Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

Nadja Milanova, *Connections QJ* 19, no. 3 (2020): 67-75
https://doi.org/10.11610/Connections.19.3.05

Research Article

Institutional Resilience and Building Integrity in the Defense and Security Sector

Nadja Milanova

NATO International Staff, https://www.nato.int/

Abstract: The concept of resilience in defense and security is evolving towards the inclusion of a wide-ranging and multidimensional set of vulnerabilities and associated mitigation strategies across the spectrum of military and non-military mechanisms of response. This article argues that while corruption and poor governance are now recognized as a security threat, as articulated in the NATO Warsaw Summit Declaration, the strengthening of defense and related security institutions in both Allied and partner countries remains to be further embedded as an integral part of the concept of resilience. Institutional resilience based on integrity, transparency, and accountability is critical for ensuring the fulfillment of NATO's resilience commitment and its baseline requirements, which include *inter alia* continuity of government with the ability to make decisions and provide services to the population. Corruption and poor governance undermine public trust and perpetuate instability and fragility. NATO's Building Integrity policy contributes to the fulfillment of the Alliance's three core tasks – collective defense, crisis management, and cooperative security. NATO's work on Projecting Stability vis-à-vis partners has recognized the role of good governance as a component of improving partners' resilience. This needs to be further institutionalized through consistent efforts at strengthening defense institutions. The contribution of institutional resilience to NATO's defense and deterrence task needs to be further conceptualized. The article argues for a more consistent approach to operationalizing Building Integrity as an integral part of the concept of resilience and the need for robust institutional capabilities to mitigate vulnerabilities stemming from the risk of corruption as a security threat.

Keywords: NATO, defense and security sector, institutional resilience, Building Integrity, BI, transparency, accountability, corruption, good governance.

Partnership for Peace Consortium of Defense
Academies and Security Studies Institutes

Introduction

Resilience is one of those newly coined concepts that is witnessing an exponential increase in use across a wide range of areas and international organizations. The ubiquity of the concept is at once promising as it focuses on the causal effect of a host of factors and their interlinkages but is also exposed to the danger of being overused—and thus misused—without the development of its solid foundation and conceptual framework. In this regard, will the potential of the concept of resilience be used by international organizations as a true signpost for practical solutions to complex problems, or is it going to be used as a "fig leaf" when it is impossible to reconcile the under-ambitious and the over-ambitious extremes of their policy-making agendas?

A perusal of the use of resilience across international organizations as part of their agenda and policy-making shows the following trends. In the UN discourse, resilience has been introduced in the context of sustainable development, whereby the resilience of social and ecological systems is used as a measure for the implementation of the Sustainable Development Goals (SDGs). The United Nations (UN) approach to resilience is geared primarily towards risk reduction and disaster management and seeks to provide an analytical framework of indicators to measure sustainability within this context.

On its part, the Organization for Economic Cooperation and Development (OECD) emphasizes the need for collaboration among different policy communities working on different risks within the framework of development strategies. The OECD definition of resilience points to "the ability of households, communities, and nations to absorb and recover from shocks, whilst positively adapting and transforming their structures and means for living in the face of long-term stresses, change and uncertainty."[1] By introducing the resilience systems analysis, the OECD has advocated for more effective, cross-sectoral, and multidimensional programming through examining the interlinkages of different risks and vulnerabilities. On its side, the resilience agenda of the World Bank spans the areas of disaster risk management, climate change, and infrastructure as having an impact on development outcomes.

With its Global Strategy of 2016, the European Union has adopted an expansive approach to resilience, making it an integral part of its foreign policy role and objectives and one of the five priorities in its external action, alongside the other four priorities, namely the EU security, an integrated approach to conflicts, cooperative regional orders, and global governance.[2] In this sense, the approach to resilience in the context of the 2016 Global Strategy is a departure from the

[1] OECD, "Guidelines for Resilience Systems Analysis: How to Analyse Risk and Build a Roadmap to Resilience" (OECD Publishing, 2014), www.oecd.org/dac/Resilience%20Systems%20Analysis%20FINAL.pdf.

