that use the Internet's unique identifiers or the content that such services carry or provide". It is characterized as holding no "governmentally authorized regulatory authority". Yet, despite this in the last 20 years, the corporation has become the stage for all Internet governance-related debates and policy making. Although its primary legal obligation is towards its "contracted parties", operating through lengthy private contracts with registrars, its policies and guidelines have long become actual policy standards within the Internet governance environment. ICANN is considered the living example of multistakeholder governance, with issues discussed ranging from intellectual property to human rights, in particular privacy and freedom of expression.

ICANN's policy making is defined within its Bylaws. They reiterate ICANN's "Core Values" - what could be considered basic principles of multistakeholder policy making. They include a commitment to preserving "the operational stability, reliability, security, global interoperability, resilience, and openness of the DNS and the Internet" as well as the "maintenance of a single, interoperable Internet". In doing so, ICANN relies on "open, transparent and bottom-up, multistakeholder policy development processes that are led by the private sector (including business stakeholders, civil society, the technical community, academia, and end users), while duly taking into account the public policy advice of governments and public authorities". ICANN's Core Values provide more insight into how the multistakeholder process works in practice. The corporation and the community around it are to "seek input from the public, for whose benefit ICANN in all

events shall act; promote well-informed decisions based on expert advice, and (C) ensure that those entities most affected can assist in the policy development process" (ICANN 2018, online). Multistakeholderism also implies "consistent, neutral, objective and fair" decision making based on "documented policies". All ICANN processes must remain non-discriminatory, make no "unjustified prejudicial distinction between or among different parties" with ICANN remaining "accountable to the Internet community through mechanisms defined in its Bylaws" (ICANN 2018, online). ICANN principles reflect the way the Internet works and have been purposely formulated in a flexible manner, serving more as guidelines than strict norms. Effectively, their appropriate application depends directly on the nature of the situation in which they are to be used. Yet, this complex, wide-spanning and vague formula makes ICANN a unique policy battle ground, often criticized for being subject to opaque lobbying efforts from the domain name and IT businesses (Froomkin 2003). What adds to that argument is the significant economic power the California-based non-profit holds, with funds under management as per June 30, 2018, amounting to 443 million USD (ICANN 2017, online).

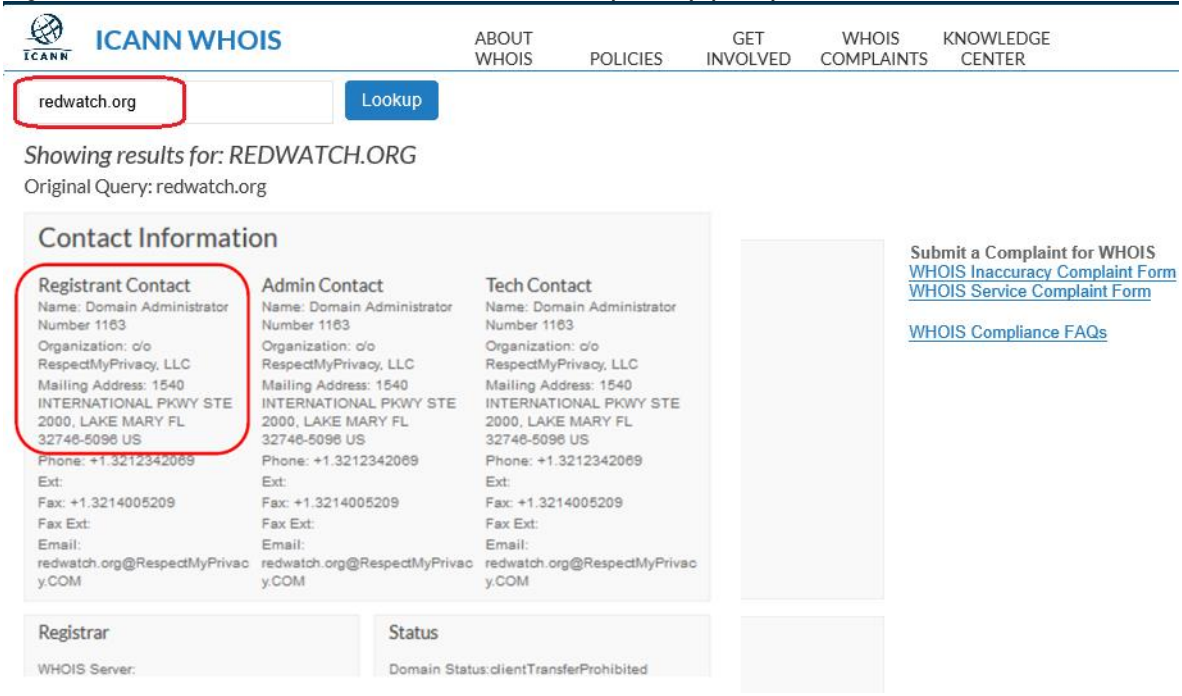
Since its creation in 1998, ICANN has struggled with implementing European standards of privacy protection in particular due to its original design comprising a WHOIS database – a data resource containing information on all domain name registrants, operated by ICANN contracted parties: DNS registries and registrars. ICANN obliged all contracted parties to hold, update and make publicly accessible data on all domain name holders. This resource has been used as a primary reference for various categories of Internet users: customers considering a purchase from an online store, communities compiling lists for anti-spam filters, law enforcement, cybersecurity professionals as well as IP lawyers aiding companies in protecting their intellectual property threatened by the rapid evolution of online communications. The crucial problem with the WHOIS has always been that it directly violated all European data protection laws. Long before the GDPR revolutionized international online contracting, European Union's data protection standards ensured data subjects that their data can only be collected and kept if there is a legitimate ground to do so, either imposed by law or a contract, and particular conditions are met (explicit consent from data subject, data necessity, accuracy and minimalization). Not all data collected by registries and registrars were necessary for the performance of the domain name contract – their scope was far broader than needed. Yet, ICANN contracted parties were obliged, under pain of financial consequences for a breach of the ICANN contract, to collect data on persons or businesses who registered a domain name, including their name, address, e-mail, phone number and administrative contact – what amounted to a WHOIS record. The registrar or registry of the domain was obliged to maintain a publicly accessible WHOIS database with these records (see Figure 1).

