



The Concept of Resilience: Security Implications and Implementation Challenges

*Philipp Fluri*¹ and *Todor Tagarev*²

¹ *School of Diplomacy and International Relations, Seton Hall University, New Jersey, USA, <https://www.shu.edu/diplomacy/>*

² *Center for Security and Defense Management, Institute of ICT, Bulgarian Academy of Sciences, <https://it4sec.org/content/csdm>*

Abstract: Aiming for a more effective and efficient response to diverse and multidimensional threats, an increasing number of defense and security organizations, the United Nations, NATO, and the EU embrace the concept of resilience in their security strategies and policies. This article provides a brief overview of the concept, a sample of definitions used in policy documents, and the types of problems they seek to resolve. Then we introduce the reader to the 15 articles published in the Summer and Fall 2020 issues of *Connections* that present the evolution of the concept of resilience and its implementation by and within political, defense, and law enforcement organizations, as well as its anticipated contribution to cybersecurity, disaster preparedness, peacebuilding, post-conflict restoration and countering hybrid threats.

Keywords: resilience, theory, concept, institutions, police force, crisis management, disaster risk, Sendai framework, critical infrastructure, cybersecurity, maturity, hybrid threats, peacebuilding, stabilization, post-conflict reconstruction, NATO, European Union.

In recent years, the notion of resilience has experienced an astonishing expansion away from the area of its original application and transformation of its meaning. Originally it denoted the aptitude of material (objects and substances) bent, stretched, twisted, or compressed to spring back into the original form – in mechanics, the work required to strain an elastic body to the elastic

limit and “the work performed by the body in recovering from such strain.”¹ In psychological and medical contexts, it was then used metaphorically in cases of illness and setbacks to describe the psychological quality that allows people to be “knocked down by the adversities of life and come back at least as strong as before.”²

Its adoption by a variety of sciences and ‘discourses’ has both augmented and arguably inflated its meaning. In the latter (medical) field, the questions of describing resilience and what creates resilience, how to build resilience, and how to use it in a recovery process after traumatic events became important foci of research and debate. Resilience, thus understood, is more than ‘coping’ with a situation. It entails the (potential) ability to surpass and grow beyond a given state. It is also understood to be a quality that could be strengthened by investing into it adequately. In this sense, ‘resilience’ is now also used in business and environmental studies and defense and security, including human security.

This special two-volume issue (Summer & Fall 2020) of *Connections* focuses on the concept(s) of resilience in the spheres of defense and security (including human security). If usage of the term ‘resilience’ abounds in the non-security field, so it does inside the defense and security field – a situation that for merely pragmatic reasons necessitates a closer investigation of what different interest groups actually mean by the term. Its gross over-use may lead us to believe we understand it in all its implications which, in fact, we may not yet.

In the past decade, the concept of resilience evolved from a purely academic and engineering interest to dedicated incorporation in national and international security policies. One example of the former is Bulgaria’s 2016 cybersecurity strategy “Resilient Bulgaria 2020.”³ The resilience-based approach to cybersecurity, where resiliency is defined as “the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources,”⁴ is turning into a *de-facto* standard guiding both systems engineering and the search for adequate organizational arrangements.

The United Nations embraced the concept at the beginning of this century. In 2005, the World Conference on Disaster Reduction adopted the “Hyogo Framework for Action 2005-2015,” which placed the focus on strengthening

¹ Noah Webster, *Webster's Revised Unabridged Dictionary* (G. & C. Merriam Co, 1913).

² “Resilience,” Center for development of Security Excellence, n.d., accessed August 12, 2020, <https://www.cdse.edu/toolkits/insider/resilience.html>.

³ George Sharkov, “From Cybersecurity to Collaborative Resiliency,” Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense, Vienna, Austria, October 2016, pp. 3-9, <https://doi.org/10.1145/2994475.2994484>.

⁴ Ronald S. Ross, Victoria Y. Pillitteri, Richard Graubart, Deborah Bodeau, and Rosalie McQuaid, *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*, NIST Special Publication 800-160, vol. 2 (Gaithersburg, MD: National Institute of Standards and Technology, November 2019), p. xiv.

the resilience of nations and communities to disasters.⁵ The United Nations Office defined resilience for Disaster Risk Reduction as “the capacity of a system, community or society potentially exposed to hazards to adapt, by resisting or changing in order to reach and maintain an acceptable level of functioning and structure,” where this capacity “is determined by the degree to which the social system is capable of organising itself to increase this capacity for learning from past disasters for better future protection and to improve risk reduction measures.”⁶ Respectively, the Hyogo Framework for Action emphasized efforts to build resilience through enhanced national and local capabilities to manage and reduce risk and the use of knowledge, innovation, and education to promote a culture of resilience at all levels. The follow-up Sendai Framework for Action, adopted in 2015⁷ with a “renewed sense of urgency,” called for the integration of “both disaster risk reduction and the building of resilience into policies, plans, programmes and budgets at all levels.”⁸

