INSTITUTE OF INTERNATIONAL RELATIONS PRAGUE

Norwegian Institute of International Affairs

Iceland Liechtenstein Norway grants
Norway grants

CZECH AND NORWEGIAN PERSPECTIVES ON RESILIENCE IN A POST-INVASION-OF-UKRAINE CONTEXT

JAN DANIEL,
ESKIL JAKOBSEN,
PERNILLE RIEKER

SUMMARY

The resilience thinking in the Czech Republic and Norway has been significantly influenced by the membership of both countries in NATO; however, a closer inspection reveals some significant differences between them and opens a space for their mutual learning.

Norway should pay attention to which aspects of national security resilience are strengthened by the membership in the EU as well as the longer debate on the resilience to disinformation in the Czech Republic.

The Czech Republic could learn from the Norwegian thinking about the coordination of civil and military efforts in addressing security and military threats.

POLICY PAPER

24. 5. 2023

INTRODUCTION

Resilience has become one of the key concepts that were put forward in the past decade to react to a worsening security environment in Europe and beyond. In response to the Russian invasion of Ukraine, the calls for enhancing the resilience of European security systems became even more pronounced. The aim of this policy paper is to unpack the concept of resilience by showing how it has been operationalised and put into practice by the two key security institutions in Europe – NATO and the EU – and how it has been understood at the national level in the Czech Republic and Norway. By doing so, the brief foregrounds the two countries' different ways of thinking about and practices of resilience that stem from their (lack of) membership in NATO and the EU as well as their different national threat perceptions. In conclusion, it argues for their mutual learning from these diverging experiences, which were marked by the Czech integration into the EU resilience efforts and the Norwegian tradition of civil-military integration.

However, what does the famously ambiguous concept of resilience mean for us in the first place? Resilience has on the most general level been defined as an ability to withstand external shocks without a significant disruption of a given system or subject's functions, combined with an ability to recover in a timely manner LINK. Nevertheless, widely non-matching specific understandings of resilience have been employed in present and past policies. These have ranged from treating resilience as a basic ability to withstand an external shock through mere system robustness to the (partially complementary) understanding of resilience as a dynamic process of adaptation driven by local and decentralised responses. Others then understood resilience rather as a set of qualities of individuals, systems or communities that are required for appropriate reactions to external disruptions and stressed the need to foster these qualities LINK. In consequence, although the policies and strategies that in various ways invoke resilience have kept proliferating, it is impossible to understand what is meant by resilience without understanding the specific context. This particularly means the institutional setting in which these strategies operate, what threats they are supposed to react to and what subjects they actually aim to make resilient LINK.

NATO: NATIONAL RESILIENCE IN SUPPORT OF THE COLLECTIVE DEFENCE

NATO has been among the main actors introducing resilience to the European debates on security. NATO's primary task remains collective defence. NATO's increased emphasis on resilience as a concept which could help coping with unexpected and unforeseen disruptions must be understood as a way of adjusting its collective defence capacity to a changing security environment with a variety of different threats. This is also why resilience has become so strongly reflected in NATO's strategic thinking and gradually led to an increased number of areas where resilience is identified as critical for Alliance security.

The shock posed by the Russian annexation of Crimea and the start of the war in Eastern Ukraine in 2014, which was associated with diverse covert, asymmetric, and hybrid methods of warfare, reinforced the position of resilience as one of the main concepts that guide security and defence planning in Europe and beyond. The Alliance stressed the need to enhance resilience in the outcomes of the Wales Summit in 2014 LINK and then even more strongly in the key decisions of the Warsaw Summit from 2016 LINK. While the former called for bolstering the resilience of the Alliance as such and enhancing the resilience of cybersecurity systems, the latter raised resilience to the status of one of the key tasks of the collective reaction to the more assertive Russia. In particular, the conclusions of the Warsaw Summit called for strengthening the civil preparedness among the member states of the Alliance as civilian (health, transport, communication or other) infrastructures and societies more largely came to be seen as crucial underpinnings of national and Alliance defence LINK.