Figure 1: Archived ICANN website on WHOIS



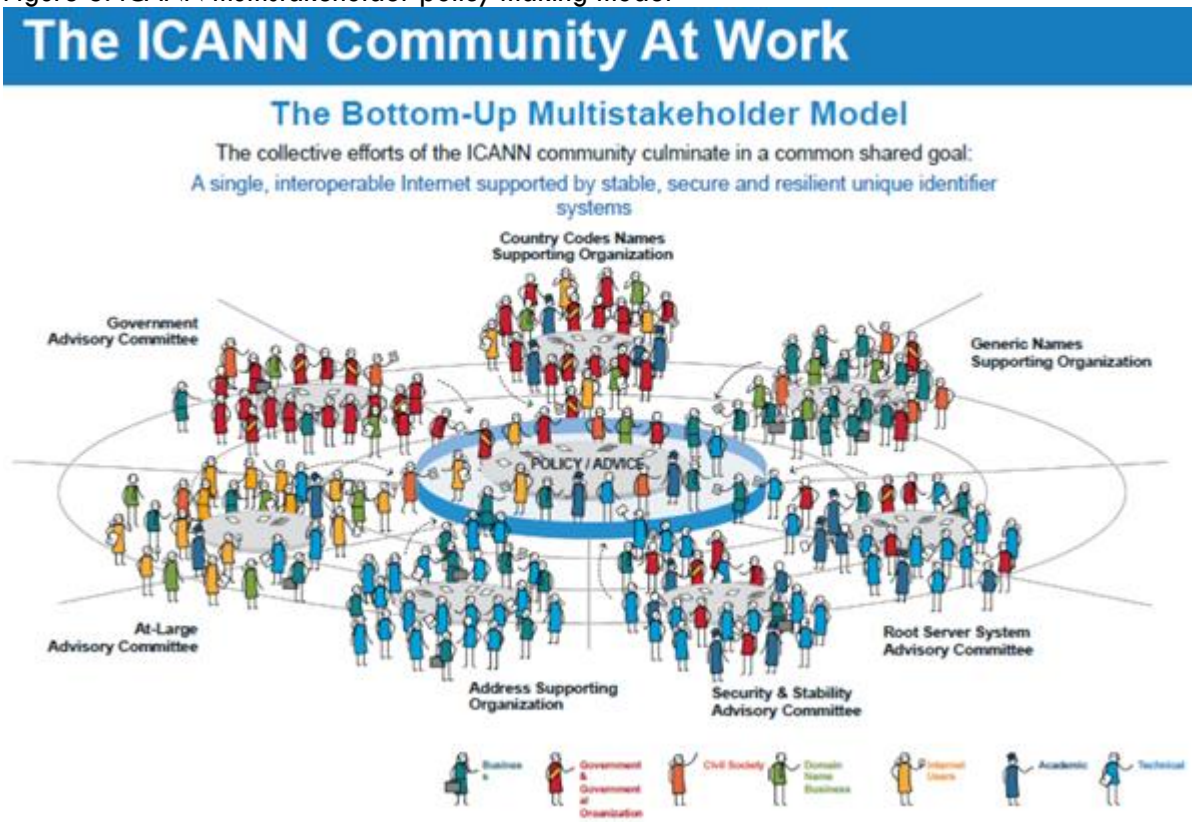
This practice has met with long-standing opposition from civil society and European data protection ombudsman, including the Article 29 Working Party (WP29), including letters of December 2017 and of April 2018 (WP29 2017, 2018). This was for two primary reasons: the broad array of data was collected and made public without a valid aim and left data subject with no possibility to have their data removed. Moreover, the data has been subject to commercial enterprise, with companies like MarkMonitor or Domain Tools monetizing the data for the sake of brand protection companies. While brand protection and the pursuit of trademark infringers is a legitimate aim as per GDPR, the automated collection and distribution of data has always been far beyond what is considered due process and privacy law in the EU. The second argument against WHOIS has been the inaccuracy of WHOIS data – the market gave rise to a vivid enterprise of privacy proxies: companies offering commercial services to those willing to keep their trademark owner details secret (see Figure 2). This practice largely deemed futile all law enforcement efforts to identify online law infringers. On the other hand however, those who could not afford the services of privacy proxy were forced to have their data revealed, accessible to potential spammers or, more significantly, to law enforcement authorities of non-democratic regimes, e.g. a LGBT website owner in Russia who would not use a privacy proxy could be easily identified by local police, surrendering them to national laws setting specific limits on freedom of expression.