The uncertainty and the unpredictability of the security environment are another reason to embrace the concept of resilience. Given the broad spectrum of threats and security challenges, the proliferation of conventional and unconventional conflicts, the fuzzy boundaries between military, asymmetric and hybrid threats, and the challenges brought by the COVID-19 pandemics, NATO turned to the need to enhance the resilience of each member state and the alliance as a whole.⁹

⁵ *Hyogo Framework for Action 2005-2015: Building the Resilience of Nations and Communities to Disasters*, World Conference on Disaster Reduction, Kobe, Hyogo, Japan, 18-22 January 2005, <https://www.unisdr.org/2005/wcdr/intergover/official-doc/L-docs/Hyogo-framework-for-action-english.pdf>.

⁶ *Hyogo Framework for Action 2005-2015*, p. 4.

⁷ *Sendai Framework for Disaster Risk Reduction 2015-2030*, Third UN World Conference, Sendai, Japan, 18 March 2015, <https://www.undrr.org/publication/sendai-framework-disaster-risk-reduction-2015-2030>.

⁸ *Sendai Framework for Disaster Risk Reduction 2015-2030*, p. 9. The Sendai framework uses a definition of resilience that was updated by UNISDR in 2009: “The ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions.”

⁹ NATO defines resilience as the society’s ability to resist and recover easily and quickly from such shocks as natural disaster, failure of critical infrastructure, or a hybrid or armed attack. Such ability combines both civil preparedness and military capacity. Robust resilience through civil preparedness in Allied countries is seen as “essential to NATO’s collective security” with a major contribution to “the credibility of NATO’s deterrence and defence.” NATO’s approach is anchored in Article 3 of its founding Treaty: by committing individually to maintaining and strengthening resilience, Allies reduce the “vulnerability of NATO as a whole”; hence resilience a national responsibility. Seven baseline requirements for such national resilience have been agreed – they concern the core functions of “continuity of government, essential services to the population and civil support to the military” (military efforts to defend the Alliance territory and populations needing ‘robust civilian preparedness to reduce po-

Resilience is also the central pillar of the European Union's strategy to deal with multidimensional hybrid threats that combine coercive and subversive measures, including CBRN hazards and disinformation.¹⁰ Again, member states are mainly responsible for strengthening resilience and enhancing response capabilities, while EU institutions reinforce national efforts.

Furthermore, the 2020 EU Security Union Strategy¹¹ and Counter-Terrorism Agenda¹² stress the importance of resilience and, in particular, the resilience of critical infrastructures. Hence, taking into account new policies and the lessons from the implementation of the 2008 European Critical Infrastructure Directive,¹³ the European Commission proposed replacing it with a new directive aimed at enhancing the resilience of critical entities providing essential services in the EU.¹⁴

Resilience has in the meantime been addressed and discussed by scientists, policymakers, and military planners seeking novel ways to increase the safety and security of organizations, communities, industrial sectors, critical infrastructures, armed and security forces and services, and societies in the face of new and unforeseen threats and challenges.

To reflect on conceptual and practical developments and outline options for shaping security and defense policies, we invited authors to comment on:

- the evolution of the concept of resilience
- investing in resilience vs. investing in prevention and preparedness
- measures of effectiveness and measures of performance

tential vulnerabilities – military forces again depend on the civilian and commercial sectors for transport, communications, and basic supplies such as food and water). See “Resilience and Article 3,” *NATO Topics*, Last updated: 16 November 2020, www.nato.int/cps/en/natohq/topics_132722.htm.

¹⁰ “Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats,” Joint Communication to the European Parliament, the European Council and the Council, JOIN/2018/16 final (Brussels: European Commission, 13 June 2018), <https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52018JC0016>.

¹¹ European Commission, “Communication from the Commission on the EU Security Union Strategy,” Brussels, 24 July 2020, COM(2020) 605 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605>.

¹² European Commission, “A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond,” Brussels, 9 December 2020, COM(2020) 795 final, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2020:795:FIN>.

¹³ “Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection,” *Official Journal L* 345, 75–82, 23 December 2008, <http://data.europa.eu/eli/dir/2008/114/oj>.

