IESW
REPORTS

Anna Visvizi and Tomasz Stępniewski (eds)

Poland, the Czech Republic and NATO in Fragile Security Contexts

IEŚW
INSTYTUT EUROPY ŚRODKOWO-WSCHODNIEJ
INSTITUTE OF EAST-CENTRAL EUROPE

Asociace pro mezinárodní otázky
Association for International Affairs

DECEMBER 2016

IESW
REPORTS

This report was written in the framework of a project titled *Poland, the Czech Republic and NATO in Fragile Security Contexts* [Polska i Czechy w środowisku (nie)bezpieczeństwa].

Project co-financed by the Ministry of Foreign Affairs of the Republic of Poland [The Polish-Czech Forum for bringing both societies closer together, enhanced cooperation and good neighbourhood 2016, grant no: BDG-687/2016].

The content of this report reflects only the views of its authors and should not be associated with the official position of the Ministry of Foreign Affairs of the Republic of Poland.

Ministry
of Foreign Affairs
Republic of Poland

Niniejszy raport powstał w ramach projektu pt. *Polska i Czechy w środowisku (nie)bezpieczeństwa* [Poland, the Czech Republic and NATO in Fragile Security Contexts].

Projekt współfinansowany przez Ministerstwo Spraw Zagranicznych Rzeczypospolitej Polskiej [Zadanie publiczne: Forum Polsko-Czeskie na rzecz zbliżenia społeczeństw, pogłębionej współpracy i dobrego sąsiedztwa 2016, grant nr: BDG-687/2016].

Publikacja wyraża jedynie poglądy autorów i nie może być utożsamiana z oficjalnym stanowiskiem Ministerstwa Spraw Zagranicznych RP.

Rzeczpospolita Polska
Ministerstwo
Spraw Zagranicznych

To cite this report: A. Visvizi and T. Stępniewski (eds), 'Poland, the Czech Republic and NATO in Fragile Security Contexts', *IESW Reports*, December 2016, Lublin: Institute of East-Central Europe (IESW).

IESW
REPORTS

Anna Visvizi and Tomasz Stępniewski (eds)

Poland, the Czech Republic and NATO in Fragile Security Contexts

IEŚW
INSTYTUT EUROPY ŚRODKOWO-WSCHODNIEJ
INSTITUTE OF EAST-CENTRAL EUROPE

Asociace pro mezinárodní otázky
Association for International Affairs

Lublin 2016

DECEMBER 2016

Language editors and proofreading
Bartosz Czuwara and the authors

Cover design and typesetting
Amadeusz Targoński

Published and edited by

ul. Niecała 5, 20-080 Lublin
www.iesw.lublin.pl

ISBN
978-83-60695-90-6

Table of contents

Part 2

Defining the fragile security contexts 29

Part 3

Charts, figures, tables, maps:

Acknowledgments

The authors of the report wish to thank Mr. Martin Michelot, EUROPEUM, for acting as a reviewer of the initial draft of the report. A warm 'thank you' is extended as well to the participants of the expert seminar titled 'Poland, the Czech Republic, and NATO in fragile security contexts' that was held in Lublin, Poland, on 25–26 November 2016. Their feedback has been invaluable. Usual disclaimers apply.

Executive summary

The background: this report presents the outcomes of a project run jointly by the Institute of East-Central Europe (IESW) and the Association for International Affairs (AMO). The objective of this project was to examine the fragile security contexts in which Poland and the Czech Republic operate and – by inserting these findings in the context of the NATO Warsaw Summit and its follow-up – to rethink the strategy and the policy-making options open to both countries today.

The context: this report's objective of examining the security contexts in which Poland and the Czech Republic operate was driven by the recognition that dramatic shifts had taken place on NATO's eastern flank and that these had serious implications for the stability of the region. The NATO Warsaw Summit contributed to improving the Alliance's prospective capability to cope with those shifts. Nevertheless, it also confirmed that NATO members remain divided over the perception of (the sources of) threat and the required locus of their engagement.

The key points: the discussion in the report suggests that Poland and the Czech Republic face several challenges to their safety and security, whereby these can be associated with conventional-, soft- and cyber risks and threats. The report makes a case that the soft risks and threats to safety and security have acquired a prevalent status in the contemporary security contexts in which Poland and the Czech Republic operate. Nevertheless, a holistic take on the risks and threats, and by extension also on anticipating, identifying and addressing them, is needed.

The structure: this report consists of three main parts: (i) an overall assessment of the context in which the NATO Warsaw Summit was held, (ii) a detailed examination of the conventional, soft- and cyber security concerns as they apply to the cases of Poland and the Czech Republic, and (iii) conclusions and recommendations for these countries.

The methodology: in the course of research leading to the present version of this report, its authors employed largely qualitative research methods utilising primary sources, e.g. data bases and interviews, as well as secondary sources of data and information, e.g. reports, books, and journal articles. At the conceptual level, the discussion in this report was founded on the precepts of Beck's risk society theory and the resultant distinction between risks and threats to safety and security along with their policy-making implications. The major takeaway of this approach is that we can anticipate the impending risks and, by preventing them from happening, avert catastrophes.

The NATO Warsaw Summit and its provisions, so deeply linked to nearly simultaneous developments at the EU level, such as the presentation of the EU Global Strategy, constitute a very welcome shift toward improving the Alliance's capacity to anticipate, model and avert risks to safety and security in the region. Throughout the report the case is made that Poland and the Czech Republic turn these developments into their strategic and political opportunity.

Project background

Several developments in the external environment of Poland and the Czech Republic have added to a perception that the security contexts in the region have undergone a dramatic evolution over the past years and, hence, require a re-conceptualization. The euro area crisis and its social and economic implications as well as its political toll exacerbated the nascent divisions at the EU supranational and intergovernmental levels. The war in Ukraine and the annexation of Crimea, followed by the exodus of ca 1 million of Ukrainian citizens to seek work and better life in neighbouring Poland, only added to the perception of instability and imminent threat of inter-state conflict in the region. The information warfare in the Baltic states, i.e. countries particularly vulnerable to the influence of Russian propaganda, has left neither Poland nor the Czech Republic intact. On the contrary, the Kremlin-directed disinformation campaign and the direct propaganda have pushed both countries in the midst of the power struggle, effectively denying them the option to remain neutral. The twin migration and refugee crises that reached their peak in 2015 and 2016 confirmed that constructive dialogue across the EU was not to be taken as a given. In a similar vein, the Brexit referendum encouraged voices that disintegration was also an option and that the accomplishments of the Single Market may be reversible.

In this context, the terrorist attacks in Paris, the war in Syria and Russia's involvement in it added to an overall perception that the security contexts in which Poland and the Czech Republic operate are increasingly fragile. As the EU seemed to be in disarray, not least because of questionable developments concerning the energy market and the Nord Stream 2 pipeline, the strength of the very articulate message conveyed in the June 2016 EU Global Strategy was yet to be tested against its role in triggering cooperation at the EU level. The stakeholders, therefore, had great expectations vis-à-vis the NATO Warsaw Summit held on 8–9 July 2016. In a symbolic way, the Warsaw Summit seemed to have been bridging the end of the Cold War and the beginning of a new era in security worldwide. The July 2016 NATO Warsaw Summit served as a reminder and a confirmation of the righteousness and the relevance of the decision taken during the 1999 NATO Washington Summit to admit Poland, the Czech Republic and Hungary to the Alliance. From this perspective, the NATO Warsaw Summit was bound to produce important outcomes.

The objective of this project was to examine the fragile security contexts in East-Central Europe as they have evolved over the past years and to assess the implications of the NATO Warsaw Summit for improving Poland's and the Czech Republic's resilience to the mounting risks and threats to their safety and security. To this end and with the kind support of the Polish-Czech Forum of Cooperation, the Institute of East-Central Europe (IESW), the Association for International Affairs (AMO) and invited experts from other leading regional think-tanks joined their forces to examine the specificity of risks and threats that Poland and the Czech Republic are exposed to today. This report offers a detailed insight into the particulars of the security context, perceptions and prospects as seen from the perspectives of Poland and the Czech Republic following the 2016 NATO Warsaw Summit.

Understandably, the developments on NATO's eastern and southern flanks triggered a lively debate on their likely implications for East-Central Europe. This report inserts itself in this debate by focusing explicitly on the cases of Poland and the Czech Republic to assess the status quo and produce policy recommendations. These have been presented and discussed with the international experts during an expert seminar held in the IESW on 25–26 November 2016.

PART 1
An overview

1.1. The conceptual framework

Anna Visvizi

Typically, discussions on security revolve around threats to security and consequently ways of ensuring deterrence and defence capacities of a given country and/or alliance. In this context, due emphasis is given to conventional and new threats to security and corresponding measures to address these threats, usually in a re-active manner. By means of adding to the debate, this report takes a slightly different angle to examine the increasingly fragile security contexts that define East-Central Europe and those in which Poland and the Czech Republic operate. In line with this approach, rather than dwelling solely on threats to security, this report makes a case for the re-introduction of the concept of *risk* to security arguing that this seemingly trivial distinction between risk and threat has far-reaching policy implications. The following paragraphs shed the necessary light on this issue.

In the risk society theory[1], 'risk means the anticipation of catastrophe (...)'[2]. It also assumes that catastrophes may be prevented by their anticipation in the present. The

1 U. Beck, *Risk Society. Toward a New Modernity*, London: Sage, 1992.

2 U. Beck, 'Living in and Coping with World Risk Society: the Cosmopolitan turn', *Deutschlands Perspectiven*, no. 10/2012, Friedrich Ebert Stiftung, p. 4.

concept of risk, as defined in the risk society theory, offers 'an image of the world that replaces the fateful catastrophe, the *too late*, by the *exhortation to act*'[3]. In other words, the recognition of its existence and the identification of the specific risk, enable us to undertake action to prevent it from happening; rather than reacting to imminent threats that we already face. In this view, risk prompts anticipation and prevention, whereas threat requires urgent re-action.

By distinguishing between risks and threats to security, it becomes necessary to rethink the concept of security as well. Indeed, security denotes 'the absence of threat or the state of being free from danger or threat'[4]. The notion of risk is better captured by the concept of safety that denotes the 'condition of being protected from a danger, risk, or injury'. Clearly, the concepts of security and safety and inextricably linked together and offer matching, but not identical, approaches to risk and threat.[5] In the context of social and political life, 'safety' tends to be understood as 'public safety'. Interestingly, its legal definition – ascribed to the 19th century Prussian administrative courts – links it to public legal order, individual life, health and freedom, as well as the institutions of government and public goods designed to enforce public legal order.[6] In this view, at the conceptual level, safety is more apt to depict the specificity of the domestic context with its emphasis on public order, whereby security of the external context with its emphasis on defence.

Table 1: Risk and threat: definitional concerns and their policy implications

		emphasis on	measures employed	objective	policy responses	regulatory options
risk	**safety**	anticipation	pro-active	pre-empt	soft	non-intrusive
threat	**security**	identification	re-active	deter/defend	hard	intrusive

Source: Adapted from A. Visvizi, 'Safety, risk, governance and the Eurozone crisis: rethinking the conceptual merits of 'global safety governance'', in: P. Kłosińska-Dąbrowska (ed.), *Essays on Global Safety Governance: Challenges and Solutions*, Warsaw: ASPRA-JR, 2015, pp. 21–39.

3 Loc.cit.

4 Oxford Dictionaries, http://www.oxforddictionaries.com [2016-11-20].

5 This otherwise very important issue on progressive 'securitization' of policy analysis at the expense of indifference to the definitional distinctiveness of 'safety' and their policy implications was elaborated in A. Visvizi, 'Safety, risk, governance and the Eurozone crisis: rethinking the conceptual merits of 'global safety governance'', in: P. Kłosińska-Dąbrowska (ed.), *Essays on Global Safety Governance: Challenges and Solutions,* Warsaw: ASPRA-JR, 2015, pp. 29–33.

6 W. Heun, 'Risk Management by the Government and the Constitution', in: G. Duttge, S. Won Lee (eds), *The Law in the Information and Risk Society*, Göttingen: Universitätsverlag Göttingen, 2011, p. 17.

The complexity of risks and threats to safety and security increases, rendering it increasingly difficult to identify their sources and at times distinguish between the cause and the effect. In a similar manner, as risks and threats transcend state borders, the two theatres of modern warfare, i.e. the domestic and the external, are increasingly interconnected. Indeed, 'the neat dividing lines between hard and soft, civil and military security are rapidly dissolving, requiring far more flexibility and causing much confusion (…) about how to manage such complexity.'[7] Therefore, if our goal is to improve our countries' strategic resilience, it is crucial that the distinction between risk and threat, on the one hand, and safety and security, on the other hand, be taken seriously. Only in this way, will we be able to model and anticipate possible risks and prevent them and/or react to threats as they have already consolidated.

The really important point here is that through its emphasis on the domestic theatre, safety presupposes soft security means borne out of our thinking about public order. These policy means originate in the logic underpinning our policies of interior, at the most including policing. In contrast, security, with its focus on the external threats, typically presupposes harder and more intrusive policy measures, most closely associated with our defence policy and the military's involvement. Table 1 offers an insight into the implications of resorting to the distinction between risk and threat. The case of cyber security discussed in this report and the dilemmas it generates at the regulatory- and policy-making levels attest to that. It also highlights how salient it is today to consider its implications at the domestic and external frontiers. The same applies to conventional security concerns and soft security components. Taking the above into account, the big question is how feasible it is to translate this conceptual framework into our thinking about the context in which Poland and the Czech Republic operate. In other words, to what extent and how the realization that a qualitative difference between risks and threat and safety and security exist can inform the threat modelling and risk assessment techniques that we employ to improve our countries' resilience. From a different angle, to what extent and how the NATO Warsaw Summit equips us with tools and concepts necessary to do just that. This report is devoted to these issues.

[7] J. Lindley-French, 'The Revolution in security affairs: hard and soft security dynamics in the 21st century', *European Security*, vol. 13, no. 1–2, 2004, p. 1.

1.2. The NATO Warsaw Summit: the context, the symbolism, the key outcomes

Anna Visvizi, Tomasz Stępniewski, Vít Dostál

The July 2016 NATO Warsaw Summit was held in a context defined by international tension, disillusionment and a feeling of helplessness vis-à-vis the divisions emerging in Europe and adding an unwelcome spin to the developments on NATO southern and eastern flanks. Therefore, if the 2014 NATO's Wales Summit was perceived as taking place at a critical time in the Alliance's history, the atmosphere surrounding this year's Warsaw NATO Summit was filled with a sense of urgency and necessity to act. Indeed, the Warsaw Summit communiqué suggests that this year's summit may have blazed a new bold trail that will leave a lasting positive mark on NATO's deterrence and defence capacities, especially as seen from NATO's eastern flank. In this view, there was something very symbolic about the NATO Summit held in Warsaw this year reminding the NATO members that the decisions to open up the Alliance to countries of Central and Eastern Europe was admittedly one owf the key strategic directions that would define NATO's future henceforth. In the following paragraphs, the context, the poignant symbolism and the major outcomes of the NATO Warsaw Summit will be discussed to offer a cognitive lens to dwell on risks and threats to security as they unfold in the region of East-Central Europe.

The context: The 2016 NATO Warsaw Summit took place in a context defined by Russia's aggression against Ukraine and Russia's involvement in the war in Syria. Topics related to information warfare and its use as a powerful tool in the war that Kremlin wages against the West had dominated the Warsaw Summit Expert's Forum. The annexation of Crimea and the unspoken of, yet obviously present, concern about the implications of the breach of the most basic rule of public international law, i.e. inviolability of national borders, added to the atmosphere of urgency and the need of increased cohesion within NATO.

The Warsaw NATO summit was influenced by the developments that have challenged the EU's political, social and economic cohesion over the past years, thus triggering debate on disintegration as a viable alternative to the 'European project'. The euro area crisis has left a heavy toll on the societies and economies in the EU reviving arguments of differentiated integration. The political implications of the sovereign debt crisis – epitomized by the crisis in Greece – have left the EU divided at a variety of levels and dimensions of the policy-making process effectively undermining the EU's resilience to increasingly complex and nuanced risks and threats to safety and security. The migration and refugee crises have further tried the EU member-states'

resolve to act in unison, whereas the outcomes of the Brexit referendum forced the EU member-states to rethink the relevance of the European integration project and its sustainability. Terrorist attacks on the EU ground and the need to counter Da'esh and extremist violence have only added to the dramatic sequence of developments that have been tearing the EU apart.

On a positive note, the NATO Warsaw Summit nearly coincided with the publication of the EU Global Strategy (EUGS)[8], a document that opens up a long-awaited debate that might lead to a re-positioning of the EU on the global scene. The wording of the EUGS reflects a new way of thinking about the EU and its role globally and tackles issues considered difficult and/or dormant for that reason until now. Specifically, the EUGS stipulates changes in the Common Security and Defence Policy (CDSP), particularly that it essentially paves the way toward a Security and Defence Implementation Plan (SDIP). In this way, and to some extent, it speaks to the idea of the common EU army. Clearly, the EUGS sets a certain ambition that the EU has vis-à-vis the world. Importantly, it turns the EU into an active agent of effective multilateralism that – for the sake of safeguarding its values and interests – is willing to engage beyond its territory by a variety of means.

Deriving from this outward strategic orientation, an important component of the EUGS concerns the EU's relations with NATO and their prospective evolution. While the role of NATO as the primary defence framework for the majority of the EU members is emphasized, a considerable stress is placed on the EU members' contribution to the Alliance. By so doing, some light is cast on the sensitive issue of the shape of the EU-NATO cooperation in the future. The following EUGS provision is representative in this regard: 'European security and defence efforts should enable the EU to act autonomously while also contributing to and undertaking actions in cooperation with NATO. A more credible European defence is essential also for the sake of a healthy transatlantic partnership with the United States'[9].

Overall, the EUGS constitutes an important step forward for the EU in defining its role and purpose at home and abroad. Importantly, the head-on take on the EU member-states' involvement in burden sharing in the Alliance, the clear attempt to make the EU stronger, and the emphasis on the transatlantic partnership, render the EUGS

8 EEAS, *Shared Vision, Common Action: A Stronger Europe A Global Strategy for the European Union's Foreign And Security Policy*, Brussels: European External Action Service (EEAS), June 2016, https://eeas.europa.eu/top_stories/pdf/eugs_review_web.pdf [2016-11-02].

9 EEAS, op.cit., p. 20.

a game-changer in the EU-NATO-US relationship; an issue particularly important now, i.e. following the US elections.

The symbolism of the NATO Warsaw Summit: In 1999, when Poland, the Czech Republic and Hungary were invited to join NATO, no one could have predicted how fragile the security context in the world would be 20 years ahead. The accession of Poland, the Czech Republic and Hungary to the Alliance in 1999, followed by the accession of Lithuania, Latvia, and Estonia in 2004, marked an end of the Cold War in Central Europe. By virtue of their accession to the Alliance, these European countries' freedom to decide about their geopolitical and economic aspirations was confirmed. Importantly, with NATO membership constituting an unwritten criterion of EU membership, the way toward these countries' membership in the EU was cleared. As a result, the Cold War divisions in Europe were bridged, the legacy of the Warsaw Pact bypassed, and a sense of hope was instilled across the region. Also Russia seemed to evolve along the lines democratization, liberalization and effective multilateralism. The past two years offer quite a different view of the world and its prospects, suggesting that especially NATO and its members ought to rethink the status quo.

