CONNECTIONS

THE QUARTERLY JOURNAL

CONNECTIONS SPECIAL ISSUE

PARTNERSHIP FOR
PEACE CONSORTIUM
OF DEFENSE
ACADEMIES AND
SECURITY STUDIES
INSTITUTES

SECURITY IMPLICATIONS OF THE CONCEPT OF RESILIENCE

EDITORS:
PHILIPP FLURI AND TODOR TAGAREV

FALL 2020

Partnership for Peace Consortium of Defense Academies and Security Studies Institutes

The views expressed and articles appearing in all *Connections* publications are solely those of the contributing authors and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium’s editors.

This edition is supported by the United States government. The Consortium’s family of publications is available at no cost at http://www.connections-qj.org. If you would like to order printed copies for your library, or if you have questions regarding the Consortium’s publications, please contact the PfPC at: PfPCpublications2@marshallcenter.org.

Dr. Raphael Perl	Sean S. Costigan
Executive Director	Editor-In-Chief and Chair, Editorial Board

ISSN 1812-1098, e-ISSN 1812-2973

CONNECTIONS

THE QUARTERLY JOURNAL

Vol. 19, no. 4, Fall 2020

Partnership for Peace Consortium of Defense
Academies and Security Studies Institutes

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

https://doi.org/10.11610/Connections.19.4

Contents

Vol. 19, no. 4, Fall 2020

Research Articles

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

George Sharkov, *Connections QJ* 19, no. 4 (2020): 5-24
https://doi.org/10.11610/Connections.19.4.01

Research Article

Assessing the Maturity of National Cybersecurity and Resilience

George Sharkov

Ministry of Defense, Republic of Bulgaria, https://mod.bg/

European Software Institute – Center Eastern Europe, Sofia, Bulgaria, https://esicenter.bg/

Abstract: This article provides an overview of maturity levels and assessment methodologies for the evaluation of cybersecurity and resilience in relation to their applicability and usefulness at sectoral and national levels. Reference maturity models and assessment frameworks, such as CERT Resilience Management Model, Cybersecurity Capacity Maturity Model for Nations, C2M2 (Cybersecurity Capability Maturity Model), are compared and analyzed for their applicability in designing and implementing national cybersecurity strategies and programs to achieve cyber resilience. Cyber readiness indexes are also outlined in view of their use to indicate possible improvements. The author explores the development of national cybersecurity strategies with a focus on cyber maturity and provides examples. A maturity-based approach for the Bulgarian cyber resilience roadmap is also described within the context of the evolving cyber-empowered hybrid threats and the need for an institutionalized collaborative public-private resilience.

Keywords: cyber resilience, capability maturity models, cybersecurity maturity assessment, maturity indicators, hybrid resilience

Introduction

Modern digitized societies and economies are globally interconnected and increasingly interdependent as a result of global digital connectivity and dependency on digital infrastructure, communications, and systems. The analysis of these interdependencies and emerging complex vulnerabilities and threats re-

Partnership for Peace Consortium of Defense
Academies and Security Studies Institutes

quires a holistic approach, which goes well beyond the personal, the enterprise, or the sectoral cybersecurity measures. The enhancement of cybersecurity and the protection of critical infrastructures require coordinated efforts at national, regional, and international levels. In addition, due to the multi-layered "cyber terrain" (a term introduced by the US Department of Defense, DoD, and further detailed by Shawn Riley[1]) and complex systems interdependencies, the new risks and threats become "unknown unknowns" and require upgrading of the established since centuries resilience principles of the society to the entirely new maturity level of "cyber resilience."

Achieving cybersecurity and resilience at the national level is a shared responsibility of all stakeholders – government, private sector, and civil society. Coordinated actions and a multi-stakeholder approach are required to develop and execute national cybersecurity strategies and plans. Various methodologies, guidelines, and templates for defining well-structured and comprehensive national or sectoral cybersecurity strategies are provided by world organizations like ITU, OECD, EU's ENISA, OSCE, standardization bodies, and academic research. Most of them have already postulated "cyber resiliency" as a new main goal to upgrade 'cybersecurity.' Strategies are also reflected in roadmaps outlining the steps and goals to achieve at different phases of the improvement plans. The challenge is how to evaluate the level of achievements, the efficiency, and effectiveness of the measures, and more generally, how to assess the overall level of readiness, capacity and objectively evaluate security and resilience capabilities at the sectoral and national level. There is also a need for a unified methodology to monitor the progress and to compare the achieved status among organizations, sectors, countries, and societies.

For decades, the approach based on maturity models has been widely used in IT companies and technology sectors, as well as by public procurement, starting with defense, to assess the organizations' readiness and capability to deliver high-quality products and services within the required scope, time and budget. On the other hand, organizations, communities, and nations must live and comply with a constantly increasing number of regulations, standards, and requirements, such as the NIST Cybersecurity Framework[2] and related NIST standards and EU Regulations, e.g., the "Cybersecurity Act"[3] with the expected Cybersecurity Certification Scheme, the "NIS Directive,"[4] and others. To cope with all that

[1] Shawn Riley, "Cyber Terrain: A Model for Increased Understanding of Cyber Activity," 2014, accessed September 15, 2020, https://www.linkedin.com/pulse/20141007190806-36149934--cyber-terrain-a-model-for-increased-understanding-of-cyber-activity/.

[2] "Cybersecurity Framework," ver. 1.1., 2018, NIST, USA, accessed October 10, 2020, https://www.nist.gov/cyberframework.

[3] "EU Cybersecurity Act," Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019, https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act.

[4] "The Directive on Security of Network and Information Systems (NIS Directive)," Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016,

and yet meet the organization's specific business goals, the maturity models and assessment methods turned out to be the most efficient and effective way for larger and smaller organizations.[5]

In this survey, we cover several most popular representatives of the huge diversity of cybersecurity maturity models and give a brief analysis of their suitability for application at a higher level for the purposes of community, sectoral or national cybersecurity maturity evaluation, and furnish national cybersecurity strategies with well-structured improvement programs, like "roadmap to maturity."

Maturity Models and Digital Society

The Origin and Types of Maturity Models

The concept of maturity models for software/ICT industry was initially sponsored by the US military who wanted to develop a method to objectively evaluate software/ICT subcontractors' process capability and maturity.[6] Due to various emerging technologies, standards, different sizes and capacities of the suppliers, there was a need to objectively assess in a unified manner the level of reliability, trust, and associated risks of software/ICT service quality. Maturity models provide a measurable transition as well between different levels (or steps, stages). They allow to compare organizations by their "maturity levels" and provide a structured and prioritized approach for improvement plans.

The maturity models can be grouped into three types:

- *Progression Maturity Models*, frequently illustrated by a 'journey,' represents a simple progression or scaling of an attribute, characteristic, indicator, a pattern where the movement up the maturity levels indicates the progression of attribute's maturity. Levels describe the next "higher states" of achievement, advancement, or 'steps' in the evolution and provide a clear transformative roadmap. In practice, however, they measure neither process maturity nor capabilities;
- *Capability Maturity Models (CMMs)*: the dimensions that are evaluated represent organizational capabilities around a set of characteristics, indicators, or patterns, often expressed as 'practices.' They are usually refer-

ongoing consultations for update in 2021, https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.

[5] Doug Hudson, Jason Macallister, and Mandy Pote, "A Guide to Assessing Security Maturity," White paper, Carbon Black, 2019, accessed September 15, 2020, https://www.carbonblack.com/resources/a-guide-to-assessing-security-maturity/.

[6] Richard Caralli, Mark Knight, and Austin Montgomery, "Maturity Models 101: A Primer for Applying Maturity Models to Smart Grid Security, Resilience, and Interoperability," White paper (Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2012), https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=58916.

red to as “process models.” The typical levels of CMM models are named around the *maturity of the processes*, for example:

ad-hoc → managed → defined → quantitatively managed → optimized

- *Hybrid Maturity Models* combine characteristics of progressive models with capability attributes from capability maturity models and reflect transitions between levels related to capabilities’ maturity while architecturally using the attributes, indicators, and patterns of a progression model. They are relatively easy to use and understand, especially in specific subject matter domains.

Maturity models, regardless of their type, have a similar structure that ensures a harmonized linkage between objectives, best practices, and assessments, and also facilitates the definition of improvement roadmaps between current capabilities and target ones within the context of business goals, standards, and domain-specific characteristics. A typical structure includes:

- *Maturity levels*: represent transitional states (also steps); in a hybrid approach they could be also mapped to “capability levels”;
- *Model domains:* groups of attributes and activities into areas, usually referred to as “process areas”;
- *Attributes:* the core content of the model, grouped by domain and level, based on practices, prescriptions, knowledge, standards;
- *Appraisal methods:* assessments in a unified manner that produce comparable and meaningful scoring (more than just checkboxes). The main use is to objectively evaluate adherence to the model, provide measurable indicators for achievements and progress, rather than comparing organizations. Appraisals could be formal (expert-led) and informal (including self-assessment);
- *Improvement plans (roadmaps):* appraisal methods provide an evaluation of the current state, gap analysis towards target level, identification of improvement scope and priorities, improvement planning, and verifying the results (achieving next or maintaining the current level).

Maturity Models for the Digital Society and Economy

The introduction and the early use of maturity models were in software/IT industry. After the first use of a staged maturity model by Richard L. Nolan in 1973, and the following work of Watts Humphrey, initially at IBM and after 1986 at the Software Engineering Institute (SEI), Carnegie Mellon University (CMU), the US Department of Defense requested a formalized process maturity framework from SEI by to be able to evaluate software contractors. In the early 1990s, SEI introduced the formal Capability Maturity Model (CMM) with five maturity levels. Subsequently, in 2002, a much more comprehensive and integrated model, Capability Maturity Models Integration (CMMI) was published, with the most popular version 1.3 of 2010. It applies to software engineering, systems engineering, software and systems acquisition, and service delivery as different constellations with a common core. The CMMI was further administered by the CMMI Institute (a spin-off of CMU), which was acquired in 2016 by ISACA. A new version 2.0 was released in 2018. The five maturity levels defined by CMMI to reflect the maturity of the established and institutionalized processes are:

Initial -> Managed -> Defined -> Quantitatively managed -> Optimizing

Since then, capability maturity models have been introduced widely in domains such as ICT infrastructure, all kinds of software engineering, service management, business process management, manufacturing, civil engineering, and cybersecurity. The CMMI Institute published in 2018 the "CMMI Cyber maturity Platform" to address the cyber resilience assessments.

Capability Maturity Models for Cybersecurity and Cyber Resilience

During the past decade, multiple cybersecurity and resilience frameworks have been proposed. A recent study [7] identified more than 25 research activities in 36 different industries attempting to achieve increased clarity about the scope, characteristics, synergies, and gaps that would facilitate scientific research advancement in this area. A 2017 technical mapping comparing maturity models used in various sectors, including education and awareness, provided another source for our survey.[8] The study classifies frameworks as either strategic or operational, by the hierarchy of their decision influence, by the attacks addressed, through the methods used and implementation area. As an exercise to determine the popularity of the terms, we conducted a simple search in Google Scholar, which brought more than 10,000 results for "cybersecurity maturity model," and around 12,000 hits for "cyber resilience maturity assessment." For our survey, we selected a few of the frameworks identified in previous research and added more recent work, as we aim at identifying the applicability at higher than organizational level (like sectors, community, nations), the similarity of assessment results, and possibilities for interdisciplinary, cross-sectoral and cross-border application. In the sub-sections below, we comment on some popular cybersecurity indexes.

CERT Resilience Management Model (CERT-RMM)

CERT-RMM became the reference model for cyber resilience developed by the CERT Division of SEI, Carnegie Mellon University. It had a strong influence on

[7] Daniel A. Sepúlveda Estay, Rishikesh Sahay, Michael B. Barfod, and Christian D. Jensen, "A Systematic Review of Cyber-resilience Assessment Frameworks," *Computers & Security* 97 (2020), 101996, https://doi.org/10.1016/j.cose.2020.101996.

[8] Angel Marcelo Rea-Guaman, Tomás San Feliu, Jose A. Calvo-Manzano, and Isaac Daniel Sanchez-Garcia, "Comparative Study of Cybersecurity Capability Maturity Models," in *Software Process Improvement and Capability Determination,* ed. Antonia Mas, Antoni Mesquida, Rory V. O'Connor, Terry Rout, and Alec Dorling (Cham, Switzerland: Springer, 2017), 100-113, https://doi.org/10.1007/978-3-319-67383-7_8.

most of the contemporary cybersecurity maturity assessment methods and frameworks. Although not explicitly stated in the title, the model is dedicated to achieving an operational resilience of organizations in a digitized society and economy, i.e., what we currently mean by *cyber resilience*. A stable version 1.1 of the model was published in 2011,[9] with an update to the last published version 1.2 in 2016.[10] The model is based on the "Operationally Critical Threat, Asset, and Vulnerability Evaluation" (OCTAVE) method for information security risk management and the experience of application in the financial and other sectors. The cyber risk management aspects have been combined with the process-oriented approach and common CMMI-related taxonomy, with terms like "process areas" and generic goals and practices, introduced along with mapping to the engineering and service delivery and continuity process areas from CMMI for services and development.

The model defines the following 26 process areas grouped in 4 categories:

- *Category "Enterprise Management"*: Communications; Compliance; Enterprise focus; Financial Resource Management; Human Resource Management; Organizational Training & Awareness; Risk Management;
- *Category "Operations Management"*: Access Management; Environmental Control; External Dependencies Management; Identity Management; Incident Management & Control; Knowledge & Information Management; People Management; Technology Management; Vulnerability Analysis & Resolution;
- *Category "Engineering"*: Asset Definition and Management; Controls Management; Resilience Requirements Development; Resilience Requirements Management; Resilience Technical Solutions Engineering; Service Continuity;
- *Category "Process Management"*: Measurement and Analysis; Monitoring; Organizational Process Development; Organizational Process Focus.

The "resilience strategy" is based on achieving resilience of the four basic assets: *people*, *information*, *technology*, and *facilities*. Thus, 'resilience' is 'translated' to *protect* and *sustain* measures for the assets. The structure of the model follows the classical CMMI architecture. For each of the 26 process areas, a set of specific goals (total of 94) are defined and must be fulfilled by implementing specific practices (251, typically with several sub-practices). The model prescribes the use of three generic goals and 13 generic practices to measure the level of maturity. To facilitate assessments, some more granulated Maturity In-

[9] Richard A. Caralli, Julia H. Allen, and David W. White, *CERT Resilience Management Model: A Maturity Model for Managing Operational Resilience*, CERT-RMM Version 1.1 (Boston, MA: Addison-Wesley, 2011).

[10] Richard A. Caralli, Julia H. Allen, David W. White, Lisa R. Young, Nader Mehravari, and Pamela D. Curtis, "CERT Resilience Management Model. Version 1.2," Technical Report, Carnegie Mellon University, 2016, https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=514489.

dicator Levels (MIL) were subsequently introduced. The mapping of capabilities levels to maturity indicator levels is shown below:

- *Capability Level 0*: *Incomplete* – MIL0: Incomplete;
- *Capability Level 1*: *Performed* – MIL1: Performed;
- *Capability Level 2*: *Managed* – with MIL2: Planned; MIL3: Managed; MIL4: Measured;
- *Capability Level 3*: *Defined* – MIL5: Defined and new MIL6: Shared (addressing the maturity for overall improvements of the community).

Cybersecurity Capability Maturity Model (C2M2) for Critical Infrastructures

The Cybersecurity Capability Maturity Model (C2M2) [11] was introduced in 2014 by the Department of Energy (US DOE) as an upgrade of an earlier version of C2M2 for the Electricity Subsector (ES-C2M2) by removing sector-specific references and making it applicable more widely to Critical Infrastructures. It was supported by the White House initiative led by the DOE, the Department of Homeland Security (DHS), and SEI, CMU. C2M2 is structured in 10 domains (listed in Table 1) and a set of practices per domain, which represent the capability in the domain. The practices are grouped by objectives and ordered by four maturity indicator levels (MIL0 to MIL3).

The 'objectives' are of two types – *approach objectives (one or more per domain, unique for domains)*, supported by a progression of specific practices, and *management objectives (one per domain),* supported by a progression of 'generic' practices that describe institutionalized activities. The progression is measured by a set of practices characterizing *maturity indicators levels*, applied to approach progression and institutionalization progression. Like in CMMI and CERT-RMM models, the MILs are 'cumulative.' The model is mapped to most of the known models and frameworks in information security and cybersecurity, like ISO/IEC 27001/2, NIST frameworks on cybersecurity, critical infrastructures, supply chains. Remarkably, all 10 domains with objectives and practices meet a subset of the CERT-RMM.[12] A new version 2.0 is currently under consultation.[13]

3-D Community Cybersecurity Maturity Model (CCSMM)

To face the problem that most government agencies, industry partners, critical infrastructure operators, school systems, nonprofit and other organizations exist and operate at the local level and are not equally prepared to defend against cyber threats that could affect the entire community, the Center

[11] Cybersecurity Capability Maturity Model (C2M2) Program, US Department of Energy, accessed September 30, 2020, www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0.

[12] Cybersecurity Capability Maturity Model (C2M2), Version 1.1, February 2014, https://www.energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf.

[13] Cybersecurity Capability Maturity Model (C2M2), Version 2.0, June 2019, https://apps.dtic.mil/sti/pdfs/AD1078768.pdf.

Table 1. The Domains in C2M2, New Version 2.0 (under Consultation).