The seven **Baseline Requirements for National Resilience**, which were reaffirmed at the 2021 Brussels Summit LINK, then specified the areas where resilience should be enhanced. The requirements aimed to ensure the resilience of allies through civil preparedness and the ability to assure continuity of government and critical services following a potential disruption. Beyond the continuity of the government, these also entailed, more specifically, resilient energy, food and water supplies, an ability to deal with uncontrolled movement of people and mass casualties as well as resilience of transportation and communication systems. This thinking about resilience and how it matters for the Alliance was reiterated also in response to the Covid-19 crisis when NATO underlined the security implications of the resilience of key economic industries and supply chains LINK, and in response to the Russian invasion of Ukraine in February 2022.

Resilience features in the latest NATO Strategic Concept, which was adopted in June 2022. Although the Concept stepped short of naming resilience as one of NATO's core tasks, as some had been calling for it LINK, the Alliance and its member states declared that they will seek a 'more robust, integrated and coherent approach to building national and Alliance-wide resilience against military and non-military threats and challenges to our security' LINK. Resilience is also a key component of the second core task of NATO presented in the current Strategic Concept – crisis prevention and management. It is, however, primarily linked to the focus on previous areas which the Alliance identified as crucial for its ability to ensure a collective defence of its members, namely the need to bolster resilience in the framework of civil preparedness among all the members as well as resilience of critical infrastructures and key supply chains. NATO's current conceptualization of resilience could be considered as a critical supporting element to the three core tasks presented in the 2022 Strategic Concept: Deterrence and Defence, Crisis Prevention and Management, and Cooperative Security.

This is also increasingly the case since the Russian invasion of Ukraine, which has forced NATO to put most of its emphasis on collective defence. The dramatic deterioration of European security since February 24, 2022 has also led to a request for increased cooperation between NATO and the EU so that they would be able to deliver on resilience within the framework of a whole of society approach to security. The launch of the joint NATO-EU taskforce on resilience and critical infrastructure protection in March 2023 is a case in point LINK.

THE RESEARCH FOR THIS POLICY PAPER WAS FINANCIALLY SUPPORTED BY THE EEA AND NORWAY GRANTS 2014–2021 FRAMEWORK (UNDER THE FUND FOR BILATERAL RELATIONS). PROJECT NAME: "CZECH AND NORWEGIAN PERSPECTIVES ON NEW SECURITY THREATS IN RELATION TO THE RUSSIAN WAR ON UKRAINE", PROJECT NUMBER: EHP-BFNU-OVNKM-4-194-01-2022.

EU: COMPREHENSIVE REGIONAL AND NATIONAL RESILIENCE

The EU defines resilience as follows: “Resilience is the ability not only to withstand and cope with challenges but also to undergo transitions in a sustainable, fair and democratic manner” LINK. With such a definition, the EU establishes a very broad approach to the concept. As the EU, in contrast to NATO, is covering all policy areas, it makes sense to take such a comprehensive approach. As in the case of NATO, specific capacities for resilience in the EU have evolved over time and often in response to specific crises. While the development of different types of policies and mechanisms to increase societal resilience has been at the core of the integration process since the beginning without being named as such, it has gradually become a more explicit goal since the early 2000s. From the terrorist attacks on the US in 2001 (which were followed by a series of terrorist attacks also in Europe) and up until the invasion of Ukraine in 2022, the EU has in many ways been in a constant crisis response mode, and it has been focusing on how to best improve its toolbox for both preventing and handling different kinds of crises.

It could be argued that the whole European integration process is implicitly based on resilience – in the sense of the idea that increased interdependence and efficient regulation will contain potential conflicts and disruptions – and most EU policies contribute indirectly to increasing societal resilience. Beyond this, there is also a set of concrete policy initiatives and mechanisms that specifically has this as its main goal:

First and foremost, there is the **civil preparedness mechanism** that was established already in 2001 as a coordination mechanism for assisting members in case of a national crisis. The EU’s civil preparedness capacity has been gradually strengthened and broadened, and as is often the case in the EU, this happened in response to crises.