Figure 2: Archived WHOIS record with data of a privacy proxy



WP29 expected ICANN "to develop and implement a WHOIS model which will enable legitimate uses by relevant stakeholders, such as law enforcement, of personal data concerning registrants in compliance with the GDPR, without leading to an unlimited publication of those data". The core of the issue is however that ICANN operates on a bottom-up, multistakeholder model of governance (see Figure 3). The California-based ICANN staff cannot impose policy onto the global community of stakeholders – states, users and businesses have to develop it themselves in a complex, bottom-up process (for a detailed record of policy development processes visit: https://www.icann.org/policy).

Figure 3: ICANN multistakeholder policy making model



Following the dawning of the GDPR, ICANN (the California-based company) decided to disable the global resource of personal data, much to the dismay of law enforcement and IP law companies: as of May 2018, WHOIS went dark. This was done through a "Temporary Specification" – an interim measure aimed at safeguarding all ICANN contracted parties against possible GDPR liabilities, imposed (temporarily) by the California-based ICANN staff. This does not mean however that a domain name registration no longer carries an obligation to provide registrant's data – quite the opposite. The current challenge for the ICANN community is to find a reasonable solution for processing registrants' data for all legitimate aims and this is to be done through the multistakeholder, bottom-up process, as opposed to top-down law enforcement by states, like the GDPR itself. Effectively, the results of the Expedited Policy Development Process (EPDP), as published in the draft report of Nov. 21, 2018, are the initial result of a bottom-up, international norm setting with a strong cybersecurity impact (EPDP 2018). Law enforcement worldwide will have to make use of what the global, multistakeholder community deems the appropriate balance between privacy and security, due process and legitimate aims. States hold equal footing with business, academia and internet users in defining what this balance is.

Implications and Lessons for the Future

When discussing governance and its evolution, Jessop argues new models of governance built upon the failures of old ones, describing the process as "second order governance" (Jessop 2015, 170). This process brings with it a reordering of the networks and improvement of commu-

nication modes, rooted in institutional changes. While his argument is focused on states, the general lessons on governance seem to be applicable also to cyberspace with its multistakeholder model. The post-World Summit on the Information Society (WSIS) decade (2005-2015) fueled discussions on specifying the ambiguous notion of "Internet governance", most significantly through defining the "respective roles" of states, business and civil society.

While governments eagerly discuss Internet governance, the current IG landscape was originally designed as the effect of bottom-up governance models, rooted strongly in the technical community, just to mention the Internet Society (ISOC) or the Internet Engineering Task Force (IETF) with its "Requests for Comments" (RfCs), community-developed common standards voluntarily followed by its members: Internet service providers or software developers. While "security by design" remains a common paradigm within both: ISOC and IETF, there is no connection to be made between this extra-legal, community-based rule making approach and the hard norm setting model of, e.g. NATO (Rescorla 2003). While ICANN, ISOC, and the IGF have been attending to the issue, this communications gap holds crucial relevance for the development of any effective international cybersecurity policies and must be addressed by whatever model of global cybersecurity will be developed. There can be no effective cybersecurity policy developed solely at a governmental level, without a strong presence of the technical community and vigilant input from civil society.

---

* Joanna Kulesza, PhD is an assistant professor of international law and internet governance at the University of Lodz, Poland. She is also a Scientific Committee member of EU Fundamental Rights Agency (FRA) and represents European internet users within the At-Large Advisory Committee of the Internet Corporation for Assigned Names and Numbers (ICANN). Views expressed herein are her own.

References

ARTICLE 29 Data Protection Working Party. 2017. *Letter of December 11, 2017 to Dr. Cherine Chalaby and Mr. Göran Marby, Chairman and President and CEO of the Board of Directors*. https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48839.

———. 2018. *Letter of April 11, 2018 to Mr. Göran Marby, President and CEO of the Board of Directors*.

Bygrave, Lee A. 2005. *Internet Governance by Contract*. Oxford: Oxford University Press.

Clark, David D. 1992. *A Cloudy Crystal Ball - Visions of the Future*. https://groups.csail.mit.edu/ana/People/DDC/future_ietf_92.pdf.

