BIZTPOL AFFAIRS

APRIL – AUGUST 2017

VOLUME 5. NUMBER 2.

CORVINUS
KÜLÜGYI ÉS KULTURÁLIS EGYESÜLET

CORVINUS SOCIETY FOR FOREIGN AFFAIRS AND CULTURE

corvinusculture.com

BIZTPOL AFFAIRS

Vol. 5. No. 2.

APRIL – AUGUST 2017

BUDAPEST

Corvinus Society for Foreign Affairs and Culture

2017

ISSN 2064-3152

Published by: Corvinus Society for Foreign Affairs and Culture,

1223 Budapest, Húr u. 9/A.

ESSAY

V4 DEFENCE COOPERATION IN LIGHT OF THE DIFFERING THREAT PERCEPTION

WOLFORD ZSÓFIA

ABSTRACT

The cooperation of the Visegrad Group (V4) traces back to the regime changes in the region after the fall of the Soviet Union at the beginning of the 1990s. Until 2004, the regional cooperation of the V4 was driven by the group's aim to join the North Atlantic Treaty Organization (NATO) and the European Union (EU). Since their accession however, cooperation was lagging behind due to lack of joint concern and vision. Nevertheless, due to the annexation of Crimea and the migration crisis, discourse on the cooperation was brought back to life, however, this time it is not driven by a common political project but by the endeavour to represent the interest of the V4 against Western European member states.

INTRODUCTION

The cooperation of the Visegrad Group (V4), Poland, the Czech Republic, Hungary and Slovakia traces back to the regime changes in the region after the fall of the Soviet Union at the beginning of the 1990s. Until 2004, the regional cooperation of the V4 was driven by the group's aim to join the North Atlantic Treaty Organization (NATO) and the European Union (EU). Since their accession however, cooperation was lagging behind due to lack of joint concern and vision. Nevertheless, due to the annexation of Crimea and the migration crisis, discourse on the cooperation was brought back to life, however, this time it is not driven by a common political project but by the endeavour to represent the interest of the V4 against Western European member states of the EU whose opinion greatly differs from current "hot topic" of European security discourse, i.e. migration. Considering the differing threat perceptions of the V4 countries, a cooperation built on their joint stance against other EU countries on the issue of migration will not last long nor will it evolve into an institutionalized cooperation despite the current rhetoric that intends to flaunt a strong V4. In this essay, I first present a brief theoretical background to regionality and security communities, then, I provide an overview of the past cooperation in light of the introduced theories. Finally, I will draw conclusions regarding the (im)possibilities of the V4 security cooperation, claiming that

REGIONAL SECURITY COMPLEX AND SECURITY COMMUNITY THEORIES IN THE CONTEXT OF THE VISEGRAD GROUP

For analysing the possible scope of cooperation between the Visegrad countries, a constructivist approach will be used along with the theories of regional security complexes (RSCs) and security communities. I apply the constructivist theory to analyse the V4 (non-)cooperation because both realism and liberalism has failed to give answers to the lack of common security policy in the region as they both presuppose that geographical vicinity and joint membership in both the NATO and EU would result in a cooperative security policy.

According to the realist idea, international actors have fixed identities and interest based on their geographical location which predestines them to a static regional interaction. They „tend to define regions on the basis of geography because of the assumption that proximity generates common interests that derive from a common culture, economic circumstances, and security concerns. But individuals can organize and define themselves based on markers that are not necessarily tied to space, suggesting something of an "imagined region," or a "cognitive region."[1] The English school of liberalism focuses on "how states construct institutions to encourage cooperation and to further their mutual interest in survival, respectively"[2], however it cannot account for the lack of common security policy within the semi-institution V4 states. Constructivism, on the other hand, may provide an explanation for the volatile nature of the V4 cooperation, since it takes into consideration material, social and normative factors too.

The concept of security communities originates from Karl Deutsch's idea on pluralistic security communities. According to him, security communities are composed of states that share the same values and ideas making conflict unlikely between them. Deutsch's idea was elaborated on later in details in the works of Emanuel Adler and Michael Barnett, thus becoming an important part of the mainstream literature of international relations. The purpose of Adler and Barnett was to refine security policy analysis, which, according to them, was focusing solely on two levels of analysis, i.e. global and national, thus leading to insufficient or inappropriate answers.

When using the method of analysis developed by Buzan and Waever, one has to differentiate between the discourse and practice related to the region and the individual security discourse and practices of member states of the RSC, the latter being the subject of analysis. In this essay, instead of studying the discourse of the region which is the Euro-Atlantic in this regard, the security discourse and practices of the Visegrad countries will be closely looked at. In the framework of the proposed analysis, security policy will be examined on four levels: the domestic security discourse and threat perceptions of member states, relations between the constituting states and that to the neighbouring regions, and the role of great powers in the RSC.

In order to refine the analysis, the concept of insulator[3] also has to be introduced. The term denotes a country or countries that are situated between two regional complexes: the V4 after the fall of communism could be considered as insulators, since they did not become members of another security community instantly, it took around a decade for them to integrate. After their accession in 1999 and in 2004 to the North Atlantic Treaty Organization[4] and to the European Union respectively, their roles and identities has changed differently, and

they are constantly changing even nowadays. Some countries are returning to the role of an insulator: for instance, Hungary introduced its Eastern Opening Strategy aiming for closer economic ties with Eastern regions parallel to a foreign policy that instead of enhancing Euro-Atlantic integration, aims to maintain a "balanced relations with the major powers that define of our region, including the United States, Russia, Germany, China and Turkey"[5], suggesting that the country now serves as a bridge between formerly two distinct security complexes.

As insulators, during their early years of membership the V4 countries could take up the role of a mediator, and were able and willing to lobby for establishing closer relations with both their Eastern neighbours such as Georgia and Ukraine and with the Western Balkans through the Eastern Partnership and the European Neighbourhood Policy. Nowadays, however, it can be observed that the V4 currently does not have a common mission, as it would be expected both from scholars and practitioners of security policy. They "Historical hatreds and friendships, as well as specific issues that trigger conflict or cooperation, take part in the formation of an overall constellation of fears, threats, and friendships that define an RSC."[6]

The Visegrad cooperation has started as a political project with the aim to help each other in the process of EU and NATO integration. Initial endeavours of integration were successful because the Visegrad countries were aspiring for political and economic integration to the liberal democracies in Western Europe and the importance of security policy was negligible at that time, the V4 articulated only the return of communism as a security threat[7]. It is important to note, that at the time of the V4 joining the EU and NATO, the two group of states both focused primarily on political and economic cooperation, while they

articulated distinct security concerns: while it was communism that was considered a security issue by the V4, EU member states started cooperating in order to prevent the return of "EU's past"[8] (which may be the reason for not having a common European army yet, the lack of shared fear from one external actor).

The fear from a possible war in Europe was reassured by the Yugoslav war, which further enhanced the integrational endeavours of the previous communist bloc. Thus, the security policy of the Visegrad Group cannot be examined independently from NATO and the EU since no matter how different the current threat perceptions of V4 states are, their security policy is confined to their membership to the two organizations.

REGIONAL SECURITY SUB-COMPLEXES WITHIN THE V4

Due to the great number of states belonging to the Euro-Atlantic security community and due to its great territorial extension, it is both extremely hard and futile to try to define one regional security complex to which the whole community belongs. In the Euro-Atlantic security community, states face security threats either on the borders of the regional security complex to which they belong or threats rooted in other security complexes but projected by the greater powers of the security community, like the United States, the United Kingdom or Germany. Thus, it is useful to define the term of sub-complex too, which "represents distinctive patterns of security interdependence that are nonetheless caught up in a wider pattern that defines the RSC as a whole."[9] The V4 may be part of a tightly-coupled security

community, but the four countries are securitizing different threats, and their defence and security policies are highly polarized, since they belong to different regional security sub-complexes at the same time.

