EUROPEUM
INSTITUT PRO EVROPSKOU POLITIKU
INSTITUTE FOR EUROPEAN POLICY

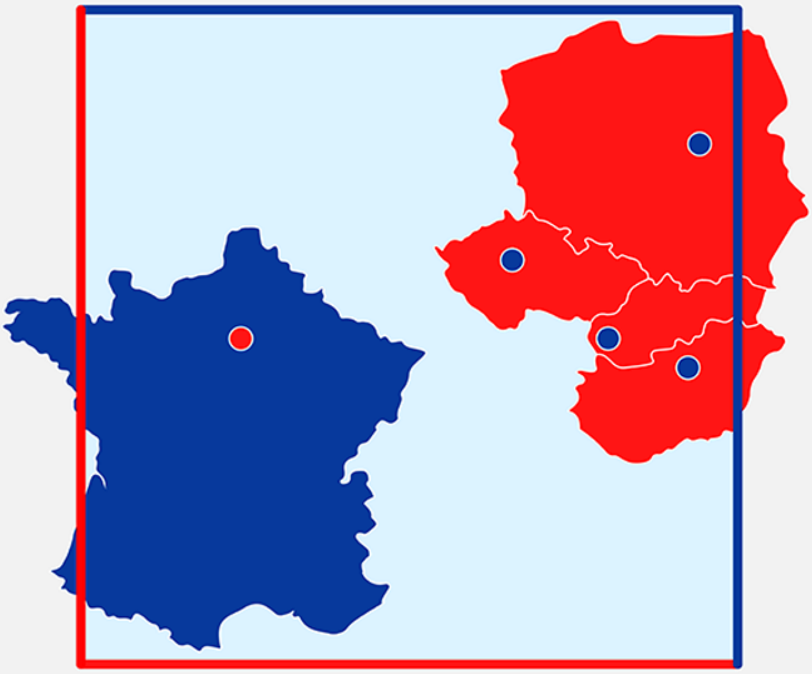
Visegrad Fund

POLICY PAPER

V4-France cooperation in the cyber space

Botond Feledy

- **The cyber space has started to engulf most aspects of our daily life. All the machines around us – cars, computers, intelligent light bulbs, watches – are communicating with us and with each other over the cyber space. Electronic waves are carrying the overwhelming majority of information at our disposal. Most supply chains of corporations depend heavily – at least in some phases – on the internet, on GPS-like systems, and on electronic communication.**



The global context

The military has long understood the significance of this development, hence why cyber defence has taken off decades ago. Similar developments in the civilian realm followed later. The true breakthrough came with the introduction of social media, which attracted a completely new and large circle of netizens (online users). Smartphones and applications permeate our life for the last decade and the trend is not changing, rather accelerating.

Cyber criminals as much as foreign governments have all well understood the window of opportunity. It is less risky, less costly to make money through cyber crime acts than in many conventional crime domains. The same is true for hostile state interference. The plausible deniability makes it comfortable for states to turn to abuse in the cyber space. The challenges of attribution – that it remains technically difficult still to prove with certainty where a certain cyber attack originates from – are making the diplomatic world, the intelligence communities and militaries uneasy, and forcing the state actors to rethink classical measures of deterrence, pre-emptive strike, proportionality and the likes.

While NATO supports the cyber build-up of its member states, the EU is trying to cover the commercial aspects through its digital single market initiative, as well as the citizen aspect through data protection and privacy requirements.

The context in the European Union

The European Commission has stepped up its efforts to drive dialogue and legislation targeting the cyber space. Since the introduction of the 2013 EU Cyber Strategy[1], the NIS[2], GDPR[3] and eIDAS[4], - among other cyber crime related pieces of legislation[5] - have been accepted and put in motion. More ambitiously, the objective of the EU block was translated into becoming a digital safe heaven in the 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**

[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

[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)

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]

The context of the V4-France cooperation potential

The Visegrad countries as well as France are sharing the same cyber space with all other nation states, corporations, private individuals. The **present study aims to identify those challenges in the cyber space that might require sub-EU level cooperation**: where it would be rational to start a joint effort of the five member states of the Visegrad four and France.