[2] "Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy," June 2016, https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf.

earlier usage of this concept by the European Union, which had its primary focus on development and humanitarian affairs, as formulated in "The European Approach to Resilience: Learning from Food Security and Crises" (2012), the Council Conclusions on the EU's approach to Resilience (2013) and the Action Plan for Resilience in Crisis Prone Countries (2013). In the EU parlance, the scope of resilience extends to the state and to societies, whereby "resilient society featuring democracy, trust in institutions, and sustainable development lies at the heart of a resilient state," while resilience itself is defined as "the ability of states and societies to reform, thus withstanding and recovering from internal and external crisis."[3] In this regard, the broader and multifaceted concept of resilience as developed and utilized by the European Union presupposes a broad range of pathways across a multitude of areas such as fostering "the resilience of democracies," strengthening "the resilience of critical infrastructure, networks and services" as well as to "nurture societal resilience also by deepening work on education, culture and youth to foster pluralism, coexistence and respect."[4] In geopolitical terms, resilience is a strategic priority for the European Union in its neighborhood policies across the east and the south, and also admits the interconnectedness between the internal and external dimensions of its operationalization.

NATO's Approach to Resilience

Similarly, as in the domain of sustainable development, the concept of resilience in defense and security is also evolving towards the inclusion of a wide-ranging and multidimensional set of vulnerabilities and associated mitigation strategies across the spectrum of military and non-military mechanisms of response. In this regard, NATO's resilience agenda tends to grow and take on new tasks as the understanding of risk factors and possible counter-strategies evolves with time.

The notion of resilience of NATO member states through maintaining and developing their individual and collective defense capacity is anchored in the Alliance's founding treaty of 1949 and, in particular, Article 3. This implicitly defined internal dimension of resilience in terms of capabilities and collective defense capacity is operationalized through NATO's defense planning and capabilities development process. The London Declaration issued at the NATO Leaders' Meeting on 3-4 December 2019 expands the conceptual scope of resilience by including, for the first time, the societies of NATO countries, alongside the resilience of critical infrastructure and energy security as well as secure and resilient systems to ensure the communications security of NATO countries. Apart from the resilience of societies, articulated explicitly for the first time, the other areas have already been part of NATO's resilience agenda.

The stronghold of NATO's resilience agenda lies within the area of civil preparedness, which comes as a necessity out of the rapidly changing security envi-

[3] "Shared Vision, Common Action."

[4] "Shared Vision, Common Action."

ronment and the strengthened defense and deterrence posture of the Alliance given the increased terrorist and hybrid threats targeting civil population and critical infrastructure on the Euro-Atlantic territory. At the Warsaw Summit in 2016, Allied leaders decided to enhance NATO's resilience to the full spectrum of threats and agreed on seven baseline requirements for national resilience against which member states can measure their level of preparedness.[5] These include assured continuity of government and critical government services; resilient energy supplies; ability to deal effectively with people's uncontrolled movement, resilient food and water resources; ability to deal with mass casualties; resilient civil communications systems; and resilient civil transportation systems.

The COVID-19 crisis tested the resilience preparedness of the Alliance and its member states, including in the health sector, which has not been explicitly identified as a distinct area of requirements prior to this, for example, in terms of medical stockpiles and preparedness in situations of pandemics. The pandemic tested the NATO mechanisms in place for consultations and coordination in times of an emergency and the speed of response to mitigate the consequences of the health crisis in both NATO countries and partners through the rapid response capacities vested into the Euro-Atlantic Disaster Response Coordination Centre (EARDCC) as NATO's principal civil emergency response mechanism. The COVID-19 crisis also exposed other aspects of resilience that need to be factored in, such as responding to disinformation in crisis situations and forging capacity to bounce back quickly from the negative social and political impact of the spread of false news in a crisis-stricken context. In parallel, the response to the pandemic has brought forward issues related to the robustness and reliability of supply chains in a fast-moving environment that warrants rapid response whereby oversight and control are expected to be limited and minimized and thus leading to the increase of the risk of fraud and mismanagement of resources. Therefore, while for NATO the resilience agenda is firmly anchored within the context of the Alliance's collective defense core task and its ensuing defense and deterrence posture and civil preparedness, the list of risks and vulnerabilities, to which resilience measures need to be developed and put in place in an anticipatory manner will inevitably grow.