For instance, Poland plays with the global league instead of the regional one (as distinguished by Buzan and Waever[10]) due to the country's size, thus having a threat perception which differs from that of other V4 countries. During the Yugoslav wars, all V4 were affected, except for Poland because it did not share borders with the conflicted area, and it belonged to another regional security sub-complex than the rest of the Visegrad group. Instead of securitizing the Western-Balkan, Poland has been focusing on EU's Eastern neighbours, especially to the threat posed by the Russian Federation's aggressive power politics in the past years. As the Polish Minister of Defence stated, Poland now focuses also on deterrence besides defence[11]. As a result, a territorial defence force was established, and security cooperation with Western allies were enhanced: a new German-Polish brigade was formed as a reaction to the annexation of Crimea, indicating that some V4 states are entering into closer security cooperation with their Western-European allies despite the adversarial rhetoric of the Polish political leadership. Poland also joined the multinational Saber Junction[12] exercise along with Germany and many other states in 2017, however, Hungary and the Czech Republic did not take part in it.

It is also important to note that Poland has always put more emphasis on V4 security cooperation in its programmes for the Polish Visegrad presidency[13] than other Visegrad countries. In 2000/2001, Slovakia's NATO accession was supported, in 2004/2005 they entered into cooperation with Austria in fighting political extremism in the region. In the same year, the Polish presidency also elaborated on the

importance of the Eastern Neighbourhood Policy and energy security. Then in 2008/2009, they lobbied for the integration of Ukraine, Georgia, and for closer cooperation with the Caucasus. In 2012-2013, emphasis was put on the establishment of the *Visegrad Battlegroup*, on *Pooling and Sharing* and *Smart Defence*. Nevertheless, during the latest Polish presidency starting last year, a shift could be perceived in a sense that in the program, Poland is taking a firm stance for the representation of V4 with regard to EU's future, and demands a greater role in tackling the Union's challenges[14]. It emphasizes the importance of V4's "strong voice" in the Union and the common heritage of Visegrad, with less focus on security cooperation with the Euro-Atlantic community in the program. This trend is also continued during the current Hungarian presidency which will be detailed below.

On the contrary to Poland, Hungary was greatly preoccupied by the Yugoslav wars in the 1990s: the country even allowed NATO aircrafts to use its airspace during the air campaign in spring 1999. Even nowadays, the Western Balkan bears a great importance with regard to Hungarian security policy due to its long border with it and to the Hungarian minorities living in Serbia. The importance of Southeast European stability was always a priority in Hungary's V4 programs along with the Eastern Neighbourhood Policy, however the active support of the latter one seems to sink into oblivion since the war in Ukraine has started. Also, maintaining troops in the Middle East and increasing capacity within NATO KFOR TACRES BN (Tactical Reserve Battalion) suggest a continued, permanent role in the Balkan rather than on the Eastern flank of NATO. However, Hungary is also taking part in other projects too on an ad-hoc basis. For instance, Hungary performed a Baltic Air Policing mission in 2015 (note that

Poland and the Czech Republic has been contributing to the mission since 2006 and 2009), it is planning to participate in the Trident Juncture NATO exercise in 2018. Notably, Hungary contributes to the work of the NATO Cooperative Cyber Defence Centre of Excellence along with all other members of the Visegrad Group.

Contrary to the offset of Bundeswehr-V4 cooperation, Hungary has proposed a national level security policy for the next decade, aspiring to outrun other V4 members in security spending and modernization within the framework of the so-called Zrínyi2026 plan, indicating that Hungary considers the rest of the V4 as its rivals rather than as possible actors for deepening defence cooperation.

Regarding the Zrínyi2026 plan on military force reform, István Simicskó, the defence minister of Hungary pointed out the main objectives: the improvement of the country's air defence capabilities, increasing spending and the size of the military reserve force, and promoting "national defence education" too. Enhancing V4 or EU level defence cooperation and interoperability was not mentioned with regard to the reform until now (however, the strategy is not public).

As opposed to the Poland's and Hungary's alienation from the Euro-Atlantic community, the Czechs have entered into military cooperation with Germany this year via the Framework Nations Concept by delegating one rapid deployment brigade to the German army, clearly signalling its position with regard to the recent fallout between the EU and the Visegrad Group despite the typically pro-Russian and Eurosceptic public opinion and rhetoric in the Czech Republic. Security cooperation with Western-Europe is beneficial for the Czech Republic also because of its export-oriented arms-industry.

During the Czech V4 presidencies, the emphasis was usually on deepening Visegrad cooperation, promoting democracy, enhancing regional communication, and also on the project of tackling extremism together with Austria. The Czech presidency was outstandingly effective during 2015/2016, because it addressed one of today's greater security issues: cyber security. The Czechs founded the Central European Cyber Security Platform (CECSP) with the help of Austria already in 2013, and the Visegrad Group Military Educational Platform (VIGMILEP), thus achieving a greater level of institutionalization of the V4 cooperation.

Along with the Czech Republic, Slovakia was also focusing on integrational issues when they were presiding the V4, as opposed to Hungary or Poland. Despite possessing a military industry, Slovakia has the lowest defence spending with regard to NATO in the V4 region. Also, their activity on security policy issues is much lower than other states'. This is also indicated by the fact that they withdrew their forces from KFOR in 2014, and the largest size of Slovak troops are stationing in Cyprus under the flagship of the UN. Also, they are quite reluctant in delegating military capabilities to the EU Battlegroups: since its establishment, Slovakia delegated forces only twice to the Battlegroup: once in the framework of the Czech-Slovak Battlegroup in 2009 and within the Visegrad Battlegroup in 2016. This indicates that Slovakia usually takes a more passive role within the V4 than other states, however, it is not reluctant to cooperate when the framework for it is provided.

Their reluctance regarding NATO and V4 is also manifested in the public opinion: according to a survey conducted last year, almost half of Slovaks would support an exit from NATO[15], and one of the opposition parties, Kotleba (People's Party – Our Slovakia) that is

gaining more and more support, has already started collecting signatures for holding a referendum on exit from NATO. This trend seemingly affects V4 cooperation besides Slovakia's disputes with Hungary regarding minority rights.

Current State of the V4 Security Cooperation and its Prospects

The regions to where each state delegates their greatest military power indicate the discrepancy between the states' threat perceptions. The largest Hungarian contingent is stationed in Kosovo, followed by the troops to Bosnia Herzegovina, and Afghanistan was only the third in the line until troops were withdrawn. The Czechs delegate the majority of their military force to the Resolute Support Mission in Afghanistan, the Polish army also has its greatest presence in the Middle East: they were the commander of the Multinational Division Central-South until 2008 (Iraq). And finally, Slovakia delegates its army primarily to Cyprus suggesting a low level of engagement with both NATO and with the security community of the region. Nevertheless, the 2016 deployment of the V4 Battlegroup is a significant achievement in the defence cooperation of the region which has been planned since 2011, originally with the contribution of Ukraine, but as the Euro-Atlantic community gave up on the country's integration, the Battlegroup was formed without Ukraine.

Military cooperation in the fields of research and development, education and training, and modernisation are also considered a long awaited progress of V4 which were adopted in the Long Term Vision of the Visegrad Countries on Deepening Their Defence Cooperation[16]

in 2014. Nevertheless, enhanced defence cooperation cannot be achieved without interoperability, which could be facilitated by joint procurements or by the joint development of capabilities, for which Poland just introduced the Regional Security Assistance Program[17], however the extent of V4 countries' extent of contribution is still to be announced. Despite the significant military industry the region had in the 20th century, no harmonization or re-establishment of the industry took place in the framework of the Visegrad cooperation on one hand due to the competition within the sector between member states, and on the other hand, due to the lack of a joint vision on security and defence projects. A coordinated armament industry in the region would significantly boost the V4's role on EU level, and member states could benefit greatly from the cost-effectiveness of joint procurements in which they are also lagging behind despite the fact that these objectives have been clearly articulated in almost every presidential program of the Visegrad Group since the early 2000s.