This is not the typical case as most efforts are done either on a national basis or at the European Union level, and of course at the international fora. Hence, practical use cases of the V4+1 co-operation might entail either 1) preparations for implementations of commonly accepted EU regulations, 2) enhancement and speed up of EU-decision making in the future 3) as well as some points of joint opinion for ongoing discussions in front of different instances of international organizations, like the United Nations Group of Government Experts on the stability of the cyber space.

In the following the paper will share propositions under five different titles. The structure will follow the **four-layer description of the cyber space** proposed by many, among others Alexander Klimburg.

1) The hardware or physical layer

2) The coding or core of software layer

3) the data layer

4) the social layer involving the information space and the human agency among others.

The paper will consider the holistic options that are either indirectly related to cyber space (but directly to cyber security) or which clearly requires action in more layers at once. At first however, we will take a look at the five states and their attitude towards cyber security.

Differing environments. Same political will?

The **preparedness is very diverse** among the five analysed countries, even the prioritisation of cyber security is not the same. While France is a leading force in legislation, military and civilian cyber operations and is home to global corporate players, the Slovak Republic and Hungary are somewhat lagging behind the Czech Republic and Poland which have invested important political capital – and hence financial resources – into the cyber domain.

The **perception of the cyber threat** is also touching on distinctive sensitivities in each of the countries. France, which endured attacks during the last wave of terrorism in Europe, with its global military operations earning enemies from far abroad must have a global understanding of cyber threats, especially with known cases of high-level incidents happened like the attack on the television broadcaster TV5 – later attributed to Russia-related Advanced Persistent Threat (APT28) group. Prague and Warsaw have also made public some of the cases, like the hacking of the Czech Ministry of Foreign Affairs email accounts, or different attacks against government and even private entities in the financial realm in Poland. Meanwhile, the governments in Budapest and Bratislava are rather reluctant to talk about incidents, eventhough the presence of APT groups has officially been confirmed, but not the potential damage caused by them.

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

The Czech Republic was one of the first among all EU nations to officially shed light on its **offensive capacities**, while France and Poland are also developing their own cyber weapons. France has a dedicated cyber command which was tasked with defining its doctrine of the use of cyber capabilities in support of military operations[8]. Possessing such tools is one thing, but it is quite another to kick off a public debate about it, let alone an impact assessment as a milestone of a parliamentary process which would aim to bring the offensive cyber measures under detailed legislative regime. Of course one should not doubt that internal regulations exist for a long time as rules of engagement on the side of the military, as well as for cases of cyber crime and other specific threat fields such as terrorism.

All of these countries are at **different stages of streamlining cyber security policies and public decision-making** and of sharing government competencies related to actions in the cyber space. While the military and most notably the military intelligence have been using cyber tools for decades (information security, network security etc.), the digitalisation of the civilian life came around quite quickly in the last two decades, putting significant pressure on the respective national legislations to cope with the challenges.

- While in Slovakia, the Ministry of Finance was originally in charge, in the Czech Republic, the Ministry of Interior was responsible before the creation of the NUKIB (National Cyber and Information Security Agency) with quite substantial powers; in Poland, the former PM Beata Szydlo introduced cyber security to the prime minister’s office. Finally, in contrast, in Hungary the domain was passed around from the Ministry of Justice and Public Administration to the Ministry of Interior in 2014, and the National Cyber Security Institute has not acquired competences comparable to the NUKIB.

Holistic solutions: Cyber security in top-down approach

It is clear that cyber security has grown up to be the other most important horizontal policy challenge of the 21th century beside climate change. Hence, it is tantamount to remind ourselves that for a successful implementation of any basic cyber security principle, we need to apply a holistic approach and quit the silo-bound thinking.