The Resilience Agenda: Anticipating Risks and Vulnerabilities

In sum, the COVID-crisis has demonstrated the unpredictability and complexity of the resilience agenda and has put to test the resilience thinking of international organizations and national governments. The Global Risks Report 2020 of the World Economic Forum, published in January 2020, does not list pandemics or infectious diseases among the top ten risks in terms of their likelihood to oc-

[5] NATO official text, "Commitment to Enhance Resilience Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Warsaw, 8-9 July 2016," https://www.nato.int/cps/en/natohq/official_texts_133180.htm.

cur.[6] For 2020, the risks with the highest expected likelihood to occur are predominantly of an environmental nature, followed by two technological risks (data fraud and theft and cyberattacks), one societal (water crisis), one geopolitical (global governance failure), and one economical (asset bubble). In terms of impact, the first two highest-rated risks are climate action failure and weapons of mass destruction, the latter being the only risk of a geopolitical nature in this list, while the impact of infectious disease is ranked at the tenth place. Compared with previous years, the pandemic was perceived as a risk in 2007 in the fourth place in the ranking and in 2008 in the fifth place, which coincides with the outbreak of H5N1 virus infection. In the subsequent years, however, the perception of a pandemic risk has decreased, and it never made it to the first ten risks with the highest likelihood to occur, and certainly not so in the period preceding the COVID-19 crisis.

Therefore, the resilience thinking cannot exist in isolation from the capacity of international organizations and national governments to predict and anticipate which one of the plethora of risks and vulnerabilities will pose a security challenge at one time or another and respectively prepare coping mechanisms, consequence management and mitigation strategies. Understanding the whole range of potential security risks in their complexity, irrespective of perceptions as to their likelihood of occurrence is a condition *sine qua non* for the design of adequate and bespoke solutions, some of which may need years to be implemented and embedded into organizational systems in order to provide an effective response when needed.

Corruption as a Security Risk: Broadening the Resilience Agenda

If we define resilience as the ability to anticipate the emergence of vulnerabilities in the first place, irrespective of their low or high probability of occurrence, the analysis of the whole gamut of potential risks and their potential to pose security challenges should become the first step in the process of demystifying and disentangling the concept of resilience in its multifaceted nature. In this regard, corruption and poor governance, though identified as security risks, do not feature strongly on the resilience agenda. This could be explained by the prevailing notion of the low-impact effect produced as a result of it versus the high impact attached to other security risks such as proliferation of weapons of mass destruction or disruption of critical infrastructure.

In the analysis of global risks by the World Economic Forum, corruption falls into the group of geopolitical risks.[7] It was identified as a high-likelihood risk on its own at the high third place only in the 2011 annual report. The publication of the World Bank Grand Corruption Database in 2012, providing a collection of cases for the period between 1980 and 2011, as well as the accumulation of high-

[6] World Economic Forum, *The Global Risks Report 2020*, Insight Report, 15th edition, https://www.weforum.org/reports/the-global-risks-report-2020.

[7] World Economic Forum, *The Global Risks Report 2020*.

profile corruption cases of public officials and private companies in the lead-up to 2011, could account for the high rating of corruption as a global risk in 2011. In the 2020 annual report, corruption accounts as one of the factors contributing to the failure of national governance, defining it as "inability to govern a nation of geo-political importance as a result of the weak rule of law, corruption or political deadlock."[8] The link between corruption and failure of national governance is substantial and corroborates the challenges to governance and sustainability posed by corruption as a security threat. In 2020, the failure of national governance was ranked higher in terms of likelihood and impact compared to the risk of terrorist attacks.