The V4 could not find a platform for concise joint military or security cooperation before 2014 since NATO missions took place primarily far away where Visegrad had no direct interest to intervene – due to their geographic distance – other than to take its fair share within the organization. At this point, it is important to note that the lack of V4 security cooperation cannot be blamed solely on member states that are reluctant to realize the impact of a possible cooperation, but it also stems from the nature of their wider security community.

On one hand, the European Union also lacks joint military capabilities and cooperation along with a common foreign policy which would serve as an incentive and framework for a deeper cooperation in the future. On the other hand, in the past decade NATO conducted primarily out-of-area missions, the support of which was not a question for Visegrad

countries despite that those security threats were not securitized in V4 countries due to significant geographical distance, but, delegating military power for these missions served primarily the purpose of showing solidarity with other NATO member states and allegiance to the alliance.

CONCLUSION

Considering that after decades of occupation by the Soviet Union and after a (more or less) parallel accession procedure to both the EU and NATO, one might think that the security policies of the four countries are driven by the same ideas, thus cooperation between them is self-evident. On a more theoretical level, it would be convenient to apply the idea of regionalism to the Visegrad Group, which denotes –as Joseph S. Nye put it – "a limited number of states linked by a geographical relationship and by a degree of mutual interdependence".[18] Nevertheless, despite the common historical and cultural background, there seems to be no Visegrad group, only a Visegrad project with occasional short-term joint projects.

Indeed, in the case of the Visegrad countries, there are several factors that could encourage their cooperation. Three out of the four are quite small countries, thus they can never have a decisive role in the international anarchy, however, by cooperating with each other their political capital could be increased significantly. The V4 has already realized it when aiming to join the Euro-Atlantic community. Since their accession, however, cooperation only existed on a rhetorical level.

As new threats are emerging over time, more closely to the V4, the lack of joint security policy is more conspicuous despite the current

political leaderships' efforts to signal the image on a unified and potent cooperation. As both NATO and the EU are focusing more and more on the region's collective security instead of out-of-area missions, greater cooperation will be needed between member states, if they want to establish a permanent V4 cooperation. Nevertheless, cooperation in different fields of security will be possible only if member states agree at least on the nature of security threats.

[1] Adler E., (1997). Imagined (Security) Communities: Cognitive Regions in International Relations. *Millennium,* 26(2).
[2] Adler E., Barnett M. (1998). Security communities in theoretical perspective. In: Adler E., Barnett M. (eds.), *Security Communities*. Cambridge: Cambridge University Press. p. 11.
[3] „Defines a location occupied by one or more units where larger regional security dynamics stand back to back" In B. Buzan & O. Waever, (2003). *Regions and Powers: The Structure of International Security*. Cambridge: Cambridge University Press. p. 41.
[4] Note: Slovakia joined NATO only in 2004.
[5]Press conference of the Hungarian Minister of Foreign Affairs and Trade on Hungary's foreign policy: http://www.kormany.hu/en/ministry-of-foreign-affairs-and-trade/news/this-year-the-goal-of-hungarian-foreign-policy-will-continue-to-be-the-representation-of-hungarian-interests Accessed: 09/24/2017
[6] B. Buzan & O. Waever, (2003). *Regions and Powers: The Structure of International Security*. Cambridge: Cambridge University Press. p. 50.
[7] History of the Visegrad Group: http://www.visegradgroup.eu/about/history Accessed 07/24/2017.
[8] B. Buzan & O. Waever, (2003). *Regions and Powers: The Structure of International Security*. Cambridge: Cambridge University Press. p. 353.
[9] Ibid. p. 51.
[10] Ibid. p. 14.
[11] The Defense Concept of the Republic of Poland, p. 6.: http://en.mon.gov.pl/p/pliki/dokumenty/rozne/2017/07/korp_web_13_06_2017.pdf Accessed 24/07/2017
[12] Saber Junction Exercise: http://www.eur.army.mil/SaberJunction/ Accessed: 07/24/2017
[13] See: Stepper Péter Visegrad cooperation beyond the Polish and during the Hungarian V4 Presidency, *Foreign Policy Review* (10) 93-107 (2017) and Stepper Péter: Consistently Inconsistent: The sinusoidal V4 Presidency struggles to find areas of cooperation which will unite the region's priorities Visegrad Insight, 2017/06/20.
[14] Programme of the Polish Presidency of the Visegrad Group, 1 July 2016 - 30 June 2017: http://www.visegradgroup.eu/documents/presidency-programs Accessed 09/24/2017
[15] https://spectator.sme.sk/c/20266421/poll-almost-a-half-of-slovaks-would-welcome-neutrality.html Accessed 09/24/2017
[16] http://www.visegradgroup.eu/calendar/2014-03-14-ltv Accessed 09/19/2017.
[17] https://www.defensenews.com/2015/10/04/poland-launches-effort-to-help-arm-e-european-allies/ Accessed: 09/24/2017
[18] J. S. Nye, (1968). *International Regionalism: Readings*. Boston: Little Brown. p. vii.

COMMENTARY

THE CZECH PERSPECTIVE TOWARDS THE DEFENCE COOPERATION OF VISEGRAD COUNTRIES

Vendula Penciková

Abstract

From my point of view, defence policy is of huge importance in recent times, regarding mostly issues like the migration crisis and terrorism. Unfortunately, it might be said that some countries do not feel threatened and their defence budget is not increasing. Of course, it is not only the question of threats that makes questions of defence cooperation important, there are other significant indicators pointing to this direction. Visegrad countries share a very similar background and this should be conspicuous in their defence cooperation.

INTRODUCTION

The similar historical background is the reason why the Visegrad Group was created. During the past years, there has been a debate whether Visegrad Group is still „alive" or it is dropping off. However, threats we are facing nowadays had awakened the members of the Visegrad Group and its importance is rising again. The level of this so-called awakening, though, is not the same across the member states.

Another question to be asked is how Visegrad countries cooperate with the West and the East. In my point of view, we can divide Visegrad countries into two groups. The first group includes the Czech Republic and Poland, the countries that are not leaning towards the East, mostly because of the historical background. The situation in the Czech Republic is really confusing, however. Czech foreign policy is, namely, rather vague and we can see different spheres of interests that are showing up in media across Europe. On the other hand, there is Slovakia and Hungary, which are, in my point of view, quite positive towards the East, especially Russia.

This is one of the reasons why different approaches towards defence policy are present in the Visegrad Group. Visegrad countries declare that these different visions should not mean a problem when discussing defence policy. In my opinion, however, this question is a taboo, something that should not come to the fore.

This brings me to the second part of my essay. The GDP 2% commitment to NATO is something that not each member country is willing to meet. This commitment is essential for determining how each country is dealing with its defence budget and its defence spending in particular. As we can see in Graph 1, only Poland's

defence expenditures are rising significantly – in fact, Poland is one of the five NATO member countries which are able to meet the 2% criterion. The main reason for this is the above-mentioned aggressive