Domains	Purpose statement
Risk Management	Establish, operate, and maintain an enterprise cybersecurity risk management program to identify, analyze, and mitigate cybersecurity risk
Asset, Change, and Configuration Management	Manage the organization's IT and OT assets, including both hardware and software, commensurate with the risk to critical infrastructure and organizational objectives
Identity and Access Management	Create and manage identities for entities that may be granted logical or physical access to the organization's assets. Control access to the organization's assets
Threat and Vulnerability Management	Establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities
Situational Awareness	Establish and maintain activities and technologies to collect, analyze, alarm, present, and use operational and cybersecurity information, status and summary information from other domains, to establish situational awareness for operational state and cybersecurity state
Event and Incident Response	Establish and maintain plans, procedures, and technologies to detect, analyze, mitigate, respond to, and recover from cybersecurity events and incidents
Supply Chain and External Dependencies Management	Establish and maintain controls to manage the cybersecurity risks associated with services and assets that are dependent on external entities, commensurate with the risk to critical infrastructure and organizational objectives
Workforce Management	Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel
Cybersecurity Architecture	Establish and maintain the structure and behavior of the organization's cybersecurity controls, processes, and other elements
Cybersecurity Program Management	Establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization's cybersecurity activities in a manner that aligns cybersecurity objectives with the organization's strategic objectives and the risk to critical infrastructure

for Infrastructure Assurance and Security (CIAS) at The University of Texas at San Antonio (UTSA) created the Community Cyber Security Maturity Model (CCSMM).[14] A program was developed to help communities (and states) im-

[14] "Community Cyber Security Maturity Model (CCSMM)," Center for Infrastructure Assurance and Security (CIAS) at The University of Texas at San Antonio (UTSA), accessed September 15, 2020, https://cias.utsa.edu/the-ccsmm.html.

plement the model and piloted in seven states helping them begin the development of their own programs,[15] as the community cybersecurity is arguably the weak link in the nation's cybersecurity chain. The 'levels' in CCSMM are less formal and defined as 'levels of improvement':

- *Level 1 – Initial*: some processes or programs may be in place, but a community does not have all the program elements for a basic program;
- *Level 2 – Established*: a basic program has been established with elements and processes in place for all four dimensions;
- *Level 3 – Self-Assessed*: a minimal viable and sustainable program has been implemented;
- *Level 4 – Integrated*: cybersecurity is integrated across the community, includes all citizens and organizations, the community is working with the state and other communities within the state;
- *Level 5 – Vanguard*: the community is maintaining a fully-vigilant cybersecurity posture.

These levels of improvement are focused on four areas called dimensions, shown in Table 2.

Table 2. Dimensions in the Community Cybersecurity Maturity Model (CCSMM).

Dimensions	Description
Awareness	Most people understand that cyber threats exist. However, not as many understand the extent of the threat, the current attack trends, how a cyber incident can impact a community, which vulnerabilities should be addressed, what the cascading effects may be if a community was under a cyberattack
Information Sharing	Addresses what to do with information on a cyber incident and where the information should be reported. In addition, how one sector can share information with another, allowing the second sector to potentially prevent the incident from occurring
Policy	Addresses the need to integrate cyber elements into the policies or guiding principles and includes all guiding regulations, laws, rules, and documents that govern the community's daily operation. Policies should be evaluated to ensure cybersecurity principles are reflected in everything we do and will establish expectations and limitations
Plans	Communities have established plans to address many different hazards and this dimension ensures cybersecurity elements are included in those plans enabling the community to address cyber incidents that could impact the operations of the community

[15] Natalie Sjelin and Gregory White, "The Community Cyber Security Maturity Model," in Cyber-Physical Security. Protecting Critical Infrastructure, ed. Robert M. Clark and Simon Hakim (Cham, Switzerland: Springer, 2017), 161-183, https://doi.org/10.1007/978-3-319-32824-9_8.

This model's distinguishing point is that it is 3-dimensional, with 'geography' added as a third coordinate, with three values: organization, community, and state. This 3-D Community Cybersecurity Model can serve to define a roadmap for individuals, organizations, communities, states, and the nation, and as:

- a '*yardstick*' to measure the present status of a community's cybersecurity program and attitudes;
- a *roadmap* to help a community understand the steps needed to improve its security posture;
- a *common point of reference* allowing individuals from different states and communities to compare and relate to individual programs.

It is declared to be compliant with other known frameworks, like the NIST Cyber Security Framework, the DoD's CMMC, and to support the Cybersecurity Workforce Framework from the National Initiative for Cybersecurity Education (NICE).

Cybersecurity Capacity Maturity Model for Nations (CMM-GCSCC[16])

CMM-GCSCC[17] is a methodical framework designed to review the maturity of a country's cybersecurity capacity. It was developed by the Global Cyber Security Capacity Centre (GCSCC) through a global collaborative exercise launched in 2014. For each of its five dimensions (shown in Table 3), the model provides factors (24 in total for this version), which define criteria to demonstrate the respective cybersecurity capacity. Most factors are examined from several viewpoints, and composed of a series of indicators within the five stages of maturity for each dimension, named as follows: *start-up; formative; established; strategic; dynamic.*

CMM-GCSCC is among the most popular assessment tools applicable to countries and regions, used by international organizations like ITU, Organization of American States (OAS), the World Bank, Oceania Cyber Security Centre, Cybersecurity Capacity Centre for Southern Africa, RAND Corporation, etc. It has been deployed to over 80 nations with more than 110 assessments and two regional studies by OAS. Many country profiles are publicly available and levels achieved could be reviewed, along with recommended improvements.[18] A new version is planned for publication in the second half of 2020. It should be noted that 'capacity' is not equivalent to 'capability,' and the model is less formal than maturity assessments, although dimensions and factors may match.

[16] Indicated here as "CMM-GCSCC" (vis-à-vis the original use "CMM"), to distinguish from the classical "Capability Maturity Model" by SEI, CMU.

[17] "Cybersecurity Capacity Maturity Model for Nations (CMM)," Revised Edition, accessed October 18, 2020, https://gcscc.ox.ac.uk/the-cmm.

[18] "GCSCC: CMM Reviews Around the World," Global Cyber Security Capacity Centre, accessed October 10, 2020, https://gcscc.ox.ac.uk/cmm-reviews.

Table 3. Cybersecurity Capacity Maturity Model for Nations (CMM of GCSCC).

Dimensions	Factors
Cybersecurity Policy and Strategy	National Cybersecurity Strategy; Incident Response; Critical Infrastructure (CI) Protection; Crisis Management; Cyber Defense; Communications Redundancy
Cyber Culture and Society	Cybersecurity Mindset; Trust and Confidence on the Internet; User Understanding of Personal Information Protection Online; Reporting Mechanisms; Media and Social Media
Cybersecurity Education, Training and Skills	Awareness Raising; Framework for Education; Framework for Professional Training
Legal and Regulatory Frameworks	Legal Frameworks; Criminal Justice System; Formal and Informal Cooperation Frameworks to Combat Cybercrime
Standards, Organizations, and Technologies	Adherence to Standards; Internet Infrastructure Resilience; Software Quality; Technical Security Controls; Cryptographic Controls; Cybersecurity Marketplace; Responsible Disclosure

Cybersecurity Assessment for Financial Institutions – CAT FFIEC Tool

In 2015, the US Federal Financial Institutions Examination Council (FFIEC) introduced the maturity-model-based Cybersecurity Assessment Tool (CAT)[19] for banking institutions to evaluate bank's risks and cybersecurity readiness by measuring levels of risk and corresponding controls. Five maturity levels are used: *Baseline, Evolving, Intermediate, Advanced, and Innovative*, based on five domains characterizing the institution's behaviors, practices, and processes that support cybersecurity preparedness. The five domains consist of a total of 15 "assessment factors" with 497 "declarative statements" used to assess the maturity level achieved per domain. The five domains are:

- Cyber Risk Management and Oversight
- Threat Intelligence and Collaboration
- Cybersecurity Controls
- External Dependency Management
- Cyber Incident Management and Resilience.

For each domain, the assessment determines a maturity level on the following scale:

- *Baseline*: The management reviews and evaluates guidelines;

[19] "Cybersecurity Assessment Tool," Federal Financial Institutions Examination Council (FFIEC), accessed September 30, 2020, https://www.ffiec.gov/cyberassessmenttool.htm.

- *Evolving*: Additional procedures and policies are set. Cybersecurity is increased to include information assets and systems;
- *Intermediate*: Detailed processes occur, controls remain consistent, risk-management is integrated into business strategies;
- *Advanced*: Cybersecurity practices and analytics are included in all businesses; continuous improvement in risk management processes;
- *Innovative*: There is driving innovation in the people, processes, and technology (new tools, new controls, new information-sharing groups).

CAT FFIEC is meant to be completed periodically, but also after significant technological or operational changes. It is a self-assessment, which could be validated by an auditor. After disputes on the "voluntary assessment," the tool has evolved to map better to the NIST Cybersecurity Framework (revision in progress since 2019). Auditors also increasingly require that companies complete an assessment to demonstrate CAT FFIEC compliance.

Cyber Resilience Review (CRR) by DHS

The self-assessment package was designed by the Department of Homeland Security (DHS) in partnership with the CERT Division of SEI, Carnegie Mellon University, as a derivative of the CERT-RMM tailored to the needs of critical infrastructure owners and operators.[20]

As in CERT-RMM, CRR considers that an organization deploys its assets (people, information, technology, facilities) to support specific operational missions or critical services. Then the assessment of capabilities in performing, planning, managing, measuring, and defining operational resilience practices and behaviors is performed in the following ten domains: Asset Management; Controls Management; Configuration and Change Management; Vulnerability Management; Incident Management; Service Continuity Management; Risk Management; External Dependency Management; Training and Awareness; Situational Awareness. The domains are derived from CERT-RMM and are similar to the ten domains of C2M2. The assessment is based on the CERT-RMM method and could be performed in two ways: self-assessment or in a facilitated session.

Cybersecurity Maturity Model Assessment (CMMC) by US DoD

CMMC is the new Cybersecurity Maturity Model Assessment requirement for all Defense Industrial Base (DIB) members that are suppliers to the DoD. All DIB companies will be required to get third-party certification to meet one of five maturity levels required to submit proposals on government contracts.[21] We include this model in the review as it contains the most detailed up-to-date requirements and assessment criteria not only for the organization's resilience but

[20] "Cyber Resilience Review (CRR)," Cybersecurity & Infrastructure Security Agency, accessed October 10, 2020, https://us-cert.cisa.gov/resources/assessments.

[21] Cybersecurity Maturity Model Certification (CMMC), www.acq.osd.mil/cmmc/.

for the entire ecosystem (such as national security and defense). The model specifies 17 capability domains with 43 capabilities and 171 practices across five maturity levels to measure technical capabilities: *Performed*, *Documented*, *Managed*, *Reviewed*, *Optimizing* (somewhat different from the levels in CMMI and CERT-RMM). The logic of the CMMC levels is different, as it provides a means of improving the alignment of maturity processes and cybersecurity practices with the sensitivity of the information to be protected and the range of threats. Accordingly, the levels are defined as:

Level 1: Safeguard Federal Contract Information (FCI)

Level 2: Serve as a transition step in the progression to protect CUI

Level 3: Protect Controlled Unclassified Information (CUI)

Levels 4-5: Protect CUI and reduce the risk of Advanced Persistent Threats.

The domains correspond to the security-related areas in Federal Information Processing Standards (FIPS) and the related security requirements from NIST frameworks. The 17 domains are: Access Control; Asset Management; Audit and Accountability; Awareness and Training; Configuration Management; Identification and Authentication; Incident Response; Maintenance; Media Protection; Personnel Security; Physical Protection; Recovery; Risk Management; Security Assessment; Situational Awareness; System and Communications Protection; System and Information Integrity.

Cyber Resilience Metrics of MITRE

We briefly cover one more systematic and architectural view of the MITRE methodology for assessing cyber resiliency which is based on the Systems-of-Systems (SOS) [22] approach and allows to define and assess the cyber resilience metrics at different levels and scope, going up to national and transnational enterprises:

- At the systems level, including directed systems-of-systems (SoS);
- Missions, including acknowledged SoS within an organization;
- Organizations where the CERT-RMM or the DHS CRR could be applied;
- Sectors (e.g., critical infrastructure sectors or sub-sectors), regions, and missions supported by multiple organizations, via collaborative SoS;
- Nations and transnational enterprises supported by virtual SoS.

The proposed metrics can facilitate the development of technical indicators to assess the risks and dependability (thus the possible cascading effects, escalating impact) of systems and then prioritize improvement programs.

[22] Deborah Bodeau, John Brtis, Richard Graubart, and Jonathan Salwen, "Resiliency Techniques for System of Systems: Extending and Applying the Cyber Resiliency Engineering Framework to the Space Domain," MTR 130515 (Bedford, MA: MITRE, September 2013), www.mitre.org/sites/default/files/publications/13-3513-Resiliency Techniques_0.pdf.

Cybersecurity Indexes and Maturity

With the increasing interest and ambition of nations to accelerate improvement programs and promote their achievements internationally, another instrument of evaluation and ranking countries' status is the international/global indexes. There are many indexes established already for decades in areas like information society development, digital readiness, internet connectivity, computer literacy, etc. ITU published in 2017 an "Index of cybersecurity indices" [23] with the most popular international cybersecurity indexes. We will comment on three of them with a focus on assessing countries.

Global Cybersecurity Index (GCI), ITU [24]: An assessment framework based on the Global Cybersecurity Agenda (GCA) of ITU. The GCI measures the commitment of countries to cybersecurity at a global level. The assessment measures a country's level of development or engagement through a question-based online survey structured along five pillars—Legal Measures, Technical Measures, Organizational Measures, Capacity Building, and Cooperation—using 25 indicators and additional sub-indicators, and then calculating an overall score. Since the first survey in 2013, GCI promotes cybersecurity initiatives through comparison. The third issue of GCI (in 2018), covering more than 193 countries and producing three regional reports, shows considerable improvements in cybersecurity worldwide, as more countries have cybersecurity strategies, national plans, response teams, and specific legislation. However, a significant gap between regions is still observed.

National Cybersecurity Index (NCSI) [25]: Global index, measuring the preparedness of countries to prevent cyber threats and manage cyber incidents, crime, and crises on a large scale. The Estonian e-Governance Academy develops it in cooperation with the Estonian Foreign Ministry. The index emphasizes the public aspects of national cybersecurity implemented by the central government. The index has 12 main indicators with sub-indicators, divided into three groups: General Cyber Security, Baseline Cyber Security, Incident and Crisis Management. The indicators have been tied to information society and cybersecurity issues such as e-identity, digital signature, and the existence of a secure environment for e-services. NCSI provides publicly available evidence materials and a tool for national cybersecurity capacity building. The country ranking is compared to GCI (ITU), the ICT Development Index, and the Networked Readiness Index.

[23] "Index of Indices," International Telecommunication Union, 2017, accessed October 18, 2020, https://www.itu.int/en/itu-d/cybersecurity/documents/2017_Index_of_Indices.pdf.

[24] "Global Cybersecurity Index," International Telecommunication Union, www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

[25] National Cybersecurity Index, Estonia, https://ncsi.ega.ee/.

Cyber Readiness Index 2.0 (CRI 2.0)[26]: Evaluates a nation state's cyber maturity as well as its overall commitment to cyber issues, defines the meaning of being "cyber ready" while proposing actionable blueprints to follow. The index uses a set of seven indicators: national strategy, incident response, e-crime and law enforcement, information sharing, investment in R&D, diplomacy and trade, defense, and crisis response. One hundred twenty-five countries were studied, and the methodology is based on similar pillars as those of the ITU's Global Cybersecurity Agenda. Each country is assigned a score, while the addition of military capabilities goes beyond that covered by the ITU GCI. However, CRI 2.0 does not offer any ranking despite its scoring mechanism.

Although these and other known indexes (Kaspersky Cybersecurity Index, Cyber Maturity in the Asia-Pacific Region, etc.) are quite popular and easy to promote countries, their use as cyber maturity assessment indicators is doubtful. The areas and indicators look similar to those of the maturity models, but they lack the rigor and granularity of the maturity levels and the assessments. There are no levels, and improvement plans could not be prioritized and structured with clear stages and targets. A higher rank in the index could be a success indicator, but it is unlikely to be set as a target. The question-based scores depend largely on the engagement and motivation of local bodies to provide evidence.

Focus on Maturity in National Cybersecurity Strategies

The focus on cybersecurity maturity is already incorporated, and maturity assessments are recommended in most of the updated manuals and guidelines for the development of national cybersecurity strategies. In ENISA's National Cyber Security Strategy (NCSS) Good Practice Guide (updated in 2016) [27] , there are two references to maturity and assessments during the lifecycle of strategy development and implementation. To establish baseline security measures, several complex aspects should be considered: different levels of maturity among the stakeholders, differences in terms of the operational capacity of each organization, and the different standards existing in each critical sector. Among the actions recommended is to "Create *maturity self-assessment tools* and encourage the stakeholder to use them." According to Recommendation 9: "*Enhance capabilities of the public and private sector*," after baseline requirements have been defined, existing capabilities need to be evaluated to identify gaps and deviations. To develop improvement plans and assess results, governments are advised to "actively support capacity building by publishing national standards, *designing cyber security capability maturity models*, promote and encourage the exchange of knowledge….."

[26] Cyber Readiness Index (CRI), Potomac Institute for Policy Studies, https://potomacinstitute.org/academic-centers/cyber-readiness-index.

[27] "NCSS Good Practice Guide," ENISA, https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

Nevertheless, a quick review of the national cybersecurity strategies (listed on ENISA's website) shows that the word "maturity" is barely mentioned, and "maturity levels" or models are not referred to. This observation might be incomplete, as the issue might be addressed in plans and roadmaps. Some of the mentions of cyber maturity and maturity models are:

- The UK strategy adopted in 2016 states that the UK Government's level of support for each sector is defined "taking into account its cyber maturity." A Cyber Assessment Framework (CAF) by NCSC is introduced to guide organizations from vitally important services;[28]
- in the third Cybersecurity Strategy of Estonia (2019) a "tested level of maturity" is considered among the main strengths of Estonia. Various areas of capabilities and maturity type of indicators are defined, with a detailed description of 'start' and 'target' levels, clear objectives and activity areas (which indeed makes it a good example of an actionable strategy), but no further elaboration on the eventual introduction of "cyber maturity models" or assessments are covered;
- the Cybersecurity Strategy of Lithuania (2018) specifies as its first target *"to strengthen cybersecurity in the country and to develop cyber defense capabilities"*;
- the strategy of Finland (updated in 2019) recommends that "each administrative branch make its risk assessment and maturity analysis...," which is further developed in the Implementation Program, where the Secretariat of the Security Committee will "*carry out a research project to create an updated maturity model and instrumentation for the purpose of monitoring the status of Finland's cyber security and the achievement of the goals … The maturity model and the instruments will be used to provide regular reports on the status …*"

Case Study: Resilience and Maturity in Bulgarian National Cybersecurity Strategy

A maturity-based approach, encouraged mainly by the experience in implementing the CERT-RMM, was selected in the development of the National Cybersecurity Strategy in Bulgaria, targeting "Cyber Resilient Bulgaria in 2020."[29] Cyber resilience was defined as a target state upon implementing the strategy. According to the strategy, "the achievement of cyber resilience at national level necessitates coordinated activities regarding the security and reliability of all cyberspace components and assets: information, technology, people and facilities, of the

[28] UK NCSC Cyber Assessment Framework (CAF), www.ncsc.gov.uk/collection/caf/cyber-assessment-framework.