- At the most recent European Cyber Security Forum (held in Brussels on 20th February 2019 by the Kosciusko Institute) the idea was put forward of how important it is to recognize the responsibility of the state for the cyber security of its citizens. Without a doubt, the cooperation between governments, corporations and academia remains unavoidable, but nevertheless states have to cope with their increased role in the cyber space, regardless of their current willingness or hesitation, due to the exposure of their citizens and national businesses, not to mention basic national security. In the coming years, we will witness **more and more public services related to cyber security**: from standardization to monitoring through certified clouds, competition friendly online marketplaces etc. There will also be instances of the cyber space where regulation – through enforcement by state sponsored actors – will fight for preventing abuses by monopolistic behaviour, to guarantee national and European security interests and to safeguard the data of European entities and citizens. A new era of competition between global regions for dominance over parts of the cyber space has long been underway and rages on today.
- France is a leading force in this endeavour, bringing different proposals to EU level about the taxation of the GAFA (Google-Amazon-Facebook-

[8] https://www.lemonde.fr/international/article/2018/05/15/l-armee-francaise-va-etablir-sa-doctrine-cyber-offensive_5299374_3210.html

Apple), which the V4 has supported, and was first to impose a GDPR-related fine on one of these players. It has also been proven that smaller states are also important in maintaining the European unity (or trying to achieve it), as Poland and the Czech Republic have been active regarding the stance on Huawei's participation in 5G infrastructure or as much as Austria (and its competition office) started serious investigation into the practices of Amazon. These are all **possible points of interactions for executive authorities and monitoring forces** to co-operate and to get inspiration about best practice from another member state. This would be all very much meaningful in the V4-France context as well.

- **Positions for future EU negotiations** might also be co-ordinated. This might happen earlier than the late diplomatic (COREPER) stage, but rather in their infancy, by local experts and representatives of public administrations from the field with operational experience. As we are progressing towards regulatory sandbox solutions in many user cases, **the V4-France co-operation could handpick few domains where another sandbox could be jointly created**. It would be in line with the EU-level intentions to discover options of how a state could correlate local tax payments with state-offered cyber security support. For example on how to measure corporate activity in a national cyber space and to make correlate tax payments, how to measure online traffic on social media sites or on advertisement servers of global corporations, how to filter information or bots of hostile actors etc.
- The **NIS directive requires that national authorities monitor the critical infrastructure of the country**; in Poland, the requirement is to conduct this monitoring every two years. Of course, such checks on the operators of critical infrastructure are the exclusive competence of the member state, but however **a co-operation would be highly recommended** and conceivable: even if only one observer is present from another member state, this would much help to avoid blind spots, bring new ideas and help to link field agents. Most probably, such a co-operation needs years to be built, with the usual confidence building measures, from meetings to finally engagement on the field. While such co-operations are still rare among the Visegrad members themselves, France has been practicing close co-operations with allied countries in the most different domains, hence the very practical know-how may be welcomed in such a V4-France collaboration.
- The same is true for public administration leaders and **elected politicians**. In other instances, joint or interparliamentary committees exist and regular meetings of committees of national parliaments take place. Cyber security is usually not figuring among the issues. Given the model of previous cooperations, this should be implemented for cyber-related decision makers. However, one must highlight that it should not become one more international event for the MFAs or the international task force of the national level CERTs, but rather much more **an effort to expose those who are not yet involved in supranational cyber security exchanges**. For some, this might come down simply as an awareness raising event – and it is critically needed for MPs or municipalities for example. At some other cases, local directors of public procurement, heads of public IT bodies or owners of datasets should be also brought in, up to school directors and the like.
- **A dedicated Group** of Government Experts at the United Nations has been dealing with the cyber space for quite some years, to no avail. It was expected that dominant powers will hardly come to a quick consensus, but actors from the Euroatlantic space should strengthen the common positions where they exist. **France is an important player and could help to bring in more support from the V4 countries**. It could mean a very simple series of workshops for national experts coming from V4 countries to train

them in the state of the art negotiations, that would also mean more contacts between government experts. A sub-EU level cooperation could be a perfect opportunity to expand the reach out of global negotiations at UN level.

