Think Visegrad
V4 Think-Tank Platform

POLICY BRIEF
2018/December
Think Visegrad in Brussels

Cyber security and Sovereignty
Two levels of digital autonomy

Botond Feledy

Think Visegrad
V4 Think-Tank Platform

POLICY BRIEF

2018/December
Think Visegrad in Brussels

Summary

As described in the third part of the paper, two parallel processes are running. The state is being challenged on multiple fronts – online monopolies, populists and crypto-anarchists – while its citizens expect protection not only offline, but online as well. In other words, the pressure on the state apparatus to deliver is twofold. Citizens deserve the protection, as this is the most important promise of the state in the social contract. Once the sovereign cannot protect its sovereign territory – even in cyber space – the contract might become fragile or even broken. This is the state level of digital autonomy. On the other hand, citizens must enjoy their own individual level digital autonomy vis-à-vis their own state. This is the only guarantee that can hinder the birth of surveillance states inside the Euro-Atlantic space.

Introduction

While cyber security seemed to be a narrow policy question couple of years ago, it has started to break down the wall of policy conventions. The security dilemmas of the cyber space remain wide open. This has been demonstrated by each incident as our horizontal understanding of cyber security has evolved. However, **the cross-policy implications of an omnipresent cyber security policy are still up for debate**. From precision-agriculture to big data ethics, there are plenty of implications needing to be tackled. Most importantly, it is high time to rethink the legal and constitutional foundations of policies tampering with cyber space, given how cyber security is influencing the principles of our centuries old social contract between citizen and the state. One of the common goods delivered by the social contract is security, provided by the state for its citizens. As the latter moves more and more online, the protective umbrella of the state should cover the cyber space as well. Whether the state is the historically most able social unit to offer the most effective defence in the cyber space or shall it be a regional alliance of states or sub-state units, is a question posed by this paper.

The EU and cyber space

The European Commission has sped up its efforts to drive dialogue and legislation in the field. Since the introduction of the 2013 EU Cyber Strategy[1], the NIS[2],

[1] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - JOIN(2013) 1 final - 7/2/2013; and Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, adopted by the General Affairs Council on 20 November 2017.

[2] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

GDPR[3] and eIDAS[4], - among other cyber-crime related pieces of legislation[5] - have been accepted and put in motion. More ambitiously, the EU bloc's objective of becoming global leader in cyber security was translated into becoming a digital safe haven in cyber space: "The Heads of State and Government at the **Tallinn Digital Summit, in September 2017, called for the Union to become 'a global leader in cyber-security by 2025**, in order to ensure trust, confidence and protection of our citizens, consumers and enterprises online and to enable a free and law-governed internet.'"[6]

On this road, the European Union Agency for Network and Information and Security has been recently transformed into a permanent EU cyber security agency with enlarged mandate. The "European Parliament, the Council and the European Commission have **reached a political agreement on the Cybersecurity Act, which reinforces the mandate of the EU Agency for Cybersecurity** (ENISA) so as to better support Member States with tackling cybersecurity threats and attacks. The Act also establishes an EU framework for cybersecurity certification, boosting the cybersecurity of online services and consumer devices."[7]

Safety and security in cyber issues is clearly rooted in the wish to guarantee the safe use of computer networks and related technologies for the benefit of EU citizens, without interference from third states, criminals and hostile internal or external actors. For the sake of creating this secure environment for the citizens, **the recent legislation is revolving around the creation of digital autonomy for the Union** under the flag of the Digital Single Market. The digital autonomy is better understood as part of the strategic autonomy, cited often in regards to military affairs.

The above-mentioned certification plays a central role in establishing the technical-level autonomy. As long as foreign-produced software and hardware are present at all levels of life of EU citizens, security can only remain a distant dream. **Certifications will contribute to design an incentive-system for the EU industry to start engaging much deeper in cutting-edge IT sectors** and hardware verification and production. In some way, certificates might provide a way for the necessary protection of EU markets against third parties.

[3] 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, and repealing Directive 95/46/EC (General Data Protection Regulation)

[4] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

[5] e.g. Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA

[6] Proposal for a Regulation of the European Parliament and of the Counciestablishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres; Brussels, 12.9.2018, COM(2018) 630 final - 2018/0328 (COD)

[7] https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en

Horizontal challenges of cyber security

The path-dependency of the evolution of the European Union created a somewhat biased approach. It means that the EU has a very strong accent on economic integration, much less on defence or security. The Digital Single Market initiative itself remains economically focused, **cyber security is akin to climate change; it lingers as a broad horizontal policy** for the upcoming 21st century. The European Institutions are also adapting to this new reality right now. It means that one needs to disentangle cyber security from economy (digital economy, digital innovation, digital infrastructure) to assess its real societal implications. By now it is understood that cyber security touches on the very foundations of democratic institutions, free speech, economic prosperity *and* national security.