[29] "Cyber Resilient Bulgaria 2020," National Cybersecurity Strategy (in Bulgarian), 2016, http://www.cyberbg.eu.

design and deployment of communication channels and services, their interdependency and interoperability."

The strategy has an "actionable architecture" and defines nine domains (areas) with several goals per domain and sets of measures (practices) with capabilities' indicators. For the description of 'maturity,' a three-layered definition of security in cyberspace is used, based on two well-established aspects[30]:

- the implementation of the fundamental 'triad' from information security of Confidentiality, Integrity, and Availability (CIA);
- the extent of our knowledge on risks and threats – adapting the *"known unknowns"* classification, coming from the finances and structured in Nassim Taleb's "Black Swan" theory, but also used in other fields, including for national security and cyberspace.

These two aspects helped to structure goals and measures at three levels and introduce them as a generalized 'label' to express the kind of maturity levels not only of the organizations, but also of the *state, ecosystems, community and nation.* These 'nested' levels are briefly outlined as follows:

- *Level 1 – Information/IT Security ("known knowns")*: protect and defend information assets and infrastructure against known "CIA threats";
- *Level 2 – Cybersecurity ("known unknowns")*: dealing with combined threats, various advanced persistent threats (APTs), attacks against the reputation of people and organizations, disinformation campaigns, and other unpredictable consequences of the mass migration of activities to cyberspace, large-scale information breaches (on a national, regional, and global scale) requiring enhanced and systematic application of the CIA concept to all assets of the digital ecosystem – people, facilities, technologies, and information (informal description of the cyber security);
- *Level 3 – Cyber Resilience ("unknown unknowns"):* preparing for the unknown: unexpected, unforeseeable threats in cyberspace, dynamically changing risks and complex impacts with unpredictable implications necessitating flexibility and resilience of systems, processes, and organizations, as well as introducing appropriate requirements when developing and deploying systems and processes – the essential characteristics of the status of cyber resilience.

Furthermore, the strategy implementation phases are defined as achieving the "maturity levels" and a *transition from cybersecurity to cyber resilience* for the entire country, namely:

[30] George Sharkov, "From Cybersecurity to Collaborative Resiliency," in *Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense (SafeConfig '16)*, 2016, ACM, New York, USA, 3–9, https://doi.org/10.1145/2994475.2994484.

Phase 1 – Initiation ("Cyber secure institutions"): Common agreement on the priorities of the National Cybersecurity Strategy and the Roadmap. Adopt a coordinated approach and establish a common national cybersecurity system framework. Define the main structures and core capacity, development processes, and principles in coordination with key stakeholders. Catch up with NATO and the EU and ensure baseline cybersecurity. Focus on the required basic level of *information security* and build upon it to achieve cybersecurity at the level of the individual organizations. Define "cyber crisis" in the National Cybersecurity Coordination Network. Conduct sector-specific and cross-sector exercises involving entities such as state bodies, businesses, and academia.

Phase 2 – Development ("From capacity to capabilities"): Focus on cyber-resilient organizations and cyber-secure society, develop a coordinated response to cyber crises at the national level. Continue the prevention activities, institutionalize a robust mechanism of interaction and collaboration in case of incidents and crises. Monitor the overall "cyber picture" (situational awareness). Build basic capabilities for operational and strategic analysis and assessment, operational and technical collaboration with NATO, EU, and other international networks.

Phase 3 – Maturity ("Cyber resilient society"): Effectively collaborate at the operational and strategic levels on a national and international scale. Based on the engagement and commitment of all stakeholders, develop advanced joint capabilities in public, private, and research sectors. Identify niches, and work for leading positions and specialization in the region, EU, and NATO.

Subsequently, the national Cybersecurity Act (2018) utilized the "capability levels" approach to define requirements for essential services and critical infrastructures. Target capability levels are defined as follows: 'Baseline' (corresponding to cyber hygiene from the NIS Directive), 'Cybersecure' (or 'performed,' as defined by the State Agency for National Security), and 'resilient' (defined by the Ministry Defense in accordance to civil resilience plans and engagements to NATO and EU collective defense).

As seen, hybrid threats (like disinformation) have been addressed already in *"Level 2 – Cybersecurity,"* but a more systematic coverage of the "hybrid influence," especially in the context of increased specific interest in Eastern Europe, is ongoing for the current update of the National Resilience Strategy and a Roadmap, incorporating the new cyber/hybrid influence (also known as '*cybrid*') to both areas – peoples' minds and critical infrastructures.[31]

[31] Todor Tagarev, "Understanding Hybrid Influence: Emerging Analysis Frameworks," in *Digital Transformation, Cyber Security and Resilience of Modern Societies*, ed. Todor Tagarev, Krassimir Atanassov, Vyacheslav Kharchenko, and Janusz Kasprzyk (Cham, Switzerland: Springer, 2021).

Cyber Maturity and EU, NATO Strategies

The maturity levels approach was recommended for the incorporation of cybersecurity in the "EU Common Security and Defence Policy" (CSDP). In a study performed by ENISA and the Science and Technology Options Assessment Panel of the European Parliament, three aspects of a safer cyber domain in the context of CSDP are considered.[32] In the area of Capacity Building, it is stated that to facilitate capacity building, one has to be able to measure it. The study recommends using cybersecurity capacity models that allow the development and monitoring of cyber capacities and their maturity. The Cybersecurity Capability Maturity Model (CMM of GCSCC) is mentioned.

Another study on EU Financial services discusses the "…degree of digital operational resilience and cybersecurity maturity" that needs to be considered.[33]

A novel maturity assessment framework, Cybersecurity Maturity Assessment Framework (CMAF), was recently proposed and implemented as a pilot in Greece, dedicated to assessing the compliance with the requirements of the NIS Directive. Two main applications of CMAF are foreseen: for self-assessment from operators of essential services and digital service providers (identified according to the NIS Directive as adopted by the Member States) or as an auditing tool from the competent national authorities for cybersecurity.

ENISA also provided a CSIRT Maturity Self-assessment Tool [34] to assist the capacity and capabilities development of national and sectoral CERTs.

In addition to the highly demanding maturity models introduced for defense acquisitions and military supply chain (like the US DoD CMMC, presented above), NATO uses the maturity levels approach to plan and assess the nations' cyber defense capabilities development according to the ongoing Cyber Defense Pledge.[35]

[32] EU Parliament, "Cybersecurity in the EU Common Security and Defence Policy (CSDP): Challenges and Risks for the EU," 2017, accessed September 15, 2020, https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2017)603175.

[33] European Commission, "Digital Operational Resilience Framework for Financial Services: Making the EU Financial Sector More Secure," Consultation Document, 2019, accessed September 15, 2020, https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/2019-financial-services-digital-resilience-consultation-document_en.pdf.

[34] ENISA, "CSIRT Maturity – Self-assessment Tool, accessed September 15, 2020, https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey.

[35] Jamie Shea, "Cyberspace as a Domain of Operations," *MCU Journal* 9, no. 2 (Fall 2018): 133-150, https://doi.org/10.21140/mcuj.2018090208.

Conclusion

To assess the cybersecurity and cyber resilience of a sector, community, country, or region, a unified approach to define goals and measurement indicators is needed. Capability maturity models provide such a mechanism since they implement a similar architecture and regardless of possible differences in scope and definitions of domains, they produce comparable scoring of achievements and facilitate the aggregation of target states. As shown, most of the popular models could naturally map, which allows organizations to choose the most suitable for their profile and business goals. At the national level, assessments and plans could still be effectively developed, as maturity and capability levels have identical meaning. However, this challenges the 'maturity' of the maturity models. Since 'cybersecurity' covers mainly the 'protection' side, resilience must be introduced to complete the protect-sustain cycle. Besides, new areas like cyber-empowered hybrid threats (named 'cybrid') should be introduced, as none of the models studied cover yet these aspects, and "*people's minds are not a sector that we know how to protect.*" Same for new disrupting technologies like AI, Quantum, 5G – the 'innovation' capability at higher maturity levels is not sufficient, and new domains and indicators will certainly be needed. Maturity models are helpful to align ambition and programs at a higher level (like EU Member States, US States, or regions). They are also recommended to attract and involve the SMEs in the "roadmap to maturity."

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

George Sharkov is an Adviser to the Minister of Defense and served as a National Cybersecurity Coordinator in the period 2014-2017. He led the development of the National Cybersecurity Strategy of Bulgaria, adopted in 2016. He holds a PhD in Artificial Intelligence and specialization in applied informatics, thermography, genetics, intelligent financial and security systems. Since 2003, he is the CEO of the European Software Institute – Center Eastern Europe, Head of the Cyber Resilience Lab (CyResLab), and since 2014 leads the Cybersecurity Lab at Sofia Tech Park. E-mail: gesha@esicenter.bg

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

Andras Hugyik, *Connections QJ* 19, no. 4 (2020): 25-38
https://doi.org/10.11610/Connections.19.4.02

Research Article

Best Practices in the Application of the Concept of Resilience: Building Hybrid Warfare and Cybersecurity Capabilities in the Hungarian Defense Forces

Andras Hugyik

Abstract: In its Global Strategy for foreign and security policy, the EU applies resilience as a comprehensive concept of internal and external security. In parallel, at the 2016 Summit in Warsaw, Allied leaders decided to boost NATO's resilience to the full spectrum of threats. Each NATO member needs to be resilient to a major shock caused by a natural disaster, failure of critical infrastructure, a hybrid, or an armed attack. Hybrid warfare, including cyberattacks, is recognized as a significant security challenge.

The National Security Strategy of Hungary, adopted in 2020, confirms that the primary international framework of Hungary's security and defense policy is NATO and EU membership and highlights the need to enhance the country's resilience against hybrid attacks. This article provides an analysis of the application of the concept of resilience in the Hungarian defense sector. It introduces the development of the resilience of the Hungarian Defense Forces against hybrid threats, including their cyber component, while generating options for the decision-makers regarding the military and information instruments of national power. The author identifies potential hybrid threats against Hungary, a possible cyberattack scenario, and lines of effort to achieve a feasible level of resilience to such threats. He takes account of the political and military environment, as well as wider national issues in view of hybrid threats and main features and dilemmas of cyber warfare, thus aiming to facilitate the application of the concept of resilience in Hungary.

Keywords: resilience, security policy, military, intelligence, hybrid warfare, cyber defense, EU, NATO, Hungary.

Introduction: Applying the Concept of Resilience in Hungary

The purpose of applying the concept of resilience is to strengthen the abilities of systems, organizations, policies, and individuals to respond well to external impacts. Many experts agree that "the recent enthusiasm for the concept of resilience across a range of policy literature is the consequence of its fit with neoliberal discourse. This is not to say that the idea of resilience is reducible to neoliberal policy and governance, but it does fit neatly with what it is trying to say and do."[1]

The ideology of neoliberalism primarily sees the guarantee of economic growth, welfare, liberty, and the common good in the 'liberalization' of markets. The neoliberal state radically departs from the redistribution of the welfare state, takes business- and market-friendly measures to protect private equity gain, and turns citizens into entrepreneurs and consumers.

The collapse of neoliberal hegemony after 2008 has led to a new wave of populism. Populist parties and movements include both left- and right-wing actors. One of their few common characteristics is that they all criticize the ruling elite and its ideology, claiming that the people are oppressed by the elites.

According to the left-wing rhetoric, the social and economic policy of Orbán's populist government in Hungary is strengthening the nation's capitalist class, selling out cheap workforce for foreign industrial investors while disciplining those workers, and performing centralized control of the poor, primarily living in rural areas. The purpose of its cultural policy is to promote the official Hungarian ideology of the era before 1938; a conservative, Christian, nationalist ideology with historical lies, an unjust social system, hateful atmosphere, and the hidden intention to recover territories lost after World War I. Orbán perceives the neoliberal European Union, the international capitalists' secret fraudulent practices represented by George Soros, and migrants as enemies to declare his political opponents as the enemy of the nation and to take the role of the rescuer of the nation.

While the government is attacking some of the EU's values in front of the political audience and is confronted loudly, in terms of economic processes, it is a subordinated ally of European capitalists.[2] Due to constructivist elements of Viktor Orbán's regime-building politics,[3] democracy, the rule of law, and plural-

[1] Jonathan Joseph, "Resilience as Embedded Neoliberalism: A Governmentality Approach," *International Policies, Practices and Discourses* 1, no. 1 (2013): 38-52, https://doi.org/10.1080/21693293.2013.765741.

[2] Tamás Gerőcs and Csaba Jelinek, "The System of Hungarian National Cooperation in the Context of the European Union – on Hungary's EU Integration in a Historical Sociological Approach," *Analízis* (2018): 12-33, quote on p. 23, www.regscience.hu:8080/xmlui/bitstream/handle/11155/1768/jelinek_nemzeti_2018.pdf, – in Hungarian.

[3] Gábor Illés, András Körösényi, and Rudolf Metz, "Broadening the Limits of Reconstructive Leadership - Constructivist Elements of Viktor Orbán's Regime-building Politics,"

ism in Hungary have become limited and resulted in the establishment of a country with illiberal democracy. In Hungary, those in power suggest that leftists and liberals are not part of the nation, and all that is left or liberal, be it the person, any artwork, or just a point of view or an approach, should be deemed as alien and should be rejected because that goes against the official national Christian conservative course.

Perhaps this political climate also contributes to the fact that in Hungary, only NATO-related defense sciences initiate develops of resilience-based security and law enforcement concepts. However, a more plausible explanation is that, as opposed to the generally accepted, comprehensive security policy and crisis management approach, in the case of resilience, we should focus on national-level solutions. Many Hungarian experts regard this as evidence of the appropriateness of the efforts to develop a comprehensive approach at the national level, which was launched in our country in 2010.

The majority of Hungarian security policy experts consider that in 2014, during the Ukrainian crisis, both NATO and the EU found the adequate response to hybrid threats in increasing nations' resilience and in supporting military efforts with civilian tools (civil preparedness). The very essence of this solution lies in the coordinated application of military and civilian crisis management components, which is also a basic principle of the comprehensive approach.

Therefore, it can be established that the background, the fundamental principles, and the toolset applied for resilience and civil preparedness are practically the same as the comprehensive approach itself; they are a mere re-interpretation thereof in a different context. Thus, resilience and civil preparedness did not bring about a different mindset or a set of requirements; yet, these cannot be regarded as identical to any already existing sets of tasks under any legislation.

Therefore, it is necessary to statutorily appoint a national coordinator for the purpose of both resilience and civil preparedness and to define the scope of national-level tasks, the bodies and the organizations responsible for their implementation, the cooperating organizations, and the procedural rules of cooperation. Given that the task requires close and comprehensive cooperation throughout the government, the effective implementation should fall within the competence and capabilities of the system of defense administration.[4]

The British Journal of Politics and International Relations 20, no. 3 (2018): 790-808, https://doi.org/10.1177/1369148118775043.

[4] László Keszely, "Hybrid Warfare and National Resilience, or a Comprehensive Approach Reloaded," *Katonai Jogi és Hadijogi Szemle [Military Law and Military Law Review]* 1 (2018): 29-62, quote on 61-62, – in Hungarian, http://epa.uz.ua/02500/02511/00008/pdf/EPA02511_katonai_jogi_szemle_2018_1_029-062.pdf.

Building Hybrid and Cyber Warfare Resilience Capabilities in the Hungarian Defense Forces

Introduction of the Hungarian Defence Forces

The Hungarian Defense Forces (HDF) is the national defense force of Hungary. Since 2007, the Hungarian Armed Forces is under a unified command structure. The Ministry of Defense maintains the political and civil control over the army. A subordinate Joint Forces Command is coordinating and commanding the HDF units.

The armed forces have 28,000 personnel on active duty. In 2019, military spending was 1.904 billion USD, or about 1.2 % of the country's GDP, well below the NATO target of 2 %. In 2016, the government adopted a resolution in which it pledged to increase defense spending to 2 % of GDP and the number of active personnel to 37,650 by 2026. Military service is voluntary, though conscription may occur in wartime.

According to the Hungarian Constitution, the three pillars of the nation's security are the strength of the HDF, the system of the Alliance, and the citizens.

In February 2017, the Ministry of Defence disclosed the Zrínyi 2026 development program, which intends to increase the capability of active armed forces, the manpower of reserve forces, the military communication and information system, and cyber defense. These measures seem to be adequate steps for building resilience to hybrid threats.

Approach to Improve Resilience to Hybrid Attacks

Hybrid warfare denotes "the use of military and non-military tools in an integrated campaign, designed to achieve surprise, seize the initiative and gain psychological as well as physical advantages utilizing diplomatic means; sophisticated and rapid information, electronic and cyber operations; covert and occasionally overt military and intelligence action; and economic pressure."[5] In other words, hybrid attacks combine military and non-military as well as covert and overt means, including disinformation, cyberattacks, economic pressure, and deployment of irregular armed groups, and use of regular forces. Nowadays, hybrid warfare is considered a significant security challenge; within this wider threat category are cyberattacks that are perceived as one of the main threats to the modern society for every country.

Figure 1 illustrates a project for the Hungarian Defence Forces in the field of resilience development against hybrid attacks based on the findings of Adrian

[5] James K. Wither, "Making Sense of Hybrid Warfare," *Connections: The Quarterly Journal* 15, no. 2 (2016): 73-87, quote on p. 76, https://doi.org/10.11610/Connections.15.2.06.

Feher.[6] Feher followed the steps of Army Design Methodology,[7] and hence describes the desired environment, defines the problem, and recommends an operational approach. Following a modification by this author, the project approach consists of six objectives, seven outcomes, and 15 proposed outputs in order to enhance the level of resilience against hybrid threats and thus protect the country. The figure aligns instruments of national power to each outcome.