Million US dollars

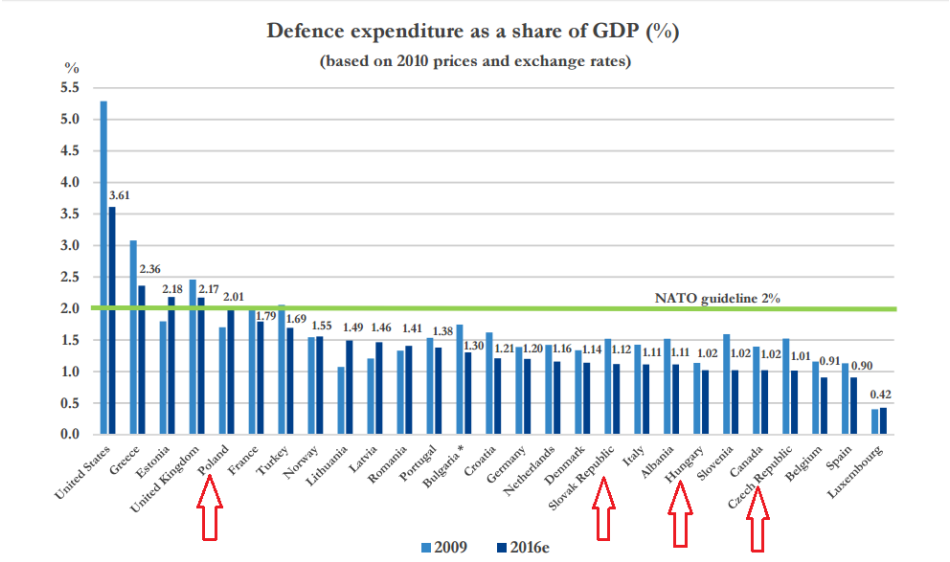
	2009	2010	2011	2012	2013	2014	2015	2016e
Current prices and exchange rates								
NATO Europe	**282,240**	**274,592**	**281,683**	**263,654**	**269,441**	**270,269**	**235,305**	**241,842**
Albania	183	186	197	183	180	178	132	133
Belgium	5,623	5,245	5,500	5,169	5,264	5,192	4,218	4,332
Bulgaria *	905	832	758	722	811	747	633	673
Croatia	1,014	920	996	865	850	805	669	611
Czech Republic	3,129	2,660	2,437	2,185	2,148	1,975	1,921	1,958
Denmark	4,337	4,504	4,518	4,423	4,216	4,056	3,364	3,521
Estonia	353	332	389	437	480	513	469	503
France	54,442	51,971	53,441	50,245	52,317	52,006	43,473	44,222
Germany	47,469	46,255	48,140	46,470	45,932	46,102	39,812	41,676
Greece	10,156	7,902	6,858	5,633	5,310	5,226	4,647	4,606
Hungary	1,476	1,351	1,472	1,322	1,280	1,210	1,131	1,258
Italy	30,486	28,656	30,223	26,468	26,658	24,448	19,566	22,146
Latvia	315	251	286	248	281	293	281	405
Lithuania	401	326	344	324	355	427	471	638
Luxembourg	202	248	232	214	234	253	249	248
Netherlands	12,131	11,220	11,339	10,365	10,226	10,332	8,668	9,127
Norway	6,196	6,499	7,232	7,143	7,407	7,336	5,815	6,068
Poland	7,475	8,493	9,106	8,710	9,007	10,104	10,596	12,706
Portugal	3,740	3,540	3,652	3,040	3,262	3,003	2,635	2,817
Romania	2,225	2,086	2,380	2,100	2,452	2,692	2,580	2,651
Slovak Republic	1,350	1,138	1,065	1,020	968	997	986	1,006
Slovenia	799	772	666	543	507	486	401	448
Spain	16,943	14,743	13,984	13,912	12,607	12,614	11,090	11,200
Turkey	12,647	14,134	13,616	13,895	14,427	13,583	11,957	12,097
United Kingdom	58,240	60,329	62,852	58,016	62,263	65,690	59,538	56,790

Graph 1. Defence expenditures by the European members of NATO. Source: NATO Public Diplomacy Division. Defence Expenditure of NATO Countries (2009-2016). URL: http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_03/20170313_170313-pr2017-045.pdf. Accessed: March 24, 2017.

foreign policy of Russia, regarding to annexation of Crimea. The other reason is Poland's quick economic growth. Czech expenditures are rising really slowly, not to mention the case of Slovakia, where defence spendings are the lowest in the region. In these latter countries, people do not perceive threats like, for example, Poland does.

The Czech Republic is not touched by the migration crisis and we are too small to be on the map of terrorism. This leads to the perception of some kind of an untouchable state. The other problem is that we rely on the West very extensively. The fact is that the influence of the United States in Europe is decreasing, and with the new American president, Donald Trump, we cannot be sure what is going to happen

because his politics is rather vague. Some might argue what he said in the presidential campaign will never become reality. Let's hope for that. On the other hand, our economy is doing really well recently and this should be the sign of our will to pay the 2% commitment by the year 2020. Slovakia has the same goal, but its economy is not developing as significantly as ours. In Graph 2, you can see how NATO members are dealing with their commitments.



Graph 2. NATO expenditures by country. Source: NATO Public Diplomacy Division. Defence Expenditure of NATO Countries (2009-2016). URL: http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_03/20170313_170313-pr2017-045.pdf. Accessed: March 24, 2017.

Regarding the problems discussed, my suggested improvements of defence cooperation are as follows. Firstly the Visegrad countries should share communication and information. This is essential to prevent terrorism not only within Visegrad countries, but also across Europe. Communication strategy should exist within the NATO countries as well. We can see the same effort in the Dublin system that is focused on migrants and their visas. Another improvement should

concern the military equipment of Visegrad countries. Military equipment should be modernised and shared in a certain way. Of course, this question is a touchy one regarding the size of the Visegrad Group. Also, for some Visegrad countries this is more expensive than for the others. Common training programmes should also be introduced for the soldiers not only from Visegrad countries, but also from other NATO countries. The final improvement that I suggest is to deepen the cooperation with V4+ countries, mainly Austria and Slovenia. We should share ideas of innovations as well as create common battlegroups.

As a conclusion, I would like to state that the Visegrad Group itself has the potential to cooperate on defence policy. On the other hand, there are many complications that lead to misunderstandings and overreactions that are visible.

ESSAY

CITIZENS' CYBERSECURITY IN THE VISEGRAD GROUP

ALEKSANDRA SAMONEK

ABSTRACT

In the programme of the Slovak presidency in the V4 Group from 2014 we find the following desiderata related to enhancing the growth of V4's digital economy: the Slovak Presidency focuses on protecting human rights and fundamental freedoms in connection with the use of information and communication infrastructure in order to harmonize the approaches taken by V4 countries.[1] This paper will present the legislative and political examples which stand to show that none of the desiderata has been properly pursued since 2014 by the Slovak presidency, or made up for by the Czech (2015 – 2016) and Polish (2017 – 2018) presidencies in the Visegrad Group.

INTRODUCTION

In the programme of the Slovak presidency in the Visegrad Group „Dynamic Visegrad for Europe and beyond" from 2014 we find the following desiderata related (although perhaps indirectly) to enhancing the growth of V4's digital economy:

1. the Slovak Presidency focuses on protecting human rights and fundamental freedoms in connection with the use of information and communication infrastructure (including the Internet), and
2. completing mutual consultations in order to harmonize the approaches taken by V4 countries.[2]

I will present the legislative and political examples which stand to show that none of the desiderata has been properly pursued since 2014 by the Slovak presidency, or made up for by the Czech (2015 – 2016) and Polish (2017 – 2018) presidencies in the Visegrad Group. In order to see this argument clearly, we shall

1. inspect the nature of protecting human rights and fundamental freedoms related to information and communication technology at the state level (section 2) and then
2. establish the means necessary to foster effective cooperation concerning such protection internationally within the Visegrad Group (section 3).

In parallel I will conduct an analysis of the progress made so far by the V4 countries in ensuring that human rights and fundamental freedoms are guarded in the domain of information and communication infrastructure, especially mobile and digital. The following conclusions shall shed new light on the stake of the V4

countries cooperation and coordination and their role in maintaining the rule of law and state's respect for democracy in the Visegrad Group.

The issue raised here becomes even more pressing in the perspective of recent V4 Cybersecurity Conference, which was held on March 7 2017 at the Google Office in Washington, DC by the Embassy of the Republic of Poland and at which the issue of protecting human rights and fundamental freedoms was not raised at all, but neglected in favour of the start-up presentations and discussions about the future of US-EU cooperation in business.[3]

This contribution aims to renew the interest declared by the Slovak presidency in 2014 and recommend the steps to be undertaken in the future, possibly even during the Hungarian presidency in the years 2017 – 2018. My main thesis is that

1. in its core the citizens' right to privacy of digital and mobile communication and information is not dependent on the discussion between the proponents and opponents of liberal policies, and
2. because this independence is not widely acknowledged among the EU politicians, the standing of national governments on liberal policies is an obstacle for cooperation on the EU-V4 axis and so
3. the international assembly of the V4 members is the only viable platform capable of facilitating the debate about protecting the citizens' right to privacy of digital and mobile communication in the V4 countries.