Drake, Willian J. 2009. "Introduction: The Distributed Architecture of Network Global Governance." In *Governing Global Electronic Networks*, edited by William J. Drake and Ermest J. Wilson, 8-9. Cambridge, Massachusetts: MIT Press.

Dutton, William H. 2012. "The Fifth Estate." In *The Oxford Handbook of Governance*, edited by David Levi-Faur. Oxford: OUP.

Expedited Policy Development Process (EPDP). 2018. *Initial Report of the Expedited Policy Development Process (EPDP) on the Temporary Specification for gTLD Registration Data Team*.

https://www.icann.org/news/announcement-2-2018-11-21-en.

Froomkin, A. Michael. 2003. "Habermas@discourse.net: Toward a Critical Theory of Cyberspace." *Harvard Law Review* 116 (3): 749-873.

Haufler, Virginia. 2013. *A Public Role for the Private Sector: Industry Self-Regulation in a Global Economy*. Washington DC: Carnegie Endowment.

Henson, Spencer, and John Humphrey. 2001. "Codex Alimentarius and private standards." In *Private Food Law: Governing Food Chains Through Contracts Law, Self-regulation, Private Standards, Audits and Certification Schemes*, edited by Bernd M. J. van der Meulen, 149-174. Wageningen, The Netherlands: Wageningen Academic Publications.

Huizer, Erik, and David Crocker. 1994. *IETF Working Group Guidelines and Procedures*. RFC 1603.

ICANN. 2017. *Budget plan for 2018*. https://www.icann.org/en/system/files/files/adopted-opplan-budget-fy18-24jun17-en.pdf.

ICANN. 2018. *Bylaws for Internet Corporation for Assigned Names and Numbers*. https://www.icann.org/resources/pages/governance/bylaws-en/#article1.

Jessop, Bob. 2015. *The State: Past, Present, Future*. New York: John Wiley & Sons.

Kingsbury, Benedict, Krisch, Nico, and Richard B. Stewart. 2005. „The Emergence of Global Administrative Law." *Law and Contemporary Problems* 68 (3): 15-45.

Levi-Faur, David, ed. 2012. *The Oxford Handbook of Governance*. Oxford: Oxford University Press.

McNair, Corey. 2018. *Worldwide Retail and Ecommerce Sales: eMarketer's Updated Forecast and New Mcommerce Estimates for 2016-2021*. eMarketer. https://www.emarketer.com/Report/Worldwide-Retail-Ecommerce-Sales-eMarketers-Updated-Forecast-New-Mcommerce-Estimates-20162021/2002182.

Rescorla, Eric, and Brian Korver. 2003. *Guidelines for Writing RFC Text on Security Considerations, Request for Comments: 3552*. https://tools.ietf.org/html/rfc3552.

Weber, Rolf H., and Romana Weber. 2009. „Inclusion of the Civil Society in the Governance of the Internet. Can Lessons be drawn from the Environmental Law Framework?" *Computer Law Review International* 10 (1): 9-15.

World Summit on the Information Society (WSIS). 2005. *Tunis Agenda for the Information Society*. http://www.itu.int/wsis/docs2/tunis/off/6rev1.html.

Binary-Coded Self, Society and State. From Bridging Homepages to Bordering Homelands

By Octavian-Dragomir Jora*

The development of cyberspace is leading to a massive increase in the number and complexity of interactions among inhabitants, generating new sources of profit, power, social capital and conflict. Despite the apparent suspension of scarcity online and of the subsequent need for proprietary limits, cyberspace fuels cooperation and competition, defining our species as well as defying our sociality. States are struggling to adapt to these evolutions by conceptualizing them in accordance with their preferred mental modes and instruments, setting borders, jurisdictions and spheres of influence. While cyberspace has not proved amenable so far, these efforts will impact cyber-governance, both in and among nations, in ways that will boost state powers and tighten the scope of freedoms online.

Key words: cyberspace, liberty, society, statehood, rights, jurisdiction.

Introduction

Information is a *commodity*, as information is power. By exchanging and extolling information, cyberspace becomes *bazaar* and *agora* (Jora 2017), a (market)place both for private commerce and cooperation, as it is for public coercion and corruption. Cyberspace immerses virtually three billion inhabitants worldwide, having transformed from a playground for technical experts to a marketplace and meeting hall for every kind of entity. Citizens and consumers, governments and armies, NGOs and corporations live these cyber-realities, seemingly outside the traditional territory of geopolitics and ahead the predicted times of geo-economy, but still mappable and marketable along the unchanging lines of *human nature* and *behaviours*.

Reproducing the real world or completing it, cyberspace electronically preserves the human action with its social, cooperative expressions as well as with its state-made, coercive ones. Societal crises can display dramatic repercussions in the virtual realm, exposed by the very nature of the information society, while creating opportunities and threats to freedom and democracy (Kempf 2012). These threats are not just the prospect of Orwell/Huxley/Zamiatin-previewed totalitarian regimes to use computers to monitor almost all feats of their citizens' lives. A more significant danger lies in hidden control and command of beliefs and actions that the majority is manipulated into embracing through manufactured consensus fuelled by light-speed chat.