For NATO, working on corruption as a security threat and on minimizing the risk of its occurrence in the defense and related security sector dates back to 2007 with the establishment of the NATO Building Integrity Program (NATO BI). This comes as a practical solution to operationalizing the NATO's Partnership Action Plan on Defense Institution Building (PAP-DIB), approved at the NATO Summit in Istanbul in 2004, with its ten principles that are considered fundamental to the development of effective and democratically responsible defense institutions, namely democratic control of defense activities; civilian participation in the development of defense and security policies; effective and transparent legislative and judicial oversight of the defense sector; effective and transparent arrangements and procedures to assess security risks and national defense requirements; effective and transparent measures to optimize the management of defense ministries and agencies with responsibility for defense matters, and associated force structures, including procedures to promote inter-agency co-operation; effective and transparent arrangements and practices to ensure compliance with internationally accepted norms and practices established in the defense sector, including export controls on defense technology and military equipment; effective and transparent personnel structures and practices in the defense forces; effective and transparent financial, planning and resource allocation procedures in the defense area; effective, transparent and economically viable management of defense spending; and effective and transparent arrangements to ensure effective international co-operation and good neighborly relations in defense and security matters.[9]

In their essence, these principles represent the requirements and the building blocks of resilience in an integrated manner – horizontally across all functional areas inherent in the operational functioning of defense institutions as well as vertically in a whole-of-government framework. Effective and efficient defense institutions are also by extension resilient institutions that have at their disposal the right mechanisms to maintain the integrity of the system in the first place and thus prevent the occurrence of negative phenomena. They also have

[8] World Economic Forum, *The Global Risks Report 2020*, 87.

[9] NATO, "Partnership Action Plan on Defence Institution Building (PAP-DIB)," January 7, 2004, https://www.nato.int/cps/en/natohq/official_texts_21014.htm.

in place coping mechanisms to bounce back from shocks to the system, should such occur.

NATO has defined the corruption-security nexus through its Building Integrity (BI) Policy endorsed by the Allied Heads of State and Government at the Summit in Warsaw in 2016.[10] The Policy itself and the Warsaw Summit Communiqué have articulated clearly that "corruption and poor governance are security challenges which undermine democracy, the rule of law and economic development" and that "transparent and accountable defense institutions under democratic control are fundamental to stability in the Euro-Atlantic area and essential for international security co-operation."[11]

At the NATO Summit in Brussels in 2018, building stronger defense institutions of NATO's partners, improving their good governance and strengthening their resilience, upon their request, has been identified as a distinct line of work within the context of the Alliance's efforts at projecting stability as part of its broad and strengthened deterrence and defense posture.[12] This is the closest that the issue of good governance and strong defense institutions has been brought to the core of the resilience agenda of the Alliance. While NATO is *de facto* working on strengthening the resilience of defense and related security institutions, the link still needs to be better substantiated, and the importance of strong institutions as a source and a guarantor of resilience requires to be articulated more recognizably. Moreover, the BI Policy applies to both Allies and partners and NATO as an organization and contributes to fulfilling the Alliance's three core tasks: collective defense, crisis management, and cooperative security.

Though not articulated visibly, the focus on good governance of the BI Policy is also aligned with NATO's resilience baseline requirements and in particular, the first one, which is related to the continuity of government and its ability to make decisions and provide services to the populations. This alignment between NATO's definition of corruption as a security threat with the resilience agenda is conceptually based on the causal link between national governance and the principles of integrity, transparency, and accountability both as a resilience mechanism in itself protecting against the probability of malpractices and malfeasance on one side and as an indicator of resilience at an institutional level, on the other.

[10] NATO, "NATO Building Integrity Policy, Endorsed by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016," July 9, 2016, https://www.nato.int/cps/en/natohq/official_texts_135626.htm.

[11] NATO, "Warsaw Summit Communiqué, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016," July 9, 2016, para. 130, www.nato.int/cps/en/natohq/official_texts_133169.htm.

[12] NATO, "Brussels Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11-12 July 2018," July 11, 2018, para. 50, www.nato.int/cps/en/natohq/official_texts_156624.htm.

Closing the Loop: Institutional Resilience and Building Integrity

The concepts of resilience and integrity share some common characteristics, particularly the positive approaches they introduce with regard to complex phenomena with negative clout in the context of security and development such as fragility, vulnerability, corruption, and poor governance. Similarly, the pathways to strengthening resilience and building integrity pass through a transformative change and normative adaptation, requiring interventions with a view to policy changes and institutional reforms at the level of organizational culture, mindset, and capabilities as well as individual capacities, attitudes, and behavior. Resilience puts the onus on the receiving end of an intervening action by an international organization, similarly as with the concept of integrity, which presupposes internal strength and endogenous capacity.