The underlying logic of the proposed approach is that Hungary needs a hybrid defense strategy to combat potential hybrid threats. The military instrument of national power has to extend its impact and facilitate the improvement of information power, the development of information deterrence capacity to protect Hungary's sovereignty through citizenry's involvement. At the same time, there is a need for support from other agencies in establishing an informational deterrence capability to protect the population against hostile propaganda and cyberattacks. Since the military instrument is highly dependent on other instruments of national power, HDF must maintain and improve the collaboration with other stakeholders to establish a "whole-of-government" approach. The domain of information and the associated information operations play an important role in hybrid warfare. Historically, military operations have primarily focused on the enemy's capabilities and only secondarily on the weakening of its determination, while information operations target determination and willpower.

The aim of information operations is to achieve leadership supremacy, information domination, and information supremacy by employing psychological operations and operations on operational security, military deception, physical destruction, electronic warfare, public information, computer network warfare, and civil-military cooperation while using military information systems and intelligence information.[8] In the information operations doctrine currently applied by the Hungarian Defense Forces, the details of the concept of information operations have not yet been developed. The elements of information operations only partially reflect the activities and capabilities to be achieved in the information environment. Experts argue that the main challenge faced by the Hungarian Defense Forces is to attain the ability to address complex information issues: to quickly obtain, process, and integrate information into the decision-making cycle and to control the narratives of conflicts in the information space.

[6] Adrian Feher, "Hungary's Alternative to Counter Hybrid Warfare," Thesis (Fort Leavenworth, Kansas: U.S. Army Command and General Staff College, 2017), 128, 123, https://apps.dtic.mil/dtic/tr/fulltext/u2/1038681.pdf.

[7] Headquarters, Department of the Army, *Army Design Methodology*, ATP 5-0.1, July 1, 2015, https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/atp5_0x1.pdf.

[8] Zsolt Haig, "Methodology for Defining Critical Information Infrastructures, Information Warfare," ENO Advisory Ltd., August 1, 2009, p. 88, https://nki.gov.hu/wp-content/uploads/2009/10/a_kritikus_informacios_infrastrukturak_meghatarozasanak_modszertana.pdf; Zsolt Haig and István Várhegyi, "Interpretation of Cyberspace and Cyber Warfare," *Military Science* (2008): 5-10, in Hungarian, http://mhtt.eu/hadtudomany/2008/2008_elektronikus/2008_e_2.pdf.

Project aim: **Protect the Sovereignty and Independence of Hungary by Enhancing Resilience to Hybrid Threats**

Objectives	Outcomes and Instruments	Outputs
Possess a military deterrent capability to stop the enemy and support the intervention of NATO forces in Hungary	Increase the capability of volunteer conventional reserve forces **(M&I)** and establish volunteer unconventional reserve forces **(M&I)**	1, 2, 3, 4, **5**, 7, 9, 10, 12, 13, 14, 15
Maintain constitutional order and support the central government	Establish volunteer civil preparedness capability (M&**I**)	1, 2, 3, 4, 6, 7, 9, 10, 12, 13, 14, 15
	Achieve commitment of the citizenry to the nation's defense **(I)**	1, 2, 3, 4, **5**, 7, 8, 9, 10, 12, 15
Assist NATO allies under collective defense condition	Increase active-duty forces' expeditionary capability (M)	1, 2, 3, **5,** 6, 7, 8, 9, 10, 11, 12, 13, 14, 15
Develop information deterrence capacity	Protect citizenry against hostile influence warfare and national power against cyberattack **(I)**	1, 2, 3, **5**, 6, 7, 9, 10, 13, 15
Prevent surprise	Build Integrated Intelligence, Surveillance and Reconnaissance – Provide operational security **(I)**	2, 3, **5,** 6, 9, 15
Follow "Whole-of-government" approach in defense	Provide for interagency cooperation **(DIME)**	1, 2, 3, 4, **5**, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15

Outputs: (1) Increase patriotism via social and traditional media; (2) Cease false sense of security; (3) Reveal and refute false news; (4) Recruit volunteers; **(5) Increase cyber warfare capability**; (6) Improve counterintelligence to identify and detect warning signals; (7) Conduct joint and combined rehearsals (exercises); (8) Eliminate/ integrate extreme groups and establish the resistance movement; (9) Identify vulnerabilities and capability gaps; (10) Establish decentralized command and control with secure communications; (11) Enable quick response through the legal system; (12) Establish a system for readiness and mobilization; (13) Provide training and equip forces; (14) Build prepositioned stocks; (15) Ensure coordination of decision makers.

Figure 1: Project to Improve Resilience to Hybrid Attacks.

Abbreviations: DIME – instruments of Diplomacy, Information, Military and Economy; M (Military Instrument), I (Information Instrument), M&I (Military and Information Instrument).

At the same time, the operational cyberspace capabilities of HDF should be developed, and their integration into both military planning and operation implementation should be established. To that end, the Hungarian Defense Forces must adopt a new mindset primarily focusing not only on the execution of combat activities but also on the desirable outcomes of such military operations, including the impact of such outcomes. In military doctrine, a broader interpretation of the information tool system is necessary. Treating it as a mere supporting function will not suffice.

Cyber Defense in Hungary

The Main Aspects and Dilemmas of Cyber Warfare

Generally, in cyber warfare, states launch their operations for intelligence purposes with disruptive or destructive intentions and do so directly or through the involvement of third parties, such as hackers. Attacks may target critical public infrastructures, specifically the IT, information and communication systems used in the defense sector. In addition, hostile activities using social media and Internet platforms to influence civil society are increasingly common. In a broader sense, cyber warfare covers all attacks realized in cyberspace with a useable result for the attacker in military or political terms.[9] Experience has shown that a cyberattack only imposes a substantial burden on a country if it is coordinated (relates military control with a strategic goal, to which each operational activity is subordinated), comes in waves (types and targets of attacks are diverse, unpredictable and consecutive), is multi-sectorial (affects several industries, while defense coordination generally covers only a small scope of industries), is supported by information acquired by intelligence (information required for attacks is not only from open sources but also from intelligence collection and analysis) and is primarily realized to cause damage to the enemy. The aim is to make the country and its citizens feel the attack, i.e., such attacks must be very obvious and must involve emotional impacts –characteristics that set them apart from cyber espionage.[10] Cyberattacks are generally not used by states for destructive purposes in peace periods, as remaining in the “gray zone” between peace and war serves their best interests. This does not mean that they would not be able to go beyond this zone if necessary.

[9] Tibor Rózsa, “Theory, Practice and Tendencies of Information Operations,” *Defence Review* 5 (2019): 82-84; Gábor Berk, “Cyberspace, Its Dangers and the Current Situation of Cyber Defense in Hungary,” *National Security Review* 3 (2018): 5-21, http://epa.oszk.hu/02500/02538/00024/pdf/EPA02538_nemzetbiztonsagi_szemle_2018_03_005-021.pdf; Zsolt Csutak, “New Warfare of New Times – Cognitive Security in the Age of Information and Cyber Warfare,” *Defence Review* 5 (2018): 33-45, http://real.mtak.hu/84099/1/hsz_2018_5_beliv_033_045.pdf. – all sources in Hungarian.

[10] Csaba Krasznay, “Protecting Citizens in a Cyber Conflict,” *Military Engineer* 7, no. 4 (December 2012), 142-151, quote on p. 144, http://hadmernok.hu/2012_4_krasznay.pdf.

The main dilemma of cyber warfare is the missing international regulation for cyberspace. Although the majority of UN Member States recognize the extension of the scope of international agreements for cyberspace, their applicability is still problematic.[11] This is because there is no internationally accepted definition of what we call a cyberattack or a cyber weapon. In addition, in a cyberattack, there is usually no clear declaration of war, attackers remain hidden in cyberspace, and the impacts to be expected also remain unassessed. Therefore, serious attention is paid to the application of relevant conventions to cyberspace operations.[12]

The Paris Call for Trust and Security in Cyberspace Initiative[13] was set up to guarantee secure cyberspace on the international level. Hungary joined the initiative, but the largest cyber-arsenal owners (the United States, Israel, Iran, China, Great Britain, or Russia) did not consider this necessary.

NATO's Cyber Defense

Combating cyberattacks is a priority for NATO. However, regarding the commonly used terms of cyberwar or cyberattack, it should be noted that there is no agreed definition of cyberwar or cyberattack in NATO's official terminology, and examples of definitions can only be found at the level of member states.

This is mainly due to the limitless nature of cyberspace and the constant expansion of the range of attack types it accommodates, but also to the interests of the Alliance. NATO does not deem the definition of cyberattack necessary because it individually evaluates simultaneous but different types of attacks to decide upon the nature of the alliance-level response.

Since 2007, NATO has been paying particular attention to cyber defense and cyber warfare. In 2012, the cyber defense was included in the Alliance's defense planning, and NATO's cyber defense guidelines were adopted at the 2014 Wales Summit. In Wales, the Alliance declared that it recognizes the validity of international law in cyberspace and included cyber defense among NATO's collective defense tasks.[14]

In 2016, in the communiqué of the Warsaw Summit, allies extended the area of operational warfare traditionally covering sea, air, and land to include cyber-

[11] "Trends in International Law for Cyberspace," NATO Cooperative Cyber Defense Centre of Excellence, May 2019, https://ccdcoe.org/uploads/2019/05/Trends-Intlaw_a4_final.pdf.

[12] David P. Fidler, "The UN Secretary-General's Call for Regulating Cyberwar Raises More Questions than Answers," Council of Foreign Relations, March 15, 2018, www.cfr.org/blog/un-secretary-generals-call-regulating-cyberwar-raises-more-questions-answers.

[13] Ministry for Europe and Foreign Affairs, "Cyber Security: Paris Call of 12 November 2018 for Trust and Security in the Cyber Space," *France Diplomacy*, www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in.

[14] "Wales Summit Declaration," *NATO e-Library*, September 5, 2014, articles 72 and 73, https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

space[15] and declared that a cyberattack against a member state could be considered by the Alliance as an attack on NATO as a whole and, if necessary, they may take collective measures in response.

In Warsaw, the Cyber Defense Pledge was adopted, wherein member states undertook a significant and rapid development of the protection of their national networks and infrastructures in line with Article 3 of the Washington Treaty, development of comprehensive cyber defense capabilities, and strengthening the cooperation in identifying and understanding threats while enhancing cybersecurity education and training. An important step in the development of NATO's cyber defense capabilities is the establishment of the Cyber Operational Center (CyOC) to coordinate the Alliance cyber operations within the Supreme Headquarters Allied Powers, Europe (SHAPE), starting in 2018.

In its cyber capabilities, NATO distinguishes passive and active defense capabilities: the former consists mainly of preventive, incident management, data and system restoration capabilities within its own network range. The latter is a capability of an offensive nature to deter and eliminate threats beyond the scope of its own networks.[16]

Cybersecurity within the Hungarian Defense Forces

In Hungary, defense against cyber threats and the definition of cyberspace as a theater of war appeared in strategic documents as early as 2012. In 2018, cyberspace as an autonomous theater of operation was incorporated in the Hungarian legislation (Section 80 of Act CXIII of 2011). The directions and modalities of the development of Hungarian military cyber capabilities are set out in the National Military Strategy (2012), the National Cybersecurity Strategy (2013), the Cybersecurity Concept of the Hungarian Defense Forces (2013), the above Warsaw Commitments, and the Zrínyi Development Program until 2026.

The National Military Strategy has identified "the creation of opportunities for network-based warfare" as one of the main goals to be attained by the Hungarian Defense Forces. On the one hand, computer-network warfare is aimed at influencing, degrading, and making impossible the operation of the opposing party's networked IT systems and, on the other hand, it seeks to maintain the operation of our own similar systems.[17] The timeline of building these cyber ca-

[15] "Warsaw Summit Communiqué," *NATO e-Library*, March 29, 2017, articles 70 and 71, https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

[16] Susan Davis, "NATO in the Cyber Age: Strengthening Security & Defence, Stabilising Deterrence," NATO Parliamentary Assembly, April 18, 2019, pp. 4-6, www.nato-pa.int/download-file?filename=sites/default/files/2019-04/087_STC_19_E%20-%20NATO.pdf.

[17] According to Haig and Várhegyi, "Computer-network warfare includes the following activities: mapping the structure of computer networks; exploring hierarchical and operational features based on their traffic characteristics; registration of the content of the data flow on the network; deceptive, disruptive activity in networks; change

pabilities was defined in the Hungarian Defense Forces' Cybersecurity Concept. In this document, the initial level of cybersecurity capabilities had to be reached until 2014, the basic level cybersecurity capabilities between 2014 and 2016, and the full cybersecurity capabilities – after 2016. The concept aims, *inter alia*, to protect vital information system components, reduce their vulnerability, and eliminate potential damages as soon as possible.

Cybersecurity developments brought forth by the Hungarian Defense Forces form an integral part of the defense policy program. The HDF Electronic Incident Management Center was established in the framework of this program. In addition, further organizational and functional changes may be needed in the Hungarian Defense Forces to create a unified cybersecurity system. To that end, the type of cybersecurity organizations for the individual command levels should also be clarified. The main challenge in cybersecurity is to reduce response times and to enhance the efficiency of intelligence.

As of today, the majority of cybersecurity tasks of the Hungarian Defense Forces are performed by the Military National Security Service (MNSS). In recent years, in the implementation of MoD Instruction No. 85/2014, MNSS invested in the development of intelligence capabilities and capabilities, enabling the management of cyber incidents.

At a parliamentary hearing in 2019, the Chief of General Staff indicated that it had been foreseen to develop the cyber capabilities (non-existent at the time) in the near future. In 2020, the Government specified the areas within the Hungarian Defense Forces' cyber capabilities and operations that need to be applied or developed, and the Parliament added to the National Defense Act special rules regarding the military operations in cyberspace.[18]

Although the details are not entirely public, the 2020 defense budget shows that the cyber development of the military is a priority.

A Scenario of a Hybrid Attack against Hungary

It goes without saying that significant progress has been made at the national level in the field of cyber defense and security over the last ten years. However, we remain relatively defenseless and vulnerable to a well-structured, coordinated series of cyberattacks. According to Feher, these attacks can lead to

> the enemy's most dangerous course of action when the aggressor conducts full-spectrum hybrid operations, and it is able to procure enough supporters to fight against the central power, thus keeping the conflict under Article 5 threshold. With covert support from Special Operation Forces and conventional forces, the enemy can achieve fundamental surprise, paralyze the command and control system, successfully fight against Hungarian security forces,

and destruction of the program and data content of the target objects, and issues of protection against similar activities of the opposing party."

[18] Prime Minister's Office, *T/8029th Bill proposal* (12 November 2019), 5, 21-22, https://www.parlament.hu/irom41/08029/08029.pdf.

and establish functional alternative political power in occupied territories. In this situation, Hungary has to struggle without official NATO assistance in occupied or unoccupied lands.[19]

Based on this assumption and the thesis of Dr. László Kovács and Dr. Csaba Krasznay on a cyberattack scenario against Hungary,[20] I would like to present an escalation process that is completely conceivable today (Figure 2).

Findings

On December 10, 2019, the European Council adopted conclusions that set priorities and guidelines for EU cooperation to counter hybrid threats and enhance resilience to these threats. The conclusions call for a comprehensive approach to counter hybrid threats, working across all relevant policy sectors in a more strategic, coordinated, and coherent way.

In the case of Hungary, control over DIME, supportive and involved population, adequate military strength, effective intelligence and counterintelligence, and improved cyber resilience seem to be the relevant priorities, where resilience is defined as "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruption… [and] includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents."[21]

Cyber resilience is the ability of an actor to resist, respond, and recover from cyber incidents to ensure the actor's operational continuity.[22] Strategic cyberattacks could target the nation's critical infrastructure and utilities, whilst operational cyberattacks are against the adversary's military.

At the same time, a cyberattack is a type of information operations within the information warfare aiming to "corrupt, deny, degrade and exploit adversary information and information systems and processes while protecting the confidentiality, integrity, and availability of one's own information."[23]

The power in the information domain is vital for the nation to prepare the citizens for the negative influence of the enemy, keep or recover interactions

[19] Feher, "Hungary's Alternative to Counter Hybrid Warfare."

[20] László Kovács and Csaba Krasznay, "Digital Mohács: A Cyberattack Scenario against Hungary," *Nation and Security* 44 (February 2010): 44-56, in Hungarian, http://www.nemzetesbiztonsag.hu/cikkek/kovacs_laszlo__krasznay_csaba-digitalis_mohacs_.pdf.

[21] "Resilience," Glossary, NIST Information Technology Laboratory, Computer Security Resource Center (source: NIST SP 800-53 Rev. 4), https://csrc.nist.gov/glossary/term/resilience.

[22] Kjell Hausken, "Cyber Resilience in Firms, Organizations and Societies," *Internet of Things* (2020), 100204, https://doi.org/10.1016/j.iot.2020.100204.

[23] Anil Chopra, "Cyber Warfare a Key Element of Multi Domain Wars – Time to Push India," *Air Power Asia*, June 3, 2020, https://airpowerasia.com/2020/06/03/cyber-warfare-a-key-element-of-multi-domain-wars-time-to-push-india/

I.	Cyberattack (the first phase of a possible hybrid attack is a cyberattack)
I.1. Psychological operations	1. Intimidation: News about the alleged weakness of Hungarian cyber defense appears on a blog supported by a foreign secret service. 2. Distribution: The news that appeared on the blog are disseminated on social media, reaching tens of thousands of users. 3. Sharing: Due to sharing through pseudo-profiles created by foreign intelligence services, the news appears in more news flow and is spread further. 4. Highlighting: Due to the large number of sharing, the tabloid press also starts to cover the topic, and soon it becomes a topic in respected media as well.
I.2. Spectacular attacks	1. Overload attacks are launched against certain government websites, making some services unavailable for hours. 2. Some municipal and support agencies' websites are hacked, and messages threatening Hungary appear on their home pages. 3. Databases containing the personal data of tens of thousands of Hungarian citizens appear on the Internet.
I.3. Influencing politics	1. In a Wikileaks-type leak, government emails are published under the title HunLeaks; the international press begins to analyze them. 2. The "Hungarian Snowden" hands over classified documents to an investigative journalist. They are being analyzed by an international team of journalists. 3. An investigation ordered as a result of previous attacks finds sophisticated malware at the IT system of a public service provider. The purpose of malware is to obtain data. According to the report on the investigation, the malware has been running for at least two years.
I.4. Infrastructure attacks	1. Attacks on telecommunications: Most telecommunication services become inaccessible. Government communication is also hampered. Defense coordination slows down and is blocked. 2. Attacks on the finance system: Online banking is paused; international financial transactions are also suspended. 3. Attacks on electricity services and transport: District level power outages occur; transport is paralyzed.
II. Aggressor conducts full - spectrum hybrid operations	The aggressor conducts a combination of special and conventional military operations, uses intelligence agents, political provocateurs, media influence, economic intimidation, proxies and surrogates, paramilitaries, terrorists, and criminal elements. The aggressor can achieve a fundamental surprise, paralyze the command and control system, successfully fight against Hungarian defense and security forces, and establish functional alternative

	political power in occupied territories. In this situation, Hungary has to struggle without official NATO assistance in occupied or unoccupied lands.