Information is seen as a *scarce resource,* despite apparent technical abundance, and poses problems of property rights both *materially* (as physical infrastructures of storage and circulation) and *spiritually/intellectually* (as devices to protect creative craftsmanship, innovative industriousness) and of regulatory jurisdiction and national security. It is an invitation to states, whether autocratic or not, to monitor its flows *within/across* borders. And such streams are diverted to circulate only inside specific groupings and for particular interests. Privacy, access, trade privilege, and public interest have been debated endlessly in history and are relevant again.

The (nation-)states, the fundamental unities of geopolitics, are perceived at the sunset of their existence, although realities seem to reject such a hasty prognosis. They conscientiously cultivate the interest that has pushed them into being, preserving their existence both in the physical environment and in any other available space – the cyber realm. The *geopolitics of cyberspace* derives from the *geopolitics of information* (Smith 1980) and is crying now for a posture of its own, ad par with the old-time geopolitics, both scholarly and mundanely. This paper tries to sketch some contours, overlappings and missing spots of the geopolitics of cyberspace as seen at the crossroads with the newer economy of global/digital interconnectedness.

The new economy of past geopolitics

When we talk about the *new economy* (Browning and Spencer 2002), we are talking about a brand new world: one where people work with their brains more than with their brawn; one where information technology creates global markets and military competition; one where innovation is more important than mass production; a world where, through investments, new concepts are acquired and ways to develop the old ones, rather than new machines; one where rapid changes are the only constant.

The latest *new economy* involves several changes of scope and scale, breadth and depth that far exceed the avatars of the traditional factors or production relations. Along with it, the whole *global polity* and all *national polities* borrow that disrupting novelty. Territory and power, the *raison d'être* of old-school geopolitics, are neither immune to novelty nor can ignore it. While geopolitics modifies its discourse from one era to the next, it stubbornly frames the world order and dismisses voices claiming its desuetude.

Space and territory – *factors of production* and *casus belli*, as well – are changing. Influenced by computerization, globalization and deterritorialization, global space challenges the traditional geometry of territory and moves towards multiple and decentralized forms challenging the sovereign power of states (Tuathail 1996). Far from being displaced by this new internet-, digital-, cyber- spatiality, geo-politicians and geo-strategists are rather concerned to re-map and manage it (side by side with economists).

Globalization, computerization and the emergence of global risk propagation have transformed the discourses and repertoires of geopolitical thinking, but a resignation of geopolitics is unlikely. Pretenders were launched under various names and disguises in postmodern times, but far from substituting classical geopolitics, they are rather complementary to it. Among them, we mention:

chronopolitics – the loss of material space consistency shifts governance to time management; *geoeconomics* – trade and investment considerations dislodge the obsolete military treatments; ecopolitics – the imminence of environmental menaces redesigns rivalries and alliances, *geogovernment* – a more integrated reality from the economic, cultural and political is cried for. Unable to be replaced and impossible to be neglected, spatiality keeps unaltered its significance in the universe of human actions.

The *Internet* (aka *cyberspace*) is the extra dimension in the new economy/polity/society. Admittedly, it is far more than the tool that the (*fake news*) media often overuses, or the simple vehicle that (*dot.com*) business abuses. It offers a new alternative for establishing communities, the habitat of online society, a spatial dimension of wealth similar to that of a newly discovered country, but still intersected by reminders of a past world. The Internet network is proper and ready for a geopolitical study. For there are geopolitical objects, in the perspective proposed by the geographer Yves Lacoste (1993), from the *Hérodote* school, that of territorial rivalries subject to contradictory representations. Power struggles that remodel our civilization deeply do not take place only in the real territories of nations or peoples; they behave in the same way within the virtual world. Still, parallelisms look less intuitive.

Running in both real and virtual dimensions, offering universal support for expressing different representations, the Internet changed the geographic scale we were accustomed to looking at, confusing, implicitly, the geopolitical dimension. The Internet is spatially physical: it is sufficient to review the planetary extension of these networks, the location of the servers and telecom operator cables, the nerve endings of personal computers. Such real architecture reveals the strengths and the domination of certain actors, public or private. But the Internet does not only signify palpable, measurable territory. There are online worlds created by *internet users*. And these users are asymmetrical in interests and power; they enter combinations and conflicts alike, they rely on state or escape state institutions, so they are *political,* in their classical jurisdictions, and *geopolitical*, in anarchical global *cyberspace*.