- **The posture of EU member states in the cyber space will shift again once the United Kingdom leaves the bloc**. Although it remains a committed NATO ally, in the cyber space, the UK might become less dependent on the Continent, while the rest of the 27 member states might use this opportunity to develop further their ecosystem in parallel to the Anglo-Saxon world. In other words, Britain has always been the bridge to and the eye of the United States in many aspects, and this time the intelligence communities might have a chance to reshape continental cooperation, just as much as PESCO and other defence related initiatives have offered fresh air and a new momentum when the UK decided to leave. France, the only nuclear power of the EU in the future, might lead the military presence of the EU militaries in the cyber space, and using this window to jump to a different level of collaboration than in the conventional military domains. This would be in stark contrast with the highly secretive attitudes of national armies, but cyber defence is again a piece of space where European joint efforts are a must and not an option. On the medium term, from the repository of vulnerabilities (and their due reporting back to developers) to the human resources of cyber enabled work force, cooperation shall be elevated to the community level. Any pilot program between France and V4 on this territory would break ice for other EU member states as well.
- This evolution has been slowed down recently. While the European Commission has been proposing avenues for cooperation, member states are seemingly more than ever feeling empowered to take back ownership of cyber security. The example of the Competence Centers – proposed by the European Commission – being brought (back) to the national level without mandatory measures of cooperation, or the quite shallow toolbox of EU cyber diplomacy, is telling. The return to the national level might have been a good first step ten years ago, but right now EU members should rather use it as an opportunity: the less path-dependency national cyber administrations have, the easier to harmonize or integrate it on EU level, which does not mean of course that national capabilities shall not be reinforced and built up. To put it differently, the lack of necessary harmonization is risking to drive the EU member states to a fragmented landscape where future efforts might be more difficult to push through.

As far as our discussions with experts from the industry allowed to understand and disclose, the redefinition of “cyber defence” in France led to difficulties for French companies. As the term of defence is understood more broadly now than before, French companies have met stricter requirements about disclosure, dual goods and all those measures that we usually associate with suppliers of military. While clearly the cyber domain and especially cyber security is full of connections to military dal use goods, it is a different model than that of Estonia which is bringing cyber to the civilian space. The discussion of corporate-state relationship and experience from France could be very informative for Visegrad countries which are still early in the development of their cyber military-industrial complex.

Hardware level

It has been repeated at most forums on cyber security **how crucial the reforms of public procurement are**. We are talking about multiple aspects: standardization, certification, security by design and its monitoring, and the awareness of member state local public administrative bodies which are otherwise running critical infrastructure like water facilities or other providers of critical infrastructure. It could prove useful to hold discussions about a horizontal understanding of the security side of public procurements in the cyber space, from Internet of Things (IoT) to softwares, from skill certificates to more and more standardized ISOs and regular curriculum in higher education.

- The Huawei-case is turning out to be a game changer and an excellent test for necessary and timely unity of EU member states. It is also a multivectorial puzzle for the decision makers, between the pressure to build 5G networks, the lobbying of the White House to exclude the Chinese from the market, and the East-West division of handling Chinese influence/investments (it is also critical to point out the lack of European alternatives for providers of 5G infrastructure systems). All this adds up to a subtle challenge and to some strong exchanges between diplomatic bodies all around European capitals, depending on their stance towards Beijing.

Software and coding

The new Multiannual Financial Framework for 2021-27 will most probably deliver on expectations about innovation and the digital economy. However, it is a major challenge for member states to share and allocate resources. Having taken a look at digital hubs in the USA or other developed economies, it is quite clear that it is far from easy for a city to gather the critical mass, and some capitals in Europe are far more behind in cyber industries than others. If France – since the mediatized issue of the EU directive on posted workers – was looking for a domain where cooperation with the Visegrad countries could be demonstrated, the cyber security industry is large enough. While Visegrad countries could benefit from **building up a joint competence center / research hub with a well defined specialization**, the French industry could enlarge its presence in these Central European member states and actually gain more financial support from future EU funds through knowledge transfers to these countries. How to make French corporate actors interested in bringing development to the V4? The MFF might provide the necessary sources and legal inspiration for such moves, to try to spread more evenly the future innovation support from the common EU budget.