Even if decisions taken at the 1999 NATO Washington Summit made an important step toward bypassing the cold-war divide in Europe, today more effort and determination have to be invested by the Alliance to bypass those Cold War divisions lastingly by adjusting at the same time to new circumstances that define the international context. Kicking off from Warsaw, the heart of the region, it is time to send a clear signal to the countries that aspire to join the Alliance for their territorial integrity is at stake. In this view, the NATO Warsaw summit, through the provisions of the final communiqué and pledges made, may indeed symbolize a new beginning, a qualitative and quantitative shift for NATO, its capabilities as well as its international clout. The NATO member-states implicitly agreed that a changed perception of risks and threats to security was needed if deterrence and defence was to be taken seriously by the Alliance.

The key outcomes of the NATO Warsaw Summit: Although the NATO Warsaw Summit was held in an atmosphere of urgency sharpened by the perception of imminent inter-state conflict in the region, views on the outcomes of the Summit are divided. That is, on the one hand, there are clear winners and losers of the summit, and on the other hand, opinions that the Warsaw Summit was a breakthrough are counter-balanced by those who argue that 'it was an important but not a seminal

summit'[10]. The key decisions taken at the Warsaw Summit can be summarized as '(1) enhancing deterrence, primarily through forward deployment along NATO's eastern flank, and (2) projecting stability beyond NATO'[11], i.e. in the Middle East and North Africa, non-NATO European countries and Afghanistan, and (3) improving interoperability of the Alliance and capacity building, including the recognition of cyberspace as an operational domain.

By defining the direction the Alliance will be moving along in the years to come, these three sets of outcomes delineate the not always converging perceptions of risks and threats to security as well as security priorities that NATO members hold. Overall, it seems that the Warsaw Summit Communiqué strikes a diplomatic balance between the diverging perceptions of threat and security priorities of NATO members. By so doing, it also minimizes possible losses in cohesion and commitment within the Alliance – an objective in itself for NATO and its members.

Enhancing deterrence: Two competing lines of threat perception are discernible among the NATO members, i.e. the perception that stresses the acuteness of the threat Russia poses to the Alliance and the view that the major risks and threats to security that NATO will incur originate from NATO's southern flank. Accordingly, in a bid to improve NATO's deterrence, the eastern flank countries, including Poland and the Baltic states, belong to the winners of the summit in that their pledge for an increased forward presence of the Alliance in the region has been addressed. Specifically, by 2017, four multinational combat battalions of 800–1,200 troops will be deployed on a rotational basis in Poland and the Baltic States.

Projecting stability beyond NATO: As if by means of balancing the communiqué's provisions on NATO's forward presence in Central Europe, also countries that see the major sources of threat on NATO's southern flank had significant takeaways at the Summit. The communiqué foresees NATO's involvement in the Middle East and North Africa, including the deployment of a NATO aerial surveillance aircraft, i.e. Airborne Early Warning and Control Systems (AWACS) to assist the Global Coalition to Counter Da'esh. Moreover, NATO has recommitted to maintaining a significant level of troops (probably 13,000 or more) in Afghanistan for the foreseeable future. NATO also agreed to launch a new naval mission in the Central Mediterranean focused on counterterrorism and enhancing situational awareness.

10 J. Stavridis, 'The NATO Summit's Winners and Losers', *Foreign Policy*, 11 July 2016.

11 P. Belkin, 'NATO's Warsaw Summit in Brief', *CRS Report*, 14 November 2016, Washington, D.C.: Congressional Research Service (CRS).

Projecting stability beyond NATO is a big category fit to encompass a variety of issues. It is a useful category, nevertheless, in that it pinpoints either the evolution of or the emergence of new topics/issues. The most important of them include:

- the toughening of NATO's stance toward Russia: Russia has been pointed out as the source of instability in Eastern Europe, while political dialogue remained the only channel of cooperation that NATO was ready to embark on given the circumstances;
- little change in NATO's stance toward Ukraine: NATO's support for Ukraine's sovereignty and territorial integrity has been stressed and Russia's aggressive actions against Ukraine condemned;
- improved prospects of dialogue and cooperation between NATO and the EU: the NATO-EU Cooperation Agreement was signed; a development particularly important in the context of the EU Global Strategy that makes a similar opening toward NATO as well as in the context of emerging risks and threats to safety and security in Europe;
- NATO enlargement and its implications: Montenegro was formally invited to join the Alliance. Georgia's prospect of membership remains a function of NATO's 'open door' policy, essentially exposing an implicit NATO's bridgehead to Russia's trial.

Improving interoperability of the Alliance and capacity building: The four most important issues that were agreed upon during the NATO Warsaw Summit include:

- the recognition of cyber space as a domain of warfare 'in which NATO must defend itself as effectively as it does in the air, on land, and at sea'[12];
- the emphasis on continued commitment to increased defence expenditures across the Alliance: while the 2% GDP threshold agreed during the 2014 NATO Wales Summit remains an important goal, the undertone of this provision is equal burden sharing among the EU NATO members and the US;
- the commitment to increased funding on such areas as cyber security, Special Forces, and unmanned vehicles;
- the stress on interoperability: what seems to be the keyword characterising the Communiqué, *interoperability* may in fact be the means to utilize the existing and emerging synergies among NATO members in view of addressing

[12] NATO, 'Warsaw Summit Communiqué', *Press Release* (2016) 100, 9 July 2016, para. 70, http://www.nato.int/cps/en/natohq/official_texts_133169.htm#cyber [2016-11-21].

and combating various risks and threats, including conventional, soft, and cyber, to safety and security.

1.3. Reactions to the NATO Warsaw Summit: a view from Belarus, Ukraine, Georgia and Russia

There has been a tendency in the media to refer to the July 2016 NATO Warsaw Summit in terms of a breakthrough. Indeed, as discussed in the introduction, several important decisions were taken during that Summit. From a different angle, several commentators[13] pointed to the wording that NATO Secretary General used in his speech at the Summit. Stoltenberg stated that the deployment of NATO military units in Poland and the Baltic states was not 'a new Cold War'[14], essentially arguing to the contrary as NATO's approach to Russia changed. Although Stoltenberg assured that 'NATO did not have any enemies, and the alliance was not directed against any other states'[15], it was obvious that Russia was not treated as a partner but rather as 'a source of uncertainty'[16]. Admittedly, it was the violation of Ukraine's territorial integrity by Russia that caused this 'uncertainty'. Finally, a thorough examination of the media discourse suggests that there was a sense of urgency prior to the Summit, whereas the war in Ukraine and the case of Georgia constituted the key issues defining that urgency. As some commentators argued, NATO's stance toward Georgia's prospective membership in the Alliance was is essence a question of NATO's foundational values and its strategic orientation.[17] In the same context, NATO's stance toward the war in Ukraine was discussed. Against this backdrop of unresolved questions and pending threats to regional stability, the NATO Warsaw Summit was carefully observed by third actors in the region, including Belarus, Georgia, Ukraine and the Russian Federation (RF). The following paragraphs present the key points and issues that the media discourse on the NATO Warsaw Summit in these countries conveyed.

---

13 A. Sobol, 'Szczyt NATO w Warszawie – rosyjski punkt widzenia' [NATO Warsaw Summit – the Russian point of view], *Komentarze IESW* [Commentary IESW], 29 July 2016, no. 19, 2016, http://www.iesw.lublin.pl/komentarze/19 [2016-11-01].

14 IAR PAP, 'Szef NATO: nie szukamy konfrontacji, nie chcemy nowej zimnej wojny' [NATO Chief: NATO is not seeking confrontation with Russia and does not want another Cold War], *Polskie Radio* [Polish Radio], 8 July 2016, http://www.polskieradio.pl/5/3/Artykul/1640853,Szef-NATO-nie-szukamy-konfrontacji-nie-chcemy-nowej-zimnej-wojny [2016-11-01].

15 Ibid.

16 Ibid.

17 A. Visvizi, 'NATO Warsaw Summit: Georgia and Other Unanswered Questions', *New Eastern Europe*, 13 June 2016, http://neweasterneurope.eu/articles-and-commentary/2026-nato-warsaw-summit-georgia-and-other-unanswered-questions [2016-11-01].

1.3.1. The view from Belarus

Alina Sobol

In line with argument raised in the Belarusian media, the issue of Belarus was treated as one of the sources of the *conflict* between Russia and NATO. Belarusian commentators argued that, from a strategic point of view, Belarus was the key element of power struggle in the region. It was argued that the bloc that *drew* Belarus to its side would gain advantage in the region. In this context, the location of Belarus, i.e. its proximity to the Kaliningrad district and the Suwalki corridor, and its geopolitical implications were stressed.

Several analysts emphasized that Belarus needed to remain neutral.[18] This was considered the only solution that would guarantee security and safety of the state and its citizens. Rapprochement with NATO was seen as impossible; alliance with Russia was considered unsustainable due to the economic problems of the Russian Federation (RF).

The Belarusian Minister of Foreign Affairs, Vladimir Makei, did not show any concern with the plans of the deployment of NATO troops in the vicinity of the border with Belarus.[19] Given the conflict in Ukraine and the annexation of Crimea, it was a justified decision on the part of NATO; a decision that Belarus, nevertheless, did not intend to support. The Belarusian authorities do not exclude the possibility of increasing the budget for the state's defence. However, Belarusian commentators note that the deployment of additional troops close to the border with Belarus will give Russia a pretext to deploy its own forces into the territory of Belarus, for instance via the construction of an airforce base or by increasing the presence of ground troops.

Poland was criticized as an intermediary between the West and NATO, on the one hand, and Russia and Belarus, on the other hand. The Belarusian media emphasized

---

18 А. Алесин [A. Alecin], 'Примет ли Минск сторону Москвы в случае военного конфликта с НАТО?' [Does Minsk take the Direction of Moscow in Case of a Military Conflict with NATO?], *Naviny.by*, 16 July 2016, http://naviny.by/rubrics/politic/2016/07/16/ic_articles_112_192122 [2016-11-01]; А. Шпаковский [A. Shpakouski], 'Саммит НАТО: выводы для Беларуси' [NATO Summit: conclusions for Belarus], *Sputnik.by*, 11 July 2016, http://sputnik.by/columnists/20160711/1024025203.html [2016-11-01]; А. Федоров [A. Fedorov], 'На пороге новой холодной войны. Беларусь обозначает нейтралитет' [On the verge of a new Cold War. Belarus stands for neutrality], *Naviny.by*, 24 July 2016, http://naviny.by/article/20160724/1469352660-na-poroge-novoy-holodnoy-voyny-belarus-oboznachaet-neytralitet [2016-11-01]; Д. Тренин [A. Trenin], 'Саммит НАТО в Варшаве закончился. Скоро начнут появляться войска' [The NATO summit ended in Warsaw. Soon the troops will begin to appear], *Belsat.eu*, 9 July 2016, http://belsat.eu/ru/news/sammit-nato-v-varshave-zakonchilsya-skoro-nachnut-poyavlyatsya-vojska/ [2016-11-01].

19 Sputnik, 'Макей: расширение НАТО не приветствуем' [Makei: NATO enlargement is not welcome], *Sputnik.by*, 7 July 2016, http://sputnik.by/politics/20160707/1023950517.html [2016-11-01].

the sovereignty of Belarus which could look after its own interests.[20] The state will eagerly enter the dialogue both with Russia and the Western countries. Belarus is interested in the *status quo*, a peaceful 'manoeuvring' (as it is called by the commentators[21]) between Russia and NATO, benefitting from the cooperation with these two blocs. The Polish interest in Belarus is explained in Belarusian media as a Polish wish to strengthen its position in the NATO structures (which would guarantee the introduction of Belarus into NATO). What was widely commented in the Belarusian media was Stoltenberg's statement concerning the fact that Belarus was not invited as an observer to the NATO summit; according to Stoltenberg, Belarus is not an independent state.[22]

1.3.2. The view from Georgia

Aleksandra Kuczyńska-Zonik

The Georgian media devoted little space to the NATO Warsaw Summit. Short reports featuring statements of the summit participants dominated the press. In-depth insights and analyses of the consequences of the summit for Georgia were absent. Georgia had high hopes in its participation in the Warsaw summit. To confirm the importance of the Georgian membership in NATO, just before the beginning of the summit, six political parties in the Parliament, including the opposition, signed a common integrative declaration which emphasized Georgia's Euro-Atlantic aspirations.[23] The declaration was presented on 8 July 2016 during the opening ceremony of the Summit. Prior to the beginning of the summit, the Prime Minister of Georgia, Giorgi Kvirikashvili, stated that extended cooperation between Georgia and NATO would have an essential impact on the degree of security in Georgia and on its defence capabilities.[24]

---

20 Sputnik, 'МИД: Беларусь обойдется без посредников в диалоге с НАТО' [Belarus will do without mediatory in the dialogue with NATO], *Sputnik.by*, 11 July 2016, http://sputnik.by/politics/20160708/1023996118.html [2016-11-01]; А. Сивицкий [A. Sibockiy], 'Политолог: саммит НАТО не станет точкой отсчета новой «холодной войны» [Expert: NATO summit will not be the starting point of a new 'Cold War'], *Sputnik.by*, 11 July 2016, http://sputnik.by/radio/20160711/1024040566.html [2016-11-01].

21 Федоров [Fedorov], op.cit.

22 Г. Шарипкин [G. Sharipkin], 'Эксперт: НАТО не воспринимает Беларусь как самостоятельное государство' [Expert: NATO does not see Belarus as an independent state], *RFI*, 18 July 2016, http://ru.rfi.fr/evropa/20160718-ekspert-nato-ne-vosprinimaet-belarus-kak-samostoyatelnoe-gosudarstvo [2016-11-01].

23 Agenda.ge, 'All political parties sign Declaration to NATO Summit', *News*, 8 July 2016, http://agenda.ge/news/61613/eng [2016-10-29].

24 Civil Georgia, 'Georgian President in Warsaw for NATO Summit', *News*, 8 July 2016, http://www.civil.ge/eng/article.php?id=29287 [2016-10-29].

Apart from the prime minister, among the members of the Georgian delegation to the Warsaw NATO Summit were the President of Georgia, the Minister of Foreign Affairs, the Minister of Defence, the Minister of Euro-Atlantic integration as well as the secretary of the Council of National Security. Their aim was to gain additional tools from NATO which would enable them to increase the defence capabilities of the state. Georgia's enthusiasm lessened following the announcement that the issue of including Georgia in the Membership Action Plan (MAP) would not be discussed at the Summit. For Georgia, this was a purely political decision, which was accepted with a disappointment; some commentators talked of a feeling of betrayal.[25] Georgia treated the MAP very seriously since it would mean an imminent accession to NATO. Following the NATO summit in Bucharest in 2008, Georgia expected a fast membership[26], but as a result of the Russian-Georgian war, the accession process slowed down to the extent that arguments of suspension of cooperation were raised. For this reason, during the Warsaw NATO summit, a decision was made to take 'a new step' toward Georgia. That is, NATO's 'new initiative' was to embrace the strengthening of the defence capabilities of Georgia, including air defence and intelligence, as well as training and educational support and strategic communication. NATO again confirmed its support for Georgia's sovereignty and territorial integrity but at the same time Georgia was reminded that it should maintain specific standards in order to join the Alliance.[27]

1.3.3. The view from Ukraine

Agata Stolarz

The Ukrainian opinions on the NATO Warsaw summit commonly refer to 'Ukraine being left alone'. Commentators, in general dissatisfied with the outcomes of the summit, emphasized its 'symbolism', understood in a rather pejorative manner. That it, it was stressed that regarding the case of Ukraine, the Summit had produced another empty, i.e. devoid of action, condemnation of the annexation of Crimea and calling on Russia to withdraw its military and financial support for Donbas' separatists. A distinctive voice of criticism came from Ukraine's Deputy Prime Minister, Ms

25 E. Kogan, 'Resetting Georgia-NATO Relations', *Georgia Today*, 27 October 2016, http://georgiatoday.ge/news/4994/Resetting-Georgia-NATO-Relations [2016-10-29].

26 Visvizi, 'NATO Warsaw Summit…', op.cit.

27 Ministry of Foreign Affairs of Georgia, 'Comment of the Georgian Foreign Minister on the results of the meeting of the North Atlantic Council at the level of NATO Defence Ministers', *News*, 27 October 2016, http://mfa.gov.ge/ [2016-10-29].

Ivanna Klympush-Tsintsadze. During the Warsaw Summit Experts' Forum[28], faced with the argument of the necessity to carry out the reforms by Ukraine, she accused the West of hypocrisy.[29] In her opinion, really essential for European integration and Transatlantic cooperation was Russia and its foreign policy conduct, rather than the reform process in Ukraine.

The Ukrainian critique was also directed at the current NATO-Russia relations. From the perspective of some of Ukrainian commentators, NATO did not seem to understand that Ukraine was the only country today that had been experiencing military confrontation with Russia, one of the greatest military powers in the world.[30] That tragic experience had not given the attention it would require. Moreover, commentators in Ukraine hinted that the Warsaw NATO Summit did not bring the desired outcomes as regards the prospect of Ukraine's NATO accession.[31] It should be noted at this point that Ukraine's President, Poroshenko, reminded that Ukraine had not applied for NATO membership.[32]

The official position of the Ukrainian authorities was of course much more balanced than the media discourse. Poroshenko stated that Ukraine was the only partner of the Alliance that was granted the opportunity to hold a separate meeting with the commanders; an opportunity that highlighted the central position of Ukraine on the Alliance's agenda.[33] The criticism of the arrangements concerning Ukraine was countered by some commentators with the signing of the Comprehensive Assistance Package for Ukraine, which for Poroshenko, was 'the first of a kind in the history of the alliance'[34]. The NATO-Ukraine package contains a plan of reforms in the Ukrainian

---

28 Warsaw Summit Experts' Forum-NATO in Defence of Peace: 2016 and Beyond (WSEF 2016).

29 P. Pieniążek, 'Szczyt NATO: Ukraina pozostawiona bez złudzeń' [NATO Summit: Ukraine left without illusions], *Krytyka Polityczna* [Political Critique], 10 July 2016, http://www.krytykapolityczna.pl/artykuly/ukraina/20160710/szczyt-nato-ukraina-pozostawiona-bez-zludzen-relacja [2016-11-01].

30 В. Червоненко [V. Chervonenko], 'Саміт НАТО у Варшаві: без прориву для України?' [NATO Summit in Warsaw: without a breakthrough for Ukraine?], *BBC Україна* [BBC Ukraine], 8 July 2016, http://www.bbc.com/ukrainian/politics/2016/07/160707_nato_summit_ukraine_vc [2016-11-01].

31 Ibid.

32 Б. Немировський [B. Nemirowskyj], 'Саміт НАТО. Що везе Порошенко з Варшави' [NATO Summit. What Has Brought Poroshenko from Warsaw], *Glav.com*, 10 July 2016, http://glavcom.ua/publications/samit-nato-shcho-veze-poroshenko-z-varshavi-360892.html [2016-11-01].

33 B.T. Wieliński, P. Wroński, M. Zawadzki, 'Szczyt NATO w Warszawie. W sprawie Ukrainy bez zmian, Gruzja rozczarowana' [NATO Summit in Warsaw. In the Case of Ukraine Unchanged, Georgia Disappointed], *Gazeta Wyborcza*, 11 July 2016, http://wyborcza.pl/1,75398,20380157,szczyt-nato-w-warszawie-w-sprawie-ukrainy-bez-zmian-gruzja.html [2016-11-01]; В. Рябих [V. Rabych], 'Саміт НАТО у Варшаві – підсумки й уроки' [NATO Summit in Warsaw – the results and lessons], *Ukrinform*, 12 July 2016, http://www.ukrinform.ua/rubric-other_news/2049186-samit-nato-u-varsavi-pidsumki-j-uroki.html [2016-11-01].