Bits, bytes, boundaries and borders

Cyberspace interests the state for a simple reason: it is a populated territory. In the world of (nation-)states, space is sanctioned at the level of territories, framed by borders, at the level of points, zones or spheres of influence. There are several studies (Pingel 2001) trying to explore the suitability of traditional (geo)political concepts to fit into new cybernetic garments. One may be guided along four axes: (a) reviewing the development and history of state boundaries theory; (b) determining a paradigm associated with the idea of a suitable boundary within which to situate cyberspace; (c) highlighting the interest of states to maintain and enhance their presence in cyberspace; (d) an inventory of state manifestations in the cyberspace.

The other side of the coin is to merely state that the anonymity and ubiquity that cyberspace allows, as well as its defiance of traditional physical and time-space dimensions, would have it become something akin to the high seas, international airspace or outer space – being considered as some *global common* or, legally, a *res communis omnium* and, therefore, immune to appropria-

tion by one state or a group of states, as Antarctica or the Moon (Heintschel von Heinegg 2013). States have persevered in imposing their authority, motivating the need to prosecute cybercrimes and terrorism. Even as they cooperate internationally for investigations, they do so using the established norms for cross-border cooperation, in respect of sovereignty.

Sovereignty is a complicated and controversial concept in political and legal theory, at least as complicated and controversial as the very concept of *state*, with which it is organically associated. Beyond the moral and ethical disputes it ignites, it is futile if the supreme authority (irrespective of its source) lacks a certain *territorialized population*.

A large number of paradigms associated with the idea of *territoriality* and, hence, *borders* have been articulated throughout the 20th century, facilitating comparisons and analogies with the situation of the cyberspace. Stephen Jones (1959) proposes some such ideas, out of which a few do seem relevant in the setup of cyber-borders (see Table 1).

Table 1: Border paradigms and border properties

Border paradigm	**Border properties**
Primitive or tribal model	The boundaries were non-linear, the territories being rather bounded by zones; blood ties prevailed over the territory as a political unity
The imperial model	There were either harsh, linear demarcations, separating civilization from barbarity (China), or flexible, fortified formula (the Roman Empire)
European Middle Age model	Distinct territories (by culture, language, etc.), allocated and inherited to/by dynastic families, not being connected whatsoever to each other
Nation-state model	With the concentration of territories on a national basis, rather than a dynasty, the aim for continuous territorial areas as well as legitimacy prevailed
The organic model	State boundaries resemble the dermis of a plant or animal, which spreads or strains as dictates the needs of the state, being poorly permeable
The contractual model	States should agree on a line and respect it; it is improper to use military force, the true forms of an establishment being represented by treaties
Power policy model	The frontier is nothing less than a biological battlefield in people's life; therefore borders being the contact lines of territorial power structures

Source: Synthesis after Jones (1959).

John R.V. Prescott (1965) articulates a concept which, due to historical similarity, was called the *American West Paradigm* and distinguishes between primary (*de facto*, rough and mostly done) setting of state-made, political borders and some secondary establishment of frontiers (*de jure*, more thorough, in progress).

There are, as well, some authors (Rosencrance 1996) predicting the very decline of the nation-state paradigm on the grounds that territory is no longer as important as it once was. This seems more attached to the idea that the resources used by one state do not necessarily mean resources refused to another. In other words, since cyberspace cannot be filled, growing continuously, it defies the obsolete physically-scarce world (Virilio 1997). But borders stay in trend.

The multi-layered cyber-spatiality

It may not be possible for states to establish an effective division of their cyber-territory. Still, since cybernetic space grows, it might be a good starting point if someone wants to use a contractual paradigm to determine how the expansion of cyberspace can match website ownership. In cyberspace, there are no rivers, no mountains, no trenches and no walls that can be digested as a mere frontier. It is fundamentally different from the real one, being composed of wires and hubs, its borders are hardly natural. But if artificial borders are not *per se* more unstable than the natural ones, they are less intuitive. As all artificial boundaries are either subjective or arbitrary, it is easier for two parties not to understand the respective boundary position. Here, the case of cyberspace is paramount.

The discussions on *mapping* the cyberspace and the selection of the most comprehensive paradigm for delineating borders and thus power and authority over a particular area are legitimate concerns. The spatial character of the *network* can be accepted as derived from the idea of an *environment* where there are degrees of *movement*: information and value move and so do power and influence. By consequence, cyberspace looks like a legitimate geopolitical (as well as a geo-economic) space, for its design of opposing interests and colliding influences, imply territorial allocation of resources. It, therefore, becomes a kind of geopolitical territory, superimposed onto a sum of private spaces, mapped rather through volatile/virtualized connections rather than concrete/rock-solid coordinates.

In an article projecting geopolitics over cyberspace, Frédérick Douzet (2014) identifies four layers for such *cyber-spatiality*: physical objects, logical infrastructure, soft applications, and interactions. At every level of this multi-layered space are rivalries of power between actors over technical issues, but whose stakes are, in a meaningful measure, geopolitical (see Table 2).