	Resilience development at the national level	Resilience development at HDF level
I. Hybrid attack	Designate a national coordinator for resilience and civic preparedness, define the national tasks, bodies, and organizations responsible for and cooperating in their implementation, and procedures for cooperation. Defense administration seems to be the right system to ensure full-spectrum government cooperation.	Implement the proposed project (Figure 1) in order to achieve the desired aim (end-state), to protect the country by improving resilience against hybrid attacks. The figure aligns instruments of national power to each outcome.
II. Cyberattack	Raising information security awareness in society, strengthening cyber defense organizations, creating alternative, emergency infrastructures, strengthening the toolbox for coordinated, centralized cyber defense, strengthening partnerships between the administrative, business, and scientific spheres.	The main task of HDF is to deal with information challenges in a complex way: both to quickly obtain and process information and integrate it into the decision-making cycle, and to control the narratives of conflict in the information space. The operational capabilities in cyberspace and their integration into military planning and execution need to be established.

Figure 2: Possible Hybrid Attack against Hungary and Provision of Resilience.

between the state and the people, and terminate the citizens' false sense of security.

On the basis of NATO's interpretation, resilience at the national level is the combination of civilian preparedness and military capability.[24] This means that we should address the following challenges: raising information security aware-

[24] Gustav Pétursson, "NATO's Policy on Civil Resilience: Added Value for Small States?" SCANSE Research Project, Policy brief no. 5 (26 June 2018): 2, http://ams.hi.is/wp-content/uploads/2018/06/NATO%C2%B4s-Policy-on-Civil-Resilience-Added-Value-for-Small-States.pdf.

ness in society; strengthening cyber defense organizations, creating alternative, emergency infrastructures (elements); strengthening the toolbox for coordinated, centralized defense; strengthening partnerships between the administrative, business and scientific spheres; improving the resilience of HDF against hybrid warfare, including cyberattacks, by the execution of the proposals in this article.

To establish resilience against cyber threats, the HDF should be able to deal with information challenges in a complex way: both to quickly obtain and process information and integrate it into the decision cycle, and to control the narratives on the conflict in the information space.

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

Andras **Hugyik**, PhD in military science, is a retired police colonel, a chief councilor of the Hungarian police. He is an engineer, economist, and political expert. He is a former adviser to GUAM, OSCE, EUBAM, and UN – OPCW Joint Investigation Mechanism. Before joining these international organizations, he served in the Military Intelligence, the internal security service of the Hungarian law enforcement agencies, and the counter-terrorism center of Hungary.
E-mail: seniorhugyik@gmail.com.

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

S. Dzebisashvili, S. Kalashiani, I. Gabriadze, R. Beradze,
& M. Ejibia, *Connections QJ* 19, no. 4 (2020): 39-58
https://doi.org/10.11610/Connections.19.4.03

Research Article

Russian Economic Footprint and the Impact on Democratic Institutions in Georgia

Shalva Dzebisashvili,*[1] *Suzana Kalashiani,*[2] *Irakli Gabriadze,*[1] *Rezo Beradze, and Mirian Ejibia

[1] *The University of Georgia, https://www.ug.edu.ge/en*

[2] *International School of Economics at Tbilisi State University, https://iset.tsu.ge/*

Abstract: This article reexamines the infamous concept of the "Energy Empire," formulated by Anatoli Tchubais, and makes an attempt to reveal the instruments and ways of Russian economic influence in Georgia that lead to the formation of the so-called Russian economic footprint in the country, which in turn is effectively instrumentalized by Kremlin as a powerful tool for malign political influence and pressure. The problem is very much related to the ability of young and fragile democracies to develop resilient political systems and institutions, to withhold the pressure, and uphold the irreversible process of democratic transformation. The analysis of the major sectors of the national economy in Georgia reveals the critical dependence of major sectors on Russian operated companies as well as the growing aggregated weight of Russia's influence in the entire national economy. The preliminary results drawn from the sectoral analysis are augmented by a regression model applied to verify the interrelation between the dynamics of democratic institutional development and a selected economic variable, i.e., exports to Russia.

Keywords: Russian influence, economic footprint, Georgia, political institutions, economic infiltration, state capture.

Introduction

In its effort to restore itself into a global power center and secure dominance in the post-Soviet area, the concept of the "near abroad" or the exclusive sphere of influence found a broad recognition in Russian political and economic elites long before the Putin regime, at the very beginning of its rule, played with the idea of friendly relationships with the West.[1]

The concept of the "energy empire," originally developed by Anatoly Chubais, matured over time into a well-functioning model, in which the trade with gas and oil acquired not only economic but also political importance and allowed Moscow to exert influence in recipient countries, capitalize on it, and penetrate other sectors of national economy.[2] Multiple studies conducted in Europe proved that increased political influence had been directly linked to the phenomenon of initial "positive economic cooperation" turning into a source of negative and malign power.[3] Georgia, a country experiencing turbulent democratic transformation, is still far from having stable and resilient democratic institutions, capable of continuing political development and functional stability despite disruptive external interference. Thus, it is of high importance to study and reveal the economic foundations of Russian political influence and its general patterns that, as demonstrated in many cases, presumes dominance in key sectors of the national economy, through which it becomes possible to infiltrate, 'infect' and weaken political institutions, ultimately enabling Kremlin to exert significant influence (state capture) over the national political decision making (making it more pro-Russian). In the end, the targeted political institutions and the system itself become Russian-like, characterized by oligarchic rule and decline of democratic culture. Not to forget that Georgia, a country that energetically aspired for EU and NATO membership, is repeatedly confronted with the need to increase its institutional resilience, with the EU placing specific emphasis on economic diversification and energy sectors, and NATO highlighting the need for partner

[1] Sergey Karaganov, "Russia Is Forced to Defend Its Interests with Iron Hand," *Russia in Global Affairs*, June 3, 2014, http://globalaffairs.ru/pubcol/Rossiya-vynuzhdena-zaschischat-svoi-interesy-zheleznoi-rukoi-16460; Eduard Ponarin and Boris Sokolov, "Global Politics in Eyes of Russian Elite," *Russia in Global Affairs*, November 11, 2014, https://globalaffairs.ru/articles/globalnaya-politika-glazami-rossijskoj-elity/; Ivan Krastev, "What Russia Wants and Why?" *Russia in Global Affairs*, August 3, 2014, https://globalaffairs.ru/articles/chto-hochet-rossiya-i-pochemu/; Dmitri Trenin, "Russia in CSIS: Field of Interests and Not a Sphere of Influence," Carnegie Moscow Center, February 9, 2010, https://carnegie.ru/proetcontra/?fa=40690. All these sources are in Russian.

[2] Fiona Hill, *Oil, Gas and Russia's Revival* (London: The Foreign Policy Center, September 2004), 23, https://www.brookings.edu/wp-content/uploads/2016/06/20040930.pdf; Anatoli Tchubais, "Russia's Mission in the 21st Century," *Nezavisimaya Gazeta*, October 1, 2003, in Russian, https://www.ng.ru/ideas/2003-10-01/1_mission.html.

[3] Heather A. Conley, James Mina, Ruslan Stefanov, and Martin Vladimirov, *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe* (Washington, DC: Center for Strategic and International Studies, 2016), v.

countries to improve resilient institutions capable of thwarting external pressure and coercion.[4]

This study aims to fully understand the complexity of the Russian economic footprint in Georgia and its distribution among major economic sectors. Key economic players (enterprises) in each sector will be identified and tested to their political and economic dependence on Russia, which, once aggregated in sectors, will render a broader picture of Russia's economic influence (footprint) in each sector and the national economy in general. Further, the major variables of Russian economic influence will be subject of correlational analysis with the strength of democratic institutions, in an attempt to establish the evidence of interdependence patterns (more influence leading to the decline of democratic institutions).

Analytical Model and Methodology

The application of means of economic expansion for political purposes is a well-established feature of Russian foreign policy. Since there is little distinction between the state-controlled and private businesses, often intertwined in Russia, large-scale direct investments abroad bear a high likelihood of the state political interest lurking behind. In addition to establishing the picture of the Russian footprint in a number of economic sectors via shares in turnovers, GDP, export, and direct investments, we will take a deeper look into the nature and sources of financial capital, structure, and form of business ownership in each relevant sector. Due to the small size of the Georgian economy, some sectors experience a strong monopolization tendency, allowing few companies to dominate entire sectors, dictate "rules of behavior," and therefore directly or indirectly exert influence over politicians associated with the business activities in those sectors.

Consequently, the degree of importance of each sector for the national economy will be accessed via indexes, based on its share in the national GDP, employment, foreign direct investments (FDI), and export. Additionally, we include in the analysis economic fields such as Energy and Communication & Transport, regarded as critically important due to their strategic relevance for Georgia, not the least from a security perspective. Once the aggregated sectoral index is established, the threshold of 4 % will indicate whether the particular sector de-

[4] European Commission, "Eastern Partnership – 20 Deliverables for 2020: Bringing Tangible Results for Citizens," 2–3, accessed July 15, 2020, https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/eap_deliverables_factsheet_2017.pdf; "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," *NATO Press Releases*, July 11, 2018, https://www.nato.int/cps/en/natohq/official_texts_156624.htm; "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," *NATO Press Releases*, July 9, 2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

serves further investigation. Sectors above 4 %-index constitute nearly 80 % of the national economy, whereas eight sectors placed below 4 % have only the marginal effect of 2.3 %. Therefore, only in sectors that rank 4 % and above, major companies will be shortlisted and categorized in two groups: *Category-1* and *Category-2*. Companies with an annual income above 100 mln GEL and asset value over 50 mln GEL belong to the first category, and those companies with income from 20 to 100 mln Gel and asset value from 10 to 50 mln GEL are included in the second category. Next, companies from both categories had been color-coded into black (heavy Russian influence), red (partial risk of Russian influence), and green (free of Russian influence), in accordance with the degree of Russian political or financial influence assessed on the basis of a set of indicators such as Russian citizenship of the (co)owner, availability and transparency of business information, source of financial capital, offshore registration, etc. The share of 'black' and 'red' companies in each sector made it possible to assess the approximate scale of the Russian footprint, subsequently generating the entire picture of Russian economic influence on the macroeconomic level, i.e., the national economy. Finally, a regression model had been introduced, with the possibility to track the interdependence of the economic variables of Russian influence (such as export, direct investments, and money transfers) with the strength of the domestic (in Georgia) democratic institutions, evaluated on the basis of Freedom House and World Bank indicators.

Major Sectors of the Georgian Economy

Identifying major sectors allows us to analyze the national economy from a macroeconomic perspective and spot the true size and emphasis of Russian influence in the Georgian economy.[5] From the list of 14 economic sectors, those exceeding 4% share of the national GDP will be selected first and adding sectors' shares in national employment, FDI, and Export, an aggregated sectoral index will be created, allowing for a much more nuanced (relevance dependent) ranking of most critical sectors.

The aggregated index calculation applies the same 4 % threshold for the sectors under consideration and is based on 2003-2018 data. The results are not surprising, with Manufacturing, Transportation, Trade, and Construction as the top sectors in every regard. Accordingly, the next step of the study aims at measuring Russian footprint in the top sectors of the national economy and Russia's contribution to major economic indicators such as FDI, Export, and Visitors as major drivers and indicators for growing (or declining) Russian economic influence.

[5] "NACE Rev. 2 – Statistical Classification of Economic Activities," Eurostat, accessed February 5, 2020, https://ec.europa.eu/eurostat/web/nace-rev2; "Statistical Information," National Service of Statistics, accessed February 8, 2019, www.geostat.ge/ka.

Table 1: Sectoral Shares and the Aggregated Index.

Sectoral Share in GDP	%	Sectoral Share in Export	%	Sectoral Share in FDI	%	Aggregated Index	%
Wholesale and retail trade	19.4	**Manufacturing**	43.8	Transportation	23.2	**Manufacturing**	19.3
Agriculture, forestry and fishing	11.8	Wholesale and retail trade	28.7	Electricity, gas, steam and air conditioning supply	13.0	Mining and quarrying	3.0
Manufacturing	11.6	Transportation	12.7	**Manufacturing**	11.6	Trade	17.2
Transportation	9.4	Mining and quarrying	6.1	Financial and insurance activities	11.2	Agriculture, forestry and fishing	14.2
Construction	9.1			Construction	9.6	Transportation and communication	13.7
Health and social work activities	6.7			Real estate activities	9.2	Construction	6.2
Real estate activities	6.3			Hotels and Restaurants	6.9	Electricity, gas, steam and air conditioning supply	4.9
Education	5.5					Financial and insurance activities	4.1
Other service activities	5.0						

Russian Footprint in the Georgian Economy

This section takes a closer look at several macroeconomic indicators through which the dynamics and channeling of Russian economic activities in Georgia become visible. These include the size and structure (sectoral recipients) of Russian direct investments. Additionally, the nature and dynamics of the Georgian export to Russia, as well as the number of Russian visitors in Georgia will be reviewed to assess the degree of Georgia's sectoral vulnerability against shocks coming from Russia (for instance, a politically motivated embargo).

Foreign Direct Investments

Seemingly, the Russian FDI follows the general behavioral pattern of the total FDI (variability), although from 2014 on, it shows a general growth tendency (Figure 1). It must be noted that investments originating from offshore companies constitute a considerable share of the total FDI, and hence it is not possible to identify the original source. With high probability, Russian investors actively use offshore activities to move financial capitals to Georgia, thus bringing the real size of Russian investment to a much higher point.

The sectoral distribution of Russian investments is shown in Figure 2, with Finances (27 %), Manufacturing (17 %), Transportation & Communication (8 %), and Real Estate/Construction (8 %) mostly affected.

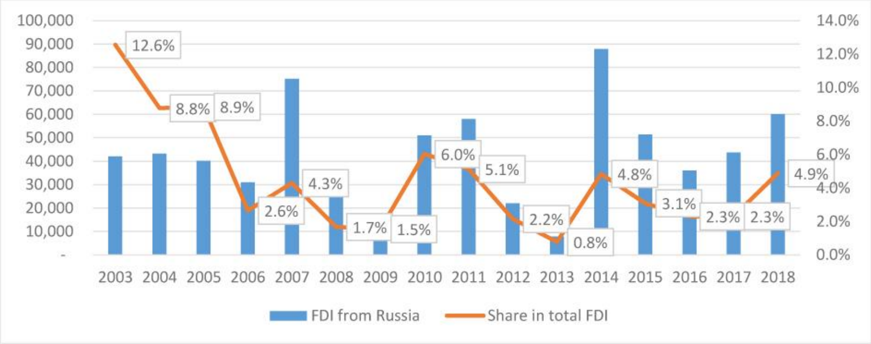


Figure 1: Russian Share in the Total FDI in Georgia.

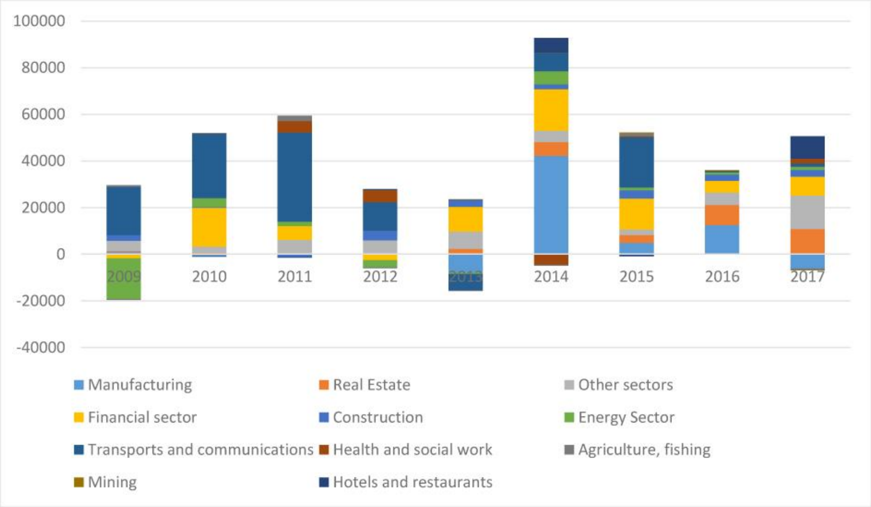


Figure 2: Sectoral Distribution of Russian FDI in Georgia (in 1000 USD).

Once again, it must be highlighted that due to the widespread practice of investments made by offshore companies, the share of sectoral distribution of real Russian investments can render a quite different picture. As for the average sectoral distribution of Russian FDI in the period between 2009-2017, Figure 3 shows a similar tendency of the biggest chunk of the pie taken by Transport & Communications (T&C), Financial sector, Manufacturing, and Real Estate.

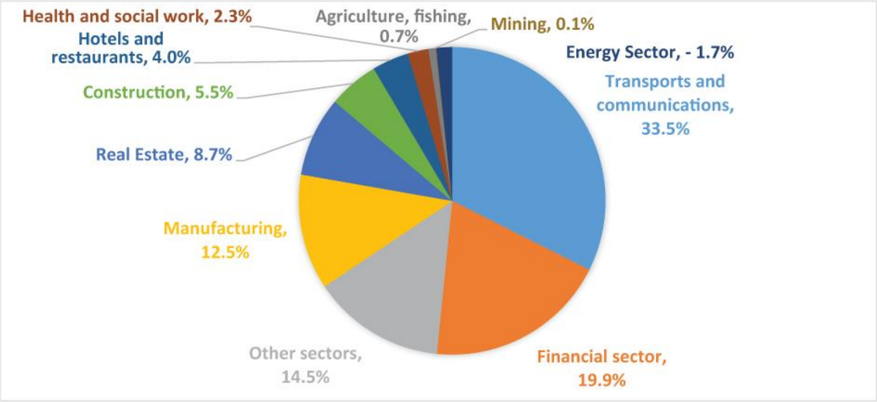


Figure 3: Average Share in FDI (2009-2017).