34 Ibid.

army. However, what was emphasized by both the Western and the Ukrainian media was that the new element was solely the trust thanks to which NATO was to help Ukraine in the fight against cyber crime, in the medical treatment of soldiers and in demining. Today, the main argument in the debate that is unfolding in the Ukrainian media highlights is the naivety of hopes that NATO or the European Union would assist Ukraine in navigating the Russian-Ukrainian conflict. If some groups believed in the help from the West, the Warsaw NATO Summit proved that it was only Ukraine's wishful thinking.[35]

1.3.4. The view from Russia

Alexey Vasilyev

The official Russian reaction to the Warsaw NATO Summit was quite reserved. The spokesman of the President of the RF stated that Russia 'carefully followed' the summit and 'attempted to identify grains of rationality'[36] in NATO leaders' statements. Stoltenberg's speech was carefully examined, in particular his statements on the lack of a direct threat from Russia and on the necessity to maintain contact with Russia.[37] Official announcements emphasized Moscow's hope that *common sense would win* as well as that Russia was open to dialogue and cooperation but only as far as mutual interests were concerned.[38] The announcement of the spokesman of the President of the Russian Federation (RF) mentioned with regret the motion of the President of the Republic of Poland on the necessity to expand the military potential of NATO.[39]

The commentaries of media close to the Kremlin, which reflect the views of the conservative part of the Russian elite, greatly resemble the Soviet rhetoric from the period of the Cold War. Here specifically, the following expressions should be highlighted: 'aggressive character of NATO', NATO's constant cheating of Russia (including the USSR), the threat of NATO expansion to the East, 'anti-Russian hysteria', which 'leads the world to war', 'a massive show of group hatred', 'informal competition' in

35 А. Октисюк [A. Oktisyuk], 'НАТО: дипломатія і реальні наміри' [NATO: diplomacy and the real intention], *TSN*, 6 July 2016, http://tsn.ua/blogi/themes/politics/nato-diplomatiya-i-realni-namiri-688998.html [2016-11-01]; cf. A. Stolarz, 'Brexit z perspektywy Ukrainy' [Brexit from the Perspective of Ukraine], *Komentarze IESW* [Commentary IESW], no. 15, 2016, 30 June 2016, http://www.iesw.lublin.pl/komentarze/15 [2016-11-01].

36 В. Петров [V. Petrov], 'Песков прокомментировал ход саммита НАТО в Варшаве' [Peskov Commented on the NATO Summit in Warsaw], *Российская газета* [Russian Newspaper], 8 July 2016, https://rg.ru/2016/07/08/kreml-prokommentiroval-hod-sammita-nato-v-varshave.html [2016-11-01].

37 Ibid.

38 Ibid.

39 Ibid.

anti-Putin announcements, etc. In general, the picture painted by the pro-Kremlin media resembles Soviet footage from 'the covens of imperial anti-Soviet forces, full of spirit of hatred for the cause of peace and progress'.[40]

Simultaneously, the media close to the Kremlin indicated that in reality there was no real force behind the statements made during the summit.[41] They described it as hysteria which showed the real weakness and deep crisis of NATO, the European Union and the West in general. A lack of any independence of Europe in its relations with the USA was mentioned. It was also stressed that the USA attempted to make a connection with Europe which would serve the interests of the USA. NATO, on the other hand, was criticized for the lack of any coherent position toward Russia. Interestingly, some commentators dubbed the summit's definition of Russia as a threat followed by a simultaneous calling on Russia to cooperation as 'a schizophrenic connection'.[42] From the perspective of media content analysis, the recipient of this information was encouraged to understand supposed that the Warsaw NATO summit was an empty show underpinned with uncertainty, crisis and lack of proper posture. Moreover, the rhetoric of NATO created the feeling of an imminent war. However, in the most dramatic moment, 'Putin calmly and in cold blood answered the hysteria of NATO'.[43] Putin stated that Russia would not lose 'its cold brain', which 'instilled the citizens of the planet with optimism and faith that war is less likely to begin'[44].

---

40 Н. Шендарёв [N. Shendarev], 'Саммит НАТО в Варшаве: чего ожидать от военно-политического шабаша в Польше' [NATO Summit in Warsaw: what to expect from the military and political coven in Poland], *Russia Nation News*, 8 July 2016, http://nation-news.ru/201778-sammit-nato-v-varshave-chego-ozhidat-ot-voenno-politicheskogo-shabasha-v-polshe [2016-11-01]; cf. Д. Родионов [D. Rodionov], 'Милитаристская истерика в Варшаве' [Militaristic Hysteria in Warsaw], *Ren.tv*, 8 July 2016, http://pzs39.ru/news/militaristskaja_isterika_v_varshave/2016-07-09-230 [2016-11-01]; cf. Sobol, op.cit.

41 Ibid.

42 А. Носович [A. Nosovich], 'Саммит НАТО решил «сдерживать» Россию с протянутой рукой' [NATO Summit decided to 'contain' Russia with an outstretched hand], *Rubaltic*, 11 July 2016, http://www.rubaltic.ru/article/politika-i-obshchestvo/110716-sammit-nato/ [2016-11-01]; А. Братерский [A. Braterskiy], 'Без объявления «холодной войны»' [Without a Declaration of 'Cold War'], *Gazeta.ru*, 8 July 2016, https://www.gazeta.ru/politics/2016/07/09_a_8386937.shtml [2016-11-01]; cf. A. Sobol, A. Stolarz, 'Polityka historyczna Federacji Rosyjskiej w świetle obchodów 71. rocznicy wyzwolenia Auschwitz' [Russian Federation historical policy in context of the 71th anniversary of the liberation of Auschwitz], *Komentarze IESW* [Commmentary IESW], no. 3, 2016, 22 March 2016, http://www.iesw.lublin.pl/komentarze/3 [2016-11-01]; A. Vasilyev, 'Jak rosyjskie elity czytają i interpretują rzeczywistość i co z tego wynika? [cz. 2]: liberalizm' [How the Russian elite read and interpret reality and to what avail? [Part 2]: liberalism], *Komentarze IESW* [Commentary IESW], no. 6, 2016, 11 May 2016, http://www.iesw.lublin.pl/komentarze/6 [2016-11-01].

43 'Начнется ли Третья мировая война после саммита НАТО?' [Does World War III will start after the NATO ummit], *Комсомольская правда в Украине* [Komsomolskaya Pravda in Ukraine], 4 July 2016, http://rus-ssmi.ru/nachnetsya-li-tretya-mirovaya-vojna-posle-sammita-nato/ [2016-11-01].

44 Ibid.

These are obvious topics of the Soviet propaganda from the Cold War period. Nowadays, however, propaganda enters a deeper semantic level. The image of 'silence' is a mark of what traditionally for Russian culture is associated with 'truth', 'our own'. 'Enemies', 'strangers' always 'make a noise', they are restless because they have no real power, 'the truth' is not on their side. That is why the NATO Warsaw Summit was described in media as a great noisy show with hysteria which was quietly answered by calm and solid Putin.[45]

The liberal and the opposition media emphasized the incredible level of the confrontation between Russia and the West, reached after the annexation of Crimea and after the outbreak of the war in the south-east Ukraine, as well as the negative influence of this confrontation for Russia's long-term interests.[46] The revival and strengthening of NATO were also indicated as the meaning was given to its existence as a result of the foreign policy of Putin's regime. Moreover, the significance of the decision on the stable presence of NATO battalions in the Baltic states and in Poland was emphasized. According to commentators, the presence of the alliance troops guarantees the performance of the mutual obligations of NATO member states (the Kremlin media usually refer to these battalions as useless from a military point of view).[47]

45 Sobol, op.cit.; cf. Vasilyev, op.cit.

46 Cf. A. Kuczyńska-Zonik, 'Russian propaganda: methods of influence in the Baltic States', *Yearbook of the Institute of East-Central Europe*, vol. 14, no. 2, 2016, pp. 43–60.

47 А. Гольц [A. Goloc], 'Сдержать Россию' [Containing Russia], *Ежедневный Журнал* [Daily Journal], 11 July 2016, http://anonymouse.org/cgi-bin/anon-www.cgi/http://ej.ru/?a=note&id=29906 [2016-11-01].

PART 2

Defining the fragile security contexts

2.1. Conventional/hard security threats in the region

2.1.1. Conventional/hard security threats: an overall assessment

Tomasz Stępniewski

The annexation of the Ukrainian peninsula of Crimea in March 2014 sent shockwaves throughout Europe. As the Russian-Georgian conflict in the summer of 2008 failed, the grab of Crimea and the continuous Russian fanning of the flames in Eastern Ukraine seemingly succeeded, i.e. governments across the EU started to reverse the declining trend in European defence spending and NATO begun implementing a balanced package to bolster its eastern flank. The bottom line is that the risk of serious interstate conflict, once almost unconceivable, has returned to Europe today.

The Russian Federation (RF) is modernizing and reinforcing its conventional forces. It is also using the theatre of Eastern Ukraine to test new strategies. Russia's involvement in Ukraine should not be viewed only in light of the conflict in Ukraine. Rather, a more holistic take on this conflict should be taken and so NATO members ought to change their approach toward conventional threats in Europe. The developments on NATO's eastern flank prove the relevance of this claim. From the point of view of convention-

al threats, it is the revanchist Russia and its neo-imperial policy that constitute the key hazard to the continent today. The following paragraphs elaborate on this claim.

Security in East-Central Europe has become an increasingly complicated affair. As far as military matters are concerned, the threat for V4 countries on the part of Western Europe is virtually non-existent because the situation in the region is stable and predictable. Therefore, threats of this nature are highly unlikely. However, threats, including conventional ones, for V4 countries may emerge from the direction of the post-Soviet states. In the 1990s, the situation in East-Central Europe and the post-Soviet space was relatively stable. In contrast, the situation in the second decade of the 21st century has undergone severe complications. This is a consequence of changes in the internal policies of the countries in the region, but also aggressive actions of third parties, e.g. Russo-Georgian war of 2008, Russo-Ukrainian war in Donbas since 2014, the annexation of Crimea by Russia. Indeed, Ukraine's crisis, a de facto Russia's armed conflict with Ukraine which has been raging since 2014, altered the perception of security in Eastern Europe and Europe in general. One could argue that the conflict in Ukraine constitutes a symbolic end of the post-Cold War international order based on peaceful coexistence of states, respect for territorial integrity and rules-based international states' system.

From its onset, the Russian-Ukrainian conflict represented so-called hybrid or 'subliminal' war. Some argue that Russia's objective was to destabilise the situation in the southern and the eastern Ukraine in order to disconnect these areas from the country, to turn them into 'occupied territories', or establish a quasi-state in the area, as in the case of Transnistria. As the so-conceived conflict unfolds in the vicinity of the V4, it is bound to create concerns about its likely security implications. Part of the problem is the unpredictable nature of the direction of Russia's foreign policy. In this context, Carl Bildt argues that Russia has transformed from the West's 'strategic partner' to its 'strategic problem'.[1]

Russia's engagement on the international arena aims at restoring the *status quo ante,* i.e. the status quo as it was prior to the end of the Cold War. Specifically, Putin's main objective is to influence on the country's peripheries. According to Zbigniew Brzeziński[2], one of the possible ways to put a stop to Russia's revanchist policies is

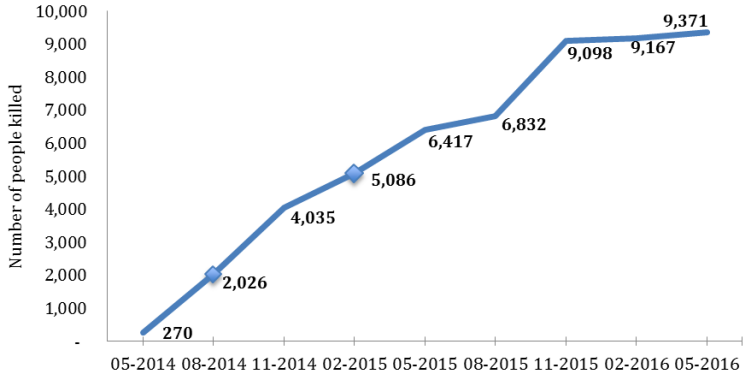
1 C. Bildt, 'Russia, the European Union and the eastern partnership', *ECFR Riga Papers*, 19 May 2015, http://www.ecfr.eu/page/-/Riga_papers_Carl_Bildt.pdf [2016-11-11].

2 Cf. T. Stępniewski, *Geopolityka regionu Morza Czarnego w pozimnowojennym świecie* [The Geopolitics of the Black Sea Region in the Post-Cold War World], Lublin: Wydawnictwo Instytutu Europy Środkowo-Wschodniej (IESW), 2011.

to strengthen European security along the Paris-Berlin-Warsaw-Kyiv line. Therefore, in context of the war in Ukraine, it is extremely important to support authorities in Kyiv (in Minsk and Kishinev) in building democratic rules. This would contribute to restraining Russia's neo-imperialistic endeavours.

As of November 2016, one-third of the Donbas region (part of Luhansk and Donetsk regions), or close to 3% of the Ukrainian territory, is controlled by the combatants (or terrorists) of the so-called 'Donetsk People's Republic' and 'Luhansk People's Republic', not by Ukraine's government.[3] Research suggests that despite the Minsk agreements, the Donbas conflict continues.[4] Figure 1 outlines the details.

Figure 1: Death Toll in Russia-Ukraine Donbas War (UN Data)



Note: Markers show the Minsk 1 and Minsk 2 ceasefire accords.

Source: M. Alexseev, 'The Tale of Three Legitimacies: The Shifting Tone and Enduring Substance of Moscow's Ukraine Policy', PONARS *Eurasia Policy Memo*, no. 431, June 2016.

Viewing the map of Eastern Europe, Russia's military presence in the region ought to be taken into account. As Map 1 suggests, Russia's potential in Eastern Europe is substantial. Moreover, Russian continuously reinforces its forces in Crimea, Kaliningrad and Belarus Eastern Europe may be perceived as 'a grey zone of security'. Fro-

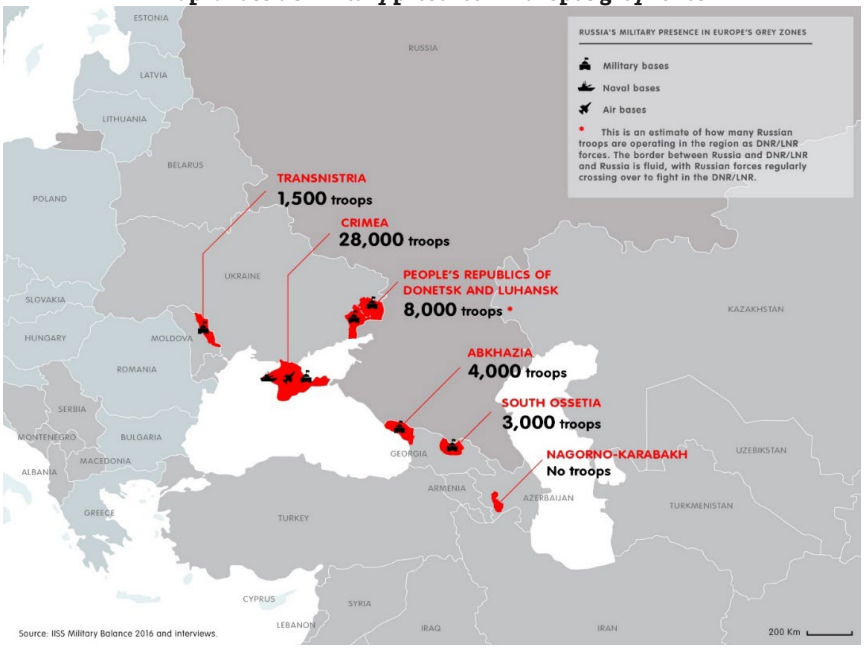
3 H. Shelest, H. Maksak, *Ukraine's Security Options: Time for Strategic Choices, Smart Partnerships, and Comprehensive Reforms*, Caucasus Institute for Peace, Democracy and Development/CIPDD, Tbilisi, June 2016, pp. 6–7.

4 M. Alexseev, 'The Tale of Three Legitimacies: The Shifting Tone and Enduring Substance of Moscow's Ukraine Policy', PONARS *Eurasia Policy Memo*, no. 431, June 2016, http://www.ponarseurasia.org/sites/default/files/policy-memos-pdf/Pepm431_Alexseev_June2016_8.pdf [2016-11-13]; also: UN, 'Death toll in Donbas conflict nearing 7,000 men', UN Update, 29 July 2015, UNIAN, 29.07.2015, http://www.unian.info/war/1106015-un-update-death-toll-in-donbas-conflict-nearing-7000-men.html [2016-11-13].

zen conflicts lingering in the region may directly or indirectly exert impact upon the stability and security of V4 states.

Poland is the only V4 country that shares a border with Russia, i.e. the Kaliningrad Oblast. The fact that Iskander (range of up to 500 km) and Bastion (range of up to 400 km) missiles are located in the Oblast poses a potential threat to the north-east Poland and the Baltic states. Moreover, Russian sources indicate that Iskander is considered to be more than a mere missile and is understood as a guidance and homing system along with mobile launchers. Russian multi-level A2/AD (anti-access/area denial) system is worth making a reference to at this point. The A2/AD revolves around the capability of detecting and jamming electronic guiding systems, spatial orientation and communications, and subsequently eliminating enemy means of aerial warfare including planes, cruise missiles and drones. Russian Kaliningrad constitutes NATO's northernmost threat. The range of anti-aircraft weapons located there reaches far into Polish airspace and, in case of a crisis, may eliminate NATO reinforcements for Baltic states. The Crimean Peninsula has recently become another threat zone due to its annexation by Russia.

Map 1: Russia's military presence in Europe's grey zones



Source: S. Pugsley and F. Wesslau (eds), 'Russia in the grey zones', *ECFR's grey zones series,* Part II, 1 September 2016, London: ECFR, http://www.ecfr.eu/wider/specials/russia_in_the_grey_zones [2016-11-14].

The RF established a significant A2/AD presence in the area, which offers the control over virtually the entire Black Sea Basin.

Another problem associated with the conventional security of the region involves violation of NATO members' and Scandinavian countries' airspace. 'Dangerous military-military and military-civilian incidents involving ships or aircraft of Russia, NATO member states, and third parties continue to pose a serious threat to Euro-Atlantic security.'[5] In particular, the post-annexation period witnessed Russia's increased military activity, violations of NATO's airspace and territorial waters, and deterioration of NATO-Russia relations.

The fact that Russia, along with the USA, are in the possession of 90% of the world's nuclear warheads is noteworthy. More specifically, estimates suggest that 'as of early 2016, the [RF] had a stockpile of approximately 4500 nuclear warheads assigned for use by long-range strategic launchers and shorter range tactical nuclear forces. In addition, as many as 2800 retired but still largely intact warheads awaited dismantlement, for a total inventory of about 7300.'[6] In addition, Russia considers its threat of tactical nuclear weapons' as a significant strategic instrument which may be applied in order to isolate the post-Soviet space from Western support. So far, Russia has not been overtly inclined to play this card. However, its colossal nuclear potential presents a threat for Western Europe's, and broadly European, security.

2.1.2. Conventional/hard security threats: the view from Poland

Justyna Gotkowska

Since the outbreak of the 2008 Russian-Georgian war, Poland has perceived Russia as an increasingly aggressive actor in international politics that was willing and able to use military force to achieve its foreign policy goals. The 2014 Russian annexation of Crimea and Russian military intervention in eastern Ukraine have only confirmed that. From the Polish perspective, Russia – with its unstable political and economic systems – generates not only a political and economic challenge but also a military threat to Poland. Russia is seen as a revisionist power that not only seeks to restore its domination in the post-Soviet space, but also to change the post-Cold War order. Kremlin aims to under-

5 Ł. Kulesa, T. Frear, D. Raynova, 'Managing Hazardous Incidents in the Euro-Atlantic Area: A New Plan of Action', *Policy Brief*, November 2016, London: European Leadership Network, http://www.europeanleadershipnetwork.org [2016-11-05].