The expert community[8] introduced already two decades ago the expression "internet sovereignty" for describing what the EU understands as digital autonomy. Mostly it is applied to China and Russia, where it is more expressly embedded the related national strategies that these countries see their national cyber space as part of their sovereign territory – and thus desire for the same level of control over it as they do with their physical territory. For democratically non-performing states and for competitive autocracies it is also a pretext to supress their own population and not just to defend them from outside influence and threats. It is an easy way for population control – like the more and more widespread social scoring system in China - for massive psychological operations – like tampering with election campaigns at individual level through social media platforms – or for strategic deception campaigns – like the disinformation surrounding the so called "referendum" regarding the Crimean independence. .

For the Euro-Atlantic countries – the EU member states and the USA – the challenge is double: **they need to defend their own citizens in the cyber space and at the same time they have to provide guarantees for the same citizens that their own states will not abuse** the technical power that is necessary otherwise for their security.

It is the very classical question of not using the military at home but only under very limited mandates and extraordinary circumstances. The statute of the military has been evolving over centuries to reach the current level of sophisticated regulation. While certain parts of cyber defence are embedded in military regulations, the overarching nature of cyber security touches upon much more critical questions than *just* military-wise. How can the inviolable rights of citizens, upon which western democratic institutions are founded, be reconciled with the heightened state activity in cyber space, which infringes upon those same rights?

[8] As early as end of the '90s: Timothy S. Wu, „Cyberspace sovereignty? – The Internet and the International System" in Harvard Journal of Law & Technology Volume 10, Number 3 Summer 1997, p. 647.

Chance for an EU leapfrogging

The EU faces another layer of challenge when addressing cyber security. Similar to the common defence dilemmas, the questions of delineation of competences, organization and level of cooperation between the EU and Member States apply to cyber security. The EU28 has started long ago with their own national cyber security strategy and establishment, in the civilian (law enforcement) as well as in the military structures at member state level. While subsidiarity applies here without doubt, it is also important to notice that **actors are less bound by centuries-old path-dependent establishments** – like in the military. It means a chance for the member states to create a supranational structure for cyber security at the European level (or event at V4 or Benelux regional level for example), without the need to substantially transform long existing member state practices. This is a quite unique chance for deepening the EU at a new domain of co-operation, where **leapfrogging is possible, necessary and relatively less costly in political terms**.

Co-operation is more or less inevitable: poorer member states have to pool resources in order to hire the best cyber security personnel; more member states might together start common higher education initiatives to cover certified cyber security degrees valid all over Europe; or simply joint-efforts in cyber security public procurements, especially when it comes to (future EU-)certified hardware or software. Economy of scale will be also necessary to bring life to EU-level cyber security corporate champions. All these are already under way, mostly in early stages. However, **the reckoning of the political elite with this period of grace is still to come**.

II. Rights in the cyber space

In 2018, member states hold the most legal competence to act and enhance cyber security. Meanwhile, **cyber space hosts actors from all levels of international relations: from individuals to regional powers**. The individual-level is unusually strong when it comes to cyber space, even when compared with other international civic movements or transnational NGOs. The cryptocurrency movement, the transnational start-up ecosystem, where empowered individuals are trying to fix societal problems with bottom-up solutions. This equation reminds us that **the state is just a middle-man** here, not exactly mainstreaming the development of cyber security, but trying to catch up all the time. Meanwhile, the industry and individuals are speeding up their revolution through disruptive technologies, other global regions and regional players are vying to create their own sovereign cyber spaces, like China, Russia or Iran, at the level of internet backbone cables, firewalls or by the means of software-enhanced filtering. Thus, most other states on the globe are left fighting for their own national cyber security against intrusive regional hegemons and empowered individuals.

In this context, digital autonomy might gain significance at two strategic levels: **first**, as a digitally autonomous and **safe region of the cyber space inside the European Union**. It might get translated by multiple efforts at all layers of cyber space: hardware, programming or information-level.[9] Hardware might involve for example the FPGA-enhanced filtering, [10] software security audits and certification are for the programming level, while the information space is already policed by the East StratCom Task Force, an official EU body, countering disinformation, a job carried out by several other actors as well.