STATE-LEVEL PROTECTION OF HUMAN RIGHTS RELATED TO INFORMATION AND COMMUNICATION

We can only discuss the protection of human rights and fundamental freedoms in the V4 countries after introducing the following division: on one hand we consider the protection of the rights of citizens (either of the given state, or V4, or the EU in general), on the other we extend this protection to the foreigners, usually defined as non-EU citizens. This division may strike us as counterintuitive, because it would seem that human rights protection should benefit whoever qualifies as a human. The practice, however, especially in the domain of digital and mobile technology forces us to confront a rather different situation.

All V4 countries share a particularly defensive attitude towards the foreigners, be it the refugees coming from the Middle East or just foreign students who legalized their stay in order to pursue higher education. The distrust that V4 countries display towards the EU and the non-EU actors (with the exception of business allies like the US) has been on the rise recently and even though V4 countries lost their blocking minority in the European Council in 2014, the strong wave of illiberalism and the belief in the existence of various extra-national threats spreads from V4 and influences countries like Romania and Bulgaria[4]. And so it would be rather naive to ask of the V4 countries to invest significant resources into protecting the foreigners, even if the protection relates to rights and freedoms guaranteed by the European Convention on Human Rights (ECHR). Nevertheless one could still hope that the restrictions and violations of human rights which are inflicted on the foreigners should not harm V4 countries'

citizens. As we shall see, upon careful analysis of legislation and mass surveillance data, this hope quickly disappears.

DATA PROTECTION AND MASS SURVEILLANCE IN THE V4

From the perspective of the state, citizens only need to be protected against other citizens, corporate or institutional actors or foreign intelligence. The usual meaning of the expression "citizen's right to privacy" corresponds to state's obligation to provide necessary means of protection against the above mentioned third parties. In line with this description, V4 countries are well-equipped in institutions dedicated to pursuing this type of privacy protection, generally referred to as DPAs (Data Protection Authorities).

In Poland the Inspector General for Personal Data Protection (GIODO) is responsible for supervising the compliance of data processing with the provisions on the protection of personal data, initiating the steps necessary to improve the protection of personal data, issuing administrative decisions and considering complaints with respect to the enforcement of the provisions on the protection of personal data, based on the provisions of the Act of 29 August 1997 on the Protection of Personal Data[5]. The Office for Personal Data Protection in the Czech Republic was created to supervise the fulfilment of the legal obligations laid down for processing of personal data, maintain the register of notified data processing operations, deal with initiatives and complaints from citizens concerning breach of law (mostly concerning the commercial sector), based on Act No. 101/2000

Coll. of April 4, 2000, on the Protection of Personal Data and on Amendment to Some Acts[6].

Similar responsibilities are covered by the Office for Personal Data Protection of the Slovak Republic.[7] Seemingly none of the institutions mentioned above undertakes any activities aimed at protecting the citizens from the mass surveillance conducted by the state, either legally or illegally. The very topic of preventing illegal mass surveillance or educating the citizens about their rights to privacy was not brought up during the meeting of the DPAs of the V4 counties which took place on March 23 2017[8]. Among the V4 DPAs, the only one declaring its extended competence in the state sector is the Hungarian National Authority for Data Protection and Freedom of Information.[9] Its operation is regulated by Act CXII of 11 July 2011, on Informational Self-determination and Freedom of Information. The Hungarian Act CXII is more comprehensive than data protection acts of other V4 counties and covers protecting personal data, data in the public interest and data made public on the grounds of being in the public interest. The DPAs of the other V4 countries also boast some involvement in the state sector, but only to the extent of controlling mass databases created and maintained by the organs of the public administration for the sake of public service (healthcare, education system *etc.)* and everything that is tagged as the matter or state security or public interest remains outside the scope of their competence. Therefore in practice preventing illegitimate surveillance by the state in all V4 counties, including Hungary, remains the domain of the national and constitutional courts, and citizen initiatives, but not of the DPAs.

THE CASE STUDY OF POLAND

For a long time after the fall of communism in Central Europe the citizens of the V4 countries have taken their right to privacy for granted. Since the new governments had no apparent agenda to spy on their citizens, who would we invest resources and lobby for protection of our privacy? Under the Polish law for example, the first and last place where the right to privacy is mentioned is Article 47 of the Constitution. It is not at all clear in the legal doctrine that the right to privacy is a standalone right at all, as every time one needs to refer to their right to privacy under the Polish law, they need to use it via proxy of article 23 of the Civil Code and refer privacy to the more general right to maintain personal dignity and good name for oneself. But what if mass surveillance does not harm our good name, because the results of surveillance are never made public? Does it take away our dignity to be spied on if we do not know what is happening? Both questions need to be taken up every time we face the need to exert citizen's right to privacy under the Polish law. To make matters worse, on the wave of retreat from liberalism, in 2016 Poland has adopted an act known the *Antiterrorist Act.*[10] Under the laws contained in this act, the government is entitled, among other things, to seize the belongings or real estate of a citizen, or conduct surveillance in their workplace or home without answering to any independent institution, whenever the government sees fit for the sake of public safety. The motivation of the government, however, is not in any way controlled by the public, does not demand justification and does not involve informing the citizen about what exactly is going on and whether the operations of the government are appropriate to the threat. In many

cases, so far mostly involving the foreigners who are being successively expelled from Poland, it becomes more and more evident that the threat is purely fictional, conjured up for the purposes of abusing the antiterrorist laws. The Antiterrorist Act does not confine the list of potential threats to foreigners. It is not clear who and for what reason may become a threat to the public safety. In 2016 and early 2017 the Polish police took up on publishing and pursuing the non-violent protesters who gathered in front of the Polish parliament at the night of December 16-17 2016. Although the demonstration in front of the Parliament gathered to peacefully support the protest conducted by the opposition inside the election chambers, the people who were photographed participating in it were wanted for what was described as "breaking the law", even though no particular article was ever mentioned. The images showing the faces of some of the protesters are still available now in the police public database.[11] As the main economy in the region, Poland created a terrifying example likely to spread to other members of the Visegrad Group and provided a preliminary display of a dystopian future of the whole EU.

The recent events in Poland allow the hypothesis that without outside support Polish citizens do not stand a chance against the government even in cases which ought to be – and without any controversy – resolved in their favour in a democratic state. In the absence of anti-surveillance laws, potent data protection authority and with only a stub of a civil society, the Polish have no tools to counter the hostile government policies. The rule of law is being gradually eliminated from the Polish political order and in many ways it hangs on privacy and public safety. How can one prevent further negative changes in political systems like the Polish? Due to the current hostile political relations between the government of Poland and the European

Commission, it seems unbelievable that intervention from the EU authorities would bring any effect. But one can still uphold the case that human rights should not be reserved for the enthusiasts of liberal politics. In this essay I aim to offer a perspective in which the right to privacy in its basic dimension is neutral in the liberalism – anti-liberalism debate. The failure to acknowledge this neutrality results in political isolation of countries which embrace new liberal policies and those who avoid or reject them. This in turn makes the cooperation among all the EU countries impossible. But since V4 countries share the propensity to adopt increasingly illiberal politics, intensive international cooperation within the V4 might be the last chance to salvage whatever is left from the right to privacy of their citizens.

CITIZEN'S RIGHT TO PRIVACY OF MOBILE AND DIGITAL COMMUNICATION

Let us now examine the ethical and legal basis for protecting citizen's right to privacy of mobile and digital communication and information. We shall refer this right to the problem of maintaining public order and ensuring public safety, in particular:

1. protecting the citizens from attacks on their life and well-being (including the threat to the functioning of the public institutions insofar it makes citizens' situation financially or practically more difficult), and
2. protecting the members of government administration or the public institutions from the citizens or protecting the national

budget from spending which will not bring immediate economic returns.