6 H.M. Kristensen, R.S. Norris, 'Russian nuclear forces 2016', *Bulletin of the Atomic Scientists*, 3 May 2016, http://thebulletin.org/2016/may/russian-nuclear-forces-20169394 [2016-12-02].

mine NATO and to disintegrate the European Union (EU). The Kremlin's main non-military instruments against the West are corruption, espionage, subversion, propaganda and disinformation campaigns aimed at driving a wedge within the EU, NATO and in the Transatlantic relations. However, military means are for Moscow equally important instruments, which the Kremlin is ready to use in order to seek a new balance of power.

From Russia's perspective, the Baltic Sea region may be a convenient test bed for trying to achieve its geopolitical objectives, i.e. to undermine trust in NATO's collective defence principle and NATO's credibility and to show that the US security guarantees are non-binding. The political and military geography of the Baltic Sea region allows for that. The three Baltic states with their small military potential constitute NATO's most exposed peninsula vulnerable to potential Russian aggressive actions. However, also Poland fears direct Russian military aggression as it is the biggest country on NATO's eastern flank and it borders the highly militarized Russian Kaliningrad Oblast to the north and Belarus with its military system integrated with Russia to the east.

In Russia's view, Poland is also the main country that openly favours both in the EU and NATO countering Russian influence and policies. Due to its threat perception, Poland was the forefront country in NATO (along with the Baltic states) that has been calling for more allied presence on the eastern flank since 2014, perceiving this as a measure that deters Russia from taking any military action against flank NATO member states. Poland has also strongly supported EU sanctions on Russia because of its actions against Ukraine. At the NATO Warsaw summit in July 2016 Poland secured a large NATO/US military presence in its territory, that comprises of a US-led battalion-sized battle group under NATO umbrella and a US division headquarters together with main components of the US heavy armoured brigade being part of US European Reassurance Initiative. Due to its high-end military capabilities and political will to use them, USA is perceived in Poland as the main ally. With its threat perception Poland clearly belongs to the Baltic Sea region, where all NATO and non-NATO countries fear more direct provocations and aggression from Russia in the years to come and intensify politico-military relations with the US. In accordance with its threat perception Poland maintains relatively high military expenditure, belonging within NATO to the group of countries that spend most on defence. According to the recent NATO data, Poland's defence budget has reached over 2% GDP since 2014 (based on 2010 prices), i.e. ca. 10 bln USD, and since 2015 Poland has spent more than 20% for equipment. Thus Poland has met all of the NATO guidelines.[7] The current government pledged maintain

[7] NATO, 'Defence Expenditures of NATO Countries (2009–2016)', *Press Release* (2016) 116, 4 July 2016, http://www.nato.int/cps/en/natohq/news_132934.htm [2016-11-20].

the 2% of GDP spending level also in the coming years. The Polish Ministry of Defence is currently working on Strategic Defence Review that shall be published early 2017. It is also reworking the long-term Technical Modernization Plan for the Polish Armed Forces.

2.1.3. Conventional/hard security threats: the view from the Czech Republic

Vojtěch Bahenský & Jakub Kufčák

The threat perception according to the official documents: The worsening of the security situation during the year 2014 brought about the preparation of an update of the Czech security strategy since the current one from 2011 had been rendered out-of-date by the events. The updated version of the Security Strategy of the Czech Republic (Strategy) was published in February 2015 by the Ministry of Foreign Affairs, which supervised the preparation of that document.[8] Two relevant threats are mentioned in this strategic document:

- 'weakening of mechanisms of cooperative security and political and international law based commitments in area of security'; and
- 'instability and regional conflicts in Euro-Atlantic space and its neighbourhood'.

Direct military confrontation with the Czech Republic has not been explicitly mentioned among the threats identified in the document. However, the possibility of a direct military threat to the territories of NATO and EU member-states is mentioned in the Strategy. Yet, it is not explicitly identified in the 'threat summary' among other threats, some of which were mentioned above, but it is 'buried' in the body of the Strategy.

In contrast to the Security Strategy of the Czech Republic from 2015, the Long Term Perspective for Defence 2030[9] prepared by the Czech Ministry of Defence in 2015 does explicitly list the following threats and risks:

- growing military threat to allies;
- risk of political use of military power stemming from growing Russian military expenditures;
- continuation of redistribution of political and military power in the world.

8 Ministry of Foreign Affairs, *The Security Strategy of the Czech Republic*, Prague: Ministry of Foreign Affairs, February 2015.

9 Ministry of Defence, *The Long Term Perspective for Defence 2030*, Prague: Ministry of Defence of the Czech Republic – Military History Institute, July 2015.

The Long Term Perspective for Defence also, at least partially, mentions necessary actions to counter growing threat of military confrontation, including reiteration of the need for capabilities in the area of air superiority, close air support, joint operations, interoperability with allied forces and adequate material reserves for unexpected deployment of forces.

The threat perception according to the actions – big words, little action: It is clear that the Czech government, however vaguely or reluctantly, recognizes the growing threat of intrastate war. However, official recognition is not sufficient to judge the actual perception of the threat. That can be judged only by according acts to counter the threat.

The 'flagship' of political efforts to address the worsening security environment and a growing conventional threat is the increase of defence expenditures, which should, according to an agreement of Czech coalition parties from 2014, eventually rise to 1.4% of GDP in 2020. But scepticism about this pledge privately voiced by security community seem to be confirmed, since the budget of the Ministry of Defence so far rises only in absolute numbers. With the continued growth of the Czech GDP it seems very likely that the reality will be, and current plans of the Czech Ministry of Finance seem to reflect this (only about 1.19% in 2019).

That is hardly a behaviour of a state that feels militarily threatened. The Czech Republic in 2015 even became perhaps the first country where the Minister of Defence refused additional funds for the defence budget because he was not sure his Ministry would be able to spend them. A look at military modernisation and procurement priorities also does not provide much of evidence that would warrant the notion that Czechs are concerned about conventional conflict.[10] By 2025, the Ministry of Defence is planning to merely repair the damage incurred to the military capabilities during the austerity cuts in the previous decade. Only after that date is the real development of capabilities to take place. Recently, the Ministry of Defence proposed to create a new third brigade after 2025. This would mean that the military capabilities would be strengthened by a third. Accordingly, the Czech army would grow from around 20 thousand soldiers at the moment to 27 thousand around 2025; it would

[10] Despite the proclamation included in the Long Term Perspective for Defence 2030 about the importance of interoperability, modernization of artillery systems of Czech Army recently changed from buying new platforms to mere modernization of existing without plans to switch to standard NATO 155 mm calibre. Plans to buy new multifunctional helicopters are feared to be driven by their potential use for civilian emergency medical transport than by their utility for (conventional) conflict.

reach the size of approximately 32 thousand soldiers in the following years while the combined spending would total ca. 8 billion USD.[11]

Behind the façade: It seems that the official documents *do*, in somewhat clumsy and implicit way, recognize the threat for the European security architecture posed by the Russian revisionist policy focused on the creation and possession of a sphere of influence and the ramifications of the Russian-Ukrainian conflict. Even on a political level within NATO, the Czech Republic does not vocally advocate expansion of NATO military presence on the 'eastern flank'. Well-known and sometimes ridiculed aversion of Czechs to be identified as Eastern Europe seems to project itself in perception of conventional threats to NATO's eastern flank. A potential Russian aggression and a resulting conflict are perceived as a threat to Eastern Europe which is somehow 'distant' from 'Central European' Czechs, who seem to be prone to see such a conflict as 'a regional conflict'. The Czech contribution to such a conflict is then considered in terms of the necessary minimum rather than the possible maximum. We, therefore, posit that the actions (or rather the lack of them) to counter the threat of conventional conflict warrant clear assertion, i.e. Prague focuses on a mere generation of an image of being a 'reliable ally' for the domestic audience and the allies.

This excurse into the perception of the conventional threats within the Czech Republic may fail to satisfy the reader since the absence of appreciation for the gravity of the Russian threat can be easily ridiculed. But in conclusion of this part it is also important to note both virtues and sins inherent to the current posture when facts on the ground are taken into account.

In many respects, we concede that the absence of urgent preparation for conventional conflict can make perfect sense. The Czech Republic neighbours only EU/NATO member states, which are clearly do not pose any threat. This also means that an attack on another NATO member state is prerequisite for the Czech Republic having to defend its own territory. Despite this fact, the Czech security is definitely at risk because of conventional threats faced by its allies since conventional military confrontation of NATO member state with a foreign power would have far-reaching consequences for the future of NATO and the security and prosperity of the Czech Republic. Given its size and geographical location, the Czech Republic benefits greatly from the NATO security um-

[11] M. Biben, L. Prchal,'Češi posilují armádu. V plném stavu má mít 34 tisíc vojáků, vytvoření třetí brigády by vyšlo na 100 miliard' [The Czechs strengthen the army. It should reach 34 thousand soldiers, creation of a third brigade would cost 100 billion Czech Crowns], *Hospodářské noviny*, 29 November 2016, http://archiv.ihned.cz/c1-65535390-ce-si-chystaji-moderni-bojeschopnou-armadu [2016-11-29].

brella. Maintaining that umbrella should, therefore, be prioritized accordingly. However, as we have tried to demonstrate in our conclusion, this is not the case today. Therefore, the Czech Republic needs to disregard theoretical safety of its location and become more attuned to threat perception of the vulnerable eastern flank of NATO. On a practical level, this would mean enhanced military deployment along the eastern flank. This should provide the 'building blocks' on which the sense of Czech 'stakeholdership' in our shared 'eastern backyard' could be built. Only through active engagement can the Czech society begin to overcome the prevailing perception that historically their destiny was defined by big powers and that it will be the case in the future.[12]

2.2. Soft risks and threats to safety and security in the region

2.2.1. Soft risks and threats to safety and security in the region: an overall assessment

Anna Visvizi

Traditionally, soft security threats, aka new security challenges, have been associated with the non-military combat aspects of security. Several typologies sought to organize this, to organize this broadly defined spectre of risks, threats and challenges to safety and security. Accordingly, depending on the criteria employed, soft security has been defined as related to cyber security, energy security and national identity security.[13] However, it is not uncommon in the literature to argue that soft security includes such concerns as poverty and unemployment, demographic shifts, environmental degradation, resurgent nationalism and social tensions, uncontrolled migration and coerced displacement, as well as the proliferation of narcotics, crime and small arms.[14] As definitions and typologies are bound to overlap, what really matters is how risks and threats to soft security are prioritized in national security strategies and, accordingly, what actions are taken to navigate them pro-actively. Indeed, technological progress, information revolution and the resulting evolution of the nature of warfare, have opened up new theatres of combat, including those associated with soft risks and threats to safety and security. As we have only begun to comprehend

[12] 58% of the Czech respondents seem to think that defence is futile since the decisions are made by the big powers. CVVM. Source: CVVM, 'Postoje českých občanů k NATO a obraně ČR – leden 2015' [Opinions of Czech citizens towards NATO and the defence of the Czech Republic], *Press Release*, 12 February 2015, http://cvvm.soc.cas.cz/media/com_form2content/documents/c1/a7337/f3/pm150212b.pdf [2016-11-03].

[13] M. Crandall, 'Soft security threats and small states: the case of Estonia', *Defence Studies*, vol. 14, no. 1, 2014, p. 30.

[14] F. Moustakis, 'Soft security threats in the New Europe: the case of the Balkan region', *European Security*, vol. 13, no. 1–2, pp. 139–156.

the mid- and long-term implications of the soft risks and threats to security and their role in undermining the functioning of democratic societies, consensus consolidates that soft security concerns should be prioritized in our security strategies.

For the purpose of this report, the set of possible risks and threats to soft security has been narrowed down to include five specific categories that, in the view of the authors of this report, represent generic groups of issues and concerns that depict the realities of the region. These categories include:

- risks and threats related to economic and social stability;
- risks and threats related to energy supply;
- risks and threats related to propaganda/disinformation;
- risks and threats related to the spread of terrorism and extremist violence;
- risks and threats inflicted by migratory movements.

In the following sections these categories will be discussed briefly and their major security implications will be highlighted. Against this backdrop, the soft risks and threats to the security of Poland and the Czech Republic will be examined.

Risks and threats related to economic stability and economic performance of a country: Although frequently remaining only at the sublime level of discussions on security, an insight into this category of risks and threats to security is quintessential if we are to understand a country's security as well as its security strategy options and choices. Traditionally, economic security has been defined in the literature by reference to a country's ability to militarize and increase its defence and deterrence capacity.[15] However, on the wave of the constructivist turn in international relations theory, a broader understanding of economic security unfolded. Now, it includes also such issues and policy goals as the society's prosperity, well-being, access to markets, to financial and natural resources, i.e. conditions necessary for a country's growth, development and maintenance of its position on the international scene.[16] In this view, economic security and, correspondingly, risks and threats that may challenge it are fundamental in any discussion on security in the region of Central Europe, including Poland and the Czech Republic.

15 K. Żukrowska, 'Pojęcie bezpieczeństwa' [The concept of security], in: K. Żukrowska (ed.), *Bezpieczeństwo międzynarodowe. Przegląd aktualnego stanu* [International security. Review of current developments], Warszawa: IUS at TAX, 2011, p. 21.

16 J. Czaputowicz, 'Bezpieczeństwo w teoriach stosunków międzynarodowych' [Security in International Relations' theories], in: Żukrowska (ed.), op.cit., p. 96; cf. D.K. Nanto, 'Economics and National Security: Issues and Implications for U.S. Policy', *CRS Report for Congress*, 4 January 2011, Washington, D.C.: Congressional Research Service (CRS).

Threats and risks to the economic security of these two countries are a function of their membership in the EU. They are linked to their ability to catch up and converge with the more advanced EU member states in a sustainable manner. In this view, the key factors to be considered include their competitiveness level and sources of their competitiveness. Therefore, if we agree that (i) a country's economic performance and stage of development determine its ability to build its deterrence and defence capacity in the mid- and long-run and (ii) a country's economic performance is a function of its competitiveness, then (iii) a country's security is a function of innovation, innovativeness and the degree of business sophistication.[17] In this sense, macro- and micro-economic factors and policies matter for a country's ability to navigate risks and threats to its security.

From a different angle, one-off events, such as the Euro area crisis or Brexit, represent explicit risks and threats to economic security of the EU member states. The implications of the Euro area crisis for East-Central Europe, and especially for these EU members that have not adopted the single currency, have been largely neglected in the literature.[18] Nevertheless, their prolonged domestic, social and economic implications did not pass unnoticed. Today, it is the prospect of Brexit, especially in Poland – given the size of the Polish diaspora in the United Kingdom – that raises serious concerns regarding its possible future economic, social, and political implications.

Finally, from a broader international perspective, issues of international cooperation, FDI flows, and international trade, including possible losses resulting from trade restrictions and embargoes, are important in any discussion on Poland's and the Czech Republic's economic security. In other words, geoeconomics, geopolitics and international security are closely related. They acquire strategic role in times of tensions between states. The annexation of Crimea and the war in eastern Ukraine attest to that. Certainly, the exact impact and the role of the leading sources of risks and threats to economic security of Poland and the Czech Republic vary and this shall be reflected in the specific focus of respective parts of this report devoted to Poland and to the Czech Republic accordingly.

Risks and threats to energy supply and energy price shocks: Risks and threats to energy supply and energy price shocks are the two single groups of factors that define the energy security landscape in Central Europe. Energy security is understood as 'the

17 Cf. J. Stryjek, 'Economic security aspects of the potential EMU membership of Poland', *Yearbook of the Institute of East-Central Europe* (IESW), vol. 11, no. 5, 2013, pp. 47–64.

18 But, cf. A. Visvizi, 'The Eurozone crisis in perspective', *Yearbook of the Institute of East-Central Europe* (Special Issue: A. Visvizi and T. Stępniewski (eds), The Eurozone Crisis: Implications for Central and Eastern Europe), vol. 10, no. 5, 2012, pp. 13–32.

uninterrupted availability of energy sources at an affordable price.'[19] Accordingly, it is necessary to consider long- and short-term aspects of energy security, i.e. timely investments to supply energy in line with economic developments and environmental needs and the ability of the energy system to react promptly to sudden changes in the supply-demand balance.[20] Implicitly, this definition of energy security highlights its four key dimensions, such as: the availability and diversification of fuels used as well as facilities using those fuels; affordability for consumers and reduced price volatility risk; efficiency; and stewardship, i.e. protection of natural environment, communities and future generations.[21] In 2014, the energy dependency of the European Union (EU) stood at 53.4%, meaning that the EU needed to import just over half of the energy it consumed in 2014. For the Czech Republic and Poland, energy dependency in 2014 was at the level of 30.4% and 28.6% respectively. Nevertheless, in order to understand energy security prospects in both countries, it is necessary to include in the analysis more specific data on energy dependency rate per each fuel category per year. Table 1 offers an overview. Accordingly, e.g. Poland needs to import 93.1% of petroleum products it consumes, and 93.6% of natural gas it needs to meet the domestic demand over a period of one year.

Table 2: Energy dependency in Poland and the Czech Republic: in %, as a share of imports, as of 2014

	overall	petroleum products	solid fuels	natural gas
EU 28 average	53.4	87.4	45.6	67.4
Poland	28.6	93.1	-5	96.3
Czech Republic	30.4	97.6	-8.7	72

Source: The Author's compilation, based on Eurostat, Energy Dependence, http://ec.europa.eu/eurostat/tgm/table.do?tab=table&init=1&language=en&pcode=tsdcc310&plugin=1 [2016-11-06].

As discussed elsewhere in this report, the RF remains the single largest source of crude oil imports in Poland and the Czech Republic. The same applies to natural gas imports. Taking into account data displayed in Table 1, both countries are positioned in an at least uncomfortable position vis-à-vis the RF. A more detailed examination of the infrastructure networks in both countries, including the existing and non-existent infrastructure in diverse energy markets, makes this picture more complex and highlights opportunities and limitations vis-à-vis the options both countries have in

19 IEA, 'Energy security', *Topics*, International Energy Agency (IEA), http://www.iea.org/topics/energysecurity/ [2016-11-06].

20 Ibid.

21 S. Somosi, 'Energy security in Central and Eastern European countries: challenges and possible answers', *Yearbook of the Institute of East-Central Europe*, vol. 11, no. 5, 2013, p. 83.

the field of securing alternative sources of energy supply. Given the infrastructure development process underway in Europe, e.g. Nord Stream 2 and its political and strategic intricacies, energy security becomes a source of strategic concern in both countries. Overall, we identify three major areas in the field of energy security that deserve particular attention and such should be taken into consideration in discussions on energy security prospects in both countries. These include: diversification of suppliers; infrastructure development and critical infrastructure protection.

Risks and threats related to propaganda/disinformation: The war in Ukraine and the annexation of Crimea by the RF have led to the recognition that Kremlin engages in strategic and instrumental use of information for a variety of purposes. The specific case of Ukraine, much more so than the earlier cases of Chechnya wars and the aggression against Georgia in 2008, led to the emergence of a consensus that – in a similar way as during WW2 and Goebbels' propaganda, also today – the misuse and abuse of information may bear serious security-related implications. Indeed, evidence from the field suggests that:

> The EU has been the primary target of Russia's propaganda since the outbreak of the crisis in Ukraine: Brussels was blamed for orchestrating a coup d'état in a neighbouring state after failing to impose an unfavourable association agreement. However, it was not until the migration crisis that the information campaign against the 28-member state block became an undeclared information war. (…) Since then, a multitude of complementary narratives on topics such as Brexit, TTIP, the Greek debt crisis, Schengen, and migrant relocation have been employed in the anti-EU campaign.[22]

Research into the ways and methods of Kremlin's propaganda machine abound.[23] It highlights how skilfully Kremlin manipulates information via TV channels and the social media at home and abroad, thus influencing people's perceptions of the war in Ukraine, of the West, of Russia's role in Syria, of the nature of the EU embargo imposed on Russia, etc.