Hostile actors – stealing intellectual property, threatening the critical infrastructure – must be closed out from the EU cyber space. At the same time, **EU citizens must get all the guarantees that the tools installed for their protection are not transforming into a surveillance society**. This is where the **second** level of digital autonomy lies: **the digital autonomy of the individual vis-à-vis the state** or other mandated regional law enforcement agencies, perhaps the future EU Cyber Security Agency.

After the Patriot Act in the United States, with all the debates surrounding Wikileaks, Edward Snowden and mass meta-data surveillance, it is clear that the future generation of fundamental rights must deal with digital autonomy at the individual level and interpret it according to the evolution of the information and communications technology (ICT) environment.

So far, the European debate – Commission papers and policy in effect – has much focused on trade: "**introduction of controls on the export on critical cyber-surveillance technologies that could cause violations of human rights** or be misused against the EU's own security (…)"[11] In other words, the European decision-makers are already having the right focus on exporting technologies that might hurt human rights abroad in third countries, as well as not offering to sell our own weaponry to be used against us.

What is taken for granted is the fact that these technologies will not get used against member state populations. This is not yet supported by facts: the widespread empowerment of covert activities of intelligence services after the recent wave of terrorist attacks in 2015, the stepped up efforts to counter foreign online intelligence

[9] C.f. Botond Feledy, "Challenges of theoretical approaches to cyber security" in *Theorising Security in the Eastern European Neighbourhood: Issues and Approaches*. Edited by Richard Q. Turcsányi, (Strategic Policy Institute, Bratislava) and Maryna Vorotnyuk (Central European University, Budapest), 2018, pp. 147-163. http://stratpol.sk/wp-content/uploads/2018/04/Theorizing-e-book.pdf

[10] FPGA stands for field-programmable gate array. For applied use, see for example Ajami, Raouf and Dinh, Anh.: „Design a hardware network firewall on FPGA", 2011, pp. 674-678. 10.1109/CCECE.2011.6030538.

[11] JOIN (2017) 450 final, P.19.

activity, the eavesdropping by allies on allies that came to light, these all demonstrate that member states are yet not fully able **to level the protection of EU citizens against their own state apparatus**, potential abuse or misuse of online power projection capabilities of law enforcement and intelligence services. Given the number of investigative reports how much semi-official backdoors might be used in practice by state authorities, citizens need articulated options to defend themselves against it.

Much more attention should be paid to the general principles of their use and the **time-proof ethical frameworks that all new developments should always respect**. In this context, time-proof principles refer to principles that are not bound to a specific technology, but are linked to human rights. By the use of ethics – instead of hard law – one can gain time and momentum. While lawmakers are lagging behind and are hindered by the national borders of legal systems, an EU-level consensus on cyber ethics is more easy to imagine. Perhaps the Economic and Social Committee or other consultative bodies of the EU institutions might get an extension responsible for cyber ethics and its control.

Another good example is the “security by design” principle of GDPR. It is about avoiding that devices used in the EU might be easily penetrated, so it is a defence against third players. It is a principle which helps to protect the EU cyber space (regional level) and, at the same time, offers security for citizens (individual level). Such principles must be tailored to be compatible with all future ICT pieces of legislation.

The Hague-based Global Commission on the Stability of Cyberspace (GCSC), or the Paris Call for Trust and Security in Cyberspace are excellent first steps, but the 500 million Europeans need to push for more; It is worth remembering how long it took for the constitutional legal practice to embrace the so-called third generation of fundamental rights, where the right to healthy environment was accepted.

Finally, policy-makers across the EU-level should be aware of political developments in certain member states where democratic principles are under scrutiny either officially by the European Commission (rule of law procedure) or have been criticized in high-level dialogues. One should not ignore the possibility what those governments with weak commitment towards the strengthening of democratic institutions – failing democratic transitions or populist pressure on institutions – might do once in possession of rising surveillance capabilities.[12] The EU-level might be the necessary level to bring in guarantees and **offer interpretations of the Charter of Fundamental Rights of the European Union regarding its application in the cyber space.**

The European Commission and most member states openly **support the application of international law and the UN charter’s principles in the cyber space**. Nevertheless, their application is not as straightforward as it seems to be at first sight: it needs to be developed on a case-by-case basis, creating a legal body of soft

[12] Like the case of the raid against leaders of the Austrian Intellgicen Service BVT in March 2018: https://www.dw.com/en/austrian-police-raid-on-agency-prompts-outrage/a-42960940

law and hard law to support citizens. In other words, not only financial investment or digitally safe products are needed, but a legal body enshrining cyber security at both level of digital autonomy is also needed.