The Covid-19 pandemic is a good example of this as it led to a series of initiatives during the heat of the crisis that also paved the way for the establishment of new mechanisms to improve the EU’s resilience in a number of areas. The establishment of RescEU LINK is a case in point. It represents a reinforcement of the Union’s crisis preparedness mechanism as it has led to the acquirement of assets (including a fleet of firefighting planes and helicopters, medical evacuation planes, a stockpile of medical items and field hospitals that could respond to health emergencies) at the EU level for the purpose of better assisting member states in dealing with their national crises. Another example, which is also linked to the Covid crisis, is the agreement to establish a Health Union LINK to improve the Union’s joint preparedness in case of potential future pandemics and other transnational health crises.

In addition to these initiatives, there is a series of instruments that have been developed to make the EU more resilient against **various forms of foreign interference**, often in the framework of security and countering hybrid threats. These include some early initiatives, such as the Joint Framework on Countering Hybrid Threats (2016) or the Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats (2018) see LINK, but also the European framework for screening of foreign direct investment (FDI) that allows EU Member States and the Commission to cooperate and exchange information on investments from third countries that may affect security or public order in the EU. Furthermore, a series of initiatives to regulate and protect the digital space

THE RESEARCH FOR THIS POLICY PAPER WAS FINANCIALLY SUPPORTED BY THE EEA AND NORWAY GRANTS 2014–2021 FRAMEWORK (UNDER THE FUND FOR BILATERAL RELATIONS). PROJECT NAME: "CZECH AND NORWEGIAN PERSPECTIVES ON NEW SECURITY THREATS IN RELATION TO THE RUSSIAN WAR ON UKRAINE", PROJECT NUMBER: EHP-BFNU-OVNKM-4-194-01-2022.

(Digital Market Act, the Digital Services Act, the Cyber Strategy) and physical space (the Space Strategy) was adopted in the name of increasing the EU's resilience against various forms of foreign interference.

More directly, the Strategic Compass that was adopted in March 2022, explicitly points out the need to improve the Union's collective capacity for crisis response and resilience LINK. While the process of the Strategic Compass formulation predates the Russian aggression against Ukraine, many initiatives that stem from it came to be developed with an increased sense of urgency due to the conflict. Particularly interesting is the emphasis that is put on the need to establish a Hybrid Toolbox LINK and an FIMI Toolbox LINK to address foreign information manipulation and interference and "bring together different instruments to detect and respond to a broad range of hybrid threats", but also the need to further develop the EU Cyber Defence Policy so that the EU would be "better prepared for and respond to cyberattacks".

Similarly, in the past months following a longer process of drafting and negotiations, the EU also updated the Directives on Network and Information Security 2 LINK and Critical Entities Resilience LINK. While the former focuses on increasing the cybersecurity of **critical infrastructure systems**, the latter proposed enhancing the resilience of critical infrastructure in areas ranging from transport and energy to financial services, food and water systems and public administration. Especially the Directive on Critical Entities Resilience manifests a strong orientation toward harmonizing the policies aimed at increasing the resilience of critical infrastructure (as opposed to mere protection of it) across the EU member states LINK.

With all these initiatives and instruments, the EU is adopting a whole of society approach that seemingly complements NATO's approach, which is a bit narrower in scope and oriented primarily towards supporting defense capabilities.

CZECH REPUBLIC: FROM RESILIENCE OF SYSTEMS AND INFRASTRUCTURES TO A RESILIENT SOCIETY

The notion of resilience has been strongly present in the Czech security debate in the past decade. Being introduced by various national security documents, it gradually found its way to other policy areas as well. It was specifically the understanding of resilience that was impacted by the previous discussion about hybrid threats as well as resilience of infrastructure systems and supply chains that came strongly to the forefront of the public and policy debate in the aftermath of the Russian invasion of Ukraine in February 2022.