In a context ripe with tension and uncertainty, skilfully manipulated issues and topics, otherwise neutral, turn into a resource of conflict at the level of a community, country, region. Disinformation undermines trust and spreads doubt. As a result, di-

[22] M. Šuplata, M. Nič, *Russia's information war in Central Europe: new trends and counter-measures*, Bratislava: GLOBSEC Policy Institute, 2016, p. 5.

[23] Cf. I. Reichardt, 'Russian propaganda in the West', *Yearbook of the Institute of East-Central Europe*, vol. 14, no. 2, 2016, pp. 9–22.

alogue may be broken, consensus challenged, internal cohesion distorted, political stability affected and, as a result, resilience to other threats and risks undermined. In other words, it is necessary to view the risks and threats related to propaganda and misuse of information in a two-pronged way. On the one hand, misuse and abuse of information are themselves a source of direct, explicit threat. On the other hand, disinformation and propaganda can produce indirect and implicit risks and threats to safety and security. As their influence is silent, prone to be unrecognized, the extent of damage tends to be understood only once it is irreversible. Indeed, several voices in the debate on the EU's apparent disarray today, pinpoint the possible connection between the EU's political instability and Kremlin's comprehensive disinformation and propaganda strategy.

Outstanding issues: As risks and threats to security borne out of misuse and abuse of information by hostile agents in international affairs have become subject of debate among experts and politicians, it is time to shed light on two more related issues. We argue that these issues may in fact be as important as the initial act of disinformation and propaganda and should be prioritized in national security strategies for the sake of improving our modelling, anticipation, and early detection capabilities. These two aspects have been defined as follows:

- Regulatory, policy-making and ethical challenges and risks related to the identification of commensurate and effective measures to counter disinformation and propaganda.
- Info-phobia and its implications for our ability to objectively assess risks and threats related to information misuse and our ability to devise effective and commensurate responses to them.[24]

Risks and threats related to the spread of terrorism and extremist violence: In 2015, global terrorism continued to evolve, becoming increasingly decentralized and diffuse.[25] In 2014 alone, more than 32,000 people were killed in terrorist attacks in 93 countries.[26] A wave of terrorist attacks swept across Europe only in 2014, killing at least 274 civilians and leaving over 960 wounded.[27] Europe was exposed to foreign terrorist organizations operating out of Iraq and Syria and from foreign terrorist fighters who returned home to Europe to plot and carry out attacks. At the same

[24] For a viable strategy to counter propaganda and disinformation, cf. R. Hornik, 'A strategy to counter propaganda in the digital era', *Yearbook of the Institute of East-Central Europe*, vol. 14, no. 2, 2016, pp. 61–74.

[25] US Dept. of State, *Country Reports on Terrorism 2015*, Washington, D.C.: Bureau of Counterterrorism and Countering violent extremism, 2015, https://www.state.gov/j/ct/rls/crt/2015/257513.htm [2016-11-01].

[26] WEF, *Global Risk Report 2016*, Geneva: World Economic Forum.

[27] GLOBSEC, *GLOBSEC Intelligence Reform Initiative. Reforming Transatlantic Counter-Terrorism,* Bratislava: GLOBSEC Policy Institute, October 2016, p. 4.

time, violent extremist groups espousing left-wing and nationalist ideologies, such as the Revolutionary People's Liberation Party/Front (DHKP/C) and Kurdistan Workers' Party (PKK) in Turkey, continued to operate in Europe.[28]

In this view, terrorism and extremist violence constitute vital sources of risks and threats to safety and security in Europe. With regards to Poland, the risk of terrorism has been estimated at the medium level. It has been argued that 'Poland has no indigenous terrorism, and no known terrorist organizations have been identified operating in Poland.'[29] However, since Poland was part of the Coalition in Iraq, currently its troops participate in the succeeding mission 'Resolute Support', and finally its troops are part of the International Security Assistance Force (ISAF) mission in Afghanistan, speculations were made that Poland could become a target for terrorist operations.[30] Indeed, the official statements of the Polish MFA read:

> Poland is a country not directly threatened by terrorist attacks. But we cannot completely exclude the increased interest in Poland on the part of terrorist organizations, especially in the context of our involvement, among others, in Afghanistan. Like in the case of Poland, the threat of terrorism in Central Europe is currently low.[31]

Unlike in the case of Poland, the risk of terrorism in the Czech Republic has been set by the US State Department as relatively low.[32] 'However, the Czech Republic's open borders with its neighbours allow for the possibility that terrorist groups may enter or transit the country undetected.'[33] The Czech authorities stress that 'although the Czech territory has so far not witnessed an action that could be classified as a classic terrorist attack, the risk of such an attack persists'[34]. As the data revealed by Europol indicates:

---

28 US Dept. of State, 'Country Reports: Europe Overview', *Country Reports on Terrorism 2015*, Washington, D.C.: Bureau of Counterterrorism and Countering violent extremism, https://www.state.gov/j/ct/rls/crt/2015/257516.htm [2016-11-02].

29 OSAC, 'Poland 2015 Crime and Safety Report', United States Department of State, Bureau of Diplomatic Security, 15 June 2015, https://www.osac.gov/pages/ContentReportDetails.aspx?cid=17806 [2016-11-05].

30 Ibid.

31 MFA, 'Counter-terrorism activities of Poland', *Countering International Terrorism*, Warsaw: Ministry of Foreign Affairs, Republic of Poland, http://www.mfa.gov.pl/en/foreign_policy/security_policy/international_terrorism/ [2016-11-05].

32 OSAC, 'Czech Republic 2016 Crime & Safety Report', *Research & Information Support Centre (RISC)*, United States Department of State, Bureau of Diplomatic Security, 2 September 2016, https://www.osac.gov/Pages/ContentReportDetails.aspx?cid=19029 [2016-11-05].

33 Ibid.

34 Security Policy Department, *Strategy of the Czech Republic for the fight against terrorism from 2013 onwards*, Prague: Ministry of the Interior, 2013, p. 5, www.mvcr.cz/terorismus/soubor/nap-2013-en-pdf.aspx [2016-11-05].

> the Czech Republic, sometimes used as a transit country, reported the arrest of a Bosnian jihadist attempting to travel from Prague to Istanbul using a counterfeit passport, and a jihadist from Germany was arrested in similar circumstances.[35]

With regard to extremist violence, the data revealed by the Europol depict that Poland and Austria reported closer cooperation between neo-Nazis and football hooligans in 2015, a development flagged up by Germany already in 2014. In line with the same report, 'Poland considered that hooligans constituted a group prone to extremist ideology, which facilitates their recruitment into right-wing militias'[36]. The major challenge in this context is that right-wing extremist groups continued to have access to weapons ranging from knives to firearms. Equally important is that they receive self-defence and weapons training.

> Poland reported that in 2015 Polish nationalists participated in a military training in a camp located near Moscow, Russia. In addition, instructors of combat training schools in Russia posted on the internet that they came to Poland to set up and run military camps. The camps provided combat training, such as fighting using knives and firearms, and military tactics.[37]

In 2015, Islamophobic crimes against mosques and the Muslim community increased. Poland, for example, reported that in comparison to 2013/2014, the number of cases concerning Muslims and Muslim institutions has doubled. In March 2015, 'police in Poland arrested 13 members of the right-wing extremist group Blood & Honour, including a man accused of conspiring to burn down a mosque in Gdansk.'[38] From a different angle, in 2015, Poland reported two incidents involving the theft of radioactive sources, which are commonly used in various authorised applications in industry, medicine and research. However, 'there were no reported cases of radioactive materials being used to deliberately injure or poison people.'[39]

Risks and threats inflicted by migratory movements: In the past, debates on risks and threats related to migratory movements would highlight such issues as export

---

35 Europol, *European Union Terrorism Situation and Trend (TE-SAT) report 2016*, The Hague: European Police Office, 2016, p. 28.

36 Europol, op.cit., p. 42.

37 Loc.cit.

38 Loc.cit.

39 Europol, op.cit., p. 14.

of conflicts, drugs and terrorism.[40] Today, following a wave of terrorist attacks in Europe, in the dominant discourse on migration, an unwelcome, poignant and biased nexus was constructed that essentially blends migration and terrorism in Europe. In this sense, it is imperative that a clear distinction be made between terrorism and violent extremism, on the one hand, and people in need, i.e. refugees and asylum seekers that enter Europe[41], on the other hand. Seen in this way, migration and the likely risks and threats related to increased migratory movements sum up to national authorities' ability to manage migratory flows effectively and to integrate the newcomers in the host countries' economies. Migration, in other words, is an issue that is related to economic security and should be discussed in this context. Certainly, the specificity of the European Union and the Schengen area requires that concerted action be taken in this respect.

2.2.2. Soft risks and threats to safety and security: the case of Poland

Anna Visvizi

In line with the introductory part of this section, soft risks and threats to security constitute a growing field of concern due to their multifaceted implications for a country's military capacities, deterrence and defence capabilities, and an overall resilience to hostile incidents originating within and beyond its territory. The prioritisation of soft risks and threats to security is a function of country-specific factors. In the case of Poland, the most important interrelated soft risks and threats to security include those related to: economic and social stability, energy supply (discussed in the overall assessment section) and propaganda and disinformation.

Risks and threats to economic and social stability: The most recent Global Competitiveness Report (GCR)[42] depicts that the Polish economy, all factors included, remains a transition economy 27 years after the collapse of Communism. In contrast, the Czech Republic is considered an innovation-driven economy (see Graphs no 1 and 2 for a comparison). Certainly, at the same time, the 2016 EBRD report presents Poland as a success story. As Chart 1 (on the next page) illustrates, in Poland, unlike in

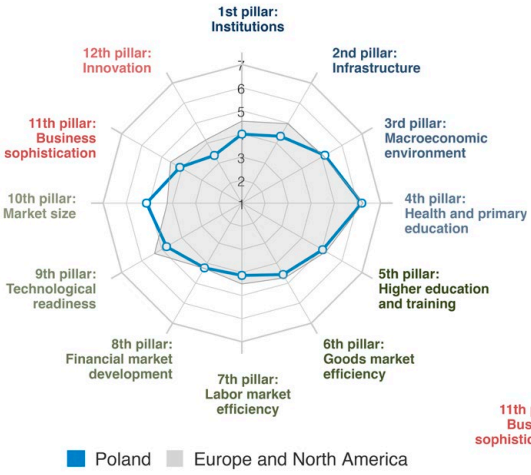
40 V. Perthes, 'Germany Gradually Becoming a Mediterranean State', *EuroMeSCo Papers*, no. 1, 1998, EuroMeSCo, http://www.euromesco.net/index.php?option=com_content&view=article&id=132%3Apaper-1-germany-gradually-becoming-a-mediterranean-state&catid=102%3Aprevious-papers&Itemid=102&lang=en [2016-10-31].

41 Cf. M. Pachocka, 'The twin migration and refugee crises in Europe: examining the OECD's contribution to the debate', *Yearbook of the Institute of East-Central Europe* (Special Issue: A. Visvizi (ed.), Re-thinking the OECD's role in global governance: members, policies, influence), vol. 14, no. 4, pp. 71–99.

42 WEF, *The Global Competitiveness Report 2016–2017*, Geneva: World Economic Forum (WEF), 2016.

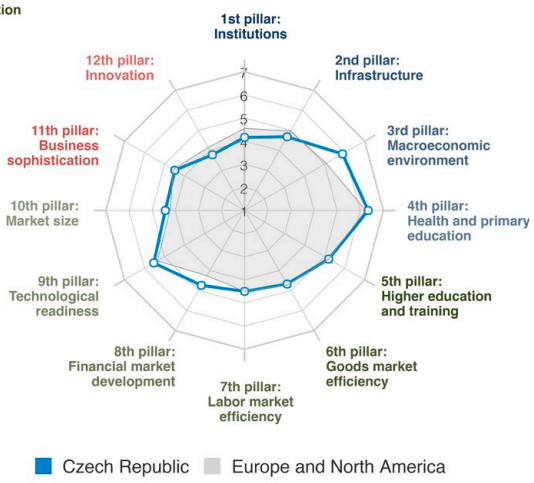
many other countries, the entire society is said to have benefited from the processes of transition and transformation and today income levels are higher than in 1989.[43]

Graph 1: Poland's competitiveness index in detail



Source: WEF, 'Country/Economy Profiles: Poland', *The Global Competitiveness Report 2016–2017*, Geneva: World Economic Forum (WEF), 2016, p. 298.

Graph 2: The Czech Republic's competitiveness index in detail



Source: WEF, 'Country/Economy Profiles: the Czech Republic', *The Global Competitiveness Report 2016–2017*, Geneva: World Economic Forum (WEF), 2016, p. 152.

This undeniable success notwithstanding, the nature of any debate on security requires identification of spots on a seemingly spotless sky, and hence anticipation of possible future risks so that likely catastrophes can be averted. It is in this context that one should interpret the findings of the GCR. Specifically, with regard to the key innovation and sophistication factors discussed in that report, including business sophistication and innovation, Poland ranks 55 and 64 (out of 140) respectively. The Czech Republic ranks 30 and 35 respectively. The major efficiency enhancing factor

[43] EBRD, 'Transition for all: Equal opportunities in an unequal world', *EBRD Transition Report 2016–2017*, London: European Bank for Reconstruction and Development (EBRD), p. 17.

in the Polish case is the size of its market. However, that factor may turn into a liability if labour market efficiency remains at today's level, i.e. 81 out of 140. Reports suggest that the Polish labour market is facing significant challenges, such as an ageing labour force, low productivity and high segmentation of the labour market. Shortcomings in the education system, identified at several levels, add to that challenge in a number of ways. One of them is its negative impact on Poland's ability to innovate and maintain, and possibly improve, its competitiveness, thus creating conditions conducive to sufficient spending and investment in Poland's deterrence and defence capacities and capabilities.

As the relative influence of traditional efficiency enhancers on maintaining a country's economic position decreases and so Poland cannot rely indefinitely on the size of its market. The prospect of Poland's sustained and sustainable growth and development depends on Poland's ability to innovate. In this context, education and the education system are crucial, similarly as regulatory frameworks that are business and investment friendly and, ideally, favour public-private partnerships that boost employment, innovation and business sophistication. In other words, Poland's economic performance and stage of development determine its ability to build its mid-term and long-term deterrence and defence capacity. Simultaneously, Poland's economic

Chart 1: Percentiles of the population with income growth above/below the G7 average, 1989–2016

Source: EBRD, 'Transition for all: Equal opportunities in an unequal world', *EBRD Transition Report 2016–2017*, London: European Bank for Reconstruction and Development (EBRD), p. 17.

performance is a function of its competitiveness. However, competitiveness today is a function of Poland's ability to innovate rather than rely on cheap labour or market size. What follows is that Poland's deterrence and defence capacities are a function of its ability to innovate. The urgency to innovate fast, to innovate smart, and to innovate effectively is apparent in the EU today, similarly as it is in Poland. Time will show if Poland will succeed in closing the innovativeness gap and thus improve its ability to effectively manage risks and threats to its security.

From a different vantage point, one-off events, such as Brexit, for instance, constitute an important source of risks and threats to economic and social stability and hence, though indirectly, have a bearing on Poland's safety and security. Brexit, should it happen, creates similar challenges to all V4 members, i.e. uncertainty related to the legal status of V4 nationals employed in the UK; possible future pressures on home country labour markets, if today's emigrants return, and their socio-economic implications; decrease in remittances, e.g. only in 2015 the value of remittances sent home by Polish and Czech workers in the UK amounted to 1,144 million USD and 209 million USD respectively. This makes ca. 1.4% and 1.5% of GDP 2015 in both countries respectively. [44]

Risks and threats related to propaganda/disinformation: Compared to the scope and scale of Kremlin's propaganda and disinformation activities in the Baltic States, the influence of Kremlin's propaganda in Poland is limited. In the Baltic States, a considerable share of the population is fluent in Russian and a sense of loyalty and affiliation to the USSR is still discernible in certain groups of the society. As those channels of influence have essentially no bearing in Poland, the objectives and methods of Kremlin's disinformation activities are arguably less direct in this country. Accordingly, rather than convincing the audience of Putin's righteousness and the necessity to fight with the West, '[t]he goal of the Russian propaganda aimed at Poland is social disintegration... Russia promotes toxic memes that do not create new messages, but aim to accentuate existing tensions and divisions in the Polish society.'[45] Given the size of the population and the depth of the media market, Kremlin's propaganda tends to target 'fringe audiences – both far left and far right'[46].

[44] World Bank, 'Migration and Remittances Data', *Brief*, 24 September 2016, https://www.worldbank.org/en/topic/migrationremittancesdiasporaissues/brief/migration-remittances-data [2016-11-11].

[45] E. Lucas, P. Pomeranzev, 'Winning the Information War: Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe', *CEPA/Legatum Institute Report*, August 2016, Washington, D.C.: Center for European Policy Analysis (CEPA), p. 30.

[46] Ibid.

Apart from trolling in the social media, the tools of influence attributed to Kremlin's disinformation activities were based on libel and/or historical provocations. In this vein, Poland accused of military intervention in Ukraine, of 'Eastern imperialism' and historical revisionism. Negative assertions against high-profile figures of Polish political life were made in the press, presumably destined to spread doubt and ignite unhealthy political gossip seen as a part of a larger strategy of manipulating with people's minds and hearts. Historical provocations in the press were equally common. Here, the most frequently used was the reference to the 'Volyn massacre', the 'Katyn Woods massacre' and the 'Polish concentration camps', all references unequivocally changing and distorting the merit of Poland's tragic history and suffering it endured from the Soviet Union. From a different angle, and away from instrumental use of historical memory and historical policy, Kremlin's activities also sought to influence Russian public opinion against Poland in the fields of trade and economic cooperation. For instance, in a series of 'hot news' on Poland's alleged attempts to smuggle to Russia certain products, the credibility of Polish companies and the quality of their products were undermined.

The intensity of Kremlin's engagement in the Polish infosphere has evolved over the past years. A case could be made that a positive relationship exists between their intensity and the electoral cycle. Similarly, debates on issues such as CETA and the U.S. elections seemed to awaken otherwise dormant 'known-unknowns' in the social media and in the fringe electronic press outlets. The influence of Kremlin's engagement in the Polish infosphere should not be underestimated. Even if the direct impact of disinformation and propaganda seem to be limited in Poland, information warfare constitutes an important component of a larger strategy of Russia against the West. Indeed, one could argue that since direct military aggression against Poland is not an option, Kremlin will place greater emphasis on its propaganda and subversion aimed at weakening Poland and the resilience of its society. In this context, elements of disinformation and psychological warfare were employed in some parts of Poland as a means of reviving conflicts in local communities.

2.2.3. Soft risks and threats to safety and security: the case of the Czech Republic

Luděk Jiráček

Following the collapse of the Iron Curtain in 1989, the Czech establishment intensively supported the U.S. engagement in Europe, which was considered at that time as a fundamental strategic interest of the Czech Republic. Essential conditions of building

a new security system included the withdrawal of Soviet troops from Central Europe, leaving the Warsaw Pact and becoming a member of the Euro-Atlantic institutions.[47] Moreover, the transformation process focused on economic reforms when our centrally planned system shifted into a market economy. All of the changes and reforms had impact on security interests, priorities and threats.