Data warehouses

It is an evidence in 2019 that data is constantly exploited for the better – or for worse. AI developers, big data firms and all kind of other IT ventures need large data sets to run, test and start products. This is far from easy in the GDPR environment, while our Chinese and US competitors are in many ways better positioned when it comes to data pooling.

More data warehouses of EU member states could be created for specific domains, in our case, in domains that are interest for French multinationals as well as their V4 outlets. Veolia, EDF, Sodexo, to name just a few, are present on many V4 markets and produce end-user data in large amounts. Their accessibility in an anonymized form – and simply the willingness of these companies to share their data with selected start-ups or multinational research teams, under strict conditions – could bolster innovation.

One must reckon that it is challenging to incentivize companies to share data, as much as it remains still difficult to put the burden of mandatory incident reporting on operators and providers of critical infrastructure. But once we are talking about critical infrastructure, a standardized anonymous data set from more EU member states could help the work of research hubs. The France-V4 cooperation with a frontrunner multinational company willing to show transparency and interest in using its data set, could prove to be a model to follow.

Social layer

This thick layer of the cyber space is the one that is the most talked about. Debates about information operations, news filtering and fake news, influence campaigns in the social media are by today common wisdom. There are plenty of opportunities to look at the national experience of regulatory efforts. France was one of those countries where Facebook introduced the flagging of fake news as a user option, and any future project together with Facebook would be easier to be carried out by a France-V4 joint project than the V4 alone.

Certain ideas are related to all layers, but still remain a very specific domain for cooperation. One such **critical issue is cyber insurance**. Some of the largest companies in Europe – and US owned companies running business inside the EU – are pushing to develop the cyber insurance market. It is still much behind the US market in numbers, and regulations are needed. Again, one cannot truly tackle cyber insurance alone. If a critical infrastructure operator wants insurance, a monitoring system needs to be place to see whether the company is fulfilling its cybersecurity obligations, which could mean certain security for the insurer. In parallel, insurance companies will definitely need to invest in educating their clients and raising cyber awareness in order to increase their client basis. This could - and should - be joined with public efforts.

- **Liability questions** abound wherever we look at: commercial drones being hijacked: how to prove the hijacking, who is responsible, and if liability stands at all? Let's suppose that the hijacked drone falls on a moving vehicle, causing a road accident. Who pays the bill? The manufacturer certainly should own a security certificate, hence later on the operator would be in the position to prove that all patches and generally expected security measures were up and running. How to prove it once the drone itself is destroyed? Shall we oblige all drone operators to connect to a protected cloud system where live fly and maintenance data are stored? Or perhaps even a footage of all flights shall be kept for 5 days or 6 months, like with some public CCTV camera records or telecommunications metadata?

- Let us recall that Mondelez, a food company fallen victim of the WannaCry attack, has sued its insurance company in Switzerland, which in turn tried to exempt itself from its payment obligations by citing that the attack occurred on behalf of a state actor in a war like situation which is not covered by the insurance policy. So where should cyber insurance end, given the mass presence of state-sponsored hostile actors in the cyber space?

Finally, we must mention the distributed ledger technology and blockchains. This is again a huge area of research, encompassing cryptocurrencies, any sort of (health or financial) information validation or just a simple and modern cadastre of real estates. Smart contracts are coming, the enforcement of which will be significantly different from today's state centered procedures.

The **French-V4 cooperation might pick up on one of the cutting-edge fields of blockchains and create a common research group**, most hopefully in a Contractual Public-Private Partnership format, with participation from the private and public sector. The new "Horizon" programme might open plenty of financial possibilities for such cooperation, and CEE research centres might still have open capacities to host such ventures.

PISM POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

CEID
CENTRE FOR EURO-ATLANTIC INTEGRATION AND DEMOCRACY

UNIVERSITAS COMENIANA BRATISLAVENSIS FACULTAS PHILOSOPHICA MCMXIX

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

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.