Resilience started to be mentioned in the Czech context more strongly in the beginning of the 2010s, as this development was mostly influenced by the debates in NATO at the time. The tasks stemming from the NATO resilience requirements have been dealt with by the national civil crisis preparedness system. The core of the system developed in the 1990s and 2000s from the previously militarized civil defence in the process of the integration of the Czech Republic into both NATO and the EU, and the harmonization of crisis preparedness policies. The National Security Strategy of 2011 identified the resilience in the security area

THE RESEARCH FOR THIS POLICY PAPER WAS FINANCIALLY SUPPORTED BY THE EEA AND NORWAY GRANTS 2014–2021 FRAMEWORK (UNDER THE FUND FOR BILATERAL RELATIONS). PROJECT NAME: "CZECH AND NORWEGIAN PERSPECTIVES ON NEW SECURITY THREATS IN RELATION TO THE RUSSIAN WAR ON UKRAINE", PROJECT NUMBER: EHP-BFNU-OVNKM-4-194-01-2022.

as a result of the unity of efforts of security institutions, the rest of the government and public services, society and various private actors. While it mentioned the need for a society-wide resilience in broader terms, it particularly singled out cybersecurity as a key domain where cooperation between the state and private actors is particularly needed in order to ensure the ability of information systems to 'bounce back' and promptly recover from a disruption LINK. The current Security Strategy of 2015 reiterated this understanding and connected it also with energy infrastructures and energy security LINK.

The notion of resilience, and, in particular, societal resilience, started to appear more strongly in the public and policy debate in 2016 during the process of drafting the National Security Audit – an assessment of the preparedness of the Czech Republic for a wide range of security issues LINK. The document was prepared in reaction to the mid-2010s security environment, which came to be defined by an assertive Russia, but also concerns over illegal migration and terrorism. The Audit manifested a strong and rising awareness of hybrid threats, often particularly interpreting them as attacks on democratic and liberal values as well as the institutions and processes underpinning them LINK, LINK. Resilience became the key notion that defined the ability of both the state and society to face a range of new and old security issues. While applied unevenly in different areas, resilience has been particularly strongly discussed with relation to cybersecurity and energy infrastructures, but also hybrid threats, which are often viewed as manifested in the Czech context by disinformation campaigns and the influence of foreign powers LINK. In these contexts, resilience came to be understood as an essential aspect of the society and its democratic values, which are needed for withstanding the foreign hostile interference. A resilient society was understood in the document as one that is united around particular values and a resolve to defend the democratic state.

The primary connection between resilience and hybrid threats in their multiple interpretations has been solidified by several documents and initiatives. Resilience plays a key role also in the National Strategy for Countering Hybrid Interference from 2021 LINK. The document identified the triad of the resilient society, state, and infrastructure as the key goal of the national reaction to hybrid threats, in particular in the areas of values, political institutions, economy and defence, and brought together the previously identified areas of societal and infrastructural vulnerabilities. Enhancing of resilience should take place also in the area of energy supply chains and foreign investments – a point that was further stressed by later policies adopted in response to the invasion of Ukraine LINK. However, a focus on resilience heavily features also in the area of public trust in governmental policies and institutions, and public awareness of potential threats, as these contribute to building a resilient society that is able to withstand a range of new threats (as argued also by, e.g., National Cybersecurity Strategy – LINK). Another initiative in this area, which was adopted in the wake of the Russian aggression against Ukraine, concerned the short-lived position of the Special Representative for Media and Disinformation LINK. However, the position was scrapped after several controversies and in February 2023 it was moved under the authority of the National Security Advisor LINK.