Figure 2: Layers of contemporary cyber-geosphere

Layer	**Fabric**
Physical objects	Submarine and terrestrial cables, satellites and radio relays, computers and other terminals – that is a set of equipment ultimately installed on a territory, subjected to the constraints of the physical and political geography, that can be built, modified or destroyed, connected or disconnected from the network
Logical infrastructure	Services that make it possible to transmit information across the web and, thus, to make it travel divided into small data packets, from sender to recipient; it is based on a common language (the Internet Protocol TCP / IP); it includes (also geo-localizable) services of routing, naming and addressing
Soft applications	User-friendly computer programs that allow anyone to use the Internet without knowing anything about computer programming (Web, e-mail, social networks, search engines, etc.); some apps (by Google, Facebook, Amazon, etc.) cunningly exploit blindly entrusted private info, to the gain of third parties
Social interactions	Users, discussions and exchanges in real time around the world; it is geopolitically relevant when it comes time to determine the most friendly countries on social networks, observing the cultural penetrations or the location of social rebellions or disinformation campaigns against governments (or other entities)

Source: Synthesis after Douzet (2014).

Various analysts observe that in spite of the illusive easement with respect to commercial espionage, malicious and exploitive cyber practices remain an extensive and exhausting feature of twenty-first century international relations. These criminal cyber operations can be grouped in three broad categories, intersecting all the above-mentioned layers of the cyberspace: (1) espionage and information leaks, (2) disrupting connections and denying access, and (3) software and hardware destruction (Watts and Richard 2018).

These cross-cyberspace-fabric and cross-national-jurisdiction practices growingly defy the old-fashion understandings of the limits on state activity confined to territorial sovereignty during times of nominal peace. States are called to reframe sovereignty to operate adequate to cyberspace texture, as they did in other episodes in the history of international relations. Absent a *lex specialis* regarding cyber sovereignty, the precedent of securing traditional territorial integrity offers a principled (yet too passé) starting point.

Cyber-geopolitics and cyber-warfare

Cyberspace evolved from Gibson's (1984) fantasy to a territory to conquer, control, monitor, and reclaim, on which everyone must respect borders, sovereignty, laws, while deviated cyber-conduct equates to an assault on the national interest/security. The *Westphalianization* of the cyberspace, in terms of sovereignty and jurisdiction, points towards the claim and crave of states to exercise full and exclusive control and command over *their* cyber-territories (Schmitt and Vihul 2017). With certain instruments, this is also possible, if not particularly effective, in cyberspace.

Nota bene, when it comes to *planting state flags* (Dossé 2010) in cyberspace, two at odds representations regarding this unusual, hybrid, multi-layered and multi-fabric territory severely enter into a collision course: the first one is that of *individual freedom*, while the second one calls for the *sovereign state* to follow-up on its citizens' rights and duties, to serve and protect them in the *digital* space as it does in the *analogic* one, with the same obscure price paid as fiscal and regulatory control in exchange for (true or false) public goods (Iacob 2016).

Among the former, by 1996, even a *declaration of independence of cyberspace* had been issued, asserting the self-sovereignty of cyberspace (citizens). In this civilization of the mind – it was considered by the liberalists –, the laws of the governments, emerging from the conventional physical world, do not and shall not be made to apply. Notably, such internet freedom philosophy was a revamped episode of the 1960's countercultural movement, preaching for openness, self-management and freedom of exchange and expression.

But cyberspace, supposedly lost in the sci-fi novel universe, reappears in the 2000s in the *realpolitik* of state institutions and officials (Deibert 2015). In 2007, Estonia, one of the most digitalized countries in the world, was under a ferocious cyber-attack – some critical infrastructures for both public administration and private economy were paralyzed –; this siege was instrumented not by tanks or airplanes, but by networks of thousands of zombie (malware infected, remotely con-

trolled) computers; a year later, it was Georgia's turn to be hit.

Realism informs us that the force of sovereignty is ultimately related to the capacity to defend it in plain battlefield long before doing it in law courtroom.

The *Great Firewall of China* (as monumental as its stone ancestor) is an utterly fortified border (access and egress being not only for people and goods, but also for information) whose acceptance grounded the idea of the exclusivity of the territory behind the wall, where China may influence the content and communications of its people. That it can be subverted with ease and people routinely do so may harm the Chinese claim to cyber sovereignty, but not wholly, as China retains, through the physical world, the ability to punish violations of its regulations and exert control over the physical infrastructures to compel obedience, should it purpose to do so.

An indirect claim of inherent territoriality, not yet formally defined and delineated, comes from the ability of countries to work together to establish governance for cyberspace, eliding the usual need first to establish who controls what. The Obama Administration added to this view of continuity between territoriality and cyber-spatiality saying that the development of norms for state conduct in cyberspace neither require a rewriting of customary international law, nor render the international norms, currently in place, outmoded, explicitly marking the fact that longstanding rules guiding (peace/war) state behaviours cover cyberspace too (Brown and Poellet 2012).