¹⁴ European Commission, “Proposal for a Directive of the European Parliament and of the Council on the Resilience of Critical Entities,” Brussels, 16 December 2020, COM(2020) 829 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:829:FIN>.

- lessons learned and good practices in the implementation of the concept of resilience.

As a result, the Summer and Fall 2020 issues of *Connections* include 15 original articles presenting the evolution of the concept of resilience in the defense and security sector, its implementation by and within political, defense, and law enforcement organizations, as well as its contribution to cybersecurity, disaster preparedness, peacebuilding, post-conflict restoration and countering hybrid threats.

In his foundational article, Peter Rogers proposes to look into the diverse and many origins of the concept of resilience, which make the pursuit of a unified theory both attractive and challenging. However, such difficulty has not deterred politicians and theoreticians alike from claiming to understand and apply the resilience concept to deal with *uncertainty*.¹⁵ Dr. Rogers argues that this desire to both reduce and totalize leads to a misunderstanding of the different points of emergence and the dynamics of the resilience concept.

Drs. Carmit Padan and Reuven Gal propose to map the multitude of definitions of resilience in a two-dimensional matrix, divided into four content categories: social, economic, political, and military.¹⁶ This matrix generates twelve sub-types of resilience and can subsequently be used for a comprehensive definition of resilience and its sub-aspects, as well as for the possible assessment of resilience in its various apparitions.

Resilience was also the dominant issue in discussions during the 2020 Transatlantic Security Jam.¹⁷ Dr. Dinos Kerrigan-Kyrou reports on the Jam's findings, with particular reference to the expectable Post-Covid future. The author states that whereas the pandemic has not created new global power conflicts, it has not resulted in enhanced cooperation needed to enhance resilience and limit human and economic losses. Its spread has exacerbated processes threatening international order, rules-based trade, international cooperation and coordination.

Dr. Nadja Milanova shows how the concept of resilience in defense and security is evolving towards the inclusion of a wide-ranging and multidimensional set of vulnerabilities and across the spectrum of associated military and non-military mitigation strategies. She argues that while corruption and poor governance are now recognized as security threats, the strengthening of defense and related security institutions in both Allied and Partners nations remains to be further embedded as an integral part of the resilience concept (as called for

¹⁵ Peter Rogers, "The Evolution of Resilience," *Connections: The Quarterly Journal* 19, no. 3 (2020): 13-32.

¹⁶ Carmit Padan and Reuven Gal, "A Multi-dimensional Matrix for Better Defining and Conceptualizing Resilience," *Connections: The Quarterly Journal* 19, no. 3 (2020): 33-46.

¹⁷ Todor Tagarev, Raphael Perl, and Valeri Ratchev, "Recommendations and Courses of Action: How to Secure the Post-Covid Future," in *Transatlantic Security: Securing the Post Covid Future*, edited by IBM (Wien: Federal Ministry of Defense, 2020), 18-41.

in the NATO Warsaw Summit Declaration). Institutional resilience based on integrity, transparency, and accountability is critical for ensuring the fulfillment of NATO's resilience commitment and its baseline requirements. These include continuity of government with the ability to make decisions and provide services to the population.

Dr. Marleen Easton and Vanessa Laureys present a case study on the effects of the terrorist attack at Brussels Airport on March 22, 2016, which explores police officers' experiences concerning their coping strategies after the terrorist attack and the (in)formal workplace social support that affected their resilience. The study provides an in-depth analysis into the coping strategies and processes of workplace social support that may contribute to police officers' resilience following a traumatic event. Besides, it offers insights into the police organization's best practices to foster its employees' resilience and job performance.

Mikio Ishiwatari, in "Evolving Concept of Resilience: Soft Measures of Flood Risk Management in Japan," shows how the concept of resilience has been evolving in light of and answer to changes in climate, the socioeconomic environment, technology adaptations, etc. Ishiwatari analyzes areas that affect resilience by reviewing the policy change of flood risk management, particularly soft measures, in Japan. Based on lessons from the evolving concept of resilience, he recommends that developing countries should not only invest in infrastructure but also consider soft measures regarding changes in socioeconomic and natural conditions.

This follow-on Fall 2020 issue of *Connections* includes contributions on resilience in cybersecurity, post-conflict peacebuilding, and human security.