Despite several efforts aimed at establishing coordination structures, resilience policies in the security area have been scattered and fragmented among different institutions with emphases on different sectors of security – e.g. dedicated ministries and then specialised agencies and other parts of the national security system and the integrated emergency response system. In general, the main coordination efforts are done by the National Security

Council (*Bezpečnostní rada státu – BRS*), which is set up at the Office of the Government and brings together representatives of key ministries (the Ministries of Interior, Foreign Affairs, Defence, and Finance and others), the Prime Minister and the newly established position of the National Security Advisor LINK.

The BRS then contains several working groups and committees tasked with resilience-relevant planning and dedicated activities – among others, defence planning, civilian emergency planning, and internal security. The Committee for Civilian Emergency Planning (falling under the responsibility of the Ministry of Interior) is the key interlocutor for the NATO civil preparedness and resilience agenda. Through chairing an interministerial working group, the Ministry of Interior – namely the Directorate General of the Fire-Rescue Service of the Czech Republic – coordinates the activities of the main ministries and other agencies responsible for implementing Article 3 of the Washington Treaty, the NATO Strengthened Resilience Commitment LINK and the Seven Baseline Requirements for Resilience.

The coordination mechanism tasked with countering hybrid threats and enhancing resilience has been concentrated in a dedicated working group of the BRS since 2017. This working group brings together the ministries which form the BRS and the representatives of other national security institutions, such as intelligence agencies, the police, the cybersecurity agency and others. The system has been further amended in 2021 with the creation of the position of the Countering Hybrid Interference Coordinator, who heads the dedicated working group on hybrid threats, and the position of the National Security Advisor, which was established in December 2022 LINK, LINK.

The Czech Republic has developed its resilience efforts on multiple tracks. While the civil crisis preparedness and specifically the resilience agenda have been closely connected to the NATO reading of the concept and integrated into the NATO planning system, there have been also other avenues of developing societal resilience. Many of these efforts in areas such as health policies, the crisis response mechanism, or protection (and resilience) of critical and digital infrastructure, have stemmed through the integration and harmonization of these activities in the EU. Finally, due to the historical and political context, a significant part of the resilience debate has focused more specifically on disinformation and countering foreign influence in the name of the campaign against hybrid threats LINK. In this respect, the start of the war in Ukraine did bring a strengthened emphasis on several issues, such as resilience of energy and other supplies, food security or societal resilience towards disinformation, but despite some minor overhauls of the system, the response followed the previously established patterns.

NORWAY: CRITICAL SOCIETAL FUNCTIONS AND TOTAL DEFENCE

Resilience has received an increasing amount of attention among Norwegian policymakers and the general public in Norway due to several major destructive events and crises in recent decades. Among the most important are the 2004 tsunami disaster, the 2011 terror attacks in Oslo and Utøya, several serious cyberattacks, the Covid-19 pandemic and the Russian war on Ukraine. These crises, in various ways, highlighted the need for well-functioning civil protection, preparedness and crisis management policies. To a varying extent they also

THE RESEARCH FOR THIS POLICY PAPER WAS FINANCIALLY SUPPORTED BY THE EEA AND NORWAY GRANTS 2014–2021 FRAMEWORK (UNDER THE FUND FOR BILATERAL RELATIONS). PROJECT NAME: "CZECH AND NORWEGIAN PERSPECTIVES ON NEW SECURITY THREATS IN RELATION TO THE RUSSIAN WAR ON UKRAINE", PROJECT NUMBER: EHP-BFNU-OVNKM-4-194-01-2022.

spurred the development in the government's approach to achieving societal resilience. The most recent government White Paper on societal security, published in 2020, highlighted 7 resilience-related issues as essential: the Covid-19 pandemic, civil-military cooperation and total defense, preventative national security, digital security, hybrid-threats, prevention and preparedness on both the local and regional levels and prevention, preparedness and rescue services in the Northern waters LINK.