The Czech Republic's ability to independently respond to the threats has been reducing, and it has become dependent on multilateral mechanisms and cooperation within NATO and the EU. In the globalized world, security interests and threats do not end at the Czech border. Soft security threats in the Czech Republic can most often be associated with interference by allied nations. The main security threats in the Czech Republic are published in the Security Strategy of the Czech Republic. Currently, the main soft security threats are interruptions of energy industries, propaganda and migration.[48]

Risks and threats related to economic stability and energy supply: The first category of threats influencing Czech stability are of economic nature. The main activities of individuals who are linked to power interest of other states are likely of Russian and Chinese origin. Many of these activities are connected with the activities of their intelligence services. The Security Information Service of the Czech Republic classified their counterintelligence activities as successful, especially in the area of energy security and Chinese influence in Czech politics and economy.[49]

Russian energy policy, and in particular, energy diplomacy, is one of the most powerful threats. It is not only a threat to countries of the former Soviet Union, but also to all European countries (stopping oil and gas supplies to Europe). It has also been used as a mechanism to maintain the stability of Putin´s regime. On the other hand, with current economic problems and lower value of the gas, this threat has been limited in the case of the Czech Republic.[50]

47 J. Glenn (ed.), *Česko-americké vztahy: jak dál?* [Czech-American Relations: A Roadmap for the Future], Prague Centre for Transatlantic Relations (PCTR), Prague: CEVRO Institut, 2015, pp. 10–11.

48 Ministry of Foreign Affairs of the Czech Republic, *Security Strategy of the Czech Republic*, Prague, 2015, p. 13.

49 BIS, *Annual Report of the Security Information Service for 2015*, Security Information Service (BIS), Intelligence Service of the Czech Republic, Prague, http://bis.cz/vyrocni-zpravaEN890a.html?ArticleID=1104 [2016-10-15].

50 L. Tichý, 'Ruská energetická politika a (ne)bezpečnost EU' [Russian energy policy and EU (in)security], *Natoaktual.cz*, 25 May 2009, http://www.natoaktual.cz/ruska-energeticka-politika-a-ne-bezpecnost-eu-fa7-/na_analyzy.aspx?c=A090525_132323_na_analyzy_m02 [2016-10-15].

In total, 75% of gas is supplied to the Czech Republic directly from the Russian Federation, but almost 50% of primary energy consumption is covered by domestic sources.[51] However, the Czech Republic is ranked among the countries with the largest share of nuclear energy to generate electricity; still nuclear fuel is imported only from the Russian Federation.[52] For this reason, the Czech energy policy should focus on trading nuclear and other energy resources from supplier nations, which are more predictable, stable, and non-authoritarian. The Russian Federation cannot be perceived as a reliable supplier because the suspension of the gas stream was not connected to technical problems but to political decisions (interruption of oil supplies from Russia to the Czech Republic occurred in 1990, 1991, 1994, 1995, 1996, 2007, 2008 and 2009).[53]

Chinese economic and political activities have become more and more apparent. In fact, the activities have an increasingly stronger influence on Czech politics and state structures. During the last meeting between the presidents of China and the Czech Republic were signed contracts worth 8.53 billion Euro (for the period 2016–2020).[54] The main issue is that most of these investments, as is the case of those in Poland, could lead to mergers and acquisitions of industries which do not create any new factories within the nation. They obtain access to technological advancements and processes, new distribution channels, and other exclusive accesses. In the case of the Czech Republic, investments are considered as strategic projects to increase influence in the region.

Dr. Raska, Research Fellow in the Military Transformations Program at the S. Rajaratnam School of International Studies in Singapore, stated that China needed energy sources, food sources and access to high-end technologies. Dr. Raska stated that China had always tried to gain power through economic clout and the Czech Republic was seen as the weakest element in the European Union. From economical point of view,

51 Ministry of Industry and Trade, *Aktualizace Státní energetické koncepce České republiky* [Update of the Czech Republic's State Energy Policy], Prague: Ministry of Industry and Trade of the Czech Republic, 2014, http://download.mpo.cz/get/52041/59168/618616/priloha001.pdf [2016-11-04], p. 12.

52 World Nuclear Association, 'World Nuclear Power Reactors & Uranium Requirements', *Facts & Figures*, http://www.world-nuclear.org/information-library/facts-and-figures/world-nuclear-power-reactors-and-uranium-requireme.aspx [2016-10-15].

53 T. Vlček, F. Černoch, *Energetický sektor České republiky* [The Energy Sector of the Czech Republic], Brno: Masaryk University, 2012, p. 185.

54 Pražský hrad [President of the Czech Republic], *Ekonomické dohody podepsané při příležitosti cesty prezidenta ČLR do ČR* [Economic agreements Signed during the State Visit of the President of the PRC in the Czech Republic], https://www.hrad.cz/file/edee/2016/03/seznam-dohod.pdf [2016-10-15].

the investments in the Czech Republic do not make any sense but through the Czech Republic and strategic projects, China wants to increase its influence in the region.[55]

Russian information and political operations: Russian propaganda is another tool which works against the stability of the Czech Republic and NATO. One of their strategies to achieve such instability is to convince the majority that the political and media establishment acts against its own citizens (social disintegration). Moreover, they are trying to undermine the confidence in democratic values and Western institutions, such as NATO and the EU. At the same time, the operations should create an impression which promotes Russian ideologies. As Ivana Smolenova from PSSI mentioned: 'When the space for a democratic, public discourse and open society is broken down, a society becomes atomized and is easier to manipulate through a policy of divide and conquer.'[56]

In the Czech Republic, Russian propaganda has been using a few streams: (1) Pro-Russian news portals; (2) radio broadcasts; (3) blogging; (4) trolls in discussions; (5) activities on social networks; and (6) organization of public events.[57] In the Czech Republic there are at this time approximately 30 Russian propaganda websites and it is quite typical that their ownership structure and financing are unclear.[58]

Strong Russian information operations in the Czech Republic are officially confirmed by Security Information Service in the Czech Republic. In fact, these operations are quite successful, because they influence Czech political leaders. Some of them use alternative media and Russian communication channels as official sources, and so they legitimize them. One of such examples is the Czech President Milos Zeman, who criticized the anti-Russian sanctions. He is known as the person who makes pro-Kremlin statements; his spokesman Jiri Ovcacek used the Sputnik website as a source for his shared articles on his personal Facebook account.

Russia also supports political parties and NGOs which influence the Czech society. It can be, for example, visible in a public opinion from 2016, where 24.5% of Czechs

55 M. Raska, 'Is China a Threat to the World Order or Guarantor of Stability?', *Public Lecture*, 3 November 2015, Prague Centre for Transatlantic Relations (PCTR), https://www.youtube.com/watch?v=WEtkJ6WQgBo [2016-10-15].

56 Lucas and Pomeranzev, op.cit., p. 30.

57 I. Smoleňová, *The Pro-Russian Disinformation Campaign in the Czech Republic and Slovakia*, Prague: Prague Security Studies Institute (PSSI), June 2015, p. 4.

58 CTK, 'Stropnický: Ruské dezinformace. Filip: Není důvod se bát' [Stropnicky: Russian disinformation. Filip: There is no reason to be afraid], *Týden.cz*, 27 November 2016, http://www.tyden.cz/rubriky/domaci/stropnicky-ruske-dezinformace-filip-neni-duvod-se-bat_407386.html [2016-11-28].

trust disinformation media more than factual ones. It can be noted that 38% of the population believe that the Ukraine crises were caused by US and NATO, and 50.2% of Czechs believe that US are responsible for Syrian refugees coming to Europe.[59] The migrant crisis is currently one of the most powerful exploitations of media for Russian propaganda used against European institutions.[60]

The main issue in the Czech Republic is that the Government is not reacting accordingly against the increasing threat of Russian propaganda. For example, it is impossible to find any official propaganda´s database, where it could be possible to find persons or medias known to destabilize democratic and liberal systems within the Czech Republic. Many Czech NGOs try to fight against Russian propaganda and inform the society about this threat. However, only 40% Czechs trust NGOs (only 5% of them definitely trust them).[61] However, the Ministry of Interior of the Czech Republic plans to open a new Centre against Terrorism and Hybrid Threats in January 2017. The centre is expected to include a team focusing on countering propaganda.[62]

Risks and threats inflicted by migratory movements: The migration crisis has become a soft security threat based around the current immigration of refugees and illegal immigrants, which has been increasing due to armed conflicts and wars in the Middle East and Africa. It has been a source of social tension and has led to the radicalization of various ethnic groups. Currently, the most strategic powers of the migration crisis are held by Russia and Turkey.

The EU and Turkey signed a plan for the coordination of actions against the migration across Turkish borders (exchange for financial support and abolition of visas). However, Turkish President Recep Tayyip Erdogan has used the migration crisis as a leverage in negotiations and his tactic is unpredictable. There is chance that Turkey will organize and support the migration process to the European continent. Russia's growing presence in Syria, and the consequences itself, is part of a geopolitical strategy – to ensure an impact in the Middle East, to destabilize the EU, and to use

59 J. Janda, M. Blažejovská, J. Vlasák, 'Impact of Disinformation Operations in the Czech Republic', *Kremlin Watch Report*, 9 March 2016, Prague: European Values Think-Tank, http://www.europeanvalues.net/wp-content/uploads/2016/09/Impact-of-disinformation-operations-in-the-Czech-Republic.pdf [2016-10-15].

60 T. Wesolowsky, 'Kremlin Propaganda in Czech Republic Plays Long Game to Sow Distrust in EU', *RFERL*, 16 June 2016, http://www.rferl.org/a/czech-kremlin-propaganda-plays-long-game-sow-eu-distrust/27802234.html [2016-10-15].

61 CVVM, 'Trust to Some Public Institutions – September 2016', *Press releases*, Prague: Public Opinion Research Centre (CVVM), http://cvvm.soc.cas.cz/en/other/trust-to-some-public-institutions-september-2016 [2016-10-15].

62 Ministry of Interior of the Czech Republic, Centrum proti terorismu a hybridním hrozbám [Centre against Terrorism and Hybrid Threats], http://www.mvcr.cz/terorismus/clanek/centrum-proti-terorismu-a-hybridnim-hrozbam.aspx [2016-11-30].

the migration crisis to distract attention from the Ukrainian crisis. The migration crisis is going to be an endurance test for all European countries, not only for the Czech Republic. Consequently, NATO declared to start with the maritime Operation Sea Guardian, which should stop or reduce the flow of irregular migration in the Aegean Sea. The plan also includes support of the EU in intelligence, surveillance and reconnaissance, and logistics.[63]

Generally, the Czech Republic is not directly and deeply affected by the current crisis but more by situations in partnered countries which influence the behaviour and the priorities of the Czech politicians and civil society. The Czech Republic is on the edge of a secondary migration stream to Western Europe and it has been more used as a transit country. As it was mentioned above, the crisis is used in information operations that can lead to a radicalization of the society and an increase of the role of populist parties and leaders in the Czech Republic. The Czech government has reacted to the crisis by increasing financial aid, and providing experts and material assistance to countries affected by the crisis. The government has sent security forces to Hungary, Slovenia and FYROM.[64]

2.3. Cyber security risks and threats

2.3.1. Cyber security: an overall assessment

Anna Visvizi

As the intensity of risks and threats that unfold in the cyber space accelerates and the cost of their likely implications multiplies, it is necessary that cyber security be continuously rethought and that flexible approaches to managing it be developed at local, regional, national and international levels. The urgent need to undertake action in this field has been prompted by a series of incidents as a result of which national-level stakeholders were affected. The most spectacular incidents of this kind involved the 2007 distributed denial of service (DDoS) attacks against Estonia; the 2008 attack against Georgia and the government servers and, quite recently, the December 2015 cyber attack-inflicted power failure that hit the Ivano-Frankivisk re-

63 NATO, 'Warsaw Summit Communiqué', *Press Release* (2016) 100, 9 July 2016, http://www.nato.int/cps/en/natohq/official_texts_133169.htm [2016-10-15].

64 Ministry of the Interior of the Czech Republic, 'ČR vyšle do Makedonie a Maďarska celkem 90 policistů k ochraně hranic před migrační vlnou' [Due to a migration wave, the Czech Republic will send 90 policemen to protect borders in Macedonia and Hungary], *Press Release,* 27 July 2016, http://www.mvcr.cz/migrace/clanek/cr-vysle-do-makedonie-a-madarska-celkem-90-policistu-k-ochrane-hranic-pred-migracni-vlnou.aspx [2016-10-15].

gion in the western Ukraine. In April 2015, the French TV network TV5Monde was attacked. As a result, for 18 hours its original broadcasts were replaced with a black screen, whereas jihadist propaganda messages were displayed on the station's website and Facebook and Twitter accounts.[65] The June 2016 DDoS attack against the ground computer system of Polish LOT affected more than 1,400 passengers, with 10 flights cancelled and another 12 delayed.[66]

Other high-profile targets of cyber attacks in 2015, this time in the form of cyber espionage, included the White House, the Pentagon, the German Bundestag, and the US Government's Office of Personnel Management. Reportedly, the latter 'lost 21.5 million personnel files, including sensitive information such as health and financial history, arrest records, and even fingerprint data.'[67] In February 2015, 78 million patient records were exposed in a major data breach at Anthem, the second largest healthcare provider in the US.[68] This case reveals plainly that drawing and securing borders in cyber space is virtually impossible and so attacks seemingly unrelated to state-administration may have national safety and security implications. The 2010 cyber espionage 'Operation Aurora' as a result of which 20 high-profile targets, including Google and Adobe were compromised attests to that.[69] Hostile disruptions of satellite communications represent a new and rapidly growing area of concern in that their implications are inherently global and the number of countries that join the 'satellite club' increases; so are the corresponding risks and threats.[70] Over the past years, a group frequently referred to as TURLA, has been 'exploiting commercial satellites to siphon sensitive data from diplomatic and military agencies in the US and in Europe as well as to mask their location'[71]. Distortions of GSP time signals, related to hostile

65 J. Lichfield, 'TV5Monde hack: 'Jihadist' cyber attack on French TV station could have Russian link', *Independent*, 10 June 2015, http://www.independent.co.uk/news/world/europe/tv5monde-hack-jihadist-cyber-attack-on-french-tv-station-could-have-russian-link-10311213.html [2016-11-01].

66 BBC, 'Polish LOT Aeroplanes Grounded by Computer Hack', *BBC*, 21 June 2016, http://www.bbc.com/news/world-europe-33219276 [2016-11-01].

67 Symantec, 'Internet Security Threat Report', vol. 21, April 2016, Mountain View, CA: Symantec, pp. 37–38.

68 Ibid., p. 39.

69 B. Koerner, 'Inside the Cyberattack That Shocked the US Government', *Wired*, 23 October 2016, https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/ [2016-11-01].

70 D. Housen-Couriel, 'Cybersecurity threats to satellite communications: Towards a typology of state actor responses', *Acta Astronautica*, vol. 128, November-December 2016, pp. 409–415.

71 E. Nakashima, 'Russian hacker group exploits satellites to steal data, hide tracks', *The Washington Post*, 9 September 2015, https://www.washingtonpost.com/world/national-security/russian-hacker-group-exploits-satellites-to-steal-data-hide-tracks/2015/09/08/c59fa7cc-5657-11e5-b8c9-944725fcd3b9_story.html [2016-11-13].

attacks, have been reported in 2016.[72] Links between Da'esh and their ability to use the satellites have been reported in the press.[73]

It is difficult to estimate precisely the scale of cyber attacks as many of cyber attacks pass either unnoticed, unreported or mistakenly taken as originating elsewhere. The Ivano-Frankivisk power-failure incident suggests as well as the time-span of a given cyber attack and the range of losses that it induced may be underestimated. The post-ante examination of that event revealed that this 'multi-pronged cyber attack (…) not only disabled power in eight provinces in the region, but also masked the activity of the attackers' throughout the duration of the attack.[74] In other words, the attackers were able to control the event and inhibit the authorities' response beyond the point it was pinpointed as an actual cyber attack.[75] Regardless of the challenges related to data collection, estimates of the scale and nature of hostile cyber attacks exist. These place the business sector and the state-administration as the key targets of cyber attacks.

The data suggest that in 2015 a record-setting total of nine mega-breaches were reported, whereby a mega-breach is defined as a breach of more than 10 million records. The total reported number of exposed identities jumped 23 percent to 429 million. At the same time, however, an increasing number of companies chose not to reveal the full extent of the breaches they experienced. Companies choosing not to report the number of records lost increased by 85 percent in 2015. Overall, 'a conservative estimate by Symantec of those unreported breaches pushes the real number of records lost to more than half a billion.'[76] Certainly, cyber security is not limited to cyber espionage or cyber sabotage. Risks and threats to cyber security should be seen as part and parcel of modern warfare where conventional modes of combat are complemented by new ones. Nevertheless, given the fact that ICT is indispensable for modern conventional means of warfare, questions of risks and threats to cyber safety and security acquire predominant role in any discussion on contemporary warfare. In this view there is an urgent need to endow these risks and threats with a corresponding priority in national-level security strategies and security doctrines across the Alliance.

72 C. Baraniuk, 'GPS errors caused '12hours' of problems for companies', *BBC News*, 4 February 2016, http://www.bbc.com/news/technology-35491962 [2016-11-13].

73 N. Kwasniewski, 'How Islamic State Takes Its Terror to the Web', *Spiegel Online*, 4 December 2015, http://www.spiegel.de/international/world/islamic-state-uses-satellite-internet-to-spread-message-a-1066190.html [2016-11-01].

74 Symantec, op.cit., p. 46.

75 Loc.cit.

76 Ibid., p. 6.

The spectre of hostile events' options in the cyber space is vast and depending on the criterion of assessment can be divided into several categories. The practical implication of devising a typology of cyber security risks and threats is that it bears direct implications (i) for the assessment of their relative importance in the overall security assessment; and (ii) for the specific policy tools and measures that will be employed to address them. Accordingly, a focused literature review allows to devise the following typology of cyber space related risks and threats to (national) safety and security:

Depending on who is attacking:

- cyber criminals (cyber crime);
- industrial competitors and foreign intelligence services (cyber industrial/white espionage);
- hackers (cyber vandalism); hacktivists (cyber activism);
- employees, or those who have legitimate access (cyber accidents, cyber misuse)[77];
- rouge-states-related actions (cyber terrorism, cyber sabotage).

Depending on the nature of the hostile attack:

- un-targeted attacks (phishing, water holing, ransomware, scanning);
- targeted attacks (spear-phishing, deploying a botnet – to deliver a DDOS; subverting the supply chain – to attack equipment or software being delivered to the organization).

Depending on the tools/capabilities employed:

- commodity capability related attacks[78];
- bespoke capability related attacks[79].

77 CERT-UK, 'Common Cyber Attacks: Reducing The Impact', London: GCHQ and CERT-UK, p. 4, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf [2016-11-01].

78 'Commodity capability' involves tools and techniques openly available on the Internet (off-the-shelf) that are relatively simple to use. This includes tools designed for security specialists (such as system penetration testers) that can also be used by attackers as they are specifically designed to scan for publicly known vulnerabilities in operating systems and applications. Poison Ivy is a good example of a commodity tool; it is a readily available Remote Access Tool (RAT) that has been widely used for a number of years.

79 'Bespoke capability' involves tools and techniques that are developed and used for specific purposes, and thus require more specialist knowledge. This could include malicious code ('exploits') that take advantage of software vulnerabilities (or bugs) that are not yet known to vendors or anti-malware companies, often known as 'zero-day' exploits. It could also include undocumented software features, or poorly designed applications. Bespoke capabilities usually become commodity capabilities once their use has been discovered, sometimes within a few days. By their very nature, the availability of bespoke tools is not advertised as once released they become a commodity.