Exports to Russia

As clearly visible from the export to Russia dynamics (Figure 4), Georgia again is reaching the point where export volumes hit their records (15 %) similar to 2006, when Russia, driven by political motives, banned Georgian products and imposed a total embargo. The possibility of similar drastic action with respective shocking consequences for the Georgian economy should not be dismissed at all.

There are a handful of sectors that dominate Georgian export to Russia, and Manufacturing (48 % growth) and Agriculture had experienced exceptional growth rates taking the lion's share in overall export, as provided by statistics of export sectoral distribution in Figure 5.

Visitors from Russia – Tourism

The growing dependence of the Georgian economy, and in particular tourism, from Russian visitors is clearly visible from the steady growth of visitors from 8.1 % (share of the total) in 2011 to 19.5 % in 2018.

Given the high susceptibility of Russian tourism to Kremlin's political preferences, i.e., a touristic boycott of the targeted country, Georgia is definitely approaching a point after which Russia's punitive measures would have serious negative implications on the Georgian economy. Travel restrictions imposed after the so-called "Gavrilov Night" in June 2019 hit the touristic sector heavily and

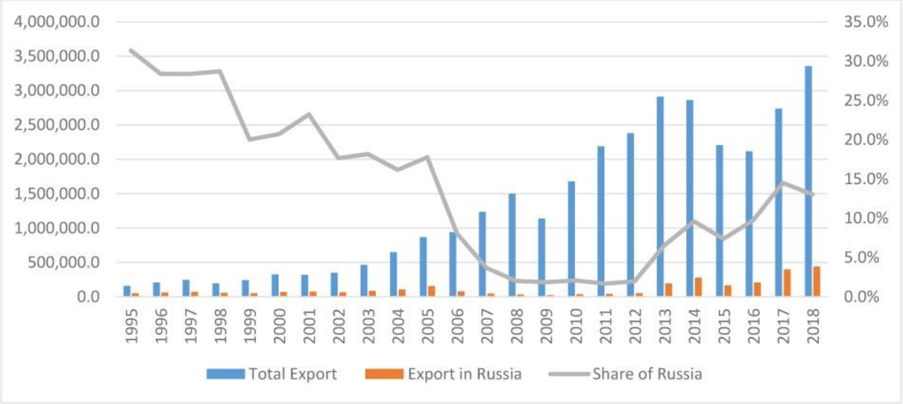


Figure 4: Export to Russia (Thousand USD).

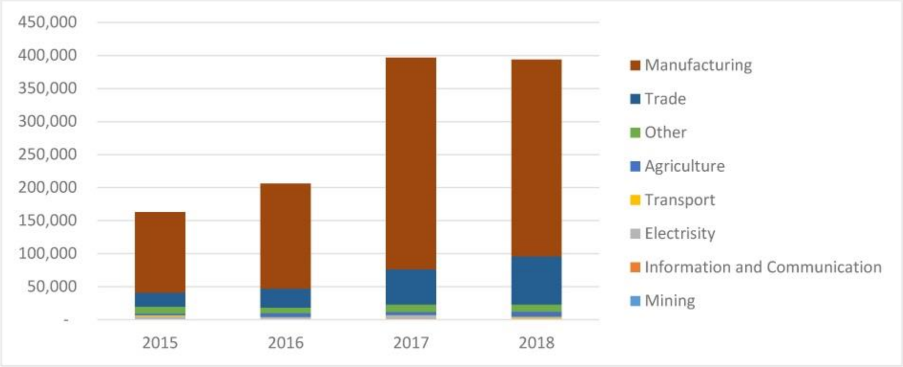


Figure 5: Export to Russia by Sector (2015-2018, 1000 USD).

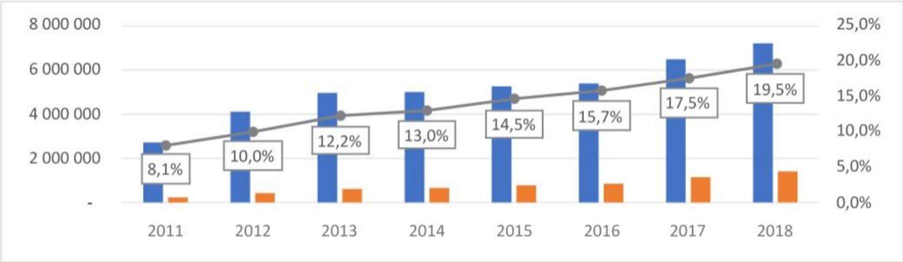


Figure 6: International Visitors (incl. from Russia).

once again proved the standard wisdom of not trusting Russia while opening up for economic cooperation.

In conclusion, we can confirm that key macroeconomic indicators for the Georgian economy, such as FDI, Export, and Tourism, show a steadily growing economic dependence on Russia. Formally traceable Russian financial capital flows go primarily into T&C, financial, and manufacturing sectors of the Georgian economy. This is rather alarming, as T&C is officially recognized as strategically important. The financial sector so far enjoyed an incomparably high degree of "freedom of action" compared to the dire conditions of the Russian financial sector, directly dependent on Kremlin's political goodwill. Although the share of Georgian export to Russia in overall export volumes reached the level of 2006, the absolute number and volume of goods exported to Russia by far exceed those in 2006. Therefore, the risk of repetitive use of economic sanctions for a political purpose has become even greater, with a much higher probability of political pressure and fear of negative socio-economic effects in Georgia.

Analysis of Major Sector Related Companies

Clearly, an article's limited scope will not allow to encompass all active enterprises in Georgia and conduct an intensive, in-depth analysis to reveal the financial sources, existing control, and thickly entangled mechanisms of influence in each sector. Rather, a more limited yet valid approach has been selected by identifying major *Category-1* and *Category-2* companies in each economic sector.[6]

Those belonging to *Category-1* had to meet the following criteria: annual income over 100 mln GEL and asset value exceeding 50 mln GEL. *Category-2* includes all companies with income from 20 to 100 mln Gel and asset value from 10 to 50 mln GEL. Smaller enterprises were excluded from the scope of analysis, despite their considerable number, since the focus on companies in dominant positions in the respective economic sectors. Thus, the study may generate an objectively limited picture of the Russian 'footprint' in major companies of the most relevant sectors of the national economy; yet, to a high degree, the results can be generalized and considered valid for the remaining companies, i.e., the entire sector. Second, companies from both categories were color-coded into black (heavy Russian influence), red (risk of or partial Russian influence) and green (free of Russian influence) based on a set of indicators for the degree of Russian political or financial influence, including Russian citizenship of the (co)owner, availability and transparency of business information, source of financial capital, offshore registration, etc. Ultimately, the purpose of this section is to calculate in percentage points the share of Russian-dominated (black and red) companies in major economic sectors, i.e., the Russian footprint in the national economy.

[6] "Useful Information," Service of Financial Accounting, Accountability, Monitoring and Audit," n.d., https://saras.gov.ge/.

Companies in 2017

The total number of companies in both categories is 397, 85 in Category-1, and 312 in Category-2, respectively. Concerning the turnover of the entire national economy, companies of both categories reach a turnover share of 37 %. Considering that we did not include smaller companies (categories 3 and 4) in our analysis, the real turnover of the "Russian influenced" companies should be related not merely to the mentioned 37 %, but to a much higher percentage. Out of 397 companies, 110 (28 %) are either 'black' or 'red.' This is a quite alarming number indicating that nearly one-third of the major enterprises in Georgia, that is to a various degree under the Russian influence, make 9.2 % of the national business turnover and heavily dominate mining (63.4 %), energy (36.6 %), and agricultural (24.7 %) sectors (see Table 2).

Table 2. Black and Red Companies in National Economy 2017.

Sectors: Red and Black	Number	Income, 2017, 000	Turnover of the Sector 2017, 000	Share
Wholesale and retail trade	40	3,402,388	32,816,300	10.4 %
Energy (power, gas, steam and air)	10	1,077,826	2,943,600	36.6 %
Manufacturing	21	764,329	8,532,100	9.0 %
Mining and quarrying	2	425,717	671,400	63.4 %
Transportation and storage	11	244,178	4,699,500	5.2 %
Information and communications	6	240,913	1,657,700	14.5 %
Construction	7	219,768	7,051,200	3.1 %
Agriculture, forestry and fishing	5	105,192	425,900	24.7 %
Real estate activities	8	101,187	1,090,900	9.3 %
Total	**110**	**6,581,498**	**71,740,300**	**9.2 %**

Fifty-one out of 397 (13 %) 'black' companies in Categories 1 and 2 make 4.7 % of the total business turnover, heavily dominate mining (63.4 %) and energy sectors (27.7 %), and have a substantial footprint in transport and construction (Table 3).

Table 3. Black Companies in National Economy 2017.

Sectors: Black	Number	Income 2017, 000	Turnover of the sector 2017, 000	Share
Wholesale and retail trade	16	1,331,814	32,816,300	4.1 %
Energy (power, gas, steam and air)	7	815,995	2,943,600	27.7 %
Manufacturing	13	438,095	8,532,100	5.1 %
Mining and quarrying	2	425,717	671,400	63.4 %
Transportation and storage	6	240,913	1,657,700	14.5 %
Information and communication	3	61,844	7,051,200	0.9 %
Construction	2	58,196	425,900	13.7 %
Agriculture, forestry and fishing	2	24,863	1,090,900	2.3 %
Real estate activities			4,699,500	0.0 %
Total	**51**	**3,397,436**	**71,740,300**	**4.7 %**

Companies in 2018

In 2018 a total of 414 companies belonged to either Category-1 or Category-2, illustrating a growth rate of 4 % as compared to 2017. They provided 34.2 % of the total business turnover (a decline of 2.8 %). Black and red companies (114 in total) make 8.6 % of the national business turnover, which is comparable to the data of 2017, though with a slight decrease (Table 4). The black companies (55 in total) make 4.5 % of total business turnover and dominate mining, energy, transportation, and construction sectors (Table 5).

Within the period from 2017 to 2018, a total of 415 companies had been extensively reviewed, of which 55 were coded as black (fully Russian dominated) and 59 as red (at risk or partially influenced), which makes 27.5 % of all companies in the Categories 1 and 2 (Table 6).

The number of red or black companies has grown from 110 in 2017 to 114 in 2018. Due to the lack of information on turnover for 34 large companies from this list in 2018, we assume the same level of turnover on average as in 2017, and thus their share in the total turnover remains around 9 % (Table 7).

Table 4. Black and Red Companies in the National Economy, 2018.

Sectors: Red and Black	Number	Income 2018, 000	Turnover of the Sector 2018, 000	Share
Wholesale and retail trade	42	4,052,831	37,409,500	10.8 %
Energy (power, gas, steam and air)	10	1,087,385	3,294,600	33.0 %
Manufacturing	22	858,090	9,212,300	9.3 %
Mining and quarrying	3	453,276	7,171,300	6.3 %
Transportation and storage	7	318,786	5,054,000	6.3 %
Information and communication	11	222,291	749,300	29.7 %
Construction	6	214,555	1,275,300	16.8 %
Agriculture, forestry and fishing	8	132,136	446,900	29.6 %
Real estate activities	5	107,873	1,750,800	6.2 %
Total	**114**	**7,447,225**	**86,625,200**	**8.6 %**

Table 5. Black Companies in the National Economy 2018.

Sectors: Black	Number	Income, 000	Turnover, 000	Share
Wholesale and retail trade	18	1,702,435	37,409,500	4.6 %
Energy (power, gas, steam and air)	7	879,467	3,294,600	26.7 %
Manufacturing	14	491,109	9,212,300	5.3 %
Mining and quarrying	3	453,276	749,300	60.5 %
Transportation and storage	6	214,555	1,750,800	12.3 %
Information and communication	3	79,879	7,171,300	1.1 %
Construction	2	61,441	446,900	13.7 %
Agriculture, forestry and fishing	2	51,169	1,275,300	4.0 %
Real estate activities			5,054,000	0.0 %
Total	**55**	**3,933,331**	**86,625,200**	**4.5%**

Table 6. Companies Reviewed and Color-coded.

Sector	Green	Red	Black	Total
Real estate activities	13	6	2	21
Transportation and storage	22	11		33
Agriculture, forestry, and fishing	3	3	2	8
Mining and quarrying	2		3	5
Wholesale and retail trade	125	24	18	167
Construction	55	4	3	62
Information and communication	7		6	13
Energy (power, gas, steam, and air)	14	3	7	24
Manufacturing	60	8	14	82
Total	**301**	**59**	**55**	**415**

Table 7. Year on Year Change of the Turnover of Red and Black Companies.

Sectors: Red and Black	Number 2017	Number 2018	Change	Share 2017	Share 2018	Change
Wholesale and retail trade	40	42	2	10.4 %	10.8 %	0.5 %
Energy (power, gas, steam and air)	10	10	0	36.6 %	33.0 %	-3.6 %
Manufacturing	21	22	1	9.0 %	9.3 %	0.4 %
Mining and quarrying	2	11	9	63.4 %	29.7 %	-33.7 %
Transportation and storage	11	7	-4	5.2 %	6.3 %	1.1 %
Information and communication	6	5	-1	14.5 %	6.2 %	-8.4 %
Construction	7	3	-4	3.1 %	6.3 %	3.2 %
Agriculture, forestry and fishing	5	8	3	24.7 %	29.6 %	4.9 %
Real estate activities	8	6	-2	9.3 %	16.8 %	7.5 %
Total	**110**	**114**	**4**	**9.2 %**	**8.6 %**	**-0.6 %**

Among the top 100 companies exporting to Russia, 23 companies in 2017 belong to category 1 or 2. Out of these 23, nine are black (7) or red (2), i.e., 39 %, and represent the manufacturing (bottling) sector of the economy exclusively.

- The *manufacturing industry* itself belongs to the risky sector, due to the 22 companies color-coded black and red, making nearly 9 % of the total turnover in the sector;
- The *wholesale trade* sector harbored 42 black and red companies with a share of the respective total turnover of 10.4 % (3.4 bn GEL) in 2017;
- Although only five black and red companies were identified in the *agricultural sector* (2017), their share in the sectoral turnover was 24.7 %;
- The *energy sector*, a strategic sector in Georgia, exhibited ten companies coded in black or red, making 36.6 % (1.1 bn GEL) of the total turnover of the sector;
- There are only six black or red companies in another sector of strategic importance – *Information and Communication*. However, their total share of the sectoral turnover is more than 14 %. Interestingly, in the field of mobile communications, Russian-owned *Beeline* controls 23.9 % of the market, which is a significant size considering the short period upon entering the local market.[7]

The companies under the full or partial Russian influence firmly occupy 9 % of the Georgian businesses. At first glance, this number seems quite low; yet, as we have included only a limited number of companies (Category 1 and 2) in our analysis, and smaller companies would have certainty exposed a large number of red and black companies as well, the real Russian footprint could be even larger. The Russian dominance exposes a significant growth dynamic once the leading economic sectors are considered, and have already approached an alarming threshold. In some sectors, the percentage of the Russian footprint is far larger than the nationwide average, often represented by a handful of companies (e.g., two companies in the energy sector controlling 25 % and two companies in agriculture with 18 %). Furthermore, in almost all dominated sectors, "Russian influenced" companies enjoy the exclusive role of natural monopolies, thus dictating price conditions and fully in control of the "rules of behavior" in the sector. Thus, it can be agreed that 9 % of the national turnover under Russian control can be accepted as the crossing line, beyond which begins the area of heavy and dangerous economic dependence.

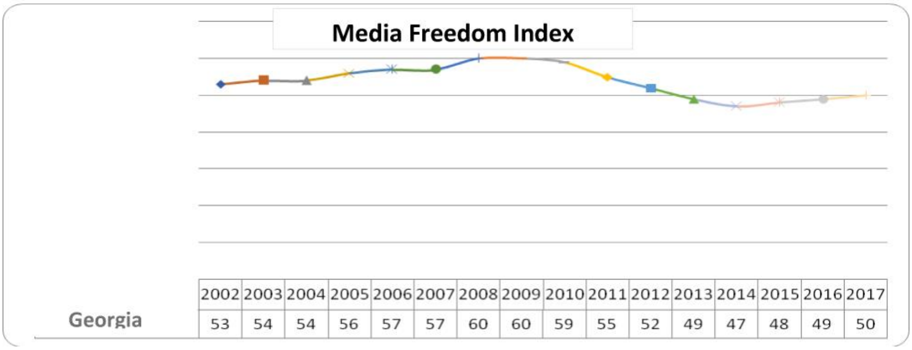
Media Analysis

Due to the immense importance of free media in the overall development of democratic institutional dynamics, we include a brief analysis of the media sec-

[7] "Analytical Portal," National Commission of Communication, n.d., https://analytics.comcom.ge/.

tor, its major actors, and tendencies. It allows us to grasp the depth and gravity of political influences on the sector and establish linkages to Georgia's overall institutional dynamics, often driven by hidden and illicit interests of particular business or political circles.

According to Freedom House, Georgia ranks best among its neighbors regarding media freedom, with its worst ranking in 2008 and the best one in 2014 (see Figure 7).[8] Despite this, with its highest index of 47, Georgia still lags behind the Eastern European countries (index 30).



	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Georgia	53	54	54	56	57	57	60	60	59	55	52	49	47	48	49	50

Figure 7: Georgia in the Media Freedom Index.

In the course of media sector analysis, we were able to identify major TV and Radio operators, their revenue sources, the structure of ownership, and market share dynamics between 2012 and 2018.[9] Based on the preliminary assessment of the market revenue distribution, all media actors reaching over 2 % of media market share had been selected for further analysis.[10] Out of seven major TV broadcasters, *TV-Imedi*, which is directly associated with the ruling party and government, owns a share of 22.7 % of the media market. Although owning less than 1 % of the market share, one more TV-company, *Media Union Objective*, was additionally selected due to its direct and open activities linked to spreading Russian narratives and supporting the pro-Russian political message. One of its founders is Irma Inashvili, General Secretary of the pro-Russian political party Patriots' Alliance. *Objective*'s incomes grew exponentially from 2012 (govern-

[8] "Georgia," Freedom House, 2016, accessed July 29, 2020, https://freedomhouse.org/report/freedom-press/2016/georgia; "Georgia, Countries and Regions," Reporters without Borders, n.d., https://rsf.org/en/ranking.