The end of the Cold War shifted the focus of the Norwegian government from state security towards public security or *societal security*. The prevailing Norwegian understanding of *societal resilience* is highly interlinked with the concept of societal security. Societal security has been defined as the ability of a society to prepare for and manage any event that threatens its core values and functions, or the life and health of its people LINK. A central component of the Norwegian conceptualization of societal resilience is critical societal functions (CSF). These functions include various essential government services as well as all types of infrastructure that are necessary for sustaining the modern Norwegian society LINK. The responsibility of securing CSFs is in large part placed on the ministry responsible for the relevant policy-field in accordance with the foundational governance principle of *individual ministerial responsibility* LINK. The Ministry of Justice and Public Security plays a key overarching role in efforts to enhance societal resilience through its development and coordination of cross-sectoral measures, many of which are under the purview of the Norwegian Directorate for Civil Protection (DSB) and the Norwegian National Security Authority (NSM) LINK, LINK.

The principle of individual ministerial responsibility is also of vital importance to the current Norwegian approach to development and implementation of general policies related to resilience and crisis management. Often referred to as the *sector-principle*, it directs each ministry to prevent and manage crises within its area of responsibility or *sector*. Within this overall structure there are four guiding principles for civil preparedness and crisis management: responsibility, conformity, proximity and cooperation. A prominent criticism levied towards the sector-principle is the negative impact it can have on the ability of the government to manage cross-sectoral challenges. The fourth guiding principle, cooperation, was included in part to remediate this challenge after the 2011 terror attacks in Oslo and Utøya highlighted the issue LINK. The lacking cross-sectoral situational awareness and coordination has, however, been a persisting issue, and the need for joint situational awareness across governmental departments was again highlighted as essential in the "Security Advisory Report" published by the NSM in May 2023. A key remediating measure recommended by the NSM is the establishment of a civil-military situation-center responsible for providing holistic and timely decision support for the ministries LINK.

A vital overarching organizational structure for ensuring societal security in Norway is the Total Defense Concept (TDC). First implemented during the Cold War, the concept entails utilizing most of the available resources in society to ensure a maximum capacity for preparedness across the spectrum of crises. In its original form the TDC was primarily constructed to handle crises related to armed conflict, but the end of the Cold War led to a significant shift towards civil preparedness. This shift manifested in the political decision to *modernize* the TDC announced in 2004. During the two subsequent decades significant efforts and resources have been directed towards making the concept fit for purpose in the modern security landscape. A vital component of the modernized TDC is the mutual support and cooperation between the Norwegian military and civil society LINK. Among a broad range of measures implemented in support of this collaboration are four principles of civilian-military logistics cooperation LINK.

THE RESEARCH FOR THIS POLICY PAPER WAS FINANCIALLY SUPPORTED BY THE EEA AND NORWAY GRANTS 2014–2021 FRAMEWORK (UNDER THE FUND FOR BILATERAL RELATIONS). PROJECT NAME: "CZECH AND NORWEGIAN PERSPECTIVES ON NEW SECURITY THREATS IN RELATION TO THE RUSSIAN WAR ON UKRAINE", PROJECT NUMBER: EHP-BFNU-OVNKM-4-194-01-2022.

The modernization process of the TDC is ongoing and the debate on the future of the concept has been greatly affected by the Covid-19 pandemic and Russia's war on Ukraine. The report of the Norwegian Defence Commission published in May 2023 identified several challenges facing the TDC. Among the most important are the capacity for civilian-military cooperation on health preparedness in times of crisis, and vulnerabilities associated with the increased privatization of functions previously provided by the government. The commission also called for further modernization of the TDC to "increase the resilience of critical societal functions" LINK.

Another commission, the Total Preparedness Commission (TPC), is examining Norway's overall preparedness and how to optimally utilize all available resources to ensure societal security. The TPC is set to conclude its work in June 2023 but has given some indications as to what fields of public security they will highlight. Among the key fields the commission has highlighted publicly are value-chains, public-private cooperation, cross-sectoral cooperation, digital security and hybrid threats LINK. It is worth noting that democratic security is not an explicit part of the commission's mandate. This underscores the limited attention this kind of resilience receives in Norway. However, some debate on related phenomena like misinformation and disinformation has occurred. This was particularly evident when considerable amounts of disinformation about various aspects of the Covid-19 pandemic were circulated. A report published by the Norwegian Defence Research Establishment (FFI) addressed the challenges such influence operations pose and how they relate to societal resilience LINK. The topic of influence operations also received attention in the "Security Advisory Report" published by the NSM, indicating that growing attention was being paid to this field of resilience LINK.