PRIVACY LAWS VS THE RIGHT TO PRIVACY

One of the key arguments in the debate over the right to privacy in general is that of existence or absence of certain privacy rights. The common perception overestimates how well-established and protected is our right to privacy. The ECHR mentions the right to privacy in Article 8 as ensuring respect for one's family life and their private life, and for their home and correspondence. There is no reason to suspect that mobile and digital communication could be excluded from under Article 8 of the ECHR. Restricting the right to privacy is allowed under ECHR only *in accordance with the law necessary in a democratic society*. Respective national constitutions cover the right to privacy either directly (like in Poland) or indirectly, as for example the Constitution of the United States of America, where the right to privacy is derived from the 4th Amendment, *i.e.* the right to be secure at home and in person, safe from unjustified searches and seizures. More often than not the right to privacy is assumed, seen as a given in countries considered modern democracies. But how does one go to protect the right the protection of which is not strongly embodied in legal acts, not accompanied by effective, affordable and available procedures of executing one's right in the situation of the right violation? The DPAs fill the gap in those cases which do not involve the leverage of public safety, terrorism and conflict of interest between the citizen and the state. Their role boils down to protecting us against abuse by the commercial actors and fellow citizens. No matter how well DPAs fulfil their roles in this respect, their work will not be

enough to ensure the full protection of our right to privacy, especially the right related to mobile and digital communication and information. In other words, the DPAs cannot protect us from the governments.

A sensible question to ask at this point is the following: does the lack of privacy rights (or the lack of their proper implementation) entail the lack of the right to privacy? To follow up on the Polish example, does the lack of protective laws indicate that Polish citizens do not have the right to privacy of mobile and digital communication as long as it involved their relationship to the state itself? Of course not. However, one may immediately ask the reverse question: what does it mean when the state does not provide privacy laws to cover the existing right to privacy of its citizens? Such state would be ignoring its most basic responsibility and so its representatives should be held responsible. Again, using the Polish case study described above, one could immediately ask: do legal acts like the Antiterrorist Act count as the law abiding by the order of a democratic society when no apparent threat is present? The answer again must be negative.

And so we conclude that the lack of privacy laws is not an indication of the lack of the right to privacy, but rather a sign of the governmental failure, either deliberate or incidental, to do justice by the state's most basic responsibility, namely to protect the human rights and fundamental freedoms related to mobile and digital communication and information of its citizens.

HOW IS PRIVACY RELATED TO DIGITAL COMMUNICATION AND INFORMATION?

Before the age of digital and mobile communication, the right to privacy has been a subject of a heated debate in almost any legal system. Most agreed that privacy was among the most fundamental values of a modern society and was worth protection at all costs. For this reason, the right to privacy found its way into the ECHR and more than 120 national constitutions. As our communication and information storing evolved, we lost sight of how privacy relates to modern technology. As a result, the main arguments for protecting privacy of digital communication and information and also for limiting or even giving it up altogether are, at least at face value, the same as they used to be when the debate on the right to privacy was originally initiated. In the following paragraphs we devote some attention to the most commonly used arguments in this debate and examine how they relate to digital communication and information in the state-related context.

Arguments supporting the right to privacy of digital communication and information include the following claims:

1. Given that the right to privacy of digital communication and information is just the instance of a more general right to privacy, there exists a privacy law (or a bundle of privacy laws) 7/18 which constitutes the right to privacy in a given legal system. Therefore, one has the right to privacy of digital communication and information. We shall refer to this claim as the statutory law argument.
2. Protecting the right to privacy is the only way to protect various private affairs and interests of an individual which should be of no interest to the state and which do not in themselves pose threat to public safety. This includes the behaviours and methods of conduct

which are not ethically uncontroversial, but which are not a crime (*e. g.* some torts which formally do break the law, but in no way constitute a victim, like walking on the red light when no cars are in view). Such private affairs and interests are needed to make human life meaningful and satisfactory. Therefore, one must protect the right to privacy, including the privacy of communication and information. We shall call this claim the freedom of an individual argument.

3. It becomes more and more evident that – with enough information at hand – the state can easily override any citizen initiatives and gain control (even total control) over the living conditions and possibilities available to the citizens. The standard of a rule of law is lost and the perspective of regaining control over the authorities becomes fictional. One must protect the democratic state of law and this means protecting the right to privacy, which naturally extends to privacy of digital communication and information. Therefore, one must protect the right to privacy, including its digital aspect. This argument shall be recalled as the rule of law argument.

First, let us deal with the statutory law argument. In the light of the above remarks on the relationship of the privacy laws and the right to privacy, one must discard this argument immediately. This does not mean of course that the premise of the argument is false. Indeed, when the right to privacy of an individual is violated, one searches for an appropriate privacy law. The situation becomes increasingly hard if the legal system is not equipped in appropriate laws, as the citizen cannot execute the protection over the right which they nevertheless have, as every human right serves every person from the moment of birth throughout their lifetime. This is a scenario in which the legal system does not protect what it should be protecting and very often it

is not possible for a private person to overcome a pathology of this sort. However, as we have established already, the lack of the privacy rights does not mean that there is no right to privacy, as laws ought to naturally follow the rights and not the other way round, they are a mere expression of the fact that a certain right exists and is available to anyone. Why then do we use the statutory law argument? The existence of a right evokes action and solidarity, however the existence of a law evokes a procedure. So the statutory law argument is not one for protecting privacy, but rather to start a process of executing the protection in a particular instance of the right's violation. Nevertheless, the statutory law argument points us in the right direction. Namely, the appropriate procedures of privacy protection are necessary. Otherwise, our right can be violated and we are left with no tools to prevent, reverse or stop the violation. This fact is widely recognized when it comes to the affairs within the commercial sector, but dangerously often they are ignored, underestimated or denied when the state is involved. The freedom of an individual argument is a crucial element of liberalism. However, one should acknowledge that protecting private data of an individual against the state's abuse is not the same as claiming that the value of the freedom of an individual is more than the security or wellbeing of a community. Obviously enough, the state does not equal community. As becomes more and more evident in the V4 counties like Poland, the community is always at the risk of being misunderstood or misrepresented by the government and no individual citizen should pay the price for such systematic mistakes. Of course, the debate over the right to privacy and its place in the moral and political systems which are not liberal goes much deeper. For our purposes it suffices to say that everyone, a liberal or not, has something to hide, even from the government. The

debate is mostly concerned with *what exactly* we have to hide and *what reasons* we have to keep it secret. In fact, the research conducted in the US suggests that an average person commits around three felonies a day and does so without even knowing it.[12] In absence of well-examined and thoughtfully structured protection procedures, we are all at risk of being exposed at our most vulnerable, and therefore being punished without a good reason. Finally, the rule of law argument brings us to the most crucial aspect of privacy protection in the V4 countries. Illiberal tendencies within the Visegrad Group are significantly motivated by the increasing feeling that the citizens have less and less control over their livelihood and legislature because of the fact that certain decisions are outsourced from the national to the EU level. The key part here is the citizens not having control over what is happening to their community and not that the national government loses control in favour of the EU institutions. The latter was the very idea of the EU, so how why would it come as a surprise to anyone? Even a nation which primarily resents liberalism for being naive or short-sighted has no business in supporting the government it cannot control. The rule of law, when breached, takes away the control that we as citizens have over the government. And so, even though the citizens of the V4 countries may oppose various decisions and resolutions originating from the EU-level structures, protecting the right to privacy is a key step to maintaining the leverage that the V4 citizens hold in the struggle to shape the future direction of their country, completely independently from whether the desired direction is liberal or not. We are now ready to consider arguments for restricting the right to privacy or eliminating it from certain contexts. For each of the arguments we ask the following two questions: how does this context relate to the privacy of digital and mobile