[9] "Annual Reports," National Commission of Communication, n.d., https://comcom.ge/ge/the-commission/annual-report.

[10] "Broadcasting – Media Incomes by Enterprises," National Commission of Communication, May 28, 2020, https://analytics.comcom.ge/ka/statistics-share/?c=broadcasting&sid=757292&f=revenue&exp=tv&sid=757293.

ment change in Georgia) to 2018 from 134,000 GEL to 1.9 mln GEL, of which 1.35 mln came from private donations. The same can be said with regard to radio broadcasting, where 11.6 % of the market is held by Radio-Imedi, and 0.4 % by Radio-Objective. As for the degree of Russian influence, *TV-Imedi* was classified as 'red' due to the dual (Russian and GB) citizenship of its two owners, Ia Patarkazshvili and Liana Zhmotova. Another media player, the MediaNetwork, received a loan from Russian VTB bank in 2016, and thus was coded 'red' as well.

Russian Economic Footprint and Democratic Institutions

This section presents a regression model created to test the dependence of democratic development (institutional strength) on the Russian economic footprint in Georgia. We will use the share of the export to Russia in overall export as the key explanatory variable and the strength of democratic institutions and media freedom as the dependent variables (Figure 8). To measure the media freedom, we will use the Freedom house measure,[11] while the institutional strength will be measured using the World Bank worldwide governance indicators:[12]

- Voice and Accountability
- Political Stability
- Government Effectiveness
- Regulatory quality
- Rule of Law
- Control of Corruption.

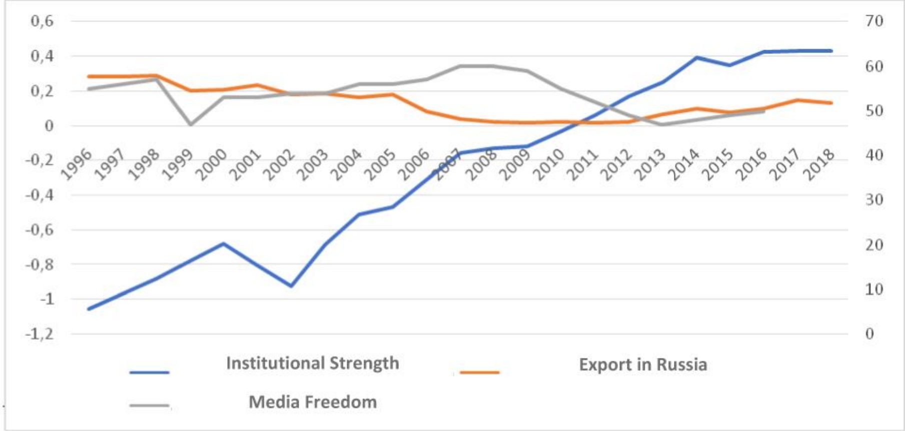


Figure 8: Media Freedom Index, Institutional Strength and Export to Russia.

[11] "Publication Archives," Freedom of the Press, Freedom House, n.d., https://freedomhouse.org/reports/publication-archives.

[12] World Bank, "Worldwide Governance Indicators," n.d., https://info.worldbank.org/governance/wgi/.

As seen in Figure 8, since 1996, the institutional development was generally positive, except for the visible slow in the last four years. Media (press) freedom similarly entered in decline since 2015, and the Export to Russia, close to zero from 2006 to 2013, exhibited rapid growth of 13 % in 2018.

The selected institutional variables are standardized and vary between -2.5 and 2.5, with the higher result indicating better institutions. To measure institutional strength, we calculated an average index of all six factors. In addition, six indicators were grouped in three groups: the first and the second formed the group of political institutions; the third and the fourth defined the group of administrative institutions; and the last two covered legal institutions. As for the Media (Press) Freedom indicators, we used the Freedom House index, which places countries in three tiers: tier 1 for free media countries (with index from 0 to 30), tier 2 of countries with partially free media (31 to 60), and tier 3 of countries with no media freedom (from 61 to 100).[13]

The application of the regression model to test the interrelation between these variables provided the following results. The regression in the first and second columns includes the average strength of institutions as the dependent variable and the export share to Russia in the overall export as the control variable. The second regression model in row 3 additionally included the lagged GDP. The regression results indicate a negative relationship between exports to Russia and institutional quality. The regression in the fourth, fifth, and sixth rows have political, administrative, and legal institutions as the dependent variables. As clearly visible, the growth of exports in Russia has a negative impact on administrative and legal institutions and no influence on political institutions. Having media (press) freedom as the dependent variable, the sixth column does not yield any statistically significant relation.

It should be noted that this regression model has certain limitations, that include a relatively small number of observations (23 for the first five dependent variables and 22 for the sixth one – media freedom), and can be balanced by a larger period of observation and data from other countries. Time series and cross-section would generate panel data that would increase the quality and validity of the generated results.

Conclusion

The state's ability to sustain effective institutions capable of withstanding external (Russian) pressure and minimize Kremlin's influence politically, institutionally and economically, constitutes the critical hallmark of the countries candidates for EU or NATO membership. Having a free, diversified, and stable economic system is the ultimate objective in the economic dimension of Georgia's aspirations to align with the EU in legal, trade, energy, and social affairs. Towards that goal, the study presented here aimed to test the validity of Georgian commitments by looking particularly at the patterns of Russian influence over Georgia's demo-

[13] "Publication Archives," Freedom House.

Table 8. Regression Model.

Variables	Export	ladgdp	Constant	R-squared
(1) Institutions	-0.0420*** (0.00826)		0.290** (0.131)	0.552
(2) Institutions	-0.00529** (0.00249)	0.000460*** (2.19e-05)	-1.367*** (0.0839)	0.980
(3) political	0.00304 (0.00412)	0.000299*** (3.63e-05)	-1.292*** (0.139)	0.856
(4) administrative	-0.0124** (0.00483)	0.000503*** (4.25e-05)	-1.085*** (0.163)	0.949
(5) legal	-0.00656* (0.00376)	0.000577*** (3.31e-05)	-1.725*** (0.127)	0.972
(6) free press	-0.236 (0.177)	-0.00449** (0.00184)	68.11*** (6.590)	0.288

Standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

cratic institutions via intensive analysis of Russia's economic footprint in the country. It was conducted in a sequence of steps. The first objective was to identify major economic sectors in the country and identify the major companies in each relevant sector fully or partially exposed to Russian influence. Out of eight sectors identified (Manufacturing, Trade, Agriculture, Transport, Communication, Energy, Construction, and Finances), the Russian financial investments predominantly went into Finances, Manufacturing, Construction, and Communication. However, it has to be reminded that the statistics shown by the FDI forms only a fraction of the entire Russian capital flows invested in Georgia due to the possibility of investments via third countries and offshore companies. As the 2020 Deliverables Report clearly states, the trade with other Eastern Partnership countries significantly decreased due to drastic sales of Russian made products in Georgia.[14]

The manufacturing industry is by far the leading branch in exporting goods to Russia. Serious questions arise in connection to multiple projects launched in the energy sector, as they exhibit close to zero feasibility and serious risks of corruption.[15] Similarly to 2006, Georgia approached a point at which the possibility of a Russian embargo could heavily hit the national economy, causing devastating effects and creating conditions of mounting political pressure from the Kremlin.

[14] "Georgia's Implementation of 20 Eastern Partnership Deliverables for 2020," Assessment by Civil Society (Tbilisi: Georgian Institute of Politics, International Society for Fair Elections and Democracy, 2020), 49, http://gip.ge/georgias-implementation-of-20-eastern-partnership-deliverables-for-2020/.

[15] "Georgia's Implementation of 20 Eastern Partnership Deliverables for 2020," 78–89.

Likewise, the exponential growth of visitors from Russia dramatically increased the share of Russian tourists in the overall tourist number and increasingly put the tourism branch under Russian strain. Almost one third (114 out of 415) of the major Georgian companies expose fully or partially linkages to Russia and occupy an average of 9.2 % of the national business turnover. In some sectors, the gravity of domination by Russia-linked companies is rather alarming (Mining – 63.4 %, Energy – 36.6 %, Agriculture – 24.7 %). Other sectors of strategic importance, such as Information and Communication, expose an ever-growing rate of influence (14.5 %). The developed regression model that put three categories of state institutions (political, administrative, and legal) in relation to exports to Russia and national GDP revealed a clear statistical dependence between the increase of exports and the decline of institutional strength in Georgia, with no statistical effects to media freedom whatsoever.

The general conclusion drawn from the study is that Georgia already reached a point of heavy economic dependence from Russia, which over proportionally affects several key industries of the national economy and continues to expand in some sectors of strategic importance. The Russian footprint located at the level of 9 % of national business turnover is already a redline and the statistical models that capture the interrelation between the growth of Russian economic influence and the decline of the institutional quality clearly confirm the mentioned threshold. Much has to be done to reverse this trend and bring Georgia back to a clear path of minimizing Russia's footprint, making credible efforts to increase resilience both in economic and political dimensions.

Disclaimer

The views expressed are solely those of the authors 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 Authors

Shalva Dzebisashvili was awarded a doctoral degree at the Institute for European Studies (IEE-ULB, Brussels) in January 2016. In 2008–09 he successfully completed an MA course in Strategic Security Studies at the National Defense University, Washington DC, and consequently took over the position of Senior Civilian Representative of Georgian MOD (Defense Advisor) to the Georgian Mission to NATO. From 2003 to 2012 and from 2016 to 2019, he served at various senior defense policy and planning related positions at the Georgian Ministry of Defense. He is an associate professor and the Head of the International Relations and Political Science Program at the University of Georgia, a member of various Georgian non-governmental organizations and think-tanks such as the Civil Council on Defense and Security (CCDS) and the Georgian Strategic Analysis Center (GSAC). E-mail: kartweli@yahoo.de

Rezo Beradze holds a MA degree in Economics from the International School of Economics in Tbilisi, Georgia (ISET) and an MSc degree in Financial Mathematics from the University of Sussex. He is an experienced financial and data analyst with a demonstrated history of working in the public and private sectors. Currently, he is a data analyst at the National Bank of Georgia, working on the implementation of the XBRL (eXtensible Business Reporting Language) for the Georgian financial sector. Since 2016, Rezo has been actively working as a lecturer at various Georgian universities teaching data related subjects. His research interests are in development economics, financial economics, and data analysis.

Irakli Gabriadze is a PhD student in the Faculty of Economics at Tbilisi State University. His primary research interests are in development economics, economic growth, transition countries, institutions, and political economy. Recently, he became head of the Analysis, Monitoring, and Evaluation department at Enterprise Georgia. Also, Irakli is an invited lecturer of Macroeconomics and statistics at the University of Georgia.

Suzana Kalashiani has 12 years of experience in the field of journalism, social research, and media communications in Georgia, working in the capacity of a project coordinator of "Russian Economic Footprint in Georgia and influence on Georgian institutions." Earlier, she has been involved in different projects focusing on combating anti-Western propaganda in Georgia and increasing awareness about the EU-NATO-Georgia relationship.

Mirian Ejibia is a MA graduate from the International School of Economics in Tbilisi, Georgia (ISET). He gained extensive professional experience in reporting and financial analysis while working for the In-depth Reporting and Economic Analysis Center. He also developed full proficiency in data analysis and web application programs and currently works as a full-stack developer (ERP system) at BSC LLC.

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

Philipp H. Fluri, *Connections QJ* 19, no. 4 (2020): 59-68
https://doi.org/10.11610/Connections.19.4.04

Research Article

Stabilization Missions – Lessons to Be Learned from Resilience-Based Peacebuilding

Philipp H. Fluri

WenZao University, Taiwan, https://english.wenzao.tw/

Abstract: International stabilization missions are often unsuccessful, as demonstrated by the fact that a large number of countries that have hosted such missions have also relapsed into conflict within 20 years. The author suggests looking to experiences of resilience-based peacebuilding for more successful examples. These remain largely unknown or ignored and still do not enjoy the attention they deserve, whether because the 'wrong' NGO crowd dominates peacebuilding programming, the 'wrong' departments and ministries are considered the main peacebuilding partners or the resilience-based projects simply are not costly enough to attract attention. A framework for resilience and examples from Guatemala, Liberia, Timor-Leste, and Afghanistan are discussed and lessons to be learned identified.

Keywords: liberal peacebuilding, stabilization, stabilization missions, SIGAR, Afghanistan, Guatemala, Liberia, Timor-Leste, resilience, resilience assessment, framework, resilience for peace.

Introduction

Liberal peacebuilding was the predominant concept for peace missions after the fall of the Soviet Union and the disappearance of the bipolar world system. Over time, the high costs associated with liberal peace missions and the rise of violent extremism and state sponsors of terrorism have led to rethinking the ends and means of intervention in fragile or conflict-affected states. Stabilization missions became the new paradigm for interventions, with a strong if not exclusive focus on security. The heavy focus on security is, however, not unproblematic. To illustrate, the Special Inspector General for Afghanistan Reconstruction (SIGAR) reports have analyzed and discussed in detail what exactly went wrong in the US-led stabilization effort in Afghanistan. In parallel to the emergence of stabilization missions, but rarely in close cooperation with them, the peacebuilding community developed a resilience-focused approach of identifying the local potential to develop and sustain positive peace. In this article, the author proposes to examine the role of resilience in peacebuilding, and how peacebuilding is a necessary complement to stabilization if viable self-sustained societies are to be the objective of international peace missions.

How We Got Here – From Liberal Peacebuilding to Stabilization

The end of the Cold War marked the beginning of an era of increasing intra-state conflict. "Liberal peace" was the guiding concept for international interventions under the auspices of regional organizations or the United Nations for almost two decades.[1] Liberal peace's main assumptions entailed the rebuilding/building of state institutions on the basis of democracy, the rule of law, human rights, and promoting a market economy as the pathway to peace and prosperity.

This liberal peace concept has now mostly disappeared, both in practice and as a concept. Liberal peacekeeping turned out to be more complicated and costly than expected. It also turned out to be less unselfishly supported by local authorities than anticipated. Host governments tended to resist interventions and pressed for mandates that aligned with the self-interests of those in power. In the wake of these developments, the traumatic experience of the attacks on the US on September 11, 2001, and the global financial crisis of 2008-9, Western democracies shifted their focus from the promotion of liberal peace norms and principles to the mix of counterterrorism and stabilization efforts which has been characteristic of international deployments since the Afghanistan intervention.

Stabilization efforts, from the establishment of the UN Stabilization Mission in Haiti in 2004, included Western stakeholders' global partners and regional coalitions. This trend may have been welcomed as fair burden-sharing and a sign of properly empowered regional stakeholders taking on greater responsibility for regional security. The Mali deployment has, however, shown that UN stabilization missions can be challenged in their impartiality. They then risk being seen as not working in support of the totality of the affected population.

The agenda of counterterrorism and preventing and countering violent extremism (PVE/CVE) was promoted by the US and other western governments to become central issues on the agenda of organizations like the UN and the OECD.[2] While US President George W. Bush launched the *War on Terror* agenda, this

[1] For a map on ongoing (2020) Multilateral Peace Operations, see the SIPRI Website at https://www.sipri.org/sites/default/files/2020-06/mpo20_fill.pdf. By 'peace operation' we understand missions conducted by one or more of the different international organizations. As such peace missions are not clearly defined in international law. In a 'minimal' definition' suggested by ZIF, https://www.zif-berlin.org/en/what-peace-operation, peace operations are: (1) deployed by an international organization; (2) with the consent of the respective host country; (3) in order to defuse crisis situations, end violent conflicts, and secure peace in the long term.

[2] Ban Ki-moon's *Plan of Action to Prevent Violent Extremism* is to be seen in this light.

continued under the Obama administration with a more sophisticated approach: the engagements in Iraq and Afghanistan were reduced, and a new, limited strategy endorsed with emphasis on special forces and drone strikes (targeted killings). Local troops were involved, trained, and equipped as part of the operational budget. The theater of engagement was thus enlarged by Mali, Niger, Somalia, and Yemen. Instead of addressing the root causes of conflicts, the approach sought to resolve such conflicts by use of force. Pressure was put on allies and partners to accept the new concept and take on part of the burden. The Trump presidency has hardly brought any conceptual change.

The inclusion of regional and *ad hoc* coalitions in UN peace operations also proved to be problematic. Local governments can be expected to have their own views of their neighbors and regional developments, including whom they see as a threat to regional stability. These views will necessarily have to be factored into mandates that seek to enlist regional cooperation.

With budgets shrinking and geopolitics returning, we are likely to see more emphasis on political stabilization through existing forms of government. Stabilization is portrayed as more effective and relevant to the current world situation and the needs of states experiencing conflict. However, given its heavy focus on security to the detriment of governance and development, it was only a question of time before its shortcomings would become apparent. This is already the case in Afghanistan and Mali.

Then, the enthusiasm over stabilization is likely to be limited in time, as it shifts the focus away from the root causes of conflict and development deficits, while enabling weak and corrupt governance, marginalization, exclusion, and lack of social cohesion. The reputation of the UN as *the* peacebuilding force has suffered accordingly. As John Karlsrud put it in his insightful article: “For the UN, the turn towards stabilization and counterterrorism is undermining the legitimacy of the organization and its work in mediation and humanitarian domains, and in particular UN peace operations, and the role of UN peace operations as a central tool in the international peace and security toolbox.”[3]

Lessons from the US Stabilization Experience in Afghanistan

In a recent Lessons Learned report, the Special Inspector General for Afghanistan Reconstruction (SIGAR) examined the US stabilization effort in Afghanistan.[4] The report details how the US Agency for International Development and the Departments of State and Defense tried to support and legitimize the Afghan government in contested districts from 2002 through 2017.

[3] John Karlsrud, “From Liberal Peacebuilding to Stabilization and Counterterrorism,” *International Peacekeeping* 26, no. 1 (2019), https://doi.org/10.1080/13533312.2018.1502040.

[4] Special Inspector General for Afghanistan Reconstruction, *Stabilization: Lessons from the U.S. Experience in Afghanistan* (SIGAR, 2018), https://www.sigar.mil/interactive-reports/stabilization/index.html.