Fulfilling the obligations Norway has under Article 3 of the Washington Treaty and the NATO Strengthened Resilience Commitment is of vital importance to the Norwegian government. Many measures dedicated towards this endeavor are implemented within the TDC structure, and the current government has placed resilience for critical infrastructure high on their list of priorities. This is in part connected to the Russian war on Ukraine as well as the sabotage attacks on the Nord Stream pipelines in September 2022. Another important factor is the increased frequency of malign activity towards Norwegian critical infrastructure and public institutions, which has largely coincided with the Russian invasion of Ukraine. These activities include increased espionage activity from Russian operatives, drone activity around Norwegian petroleum installations, the continued GPS jamming in Northern Norway, which leads to issues with communications and air traffic control, and the suspected surveillance of Norwegian critical infrastructure conducted from Russian civilian ships.

This potentially speaks to an underappreciation of resilience towards foreign interference, surveillance and potential future hybrid threats. A significant number of Russian ships can operate legally in Norwegian territorial waters despite Russia's full-scale invasion of Ukraine. The potential surveillance activity these vessels facilitate has been a concern of the Norwegian security apparatus for some time and recently an issue of public debate as well. The current Russian marine doctrine stipulates that civilian vessels can be utilized by the government to further Russian security and security interests LINK. Suspicious navigational patterns of Russian vessels near important petroleum infrastructure and critical infrastructure on the seabed have been observed LINK. The information gathered could presumably be used to plan sabotage attacks during peacetime that can contribute to creating fear and uncertainty in the Norwegian population. Such attacks could also enable

THE RESEARCH FOR THIS POLICY PAPER WAS FINANCIALLY SUPPORTED BY THE EEA AND NORWAY GRANTS 2014–2021 FRAMEWORK (UNDER THE FUND FOR BILATERAL RELATIONS). PROJECT NAME: "CZECH AND NORWEGIAN PERSPECTIVES ON NEW SECURITY THREATS IN RELATION TO THE RUSSIAN WAR ON UKRAINE", PROJECT NUMBER: EHP-BFNU-OVNKM-4-194-01-2022.

further intelligence gathering on the Norwegian civil preparedness system and responses. The intelligence could also be used for targeted strikes in a limited/total war scenario. The Russian surveillance activity towards Norwegian critical infrastructure is a serious matter and should be treated as such by the Norwegian authorities and security apparatus. The increased efforts to secure maritime infrastructure under the NATO umbrella, spearheaded by Norway and Germany, could prove beneficial with regard to deterring and handling future malign activity LINK.

It is also recognized in Norway that the EU is a crucial actor – and even the most important actor – when it comes to resilience and societal security. In the end, the EU is covering so much more than NATO does in the area of societal security. Norway is not a member of the EU, but it is still highly integrated with the Union through a set of agreements. The main agreement in this regard is the EEA Agreement, which allows Norway to take full part in the Union's internal market. In addition to this, Norway is also part of Schengen, shares the external border control, participates fully in the crisis preparedness mechanism referred to above, and has a set of agreements with the EU in foreign, security and defense policy. Still, this special construction of being partly integrated also has its challenges. And these challenges are particularly evident in a time of crises.

During the Covid crisis, Norway experienced how difficult it is to be a non-member of the EU. It was only due to Swedish goodwill that Norway in the end was included in the vaccine program as the Swedish government decided to also buy vaccines for Norway. As Covid illustrated the potential vulnerabilities of being outside the Union, there is now work being done to find out how Norway can have an agreement with the EU's Health Union LINK. As the EU is now developing new regulations, policies and instruments at a very high speed in order to improve its capacity for societal resilience in a more challenging security context, it is a potential security risk to be a non-member. Norway has also experienced similar challenges in relation to the initiatives that are under development to protect the Union's digital and physical space.