First, different forms of soft law might indicate future applications of existing human rights and their possible extension into cyber space. It is undoubtedly central to the stability of democratic societies in the coming decades to lay down the frameworks: **much more emphasis needs to be given to this ethical discourse than was given so far**. Certainly, some discussions on larger ethical questions in certain policy fields[13] have taken off, but the general population must also be oriented in this debate, which will shape the technical environment of our common European future. Politicians need to talk more and more about cyber issues, even if it implies a learning curve for them as well.

Finally, one should also consider how much the EU cyber security might become a core element of the Permanent Structured Cooperation (PESCO) and of the European Union's security and defence policy (CSDP). As with anything else, the common **defence in cyber space is only as strong as the weakest chain among the 27 member states.** European-wide networks, financial institutions, supply chains or other systems can be corrupted through the weakest link, and that might undermine the integrity of the other 26 member states as well – as it happened with NotPetya's infamous attack on the Ukrainian tax application, spreading all over the world.[14] The long favoured border between military and civilian affairs gets again blurred by cyber security and defence.

III. Individual digital autonomy and the state

Populism and crypto-anarchic movements have more in common than suspected at first. Populism is anti-elitist, anti-intellectual and anti-pluralist at its core, aimed at mainstream state administration, mainstream parties or institutions. The birth of the internet has nurtured a generation of online anti-state coders and programmers: the internet culture had inherently been very anarchic – which is also a reason for the lack of security layers in the original design of protocols stemming from the late 80s early 90s. This sentiment of anarchism is also concentrating on avoiding hierarchy, state control and dominance of given actors. This is very visible from the core structure of the protocol design and other instances of community-based decision making, which is very prevalent among the developers of internet protocols, as in the common language of computer networks building up the global internet.

[13] https://ethicsinaction.ieee.org/
[14] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Direct democracy or anarchy?

New online monopolies – social media companies, service and cloud providers, online shops – and crypto-currency developers share – at least partially - similar aims with populists: anti-elitism of populism translates into anti-hiearchy sentiments on behalf of the crypto-anarchists; anti-pluralism to legitimize dominance in political communication for the populists, while it is more genuinely driving bottom-up and peer-to-peer discussions among crypto-anarchists. **What is common in both approach is the drive for a life less dependent on a central (nation-)state**, albeit with very different motivations. [15] Bitcoin is the signature story - with all other crypto currencies - for rendering citizen life independent from financial intra- and interstate institutions and also from fiat currency. Populists use the mainstream political institutions to achieve their goals – electoral policy – while crypto-movements and supporters of the free and open internet are actually building up a parallel virtual structure to existing ones. The threat for the democratic processes – involving transparency, accountability and liability on the levels of social groups – are similar from both directions.

Curiously, the wish to avoid a self-reliant governing elite is shared among these three otherwise very different groups: monopolies, populists and crypto-anarchists. **In their world, third parties are omitted at each possible instance**: smart contracts might render obsolete many of the public notary's services, blockchain-based real estate registers are already running, cryptocurrencies – in their current status of underregulation – might be real alternatives to savings or instant payments as well. Monopolies at the digital advertisement market held by Facebook and Google drove out of play most of the actors, capturing not only incomes but also restructuring online public places, which lived from local advertisers previously.[16] it seems that the current president of the United States opted for Twitter to *directly* reach his voters instead of relying on the media as *intermediary*. Populists – technically speaking – also occupy the intermediary layer between political governance and the people, which is the administration (public service).

Evolution of the State

While in the Euro-Atlantic area the state has survived the intensive phase of globalization that followed the end of the Cold War, **the reconstruction of state responsibilities is underway**. Necessarily, if the state is responsible for the safety and

[15] See e.g. Jan-Werner Müller, What Is Populism? Penguin, 2017; Bartek Pytlas, Radical right politics in East and West: Distinctive yet equivalent, *Sociology Compass*, **12**, 11, 2018; Menno Fenger, The social policy agendas of populist radical right parties in comparative perspective, *Journal of International and Comparative Social Policy*, **34**, 3, pp. 188-209, 2018.