communication and information? Moreover, how do those particular arguments play out in the context of a relationship between the citizen and the state? Two arguments will be crucial to our purposes: the "nothing to hide" argument and the threat of terrorism argument. The former boils down to a claim that unless the mass surveillance or data processing uncovers some illegal conduct of a citizen, they have nothing to fear from the government. As the examples is the following section will show, this argument is simply misguided. Even if in certain cases data processing may end up uncovering some wrong doing on the side of the citizen (like in the example of emp@tia which I present later), there are numerous contexts in which this so called "rule" would be broken. We shall present an example of a digital assistance tool used by the Polish labour office to manifest the existence of situations where the citizen is denied access to assistance even though no fault on their side can be detected. A large number of others have rejected this argument, among them Adam D. Moore, author of "Privacy Rights: Moral and Legal Foundations"[13], on the basis of right's resistance to any kind of consequentialist arguments from the government and Emilio Mordini, who stressed that the experience of inability to hide details of one's life are psychologically damaging and humiliating even in a situation when one has nothing to hide.[14] The latter argument seems to be more popular among within the V4 countries. The question whether the declared threat of terrorism is real or not is outside the scope of our considerations. However, the question to ask here is this: do we really need to trade our human rights for security? There is no well-documented case in which massive surveillance of digital communication resulted in preventing any terrorist attack and not just in V4, but in *any* country. Considering the immense benefits such documented case would bring

to the state operations, it is reasonable to suspect that the two problems, massive surveillance and terrorism prevention, are actually unrelated. As of now terrorists are being profiled and tracked using leads from informants or based on the connection with another person who was already uncovered to be a threat to public security. With this perspective in mind, allowing the government to use mass surveillance, including mass data processing, immediately invokes the already described rule of law argument.

How is privacy in the commercial sector related to privacy in the state-related context?

In the era of the omnipresent social networks, mobile and digital services one could think that the right to privacy should be reserved to non-digital means of communication. After all at least three generations of citizens have been conditioned to exchange their private data for various services and products offered by commercial actors like Facebook, Twitter, Ebay or Google. By deciding to use these much needed services, we lose privacy of communication, but we also gain *the means* of communication, the means of acquiring the necessary goods and finding places and contacts otherwise out of our reach. How does this situation translate into a non-digital exchange of privacy rights for services or products? Imagine for example only being able to have a house or an apartment if it is under constant and versatile surveillance conducted by someone you will never get to see or make contact with. If no alternative accommodation was available and you had no roof over your head, would you take the house? Thus we learned to bear with digital surveillance as long as it does not become too evident in our everyday life and does not interfere too much

with our use of commercial products and services. Whatever solution we find to the discussion about whether the situation of privacy rights in a commercial sector is acceptable or not, we should never regard the state and its public services as in any way similar to a private company and its commercial operations. As companies are established and operated to serve the interest of its shareholders and management and adjusted to satisfy the needs of their clients only when profits and revenue are at risk, treating the state analogously will result in allowing the public servants to use the process of income redistribution to their benefit at the cost of those who should be receiving public service and governmental financial assistance. In a democratic state of law, providing good quality of necessary public service is the most basic function of the government. Obviously, different domains of public service demand different information about the citizen. In practice we can divide the information which citizens provide to the state into the following categories:

1. the information necessary for citizen's well-being (*e. g.* address during emergency calls),
2. the information necessary for states' community's well-being (*e. g .* income declaration so that taxes are justly claimed),
3. the superfluous information which serves the agenda of strengthening or widening state's control over the citizen or abusing various categories of the national budget.

As we reject the analogy between the state and the commercial sector, we note that while we most of the time choose to swap privacy for services of a private company, no one should be forced to make this swap in case of a public service. Generally speaking in order to ensure that our rights are not violated by the state we should only be required

to share the information necessary to use the public service properly and safely, *e. g.* our address when calling for help of the fire department or the ambulance, our income when we demand a tax return. Moreover, we should have full control over how our data is processed by the state, how long it is retained in the state registers and also have some reasonably limited power to remove it from the system. Such tools are rooted deeply in modern legal systems and manifest themselves in the form of, for example, the erosion of the entry in the register of convictions (after a certain period) and public service data retention regulations supervised by the DPAs. The latter is based on requirements analogous to those laid out before the commercial actors, although the data retention time and procedures in case of the citizen-state interaction are not contractual and so there is no way for a citizen to influence or customize the period or range of such retention. One could apply either of the two perspectives present in contemporary privacy rights policies: the perspective of the citizen in need of public service, or the perspective of the state in need of information. Let us briefly consider both perspectives.

From the perspective of the citizen, only the first two types of information I mentioned *should be provided* to the government, but not type III. From the perspective of the state, however, the third type of information also benefits the functioning of the state. Citizens oppose state control as a matter of principle and naturally aim at putting constraints on the government. Sometimes the effect of such citizen initiatives can be detrimental to the public safety and national well-being. Note for example that in Poland (as in many other countries) certain matters of extreme importance are excluded from under the referendum initiated by the citizens, for example the national budget and other decisions directly concerning the sector of

public finance cannot be proposed to be made in a referendum *via* citizen's right of legislative initiative. The idea behind this restriction is based on the suspicion that citizens, if given an option to not pay taxes as all, would chose to do so without considering the consequences it would bring to the community. And so in matters of grave importance, the government takes over full control over the legislative initiative. Similar arguments are used in justifying the fact that the state keeps certain matters secret from the public for the sake of public safety. Whenever citizen's privacy is involved in cases like the ones mentioned here, it is reasonable to expect the state to disregard the citizens' right, be it privacy or freedom to vote on the desired law, simply because if the rights of state's citizens would be valued over the task at hand, it is likely that soon there would be no state to speak of. Thus we have conceived the notion of state emergency – the class of situations when the well-being of the state comes before the needs of any or all of its citizens. Ever more often the state choses to interpret the events concerning the country as a threat to public security. Consequently the presumption of state emergency becomes a principle of states' operations. From matters of utmost importance to democracy, like the Polish Antiterrorist Act mentioned above, to relatively mundane abuse of public funds, the state demands more and more information and restricts our freedoms and public service availability accordingly. Let us recall two cases described by J. Niklas.[15] The first concerns the Polish national-wide service canned emp@tia (Polish for "empathy"). The second one sums up the digital assistance tool used by Polish labour offices that is institutions providing support to the unemployed. The electronic social support registry, emp@tia, was a tool introduced in 2007 and funded from the budget reserve dedicated to helping families in need of financial

assistance. The declared motivation for creating the digital registry was to customize the support a person is receiving to better serve their individual needs. And so every person who received social support was obliged to register in the system. However, the actual use of the system was to monitor how many times each person receives help and ensure that the recipients do not double on their monthly allowance. No other customization was performed, as the information from this system was never used to justify increasing the amount of support for anyone registered, even those who lived in extreme poverty. And so, the state used public funds directed to social support to increase its control over the citizens for no additional service and with no increase in the quality of service already in operation. Information in this particular database could be counted as type III of information that citizens provide the state with. Another case concerns the digital assistance tool used by the Polish labour offices. The declared purpose of the assistance tool was to assess the chances of a person registered in the labour office at the job market and customize the office's assistance to fit their individual needs.[16] Each person was placed in one of the three categories, depending on the total points for the answers in a questionnaire. The first category included those who were likely to find a job quickly and easily, perhaps even by themselves, so mostly people who in practice could do without the assistance of a labour office, but used it to browse through the recent post openings. The second category included people who were employable, but less likely to find a job offer on current listings of open post available to a labour office. The third category included people who were "permanently away from the job market", the unemployables. One could fall into the third category surprisingly easy and based on qualification that had nothing to do with one's

availability, skill, education or qualification. For example, single middle-aged woman who had someone under her care, especially if the person was chronically ill, falls under the third category – she is unemployable. Hence the labour office will not try to help her too much. The "assistance" is intensified only for the first category of registrars, so people who do not really need assistance at all. Thus with a simple operation on personal data, the operators of Polish labor offices can maximize their success rate instead of helping the ones who need assistance the most. Both databases mentioned here were financed from the funds directed to helping the poor and the unemployed. Instead of fulfilling their task, the branches of the public administration used citizens' personal data to estimate the threat that citizens pose to the national budget, single out those who would cost the most and eliminate them from the assistance programs. They also cut off the help for those who would be too hard to help out, *i.e.* those who were in actual need of increased funding or assistance. Such unjust and illegal agenda, motivated solely by the economic factors, could not be realized if citizens' right to privacy was properly protected and its processing supervised.