KEY AREAS OF RESILIENCE IN THE LIGHT OF THE RUSSIAN WAR AGAINST UKRAINE IN CZECHIA AND NORWAY

The Russian war against Ukraine and its after-effects specifically revealed several vulnerabilities in both countries that future resilience efforts should address. Leaving aside the issues of energy and food security, which are tackled by different policy papers in this project, the resilience and protection of energy and critical infrastructure emerged in the recent months as a key task for the Norwegian side, whereas the longer issue of strategic communication and relations between the government and society has been repeatedly raised in the Czech context. Both countries then thematized the resilience of supply chains in general as a key aspect of broader societal resilience, as it was highly tested already by the experience of the Covid-19 pandemic.

Comparing and contrasting the Czech and Norwegian approach to resilience policies reveals a range of commonalities as well as differences stemming from the geographical, historical, and political contexts of both countries. While the contexts are, without a doubt, significantly different, they also open space for a potential mutual exchange of best practices and institutional knowledge. Both countries are firmly anchored in NATO and have been following the conceptual understanding of resilience as well as specific resilience requirements set up by the Alliance. However, the comparison also reveals a range of policies aimed at enhancing societal resilience and resilience of key public policy institutions that are available only to the Czech Republic due to its membership in the EU. This opens up a way for broader thinking about societal resilience and the institutions underpinning it. On the other hand, the Norwegian experience with its longer tradition of thinking about the mutual support of civil and military actors, could provide a source of inspiration for the Czech thinking on societal resilience. Finally, the longer Czech debate on responses to hybrid threats and disinformation could provide material for learning about promising avenues or dead-ends in the disinformation counter-campaign.

POLICY RECOMMENDATIONS

→ Both Norway and the Czech Republic should dedicate a significant amount of resources and attention to the areas of resilience described in the NATO Strengthened Resilience Commitment.

→ Both Norway and the Czech Republic need an updated understanding of the synergies between NATO and the EU in this field (as manifested, e.g., by the novel projects on military mobility). While NATO might be a primary point of reference for defence thinking about resilience to support military activities, the broader resilience efforts of the EU significantly overlap with many of the core NATO requirements. Both countries should thus stress the need to identify synergies between the activities promoted by the two organizations.

→ Norway should make sure to have an active policy towards the EU that can compensate for its non-membership. It needs to work harder to make sure that it is included in most of the EU's resilience activities, including initiatives such as the EU Framework for Investment Screening as well as the IRIS2, which, in principle, is for members only.

→ The Czech Republic should pay attention to the more holistic thinking about societal resilience present in the Norwegian (and more largely Scandinavian) model of "total defence." While an institutional overhaul of the existing national security system is undesirable, an enhanced coordination between civilian and military institutions in clearly specified areas that are needed for societal resilience would be beneficial.

Jan Daniel is a Senior Researcher
at the Institute of International Relations Prague (IIR).

Eskil Jakobsen is a Junior Research Fellow
at the Norwegian Institute of International Affairs (NUPI).

Pernille Rieker is a Research Professor
at the Norwegian Institute of International Affairs (NUPI).

THE RESEARCH FOR THIS POLICY PAPER WAS FINANCIALLY SUPPORTED BY THE EEA AND NORWAY GRANTS 2014–2021 FRAMEWORK (UNDER THE FUND FOR BILATERAL RELATIONS). PROJECT NAME: "CZECH AND NORWEGIAN PERSPECTIVES ON NEW SECURITY THREATS IN RELATION TO THE RUSSIAN WAR ON UKRAINE", PROJECT NUMBER: EHP-BFNU-OVNKM-4-194-01-2022.