Geopolitical confrontations in cyberspace would either take the form of *lawfare*, the use of laws, institutions and norms to pursue interests outside the scope of the instruments used, or of *a mutually assured destruction warfare* type of confrontation, even of nuclear magnitude, which rewards deterrence and restraint. It is still worth mentioning that cyberweapons feature as an equalizer of power between states and also between states and non-state actors. The proliferation of cyberweapons may result in significant disruptive potential, as there are no barriers of costs to their replication and usage, while certain actors do not respond well to deterrence.

Power in cyberspace will belong to the country which can rally important stakeholders to its side. The most important stakeholders are those controlling the physical infrastructure or the virtual infrastructure of cyberspace, such as a search engine which is the gateway to the Internet for most people, or a social network. Others are international institutions and influential working groups. Power comes with the network of reliable proxies ensuring plausible deniability for the use of cyberweapons in surgical strikes against rivals' infrastructure, as power comes from the capacity to withstand severe cyber-conflicts, thereby gaining both prestige and followers.

Conclusion

Invoking the need to secure sovereignty and having as sovereign concern security, states are fighting a symbolic battle for control over identifiable swathes of cyberspace. They are increasingly defining their rule by extending their physical space of authority into the cyber one, where people, systems and, growingly, everyday items find a virtual correspondent, and by building on

the existing set-ups for sovereignties and inter-state relations: *to be online as it is in the physical world!*

The states have an abiding interest in this and, therefore, are also motivated to legitimize their policies and actions by promoting an ideology or worldview which supports their intentions, predicated as protection against solitaire criminals and, of course, rogue states. The conjoint themes of cyber-security and cyber-liberty represent the renewal of the ages-old conundrum: *might the surrender of some freedom for more security leave us at the end of the day in possession of neither?*

---

* Octavian-Dragomir Jora is Associate Professor, Ph.D., at the Bucharest University of Economic Studies and the founder and editor-in-chief of *The Market for Ideas* magazine.

References

Brown, Gary, and Keira Poellet. 2012. "The Customary International Law of Cyberspace." *Strategic Studies Quarterly* 6 (3): 126-145.

Browning, John, and Spencer Reiss. 2002. *Encyclopedia of the New Economy*. Madrid: Terra Lycos.

Deibert, Ron. 2015. "The Geopolitics of Cyberspace after Snowden." *Current History* 114 (768): 9-15.

Dossé, Stéphane. 2010. "Vers une stratégie de milieu pour préparer les conflits dans le cyberespace?" *Défense et Sécurité Internationale* 59: 82-85.

Douzet, Frédérick. 2014. "La géopolitique pour comprendre le cyberspace." *Hérodote* 152-153 (1): 3-21.

Gibson, William. 1984. *Neuromancer*. New York: Berkeley Publishing Group.

Heintschel von Heinegg, Wolff. 2013. "Territorial Sovereignty and Neutrality in Cyberspace." *International Law Studies* 89: 123-156.

Iacob, Mihaela. 2016. *Costuri și beneficii ale analizei cost-beneficiu. Înainte de pragmatism, înapoi la principii*. Bucharest: Editura ASE.

Jones, Stephen B. 1959. "Boundary Concepts in the Setting of Place and Time." *Annals of the Association of American Geographers* 49: 3.

Jora, Octavian-Dragomir. 2017. "PrestiDigital GeoPolitics. Web Spatiality and Territoriality." *The Market for Ideas* 7-8 (Sep.-Dec): 40-47.

Kempf, Olivier. 2012. *Introduction à la cyberestratégie*. Paris: Economica.

Lacoste, Yves, ed. 1993. *Dictionnaire de géopolitique*. Paris: Flammarion.

Pingel, Thomas. 2001. "Applying State Boundary Theory to Cyberspace" (draft paper), unavailable online, accessed in December 2002.

Prescott, John R.V. 1965. *Geography of Frontiers and Boundaries*. Chicago: Aldine Publishing Company.

Rosencrance, Richard. 1996. "Rise of the Virtual State." *Foreign Affairs 75*: 4.

Schmitt, Michael N., and Liis Vihul. 2017. "Sovereignty in Cyberspace: Lex Lata Vel Non?" *AJIL Unbound* 111:

213-218.

Smith, Antony. 1980. *The Geopolitics of Information*. London: Faber.

Tuathail, Gearóid Ó (Toal, Gerard). 1996. "At the End of Geopolitics? Reflections on a Plural Problematic at the Century's End." *Alternatives: Global, Local, Political* 22 (1): 35-55.

Virilio, Paul. 1997. "Un monde surexposé". *Le Monde diplomatique*.

Watts, Sean, and Theodore T. Richard. 2018. "Baseline Territorial Sovereignty and Cyberspace." *Lewis & Clark Law Review* 22 (3), 771-840.

.

VISIO INSTITUT

Visio institut is an independent, non-partisan research organization based in Slovenia. Its aim is to develop and promote public policy and institutional reform proposals to foster an open, free, developed, and just society in Slovenia. To that end, Visio institut organizes events, produces publications, and appears regularly in the media.