How to establish coordination and cooperation in the Visegrad Group?

We have overviewed the situation of citizens' cybersecurity in the Visegrad Group. As I have shown, not much was done to increase and ensure the citizens' cybersecurity with respect to the citizen-state relations since the Slovak presidency in 2014. In particular:

1. We have seen significant examples (based on Polish political and legislative situation) of violation of human rights and fundamental freedoms in connection with the use of information and

communication infrastructure (which shows that the pursuit of the first desiderata of the Slovak presidency was not effective and upheld), and

2. approaches taken by the V4 countries are far from harmonized, as the citizens' cybersecurity with respect to the citizen-state relation still remains outside the competence of the most DPAs and is not protected in any coherent way (which shows that the undertaken harmonization efforts were undertaken, brought no noteworthy effect). Moreover, the lack of public consultations and systematic education concerning the right to privacy related to mobile and digital communication and information in the V4 countries proves that no conclusive consultations were conducted at the V4-level. Since the extra-V4 intervention concerning the problems described here is likely to be more detrimental than helpful to the protection of the right to privacy in the domain of citizen-state relations, I argued that the solutions must be pursued by the V4-level institutions. In this specific area, Visegrad must solve its own problems.

DESIDERATA FOR THE HUNGARIAN PRESIDENCY (2017 – 2018) AND BEYOND

We now proceed to propose the means of fostering effective cooperation concerning the protection of the right to privacy in the domain of citizen-state relations internationally within the Visegrad Group. I propose the following desiderata, which cover both legislative and institutional solutions and shall allow to effectively reach to a social-political understanding of how the right to privacy should be protected in cases of digital and mobile communication and information in the V4 countries.

The proposed solutions include establishing and maintaining the V4- and national-level legislative bases, procedures and means of execution related to:

1. Creating the V4 assembly of the independent institutions dedicated to protecting the right to privacy of communication and information in the domain of citizen-state relations. Accordingly, creating national institutions or offices responsible for successful implementation of the regulations and measures undertaken by the V4 assembly.
2. Extending the competence of the DPAs to include the full domain of citizen-state relations.
3. Fostering the international discussion in the public media over the problem of protecting the right to privacy of communication and information in the domain of citizen-state relations. In particular, include the continuous lifelong education on the problem itself and also the procedures available to the citizens into the program of operation of the DPAs or the V4 assembly national representatives.
4. Introducing the problem into the school curriculum ranging from the kindergarten to higher education, ensuring easy availability of information about all privacy matters relating to student's newly undertaken activities, in particular their political activity and everyday life conduct related to privacy and in the domain of state's authority.

My proposal's desired results are:

1. a shared control over the democratic procedures concerning state's interference in citizens' digital and mobile communication and the processing of citizens' information;

2. proper and unbiased risk assessment concerning cyber-terrorism and outside threats;
3. V4-level evaluation of state's policies concerning anti-terrorist laws etc. (including laws against citizens) conducted by the international assembly of independent institutions;
4. a *prima facie* agreement to involve international organizations in the V4 assembly debates when necessary;
5. continuous education of the society in the topics of cyber-security in the domain of citizen- state relations, citizens' rights in cyberspace *etc.*;
6. promoting and making available all information about the protection procedures and the status of national privacy protection laws.

4. SUMMARY AND CONCLUSIONS

We examined the political, ethical and practical bases of protecting human rights and fundamental freedoms related to information and communication technology at the state level. I provided the overview of the political situation in the V4 and the analysis of some of the recent legislation using the case study of Poland and paying special attention to the problems of mass surveillance and wrongful data processing. Subsequently, we scrutinized the arguments for and against citizen's digital privacy protection and related them to the current situation in the V4 countries. The clarification which followed the overview of the debate was to show how privacy in the commercial sector relates to privacy in the state-related context.

Then I proceeded to establish what means are necessary to foster effective cooperation concerning citizen's digital privacy protection

internationally within the Visegrad Group. The two important observation were made which shed new light on the stake of the V4 countries' cooperation and coordination and their role in maintaining the rule of law:

1. the desiderata mentioned in the programme of the Slovak presidency in the Visegrad Group „Dynamic Visegrad for Europe and beyond" from 2014 were not met, and
2. considering the current political mood of the V4 (that is the retreat from various liberal policies), V4 countries' cooperation and coordination in solving the problem of insufficient protection of the right to privacy of digital and mobile communication and information is not optional, but is rather a matter of public safety, national system stability and survival of the rule of law.

However, one must remember that there is no V4-level legislation that would protect citizens from state's abuse of their personal data (by the DPAs or else). Instead, the examples were given of "antiterrorist" and other state laws that actually hurt and disadvantage the citizens (where I used Poland as a case study). Finally, I proposed the four desiderata for the Hungarian presidency starting in 2017 and the following years. I also briefly indicated their desired results

[1] The Programme of the Slovak Presidency of the Visegrad Group, June 2014 – June 2015. „Dynamic Visegrad for Europe and Beyond", section 3. 1. 1. Information/Cyber Security, p. 12.
[2] The Programme of the Slovak Presidency of the Visegrad Group, June 2014 – June 2015. „Dynamic Visegrad for Europe and Beyond", section 3. 1. 1. Information/Cyber Security, p. 12.
[3] The programme of a V4 Cybersecurity Conference held at Google Offices in Washington DC in 2017. URL: http://we4startups.wbc.us/wp-content/uploads/2017/02/Cybersecurity-Conference-Invite-Print.pdf (web access: March 22, 2017).
[4] Illiberal central Europe. Big, bad Visegrad, The Economist, The Economist Newspaper Limited (Jan 30, 2016).
[5] The Act of 29 August 1997 on the Protection of Personal Data – Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2015 r., poz. 2135).
[6] More information can be found here: https://www.uoou.cz/en/vismo/zobraz_dok.asp?id_org=200156&id_ktg=1107&n=act-no-101-2000-coll-on-the-protection-of-personal-data (web access: 15 March 2017).
[7] More information can be found here: https://dataprotection.gov.sk/uoou/en (web access: 15 March 2017) and https://www.dataprotection.gov.sk/uoou/sites/default/files/kcfinder/files/Act_122-2013_84-2014_en.pdf (web access: 15 March 2017)
[8] More information can be found here: http://www.giodo.gov.pl/259/id_art/860/j/en (web access: 15 March 2017).
[9] More information can be found here: https://www.naih.hu/general-information.html (web access: 15 March 2017).
[10] Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych, Dz.U. 2016 poz. 904.
[11] 10 More information can be found here: policja.waw.pl (web access: 15 March 2017).
[12] Harvey A. Silverglate, Three Felonies a Day: How the Feds Target the Innocent. Encounter Books. 2011. ISBN 9781594032554.
[13] Adam D. Moore, 2010, Privacy Rights: Moral and Legal Foundations, Penn State Press, ISBN 0271036869.

[14] 13 Harvey A. Silverglate, 2011, Three Felonies a Day: How the Feds Target the Innocent, Encounter Books, ISBN 9781594032554, pp. 257-260.

[15] Jędrzej Niklas, 2015, Wolność, tolerancja i dyskryminacja w społeczeństwie nadzorowanym, w: "Granice wolności" (red. Alicja Bartuś), wyd. przez Miasto Oświęcim, ISBN: 978-83-940335-7-6.

[16] More information about the system can be found here: https://empatia.mpips.gov.pl.

***

CORVINUS SOCIETY FOR FOREIGN AFFAIRS AND CULTURE

corvinusculture.com