NATO Allies and partners have agreed on a definition of integrity when discussing the BI Policy, pointing to integrity as the link between behavior and principles. Furthermore, in NATO's definition, in institutional terms, integrity is directly linked to good governance. The BI Policy reaffirms that "reinforcing an institution's integrity is a question of institutionalizing the principles that we want the institution to stand for, as well as a question of socializing these norms and values among its personnel."[13] Thus, integrity exists at two levels – institutional and individual. The two levels constantly interact and reinforce each other through a dynamic process. Through a systems-based approach, NATO BI is focused on identifying and assessing gaps and vulnerabilities from the perspective of minimizing the risk of corruption through a diagnostic tool known as the NATO BI Self-Assessment and Peer Review Process. Based on analysis of national needs and integrity requirements, NATO BI provides tailored support and bespoke solutions, thus contributing to the resilience of defense institutions against malpractices, malfeasance, and fraud in different functional areas such as human resources management, financial resources management, budgeting and planning, procurement, lifecycle management, supply chains, logistics, assets disposals, etc.[14]

In this sense, institutional resilience is based on the totality of systemic factors and on the sum of mechanisms adept at withholding risks to the system across the different institutional functional areas that are interacting and are mutually reinforcing or undermining each other. For instance, a transparent and accountable merit-based system of recruitment and promotion will strengthen the system of procurement, assets management, or any other functional area by virtue of applying the principle of "the right person at the right place." In this regard, risks pertinent to respective areas as well as risks within each area need

[13] NATO, "NATO Building Integrity Policy."

[14] The NATO BI Process involves a Self-Assessment and Peer Review process conducted in NATO and partner countries on a voluntary basis; the questions explored in the process through the Self-Assessment Questionnaire can be accessed at www.nato.int/cps/en/natohq/topics_118004.htm.

to be itemized, assessed, and analyzed in accordance with their likelihood of occurrence and impact if they occur and consequently inform the development of new policy and procedures. This process also includes the organizational ethos, the sum of values and behaviors, and the pathways of their socialization throughout the organization.

Conclusion

Resilience has become a rallying concept for international organizations to bridge across different policy communities and break down sectoral silos. Being non-contentious and incontestable, the concept of resilience is attractive to policy-makers and implementers as a reference point when designing policies and programmatic interventions in a variety of contexts across multiple disciplines and sectors. However, resilience is one of those terms that may suffer from a definitive understanding of its conceptual parameters and practical implications. An analysis of risks and vulnerabilities with a stronger emphasis on the causal effects is warranted in the context of discussions as to how to operationalize resilience. NATO's work on building effective and efficient defense institutions and on minimizing the risk of corruption in the defense and related security sector through strengthening institutional resilience and organizational ethos of integrity, transparency, and accountability can broaden the discussion on resilience.

Disclaimer

The views expressed are solely those of the author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

About the Author

Dr. **Nadja Milanova** has extensive experience in international affairs, security matters, public diplomacy, and defense policy and defense reforms within a national and multilateral context. Since 2014, Dr. Milanova has served as Building Integrity (BI) Officer at NATO HQ, where she contributes her expertise to providing strategic advice and capacity building with regard to anti-corruption and good governance in the defense and related security sector. She joined NATO in 2006 as part of the Public Diplomacy Division and had previously worked for the Organization on Security and Cooperation in Europe (OSCE) as Head of its Prague Office. At a national level, Dr. Milanova has served as a diplomat at the Ministry of Foreign Affairs and as Head of the Bilateral and Regional Cooperation Department at the Ministry of Defense of Bulgaria. She also has experience in the field of human rights with advocacy work at UN and the EU. She holds a PhD in Politics from the University of Exeter, United Kingdom, MA in International Relations from the Fletcher School of Law and Diplomacy at Tufts University, USA, and MA in English Language and Literature from the Sofia University, Bulgaria.
E-mail: nadia.milanova86@gmail.com

Acknowledgment

Connections: The Quarterly Journal, Vol. 19, 2020 is supported by the United States government.