The concept of resilience finds increasing application in the provision of cybersecurity, including attempts at measuring the level of resilience and organizational maturity. In the opening article, Dr. George Sharkov provides an overview of organizational and community cybersecurity and resilience maturity models and cybersecurity indexes and suggests that maturity needs to be placed in the focus of the second-generation national cybersecurity strategies.¹⁸

The contribution by Andras Hugi is dedicated to the development of hybrid warfare and cybersecurity capabilities in the Hungarian Defense Forces. Hugi tracks the application of the concept of resilience in Hungary, presents an elaborate scenario of a hybrid attack against the country, including a cyberattack, and, on that basis, outlines the key measures to strengthen the resilience at the national level and in the armed forces.

The theme of resilience to hybrid influence is then pursued by a team of Georgian authors led by Dr. Shalva Dzebisashvili. In the article "Russian Economic Footprint and the Impact on Democratic Institutions in Georgia," the au-

¹⁸ George Sharkov, "Assessing the Maturity of National Cybersecurity and Resilience," *Connections: The Quarterly Journal 19*, no. 4 (2020): 5-24.

thors provide sound statistical evidence on the Russian influence on Georgia's economy. On the example of media freedom, they claim that above a certain threshold, stronger Russian economic influence is positively correlated with the weakening of Georgian democratic institutes. The authors conclude that Russia's economic footprint has reached the 'redline' of 9 percent of Georgia's GDP, and significant effort is needed to reverse the trend and increase Georgia's resilience in its economic and political dimensions.

The following three articles address the resilience of stabilization and peace operations, and peacebuilding efforts. First, Dr. Philipp Fluri critically reviews the stabilization and reconstruction mission in Afghanistan and concludes that, notwithstanding numerous positive outcomes, it has been unnecessarily ambitious, not tailored to the environment, and aiming to build peace *for* Afghans rather than *with* them. In contrast, peacebuilding missions augmented with measures to enhance resilience, such as those in Guatemala, Liberia, and Timor-Leste, focus on local ownership and dialogue and may thus achieve long-lasting sustainable effects.

In her contribution, Veronica Waeni Nzioki reviews the evolution of international peace operations and how technologies are contributing to their resilience. Advanced technologies, such as drone-mounted sensors, sensor networks, and advanced communications, and innovative ways of their application, can increase the organizational agility and capacity for anticipation and foresight and thus contribute to operational success and peacekeepers' safety.

The contribution by María Julia Moreyra reminds us that women play a crucial role in family, community, and societal resilience. Hence, particularly with the account of the COVID-19 pandemics, the UN Women, Peace and Security Agenda provides a focus on governmental and international efforts to strengthen resilience and increase safety and security.

In the article "After the Crisis: The Role of Resilience in Coming Back Stronger," Giulia Ferraro examines the role of resilience in the disaster management cycle, on par with the prevention, preparedness, and response to crises of various origin. She then looks into the Sendai Framework for Disaster Risk Reduction as a good starting point for elaborating resilience measures and benchmarking within an overarching approach to crises.

Dr. Borislava Manojlovic provides the final contribution to this two-volume special issue of *Connections*. Through a series of problem-solving workshops involving South Koreans and representatives of North Korean communities living in South Korea, she explores the micro-level factors contributing to the resilience to conflict between the South and the North. Dr. Manojlovic finds out that the key to enhancing the resilience to conflict is the quality interaction among community members and promoting understanding, tolerance, and respect through education.

The editors would like to thank the authors for inspiring contributions and the Editorial Board of *Connections* for making these two volumes possible. The

combined contributions allowed us to document the evolution—and the expanding application in security policies—of a concept that may not have come to its end yet. Inevitably, therefore, this examination is preliminary and descriptive. It is certainly worth revisiting the topic in the future to examine what further developments the concept of resilience will experience, the evidence of its contribution to enhancing security, examples of good practice, and innovative ways of strengthening 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.

Acknowledgment

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

About the Authors

Philipp H. **Fluri**, DDr., is a co-founder and former deputy director of the Geneva Centre for the Democratic Control of Armed Forces (DCAF) and executive-in-residence of the Geneva Centre for Security Policy. After many years of working as a political advisor and educator on all continents, he is currently Sergio de Mello Chair, School of Diplomacy and International Relations, Seton Hall University, New Jersey. *E-mail*: drphilippfluri@gmail.com.

Todor **Tagarev** is a professor in the Institute of Information and Communication Technologies of the Bulgarian Academy of Sciences and Head of its Center for Security and Defense Management. An engineer by education, Prof. Tagarev combines governmental experience with sound theoretical knowledge and background in cybernetics, complexity, and security studies – a capacity effectively implemented in numerous national and international multidisciplinary studies, including ongoing Horizon 2020 projects in the fields of crisis management and cybersecurity. <https://orcid.org/0000-0003-4424-0201>