Depending on the subject of the hostile attack:

- state-actors, incl. public administration and critical infrastructure;
- businesses, incl. insurers, financial institutions, and production facilities;
- individuals.[80]

Further distinctions could be outlined. The point remains, though, that any attempt at devising a typology of cyber space-related risks and threats faces definitional challenges which resonate in the academic literature on the subject and perhaps more importantly in national legislatures around the world. What matters, therefore, is not only how cyber threats have been defined in national legislation but also how matters of cyber security have been prioritized in national security assessments and corresponding strategies. A 2013 RAND study offers a very interesting overview of these issues suggesting, for instance, that 'the Estonia Cyber Security Strategy is unique in rejecting cyber warfare, cyber crime or cyber terrorism divisions, and instead focuses on the chosen effects of'[81] attacks distinguishing between attacks on critical information infrastructure and cyber crime. This way of conceiving of cyber safety and security results in a holistic approach and a strategy to cyber space management in Estonia, whereby the recommended measures include the private/civil sectors, on regulation, education and cooperation.[82] The latter observation is particularly relevant in discussions on securing cyber safety and security across the system, i.e. beginning at the level of an individual user through the business sector, state-administration, critical infrastructure and to military facilities and operations. Education is particularly important in socializing with the base-line cyber security hygiene, whereby research suggests that many cyber accidents could have been easily prevented had the individuals responsible for a given point of entry been more vigilant.[83] From a different angle, inasmuch as cooperation is important, so is the interoperability of systems located at diverse levels of the cyber space. In the context of NATO and the emerging consensus on the need to pre-empt, deter and address cyber borne risks and threats to safety and security, three interrelated issues should be highlighted. These included:

- interoperability of NATO member-states national cyber security systems;
- complementarity of cyber security risk assessments and the resulting prioritization of risks and threats;

80 CERT-UK, op.cit., p. 4.

81 N. Robinson, L. Gribbon, V. Horvath, K. Robertson, *Cyber-security threat characterisation: a rapid comparative analysis*, RAND Europe, Santa Monica: Rand Corporation, 2013, pp. 13–14.

82 Ibid., p. 14.

83 Ł. Wojciechowski, 'Information Security Policy as InfoSec instrument in the Polish local government system', *Yearbook of the Institute of East-Central Europe*, vol. 14, no. 2, 2016, pp. 75–94.

- complementarity of cyber security strategies and management and implementation structures.

That being said, it is important to stress that cyber space, cyber safety and cyber security are conditioned by the tangible infrastructure and its capacity, including cables, servers, routers, satellites, etc. In other words, cyber security is inseparable from the underlying infrastructure and our capacity to manage it effectively, securely and independently from potentially hostile actors. In the context of contemporary threats that – in line with the Warsaw Summit Communiqué – have been identified as more or less Russia and Da'esh, the question of cyber security translates into the question of who has better infrastructure capacity and who manages it more skilfully.

Consensus prevails among specialists in the field, that the US has the most advanced infrastructure capacity, including cables, servers, and satellites and an overall high-tech advantage. Nevertheless, given their relative underinvestment, the Russian army may have an advantage in the field of the application of commodity and bespoke capabilities. In other words, where the US has access to infrastructure and equipment, the Russian army is faster in adapting to urgent needs using appropriate software and other means. In this view, some experts suggest as well that the US technological superiority and upper hand in infrastructure capacity notwithstanding, in a war on points the US and Russia may, in fact, strike a balance. In this context, what really matters is that NATO members build up their infrastructure capacity and improve the interoperability of their cyber security systems. This requires concerted effort in the processes of devising national security assessments and strategies, defining the nature and relative priority of cyber space risks and threats and corresponding measures to address them. Finally, it also requires that a culture of transparency and effective information sharing across the Alliance is developed. The Warsaw NATO Summit and the Cyber Security pledge may have been the most important step in just that direction.

Outstanding issues: Cyber space and cyber security form a growing field of concern at diverse levels of policy-making and implementation and safeguarding our societies from cyber-borne hostile incidents of diverse origin. Whereas the majority of them have been already discussed briefly, it is important to highlight the following outstanding issues:

- The Snowden case reveals that at the level of the legislature and, subsequently, at the policy-making process careful consideration needs to be given to the specific tools employed to address the cyber-borne risks and threats to safety and security of our societies. In other words, a balance needs to be stroke be-

tween measures aimed at pre-empting possible hostile incidents, e.g. surveillance, and addressing the actual threats. As discussed in the methodological part of the report, the distinction between safety and security and risks and threats accordingly may be of use in this respect.[84]

- Increasingly, reports suggest the cost of entry to cyber space and cyber-borne hostile activities has decreased substantially over the past years. A recent report by Interpol highlights that the proliferation of cyber crime has been matched with the development of a professional, service-based underground economy, which, in turn, enables criminals to engage in illegal activities ranging from concealing their illicit actions through identities and money laundering activities, to purchasing firearms and explosives.[85] Certainly, as the report concludes, these phenomena bear significant implications for terrorism and our ability to curb it. In a similar fashion, the lowering of the cost of entry to the cyber space, the availability of underground service economy, increased 'commodity ability' of certain individuals and the falling cost of basic equipment shed light on the emerging challenge of cheap cyber guerrilla warfare.
- Finally, the versatility of means, measures and techniques employed to conduct cyber attacks may, in fact, pose limits to our ability to safeguard cyber space.[86] The more important it becomes to improve our ability to model, anticipate and avert possible future risks. In this context, there is a need to develop threat modelling and risk assessment techniques apt to meet the challenges of modern warfare, including the cyber space.

2.3.2. The 'cyber security ecosystem' in Poland

Joanna Świątkowska

Currently there are two main strategic documents that refer to the general organization of the cyber security system in Poland, namely:

- the 2013 *Cyber Space Protection Policy of the Republic of Poland*[87], prepared by the Ministry of Administration and Digitization (MAD) and Internal Security Agency (ISA); and

84 Cf. E.G. Boussios, 'Termination or Accountability? The Controversy over the United States' Use of Cyber Intelligence', *The Polish Quarterly of International Affairs,* vol. 25, no. 2, 2016, pp. 35–44.

85 Europol, op.cit.

86 R. McMillan, J. Valentino-Devries, 'Russian Hacks Show Cybersecurity Limits', *The Wall Street Journal*, 2 November 2016, http://www.wsj.com/articles/russian-hacks-show-cybersecurity-limits-1478031535 [2016-11-02]; Reuters, 'UK spy chief sees growing threat from Russian cyber-attacks, espionage', *Reuters*, 1 November 2016, http://www.reuters.com/article/us-britain-security-russia-idUSKBN12W3PJ [2016-11-01].

87 Ministry of Administration and Digitisation/Internal Security Agency, *Cyber Space Protection Policy of the Republic of Poland*, Warsaw, 25 June 2013.

- *Cyber Security Doctrine of the Republic of Poland*[88], prepared by the National Security Bureau.

The *Cyber Space Protection Policy of the Republic of Poland* is the key document and includes the most important provisions on the division of roles and responsibilities within the system. MAD is already working on a new version of Poland's Cyber Security Strategy. Its draft version has been released in February 2016 and is publicly available. For this reason, in the author's view, it should be used as the guideline to understand how the Polish system works.

In general, the key role in the cyber security framework of Poland plays MAD. The MAD holds the main strategic, political and coordinating functions. Among other issues, it provides legislative impulses, builds private-public cooperation, leads international processes related to cyber security which at present involve mainly the implementation of the 2016 EU Network and Information Systems Directive (the NIS Directive)[89], and oversees the work of the National Cyber security Center. To sum up, MAD is the key strategic actor within civilian area of cyber security in Poland.

Discussing cyber security in civilian sphere, the role of law enforcement agencies and the justice system must be acknowledged. The main responsibility of the Polish Police and Polish prosecutors is to counteract cyber criminal activities and the use of Internet by terrorist groups. The last task is also performed by the ISA.

Ensuring cyber security requires that a well-functioning incident response mechanisms be in place. The Governmental Computer Security Incident Response Team (GCSIRT)[90], cooperating within ISA, acts as the primary computer security response team in the area of government administration. In addition, it provides assistance to the critical infrastructure operators. Apart from GCERT, the key responsibility in the area of incident response rests with the national CSIRT which works within the Research and Academic Computer Network (NASK), currently supervised by MAD.

From the strategic point of view, the main actor in the field of critical infrastructure protection is the Government Centre for Security (GCS). GCS prepares *National Crit-*

88 National Security Bureau, *The Cyber Security Doctrine of the Republic of Poland*, Warsaw: National Security Bureau (BBN), 22 January 2015.

89 European Parliament and the Council, *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*, OJ L 194/1 [2016-07-19].

90 www.cert.gov.pl.

ical Infrastructure Protection Programme. The Document sets overall priorities, actions and responsibilities for different stakeholders. In terms of relations with critical infrastructure owners and operators, including also the private ones, it sets a non-regulatory approach.

An important part of the Polish cyber security landscape is the Office of Electronic Communications. In line with the existing legal framework, operators and service providers must notify the President of the Office of Electronic Communications about breaches of security or integrity of the network as well as of services that had significant impact on the operation of networks or services.

Finally, discussing cyber security, it is necessary to highlight the challenge of data protection. The Inspector General for Personal Data Protection (GPDP) plays the central role in terms of protection of data and privacy in Poland. The key responsibility of this institution is to supervise and ensure compliance of data processing along with the provisions on the protection of personal data[91]. This also applies to data processed in cyber space. As a consequence of this year's adoption of the General Data Protection Regulation, the role of GPDP will increase.

According to the draft of Cyber Security Strategy for Poland, civil area of cyber security must be clearly distinguished from the military area where the MOD plays crucial role. In the military, the role of CERT is performed by the Departmental Centre for Security Management of ICT Networks and Services; important activities are performed by the National Centre for Cryptology.

The *Cyber Security Doctrine of the Republic of Poland* prepared by the National Security Bureau is the second crucial document in the area of Polish cyber security. It identifies the main threats stemming from cyber space. It mentions mainly cyber crime understood as 'cyber violence, destructive cyber protests and cyber demonstrations', attacks against telecommunications systems important for national security, data and ID theft, and private computers' hijacking. External threats enumerated by the document include: cyber crises and cyber conflicts, cyber war, as well as cyber espionage involving states and other entities. The document points out that 'threats (for Poland) coming from cyber space include extremist, terrorist and international criminal organizations whose attacks in cyber space can have ideological, political, religious,

[91] Marszałek Sejmu, 'Ustawa o ochronie danych osobowych' [Law on Personal Data Protection], *Dziennik Ustaw* 2016 r. poz. 922 [Official Journal 2016 r. item 922].

business or criminal motivations'[92]. Interestingly, the document underlines the need for 'pursuing active cyber defence, including offensive actions in cyber space, and maintaining readiness for cyber war'[93] protection and defence of Polish ICT systems and data, and supporting crucial private firms.

2.3.3. Cyber security threats: the case of the Czech Republic

Luděk Jiráček

The development of new technologies has moved conflicts from a conventional level to a cyber level. Due to its asymmetry, the actors (state/non-state) are capable of causing damage to critical infrastructures, causing destabilization of the Czech society without the use of conventional weapons. However, the history of cyber security in the Czech Republic is not old. For the first time in history, protection of critical infrastructure and combating cyber crime was mentioned as one of the priorities in the Security Strategy in 2003, oriented on the intellectual property protection and personal security. 8 years later, i.e. in 2011, the Czech government classified the cyber security threat as one of the main threats which could constitute a new form of warfare.

Today, cyber security is included not only in the Security Strategy, but also in the Concept of Population Protection and in the White Paper on Defence of the Czech Republic. In line with the Decision no 781 of the Czech government from October 19, 2011, the National Cyber Security Centre (NCSC) for prevention of cyber attacks was established. Cyber attacks are also monitored by the Security Information Service and/or the Military Intelligence.

Legislation: In cyber reforms, the Czech Republic has taken many preventative actions during the past few years; with a significant delay. One of the most important of these acts is the Act on Cyber Security. It was developed in cooperation with law experts from the Masaryk University in Brno[94] and came into effect on January 1, 2015. It confirmed not only the NCSC position, but also defined the basic terminology related to cyber security. Unfortunately, it took four years to prepare and pass the necessary legislation to implement it.

92 National Security Bureau, op.cit.

93 Ibid.

94 Other stakeholders, including governmental bodies, Internet Service Providers, NGOs had the opportunity to comment it.

Other important legislative documents can be found in the following:

- the governmental order 315/2014 Coll. which changes the criteria for the identification of critical infrastructure component;
- the governmental notice 316/2014 Coll; and
- the governmental notice 317/2014 Coll, which defines criteria for the identification of important information systems.[95]

In 2015, the Czech government approved two conceptual documents which were developed by the NCSC:

- the National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020; and
- the Action Plan for Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020.

The Strategy is a fundamental, conceptual document and is consistent with the Czech security interests as defined in the Security Strategy of the Czech Republic. The Action Plan, on the other hand, is based on the National Cyber Security Strategy and it specifies goals, tasks, deadlines, and responsible entities for strategic implementation.

Last but not least, the Czech Republic signed a few important international agreements and memorandums for improvement of cyber abilities. These include:

- Declaration on Co-operation in the Field of Cyber Security between the Czech Republic and Israel;
- Joint Declaration on the Establishment of the Strategic Partnership between the Czech Republic and the Republic of Korea.

In 2016, the European Parliament adopted the EU Network and Information Systems Directive (the NIS Directive)[96] which entered into force in August 2016. Due to laws and strategic documents already in force, the Czech Republic must 'only' designate an operator to provide essential services and digital service and thus be compliant with the provisions of that directive.

Threats and Challenges: As in the case of other countries, the Czech Republic faces several major challenges to security, critical issues and numerous cyber attacks. For

95 T. Rezek, *Cyber Security Legislation in the Czech Republic*, 8 October 2015, Prague: AMO, http://www.amo.cz/cybersecurity-legislation-in-the-czech-republic/ [2016-10-15].

96 European Parliament and the Council, op.cit.

example, in 2011, a Romanian gang stole emission allowances for about CZK 450 million from the Czech Electronic Registry. The European Commission therefore had to immediately stop the trade of emission allowances across the EU.[97] In 2015, the NCSC prevented over six hundred cyber security incidents.[98] Overall, risks and threats become increasingly more alarming with the proliferation of new technologies.

The Military Intelligence has highlighted growing trends in cyber espionage such as a phishing, spear phishing and malware.[99] These trends are also seen in activities of hacker groups, mainly engaged in theft of sensitive information. The Security Information Service also warned against state-sponsored cyber espionage campaigns, especially from China and Russia, which are focused on obtaining political, military, diplomatic, scientific, technical, industry and power engineering information. These groups focused on stealing personal data and ICT logins to specific systems. The data were subsequently used for tasks within the so-called social engineering methods.[100] DDoS attacks are also very common in the Czech Republic.

Overall, the Czech cyber security system faces several risks and challenges. The three most important of them include:

- insufficient number of experts: the government has to solve the issue with an insufficient number of experts as most of them prefer to operate in the private sector. Higher starting salaries in the latter attract more talent than the public sector does;[101]
- relations between suppliers of information technologies and critical infrastructure administrators: administrators of critical infrastructure do not have technical inspection rights over systems and networks;

97 A. Rašek, *Kybernetická válka pokračuje* [The Cyber War Continues], Prague: Ministry of Defence of the Czech Republic, Communication and Promotion Department (DCP), 2012, p. 78.

98 Vláda České republiky, '*Stupňující kybernetické útoky ukazují, že přijatá přísnější vládní opatření mají smysl*' [Escalating cyber-attacks demonstrate, that the adopted stricter measures make sense], *News*, 14 March 2016, https://www.vlada.cz/cz/media-centrum/aktualne/premier-sobotka-stupnujici-kyberneticke-utoky-ukazuji--ze-prijata-prisnejsi-vladni-opatreni-maji-smysl-141285/ [2016-10-15].

99 VZ, 'Výroční zpráva o činnosti Vojenského zpravodajství za rok 2015' [Annual Report on Activities of Military Intelligence in 2015], *Military Intelligence (VZ)*, 2 September 2016, http://vzcr.cz/shared/clanky/20/V%C3%BDro%C4%8Dn%C3%AD%20zpr%C3%A1va_2015.pdf [2016-10-15], p. 15.

100 BIS, *Annual Report of the Security Information Service for 2015*, Prague: Security Information Service (BIS), https://www.bis.cz/vyrocni-zpravaEN890a.html?ArticleID=1104#_Toc460416001 [2016-10-15].

101 V. Blažek, *Státu chybí IT experti a právníci. Nabízí jim ale jen 20 tisíc měsíčně* [The state lacks IT experts and lawyers. However, they offer them only 20,000 per month], *Pravni radce*, 10 May 2016, http://pravniradce.ihned.cz/c1-65285160-statu-chybi-it-experti-a-pravnici-nabizi-jim-ale-jen-20-tisic-mesicne [2016-10-15].

- lack of legal protection: some of the sectors within the critical infrastructure are not protected by law (chemical industry, medical equipment, gas industry) and consequences of attacks in those areas can become very problematic.[102]

Remarks: Over the past years the Czech government has become increasingly active in field of cyber space reforms and intelligence work. For instance, the NCSC has organized or participated in several cyber exercises. As a result, cyber security now belongs to the top priorities of the Military Intelligence. Moreover, the Czech government endowed the Military Intelligence with the task to build National Cyber Forces. In cooperation with other institutions, the National Cyber Forces will be able to face cyber space-borne threats.[103] The government also signed the second generation of Memorandum of Understanding (MOU) on cyber defence. In fact, the Czech Republic was one of the first Allies to sign it.[104] Moreover, Israeli company Cyber Gym Europe has built a training cyber centre in Prague. It is the first professional training arena in Europe that utilizes programs developed by Israeli experts from the military/intelligence special units.

The elimination of the cyber threats is not about the legal frameworks in force, but mainly about capabilities and experts capable of using these capabilities effectively to counter cyber threats. The probability that cyber attacks will take place is high and it is reasonable to expect that the attacks will target national critical infrastructure. For this reason, the Czech society must acquire a sense of psychological resistance to withstand the implications of a likely failure of critical infrastructure.[105]

[102] Novinky.cz, 'Kybernetická bezpečnost Česka má bílá místa, upozornil NBÚ' [The Czech Cyber Security has 'white spots', warned the NSA], *Novinky.cz*, 27 July 2016, https://www.novinky.cz/internet-a-pc/bezpecnost/410300-kybernetika-bezpecnost-ceska-ma-bila-mista-upozornil-nbu.html [2016-10-15].

[103] VZ, op.cit.

[104] NATO, 'NATO and Czech Republic bolster cyber defence cooperation', *News*, 12 October 2015, http://www.nato.int/cps/en/natohq/news_123857.htm [2016-10-15].

[105] N. Schmidt, *Kyberprostor bude strategickým místem budoucnosti* [Cyberspace will be a strategic place of the future], *Natoaktual.cz*, 30 June 2014, http://www.natoaktual.cz/kyberprostor-bude-strategickym-mistem-budoucnosti-fyl-/na_analyzy.aspx?c=A140630_135804_na_analyzy_m02 [2016-10-15].

PART 3

Conclusions and recommendations

3.1. Conclusions and recommendations

Anna Visvizi, Tomasz Stępniewski, Vojtěch Bahenský, Jakub Kufčák, Justyna Gotkowska, Luděk Jiráček

The objective of this report was to draw a picture of and examine the fragile security contexts in which Poland and the Czech Republic operate so as to identify the key sources of risks and threats that these countries face today. To this end, an overall assessment of the conventional-, soft- and cyber risks and threats to the security in the region were elaborated and the specificity of Poland and the Czech Republic were put in the spotlight. At the conceptual level, drawing on Beck's risk society theory, a case was made for a distinction between the concepts of risk and threat. It was argued that delineating these two concepts allows us to understand not only the nuanced differences that separate safety from security, but also their regulatory and policy-making implications. A case was also made for a careful use of the term 'hybrid' in relation to warfare, safety and security. We have argued that as convenient as the term seems to be, it may also obscure our ability to effectively convey the meanings we intend to communicate. Undeniably, risks and threats to safety and security become increasingly complex and their sources may be blurry and/or multiple. Therefore, for the sake of targeted and effective policy responses, it is neces-

sary that things are called by their names and we seek to be as precise as possible to distinguish between the domestic and the external contexts and risks and threats to safety and security borne therein.