[16] **„How Google and Facebook Have Taken Over the Digital Ad Industry”** http://fortune.com/2017/01/04/google-facebook-ad-industry/ or **Google and Facebook Killed Free Media** https://www.bloomberg.com/opinion/articles/2016-08-09/google-and-facebook-killed-free-media-with-ad-domination (both accessed on 17.12.2018.)

security of its citizens, it must be also provide the same guarantees in cyber space. In other words, if cyber space is taken as a domain of war, then the relationship between state and citizen might get extended into cyber space as well, making the European push for the direct applicability of international norms in the cyber space all the more pertinent.

Historically, the state-citizen relationship has been varying in forms and content. Core state functions have been transforming since the inception of the state itself. How much social caring, health services or education are provided by the central state still varies in the Euro-Atlantic area. However, the monopoly of power is the constant of state authority. This is exactly where the state got challenged in the cyber space: how much can it enforce its will? Protect its citizens and infrastructure?

Necessarily, **if smaller states are not able to perform this crucial task themselves, they must cooperate**[17] for their survival. This seems to be the case for the Visegrad countries, even Poland. Naturally, all these countries have their CERTs[18] installed and running a growing apparatus of cyber security. However, the more serious challenges are yet to come, and as much as we wish to link our energy infrastructure, such as gas pipelines through the natural gas pipeline interconnectors into a North-South corridor through Central-Europe, from Polish shores to the Croatian Krk, we also need to pool resources, education and human resources in the domain of cyber security.

The most important **transformation of the social contract is taking place right now**. This might be as crucial as the one around the industrial revolutionary waves in the 19th century. One may remember that our current democratic institutions were very much shaped during that period, when social groups were reformulated, and the role of the public space shifted dramatically.[19] Though there are plenty of signs of the current radical shift – from the cyber-attacks on the 2016 presidential elections to the ongoing hybrid war in Ukraine – the political path-dependencies and the zenith of the regime-changing generation currently being played out in the CEE countries are both overshadowing the significance of the present-day adjustments.

However, there seems to be no doubt that the next generation of Visegrad and European politicians will be from among the digital natives. They will – according to this paper's hypothesis – rewrite the social contract, **pledging allegiance to those parts of the sovereign structure which are capable to provide them and their constituents with the necessary level of protection**. New leaders will serve the new generations in less than 10-15 years, when major parts of voting groups will be demanding more security in the cyber space. Presumably, depending on future

[17] As the International Relations theories litterature would use: „Bandwagon" – so in this case, create alliances around the issue for enhancing the survival chance of smaller states.

[18] Computer Emergency Response Team

[19] Jürgen Habermas, Strukturwandel der **öffentlichkeit**, Suhrkamp, 1962; Ronald Inglehart, The Renaissance of Political Culture in *American Political Science Review, 82*(4), pp. 1203-1230, 1988; Iversen, T., & Soskice, D., Distribution and Redistribution: The Shadow of the Nineteenth Century in *World Politics, 61*(3), pp. 438-486, 2009.

incidents, the continuation of hybrid warfare and simply the growing personal exposure to cyber space will keep the issue high on the citizen's agenda.

If nation state structures are not capable to grasp voters support by offering to uphold both level of digital autonomy, individuals will look for other players to deliver. This is already happening by contracting multinational corporations with cyber security tasks –be it a public procurement or a purchase of security software by a single user. If more and more corporations deliver – for instance through offering health services for their employees,[20] assure cyber security of complete countries, trace cyber attacks related to incidents touching political parties[21] – the state-citizen relationship will also suffer the consequences. **The state can easily take back the initiative by stepping up regulation, forcing guarantees for its citizens**.

The European – and especially East- and Central European – experience of totalitarianism in the 20th century is a memento that **guarantees at individual level must be included in the intra- and international system of cyber security** parallel to the development of offensive capabilities. Time is crucial as once these processes get separated and guarantees would lag behind, the temptation would increase for any country, politician or party to abuse the system.

[20] „Amazon, Berkshire Hathaway and JPMorgan Team Up to Try to Disrupt Health Care" https://www.nytimes.com/2018/01/30/technology/amazon-berkshire-hathaway-jpmorgan-health-care.html

[21] „Republicans hired the same cybersecurity firm as the hacked DNC, but it's not clear that was a bad idea" https://www.washingtonexaminer.com/news/white-house/republicans-hired-the-same-cybersecurity-firm-as-the-hacked-dnc-but-its-not-clear-that-was-a-bad-idea

Co-funded by the
Europe for Citizens Programme
of the European Union