The conceptual framework employed in this report adds to our ability to extrapolate the impending risks and threats from the increasingly dynamic and multidimensional context in which Poland and the Czech Republic operate. This conceptual approach inspired the analytical angle that the contributing authors employed for the study of the security contexts that define East-Central Europe today in light of the provisions of the NATO Warsaw Summit Communiqué. This section proceeds as follows. First, the general remarks and recommendations are presented. In the next step, drawing on the discussion presented in this report, the key features defining the fragile security contexts in which Poland and the Czech Republic operate are listed. In the following move, the specific key short- mid- and long-term recommendations for Poland and the Czech Republic are presented. Finally, some more general lessons that Poland and the Czech Republic could draw from current developments in the region are elaborated.

3.1.1. General remarks and recommendations

General remarks:

The NATO Warsaw Summit produced a balanced mix of conclusions that preserved the internal unity of the Alliance. This was the main strategic priority of Prague. Poland, in turn, accomplished the goal of securing commitments regarding NATO's increased forward presence on its eastern flank. In this view, the NATO Warsaw Summit met the expectations of those NATO members that emphasized the need of security reassurance for the East-Central Europe. Clearly, regardless of the Article 5 of the Washington Treaty, and given the open warfare theatre in East Ukraine, the assurances the V4 countries (particularly Poland) received in Warsaw were of critical importance. Poland and other V4 states place significant importance on the matters of security and deterrence policy within NATO. As a consequence, the decision to establish a new Very High Readiness Joint Task Force (VJTF) in East-Central Europe has been welcomed as a vital step toward advancing those countries' security policies. Of paramount importance is that NATO broke one of its long-standing taboos, i.e. the deployment of combat forces on the territory of Eastern Allies. This could signal the end of the 'double-tiered' Alliance that existed since the countries of East-Central Europe joined the Alliance in 1999 and 2004. However, despite this expansion, the Alliance's overall military and deterrence posture remained basically unchanged until this year's Warsaw Summit. Overall, both in Poland and the Czech Republic the impression that prevailed was that the NATO Warsaw Summit's deci-

sions improved the Alliance's capacity to address threats to security, and created conditions conducive toward improving Poland's and the Czech Republic's preparedness to address them.

General recommendations:
The Czech Republic: Following the NATO Warsaw Summit, the general conclusions that the Czechs should draw are consistent with addressing the relative lack of 'ownership' that the Czechs feel toward the eastern flank. The Czech Republic should not look to others to solve the problems NATO faces on its eastern flank. It is imperative that the Czech Republic ask more of itself. On the practical level, the Czech Republic needs to reconsider the scope of its military ambitions. By 2025, the Czech Army should reach the level of capabilities originally planned during the unparalleled period of peace in Europe and the economic crisis. This could easily prove to be inadequate for future needs. The planned creation of a third Army brigade should become a stepping-stone for Prague to claim more responsibility for its security.

Poland: The overall lesson to be drawn is that continuity in foreign policy, considered as a lever for maintaining sound relationship on NATO forum, is crucial if Poland's temporarily strengthened position in the Alliance is to be maintained. Poland needs to nurture its relationship of friendship and trust with the Baltic countries, while at the same exploiting its leading position in the V4 and explore the opportunities of collaboration with a view to maintaining safety and security. From a different angle, a division of threat perception among the NATO members was apparent during the NATO Warsaw Summit. Indeed, Poland's emphasis on the threat of revanchist Russia was counter-balanced by arguments of sources of risks and threats being located on NATO's southern flank. Taking these points into account, if Poland's objective is to maintain its currently favourable position on NATO's forum, it is necessary that effort be invested in understanding the logics behind the competing threat perception. This should serve as a basis to reach out to those NATO members that otherwise group in an opposing caucus on the NATO forum. Paradoxically, this increased engagement with those NATO members might result in bridging the apparent divide between NATO's eastern and southern flanks and strengthening NATO's eastern flank. The added value for Poland would result from the leader's position dividend.

3.1.2. The key features defining the security contexts

Drawing on the discussion presented in the preceding chapters of this report, the key features that define the security contexts in which Poland and the Czech Republic operate have been identified as follows:

Conventional security threats:

- regional conflicts and instability in the Euro-Atlantic space and its neighbourhood, apart from revisionist Russia, including also the autocratic Arab state model;
- the weakening of mechanisms of cooperative security as well as political and international law-based commitments;
- the (re-)emergence of military threat to Poland's and the Czech Republic's allies;
- the increasing pressure on national borders and their role as frontiers capable of halting risks and threats to national safety and security, caused by improved military potential of hostile actors and the changing nature of warfare;
- the strengthening of capacities of non-state hostile actors on the international scene;
- the build-up of Russia's military presence on NATO's eastern flank;
- war in eastern Ukraine.

Soft risks and threats to security:

- propaganda and disinformation strategies by third actors aimed at destabilization of social and political life and hence weakening a country's societal and economic resilience;
- info-phobia and its implications for our ability to assess risks and threats related to information misuse and our ability to devise effective and commensurate responses to them;
- regulatory, policy-making and ethical challenges and risks related to the identification of measures to counter disinformation and propaganda;
- unsustainable economic policies unfit to strengthen a country's resilience in mid- and long-run;
- insufficiently embedded and consolidated culture of information sharing and appraisal, an issue particularly important in the context of terrorism and violent extremism;
- insufficient diversification of the energy supply base, over-dependence on imports of gas and petroleum, over-reliance on unreliable energy suppliers;
- suboptimal efficiency of energy production and the resultant energy price volatility;
- fragmentation of energy markets in the EU and uncertain status of energy pricing policies between individual EU member-states and external providers.

Cyber security risks and threats:

- the growing exposure to cyber borne risks and threats to safety and security, at a variety of levels and across the spectre of stakeholders involved;

- the growing vulnerability of the infrastructure to hostile activities, involving both critical infrastructure, e.g. satellites and the key fibre-optic links, and mass production appliances, such as routers;
- the decreasing cost of entry in the cyber space in view of engaging with hostile cyber activities and the resulting challenge of increased incidence of hostile cyber borne activity, including cheap guerrilla warfare;
- insufficient recognition of the salience of the baseline cyber security hygiene in view of strengthening the overall resilience to cyber borne attacks.

3.1.3. The key short-, mid- and long-term recommendations for Poland and the Czech Republic

Specific recommendations for Poland

Short-term:

- Maintain the momentum to strengthen the consensus as regards the understanding and assessment of risks and threats to security on NATO's eastern flank, but also seek to understand arguments that sources of risks and threats are located on NATO's southern flank;
- Maintain the momentum to strengthen NATO's will to showcase its capacities on NATO's eastern flank in view of improving the deterrence of the Alliance;
- Maintain the relative increase of Poland's role on NATO's forum to increase Poland's involvement in the debate on interoperability, especially in connection to cyber security;
- Engage in dialogue with those actors in Russia that are willing and seek effective communication in view of re-building trust between Russia and the West;
- Engage in programmes and strategies, possibly under the auspices of such actors as the EU and the OECD, that aim at strengthening the democratic and reformist tendencies in Ukraine, but also in Belarus;
- Re-think the high-school and undergraduate curricula in view of boosting students' critical thinking skills and news literacy in view of improving the society's resilience to propaganda and disinformation.

Mid-term:

- Continue efforts aimed at reducing the overdependence on energy supplies from unpredictable, unstable and authoritarian countries;
- Continue efforts at developing the infrastructure necessary to diversify the supply base;
- Build an EU-level consensus over the Nord Stream 2 pipeline by highlighting its geostrategic implications for the entire EU;

- Maintain the commitment regarding the value of expenditure on defence as % GDP and continue efforts at modernizing the army, including the Polish Navy;
- Continue efforts at maintaining national cyber resilience through actions at the regulatory and practical levels;
- Maintain the support and involvement in efforts aimed at taming the impact of the Kremlin's propaganda, e.g. via the STRATCOMCOE.

Long-term:

- Strengthen incentives aimed at boosting innovativeness in view of developing advanced sources of competitiveness, and improve the Polish industry's role in supporting national defence;
- Ensure a conjunction of the macro-economic policy-mix, including fiscal soundness and structural reforms, and the capacity to invest in national defence in a sustainable manner;
- Continue investing in the development of the existing experts' base in the public administration by providing access to resources and financial incentives.

Specific recommendations for the Czech Republic

Short-term:

- Deploy troops along NATO`s Eastern Flank on top of the agreed V4 initiative;
- Reduce supplies of energy resources from unpredictable, unstable and authoritarian countries;
- Rethink the mode of cooperation with countries considered as potential threat and resorting to diverse, also unconventional, means of combat;
- Increase the government's ability to recruit experts, e.g. in the field cyber safety and cyber security, and systematically invest in the development of human resources in relevant public administration domains;
- Establish official propaganda database to track and identify individuals and media outlets known to destabilize the democratic and liberal system within the Czech Republic.

Mid-term:

- Re-assess the level of military ambition needed to contribute to the preservation of NATO;
- Expand nuclear energy production as a means of reducing import-dependence (natural gas and petroleum) as well as the share of charcoal in energy production;
- Re-think and enhance the definition of critical infrastructure so as to include such sectors as chemical industry, gas industry and medical equipment.

Long-term:

- Overcome the psychological distance the Czech Republic feels towards the eastern NATO members;
- Refocus the development of military capabilities from crisis management and counterinsurgency to more conventional combat scenarios that could occur along NATO's eastern border;
- Invest in new technologies (research) or existing systems as a means of ensuring greater efficiency of energy production and lower costs for consumers;
- Strengthen science and research support to the development of existing and new technologies.

3.1.4. Drawing lessons from current developments

The relevance of the Visegrád Group (V4) and the V4 format of cooperation: In contrast to Poland, other V4 countries, i.e. the Czech Republic, Hungary and Slovakia, have different views on the challenges and threats to their security. A clear difference in threat perception between Poland and other V4 countries translates into serious limitations regarding political and military cooperation. The Czech Republic, Hungary and Slovakia are more willing to be a part of a southern flank countering illegal migration rather than an eastern flank countering Russia. However, that does not mean that possibilities of joint Visegrád projects in security and defence are non-existent.

The V4 format may be used to foster political and military cohesion in the region and motivate all countries to implement NATO Warsaw summit decisions (joint participation in VJTF/NRF, in military training and exercises, in post-Warsaw adaptation measures of NATO's structures) and to stick to the mainstream policies vis-à-vis Russia within the EU. The V4 Group will not be, however, either an engine for further changes aimed at strengthening the collective defence pillar within NATO or a group proposing the sharpening of policies toward Russia within the EU.

Cooperation between the V4 countries on security and defence may be more proactive. Since it is difficult to develop common positions and actions with regard to collective defence, it may be easier to do so within out-of-area crisis management. Having in mind the need to maintain cohesion between southern and eastern NATO member states along with the US pressure on more European military engagement in EU's southern neighbourhood, joint crisis management efforts of the Visegrád countries in Africa or in the Middle East would be of high value. One could think of a joint training mission in Iraq or in Libya/Tunisia in the future or for example joining forces in the EU or UN operations in Mali. Joint and coordinated participation in for-

eign operations are practiced by the Nordic countries, with an increasing presence of their Baltic partners; it is a sign of solidarity, credibility and ability to undertake joint actions with close partners and is treated as an important input in strengthening the relations with the USA and within NATO. In the light of the US demanding more engagement from its European allies, reshaping Visegrád cooperation this way would be a good response, and so would be launching of a to be started also with a bilateral (e.g. Polish-Czech) joint effort.

Cyber space: The NATO Summit in Wales held in 2014 shifted cyber security to a higher priority. The Warsaw Summit Communiqué reaffirmed cyber defence as a part of NATO's collective defence and endowed it with a status of a new combat domain. In order to utilize the salience of the NATO Warsaw Summit provisions concerning cyber space, it is necessary that each NATO member builds up the infrastructure capacity and that concerted actions are taken aimed at ensuring the interoperability of the national cyber security systems. As stated earlier in this report, this requires streamlining the processes of devising national security assessments and strategies, defining the nature and relative priority of cyber space risks and threats and corresponding measures to address them. Finally, it also requires that a culture of transparency and effective information sharing across the Alliance is developed. With regard to Poland and the Czech Republic, the above suggests that the following actions should be considered:

- conduct a screening of legislation with a view to identifying definitional fit and misfit across the Polish and the Czech national regulatory frameworks;
- where needed, align the definitions of risks and threats and prioritization of specific risks and threats in national security strategies to the extent necessary to enable interoperability.

Drawing lessons from the war in Ukraine: Without an active involvement of the West (including the V4 countries), Ukraine will not be able to handle the war with Russia. For this reason, the assistance of the West should be of both medium-term and short-term nature:

- the medium-term goal – to support Ukraine in implementing fundamental reforms (reform of the legal system, justice reform, the economy, public administration reform, fight against corruption and the oligarchic system, etc.). Achieving this requires that the Ukrainians be given training and expertise, the know-how, to help them in their effort to change the situation in their country;
- the immediate goal – military assistance – the V4 should provide both lethal and non-lethal items (equipment, flak jackets, helmets, etc.) as the Ukrainian forces are really poor. We need to underline that there is no purely military

solution to the conflict, but Ukraine's army needs to be shored up at this stage, regrouped and get some training in strategy and tactics. Ukraine is not capable of regaining control of the territories occupied by the pro-Russian separatists without a military intervention from the West (as the West is not ready to provide extensive military assistance). We need to realize that Ukraine has no military option to solve the conflict.

3.2. Looking ahead

The findings of this report are not exhaustive. Several issues and challenges were either left out or only mentioned in this report. What has been included in this report, however, confirms that even if Poland and the Czech Republic seem to have different threat perceptions, evidence is ripe that a convergence of perspectives is also in sight. The NATO Warsaw Summit may have been decisive in this regard in that it opened up the space for a reflection on the possibility of a new Polish-Czech relationship within NATO and in the region. In this view, it is imperative that this positive momentum is seized, for instance by engaging in a detailed bilateral risk and threat assessment activity along the following lines:

- Screen the fragile security contexts as defined in this report and as seen from Warsaw and Prague;
- Differentiate between risks and threats in respective assessments of the national security contexts;
- Compare, identify and map possible overlaps and likely differences;
- Map their prioritization in Poland and in the Czech Republic;
- Develop threat modelling and risk assessment techniques apt to address the so-defined risks and threats to national security;
- Consider the most effective policy-responses, including soft- and hard-measures.

About the authors

Vojtěch Bahenský, Associate Fellow at the Association for International Affairs (AMO), Prague. Areas of expertise: international hierarchy, international security, strategic studies and hybrid warfare.
E-mail address: vojtech.bahensky@amo.cz

Vít Dostál, Research Director at the Association for International Affairs (AMO), Prague. Areas of expertise: Polish domestic and foreign policy, Central European cooperation and Czech foreign and European policy.
E-mail address: Vit.dostal@amo.cz, Twitter: @VitDostal

Justyna Gotkowska, analyst at the Centre for Eastern Studies (OSW), Warsaw, Poland; project coordinator: Security and Defence in Northern Europe Programme. Areas of expertise: security and defence policy of Germany; security and defence policy of Nordic states (Denmark, Finland, Norway, Sweden); security and defence policy of Baltic states (Estonia, Latvia, Lithuania); military cooperation in Northern Europe.

Luděk Jiráček, Associate Fellow at Association for International Affairs (AMO). Areas of expertise: security policy and NATO.
E-mail address: ludek.jiracek@amo.cz

Aleksandra Kuczyńska-Zonik, PhD, Research Fellow at the Institute of East-Central Europe (IESW). Political scientist and archaeologist, recipient of the Mobility Plus Programme 2016–2017. Areas of expertise: history and contemporaneity of socio-political relations in the post-Soviet space, politics and security in East-Central Europe and the post-Soviet space, Russia's soft power, Russian diaspora in the Baltic States, Soviet historical memory.
E-mail address: kuczynska.a@gmail.com

Jakub Kufčák, Research Fellow at Association for International Affairs (AMO). Areas of expertise: security and defence policy, NATO, V4 security and defence cooperation, NATO enlargement.
E-mail address: jakub.kufcak@amo.cz

Alina Sobol, Research Fellow at the Institute of East-Central Europe (IESW). Areas of expertise: Russian and Soviet historiography, history of education in the Soviet Union, cultural history of the Russian emigration (1919–1939).
E-mail address: alina.sobol.kul@gmail.com

Tomasz Stępniewski, Doctor Habilitatus (Polish Academy of Sciences, Warsaw, Poland), associate professor and chair-holder of Eastern Studies Chair at the Institute of Political Science and International Affairs, Faculty of Social Sciences, the John Paul II Catholic University of Lublin. Areas of expertise: the EU eastern policy, European security, international relations of the Commonwealth of the Independent States' area, Russia's policy toward Eastern Europe.
E-mail address: tomasz.stepniewski5@gmail.com

Agata Stolarz, PhD, Research Fellow at the Institute of East-Central Europe (IESW). Areas of expertise: memory studies, incl. oral history and politics of memory in East-Central Europe.
E-mail address: agatastolarz@gmail.com

Joanna Świątkowska, PhD, Programme Director of the European Cybersecurity Forum, Chief Editor of the European Cybersecurity Journal and Senior Research Fellow of the Kosciuszko Institute. She is a member of the Advisory Group for Cybersecurity of the Republic of Poland at the Polish Presidential National Bureau of Security (NBS). Area of expertise: cyber security.

Alexey Vasilyev, PhD, Research Fellow at the Institute of East-Central Europe (IESW). Areas of expertise: memory studies, nationalism studies, cultural studies, incl. problems and issues of Polish national identity, history of Polish historical science, problems of cultural identity in East-Central Europe.
E-mail address: vasal2006@gmail.com

Anna Visvizi, PhD, Head of Research at the Institute of East-Central Europe (IESW). Areas of expertise: EU – politics and economics, Greece, the Visegrád countries (V4); global safety and security, including transatlantic relations.
E-mail address: avisvizi@gmail.com

About the partner institutions

Institute of East-Central Europe (IESW), Lublin, Poland
The Institute of East-Central Europe (IESW) carries interdisciplinary policy analysis and policy advice designed to further a thorough understanding of the specificity of the broadly defined region of East-Central Europe. To this end, IESW employs new methodological approaches to history, politics, international relations, law and economics to encourage well-founded debate and targeted dialogue on issues, problems and challenges pertinent to the region in context of European integration and Transatlantic relations. IESW's flagship publication is a quarterly titled *Yearbook of the Institute of East-Central Europe*, one of the top-ranked journals on the Polish market. In 2016, IESW successfully launched a commentary series (*KOMENTARZE IEŚW/COMMMENTARY IESW*), i.e. two-page policy-briefs on current developments in the region, addressed to the public administration and academia.

Association for International Affairs (AMO), Prague, the Czech Republic
AMO is a non-governmental not-for-profit organization founded in 1997 to promote research and education in the field of international relations. AMO:

- facilitates expression and realization of ideas, thoughts and projects in order to increase education, mutual understanding and tolerance among the people;
- formulates and publishes briefing, research and policy papers;
- arranges international conferences, expert seminars, round tables, public debates;
- organizes educational projects;
- presents critical assessment and comments on current events for local and international press;
- creates vital conditions for growth of a new expert generation;
- supports the interest in international relations among broad public;
- cooperates with like-minded local and international institutions.