Stabilization is not uniformly defined across relevant stakeholders and was consolidated as an explicit US strategy only in 2009. The SIGAR report surprises by its unusual candor and thoroughness.[5] The forces in the NATO-led International Security Assistance Force saw themselves as under immense pressure and accountable for making fast progress. As a result, Afghan citizens were left with serious doubts as to the future of their personal safety and security and their government's staying power. Interestingly, once Afghan citizens actually were asked to join the discussion,[6] a few of the coalition's assumptions were challenged: citizens found the behavior of Afghan government officials more threatening than the government's absence; they did not originally expect stabilization through extensive social services guaranteed and provided by the government (the Taliban had provided stability, "rule of law," and even a very limited social welfare system); they did not expect stabilization to succeed unless the contradictory interests of Afghanistan's leadership were overcome.

As a possible consequence of the limited results yielded by the stabilization process in Afghanistan, it could be argued to be better to forget about missions of that type. The SIGAR report does not stipulate such radical decisions. It rather alerts us to the fact that, even in the best conditions, stabilization takes time.

In light of frequent rotations, relaunches, and 'surges,' the stabilization effort in Afghanistan until 2018 appears not as *one* continuous effort and process over

[5] According to the SIGAR report, *the* "U.S. government greatly overestimated its ability to build and reform government institutions in Afghanistan as part of its stabilization strategy" (note the wording: the *US government's ability to build and reform* government institutions – emphasis by the author). The stabilization strategy and the programs used to achieve it were thus "not properly tailored to the Afghan context." The large stabilization budget the United States devoted to Afghanistan in search of quick gains "often exacerbated conflicts, enabled corruption, and bolstered support for insurgents." Because the coalition "prioritized the most dangerous districts first, it continuously struggled to clear them of insurgents. As a result, the coalition couldn't make sufficient progress to convince Afghans in those or other districts that the government could protect them if they openly turned against the insurgents." In addition, "efforts to monitor and evaluate stabilization programs were generally poor," and successes "in stabilizing Afghan districts rarely lasted longer than the physical presence of coalition troops and civilians." The report concludes that "Stabilization was most successful in areas that were clearly under the physical control of government security forces, had a modicum of local governance in place prior to programming, were supported by coalition forces and civilians who recognized the value of close cooperation, and were continuously engaged by their government as programming ramped up."

[6] The author recalls personal interviews with elected parliamentarians of all political parties in Kabul in 2010. The interviewees complained about having no say in the defense and security efforts and decision-making of the country which was said to have been entirely left to the president and his international advisors. They were equally left ignorant about the actual budget numbers, thus making a farce out of all capacity-building efforts for MPs and staffers on budget transparency and oversight. See DCAF Afghanistan Working Group, *Afghanistan's Security Sector Reform Challenges* (Geneva: DCAF, 2011), https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_RPS_Afghanistan.pdf.

17 years, but rather as 17 one-year efforts, each with an inception and a phasing-out period, with the cost of a 17-year process. Also, the type of 'stabilization' envisaged could only have been achieved with forces and approaches beyond the scope of the mission and the resources assigned to it. In other words: lasting stabilization paradoxically necessitates more than a stabilization mission and is not possible without a concomitant stabilization of government, civil society, and markets.

The *SIGAR report* concludes with recommendations on behalf of the US government. They can be considered a message to all governments interested in future stabilization missions:

- Even under the best circumstances, stabilization takes time. Without the patience and political will for a planned and prolonged effort, large-scale stabilization missions are likely to fail. The expected timeframe should be a minimum of 10 years.
- Most US government capabilities and institutions necessary in a large-scale stabilization mission should be established and maintained between contingencies if they are to be effective when they matter most.
- Increased funding alone cannot compensate for stabilization's inherent challenges and believing that it can exacerbate those challenges.
- Physical security is the bedrock of stabilization.
- The presence of local governance is a precondition for effective stabilization programming.
- Stabilizing communities requires a tailored approach.
- Stabilization efforts must be rigorously monitored and evaluated.
- Successfully conceiving and implementing a stabilization strategy requires extensive local knowledge of the host-nation government and population.

The kinds of services the US government sought to help the Afghan government deliver were unnecessarily ambitious and not tailored to the environment. While improvements in healthcare, the formal rule of law, education, and agriculture services likely helped many Afghans, the coalition and the Afghan government aimed to provide Afghans in contested areas with an array of high-quality services that went well beyond what the Taliban had provided (and the population expected). They required a level of capacity and legitimacy far beyond what the government could offer, particularly in the time available. The coalition had sought to build peace *for* Afghans rather than *with* them.

Peacebuilding

Peacebuilding organizations may become increasingly involved in the prevention of violent extremism. Whereas the *countering* of violent extremism involves a strong security posture, the *prevention* of violent conflict and violent extremism does not. Moreover, as recognized by the UN General Assembly and the Security Council in 2016, the shift away from managing and responding to conflicts towards preventing them sustainably, inclusively, and collectively, can greatly reduce costs.[7]

Peacebuilding has been defined in a variety of ways, depending on writers' and practitioners' priorities and experiences. The term 'peacebuilding' was coined by the Norwegian peace activist and scholar Johan Galtung in the 1970s, when he claimed that "peace has a structure different from peacekeeping and ad hoc peacemaking and that structures must be found that remove causes of wars and offer alternatives to war in situations where wars might occur."[8]

Resilience-based peacebuilding, as practiced by the Geneva-based *Interpeace International Organization for Peacebuilding* seeks to identify context- and society-specific capacities existing at different levels of social organization. Capacities may consist of physical possessions, norms, and values, networks. They are sources of recourse to be accessed for survival and/or conflict transformation in case of threat or stress by natural or human causes. Rather than focusing on fragility and its removal, the resilience approach focusses on a society's endogenous resources and capacities and their strengthening.

If such resilience capacities exist, how can they be identified, nourished, and put to good use? The *frameworks for assessing resilience* seek to identify absorptive, adaptive, and transformative resilience capacity. The latter may have to be analyzed and, in fact, made conscious through a multi-stakeholder dialogue process. Such concrete work on common values, interests, and resources may well bring together actors who had previously been uncooperative against each other (the Guatemala experience).[9] The resilience approach, rather than focusing solely on survival in a fragile environment, mobilizes "transformative instincts and capacities."[10]

[7] *Pathways for Peace* recommends a more concerted effort by policy makers, the integration of prevention agendas into development policies and efforts, inclusive and sustainable development as prevention and growth and poverty alleviation and departing from traditional economic and social policies. United Nations and World Bank, *Pathways for Peace: Inclusive Approaches to Preventing Violent Conflict* (Washington, DC: World Bank, 2018), p. iii, https://openknowledge.worldbank.org/handle/10986/28337.

[8] Johan Galtung "Three Approaches to Peace: Peacekeeping, Peacemaking, and Peacebuilding," in *Peace, War and Defense: Essays in Peace Research*, vol. 2 (Copenhagen: Ejlers, 1976), 282-304.

[9] The author had the privilege of being invited to assess the process in Guatemala. For an academic version of the findings see Bernardo Arévalo de León, José Beltrán Dona, and Philipp H. Fluri, eds., *Hacia una Política de Seguridad para la Democracia en Guatemala: Investigación y Reforma del Sector de Seguridad* (Frankfurt: LIT Verlag, 2005).

[10] In Timor-Leste, the National Working Group on Civic Education developed a *Guide on Civic Education* (based on resilience capacities previously identified). Additionally, the group suggested to put a National Coordination Council on Civic Education in place. The group had cooperatively concluded that lasting peace required the *right conditions* for good quality leadership at all levels. Such right conditions were understood

Whereas natural disasters and humanitarian crises are situations that allow for a return to a *status quo ante*, conflicts are not. They are the product of dynamics within a society (or between societies) and the processes behind conflicts continue to evolve – resilience for peace must therefore be a capacity to understand and transform them.

Resilience does not automatically lead to peace. Resilience is a neutral concept and can bring about both positive and negative outcomes. Therefore, it is essential to carefully analyze which capacities have the potential to lead towards peace and which would need to be mitigated.

As mentioned above, local ownership—seen universally as essential to credible and sustainable peace processes—can be brought about by a resilience-based approach. What is commonly seen as the starting point of peacebuilding interventions—the conflict assessment that identifies causes and drivers of conflict—may not be the ideal tool for bringing about such local ownership. A complementary resilience assessment focusing on a shared appreciation of existing capacities can provide a way forward for durable peace by engaging stakeholders in a dialogue on what brings and holds people together.

The experiences made with the Interpeace resilience approach led to a set of recommendations. A resilience-based approach can enrich peacebuilding strategies. It has also been shown to produce essential inputs for a national peacebuilding dialogue. Practitioners may, therefore choose to complement their conflict analyses with a resilience assessment in the very early stages of their work, designed to identify capacities existing at all levels of society. Not only should the resilience capacities potentially leading to positive outcomes be identified, but all resilience qualities, including potentially negative ones.

Resilience capacities may be expressed differently across different levels and sectors of society. In case of divergent perceptions of such capacities, peacebuilding actors should seek to address the differences in multi-stakeholder dialogues. A lack of systemic integration of such capacities may lead to a strengthening of "negative resilience."

Expressions of negative resilience need to be met with strategies that influence and incentivize using them for positive ends. They should not lead to the dismantling of the groups from which such negative resilience stems. Resilience assessment is—as the FAR program has shown—not only part of the pathway towards peacebuilding but in itself, an empowering peacebuilding exercise, mobilizing national stakeholders to take joint action.

Considering the enormous cost of a predominantly exogenous stabilization effort, the resilience approach is cost-effective and should thus be considered by all stakeholders.

to include mechanisms for leaders to be held accountable and an empowered population.

Assessing Resilience – Frameworks for Assessing Resilience (FAR)

The results of the two-year program on defining and assessing resilience for peace launched in 2014 have been documented in a variety of publications, among them the *Guidance Note for Assessing Resilience for Peace*, and a series of publications on its pilot application *in situ* in Guatemala, Liberia, and Timor-Leste.[11] According to this view, successful conflict resolution presupposes not only analysis of the root causes, but also investigation and, ideally, strengthening of the endogenous capacities and resources to address and overcome such conflicts. The FAR approach thus goes beyond the traditional focus on fragility and finding solutions to it. Local stakeholders were invited to share views on how they understood resilience in dialogue with national practitioners, international scholars, expert-practitioners, and policy specialists. In the execution of the program, Interpeace partnered with the Harvard Humanitarian Initiative (HHI). The countries were selected on the basis of their post-conflict context and level of fragility, as well as their different geographical contexts. Liberia and Timor-Leste, at the time of the program implementation, were seeking to address state-building in the context of peacebuilding. Guatemala had one of the world's highest homicide rates.

Even in the most challenging situations, be they caused by conflict or natural disasters, individuals and communities can be found which seek to address and counter the situation. Peacebuilding interventions frequently overlook and neglect such efforts to the detriment of what could be a concerted peacebuilding effort rooted in local communities and their resources, which could be recruited for transformative processes transcending the mere response to fragility.

Conflicts often come with histories of social asymmetries and exclusion. The resilience approach leverages 'auto-immune' resources by which a society transforms circumstances and conditions which lead to the eruption of conflicts. Such resilience capacities can be found at different levels of society, and they may be interrelated or inter-relatable, both horizontally (with other communities and individuals) and vertically (with institutions of higher levels, including state institutions). This interrelatedness may seriously influence peacebuilding efforts, especially when not detected and mobilized. 'Resilience' is by itself value-neutral – it concerns mainly the self-preservation instincts of a given entity within a larger context. It can manifest itself negatively if group solidarity comes at the expense of the success of peacebuilding for a society in its totality. It is therefore important that peacebuilding efforts comprehensively address such groups in their identities. This is especially relevant for (indigenous) ethnic groups with a high level of self-organization which provides not only a sense of identity but also "social capital," insofar as these groups therewith gain access to public goods which otherwise would be denied to them (such as education and healthcare).

[11] All accessible via https://www.interpeace.org/programme/far-1/. For the above see "Using Resilience to Build Peace," Practice Brief: Resilience and Peacebuilding, Interpeace, 2016, p. 1ff.

In Guatemala these strong bonds clearly benefit the communities concerned but do not necessarily lead to greater cohesion of the society, nor trust in and willingness to cooperate with the institutions of the state:

> As a result, indigenous groups become even more marginalised from the state. This is an example of how the inability to connect resilience capacities across levels—here between the community level and state level—can feed into conflict dynamics. There is thus a powerful case to be made for identifying informal leaders or intermediary institutions that can bridge the divide between the indigenous community and the state, so that the strong social cohesion within indigenous communities can be harnessed for greater peace at the society level.[12]

The question that needs to be asked in such a case is then: how can the cooperation between groups be improved? And what policies would need to be put in place to enhance the mechanisms for cooperation typical for a given society? *Resilience does not necessarily and automatically lead to peace.*

Similarly, stakeholders in Timor-Leste identified culture, religion, leadership, law, and security as ambivalent and at times used for exclusionary purposes. Therefore, a resilience analysis should lead to a careful distinction of factors potentially enabling peace from others that need to be mitigated. The essential difference of a resilience-based approach from a fragility-focused one becomes evident in this context: whereas the fragility-focused approach would rather stop and eliminate negative factors, the resilience-based approach would seek to build on existing capacities while mitigating negative factors.

Whereas traditional peacebuilding would start with an analysis of conflict causes and drivers, the resilience-based approach complements such analysis with one of the resilience resources—and in doing so by enlisting local stakeholders—situates the discourse in the midst of local ownership while being solution-oriented from the beginning. Therefore, it is recommended to complement the conflict analysis at the beginning of a program cycle with a mapping of resilience capacities at all levels of society, including those of an ambivalent or negative connotation. Negative resilience can be avoided by paying attention to how resilience capacities are expressed and put to use at different levels of society. Programs then need to be designed in a way that allows for the mitigation and positive use of such capacities.

The FAR program would seem to have demonstrated that resilience is indeed a useful addition to the peacebuilding approach with the potential to inform peacebuilding practice in ways that help prevent the onset and re-emergence of conflict and foster sustainable peace. Resilience strongly enhances the conflict prevention agenda and presents an added value to the international community. While an assessment of resilience aims at influencing action and policy towards sustainable peace at all levels in the long term, the FAR program has demonstrated that assessing resilience is also an empowering peacebuilding exercise in

[12] "Using Resilience to Build Peace."

and of itself as it mobilizes in-country stakeholders to take collective action towards peace. This holds great potential both in terms of prevention and cost-effectiveness and should therefore be considered by donors in all initiatives for peacebuilding, state-building, humanitarian aid, and development. Apart from its inherent peacebuilding potential, the resilience approach presents the opportunity for greater collaboration among practitioners, donors, and policymakers working in various fields of international development.

Conclusions

Peacebuilding programs and international peace missions traditionally take place in relative isolation from each other. The way peace missions are set up leaves little flexibility for mandate adjustments once a mandate has been negotiated and budgeted. Against a 'mechanistic' stabilization mandate implementation that rests on a strong security posture to which all other activities are subordinated if noticed at all, the author argues in favor of peace missions informed by resilience-based peacebuilding. Societies could likely be consolidated and made viable again in a locally owned cooperative process based on resilience capacities already existent within (parts of) the society in question. Organizations and nations participating in peace missions would thus be spared the embarrassment of having to leave countries with mission objectives still unaccomplished.

It is the peacebuilding community that supposedly has the linguistic competence and leadership qualities to find common language and discuss and define common values, norms, and procedures in difficult situations. For this to happen, the peacebuilding community and the ministries and organizations supporting them should envisage stepping out of the cocoon of isolation they have been working in by proactively starting to practice in regard to the security community what they themselves do best on the ground: reach out, find that common language, and define policy frameworks for enduring cooperation.

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

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 a visiting professor at WZU Taiwan. *E-mail*: drphilippfluri@gmail.com.

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

Veronica Waeni Nzioki, *Connections QJ* 19, no. 4 (2020): 69-85
https://doi.org/10.11610/Connections.19.4.05

Research Article

Technology as a Resilience Factor in Peace Operations

Veronica Waeni Nzioki

Ministry of Foreign Affairs, Kenya, http://www.mfa.go.ke/

Abstract: Peace operations have undergone significant shifts since their conceptualization. They have transitioned from monitoring ceasefires in interstate conflicts to supporting the implementation of comprehensive peace agreements. Some peace operations are now involved in stabilization and increasingly in the protection of civilians. Others are operating in areas experiencing violent extremism, terrorism, transnational organized crime, and violent intrastate conflict largely involving non-state armed groups. These changes, coupled with transformations in the global order, call for adaptation and resilience of peace operations to ensure that they are "fit for purpose" to meet present and future security needs. Central to this adaptation and resilience are the 'tools,' 'technologies' and 'equipment' peacekeepers employ. This article looks into the resilience of peace operations from a technological and innovation angle, examining how technology can/is enhancing the resilience of peace operations and how peace operations are adopting and leveraging new technologies to implement their evolving mandates and adapt to changing conflict dynamics. Actors in peace operations and their national technological capabilities (or lack thereof) strengthen or undermine the collective resilience of the wider peace operations' architecture. The article argues that agility, foresight, and anticipation, matched with timely adaptation to technological developments and innovative systems of operations, are essential components in the resilience of peace operations amidst changing security dynamics.

Keywords: innovation, technology, foresight, adaptation, resilience, peace operations.

Introduction

> *UN peacekeeping can evolve to become a learning enterprise that seeks out and applies new technologies and innovations on a continuous basis, thereby enabling it to be better prepared for the future*.[1]

International peace and security remain at the heart of the United Nations (UN) since its foundation when nations committed to "save succeeding generations from the scourge of war."[2] The UN Charter (Chapter VII) makes provisions for the Security Council to "decide what measures shall be taken in accordance with Articles 41 and 42 to maintain or restore international peace and security," including regional Arrangements (Chapter VIII).[3] In this regard, the UN has often resorted to peace operations[4] (particularly peacekeeping) as one of the 'tools' to address threats to international peace and security.[5]

Since its first peacekeeping mission, the UN has deployed over 70 peacekeeping operations around the world.[6] Currently, the UN has 13 peacekeeping missions across Africa (7), Asia (1), Europe (2), and the Middle East (3)[7] (see Figure 1).

Regional and sub-regional organizations, as well as coalitions of States, have also been active in leading peace operations, particularly the North Atlantic Treaty Organization (NATO), the African Union (AU), the Organization for Security and Cooperation in Europe (OSCE), and the Economic Community of West African States (ECOWAS). Alongside multiple actors in peace operations are the rising complexities in both security and conflict dynamics (such as the increased use of Improvised Explosive Devices /IEDs/ by non-state armed groups), new threats (such as the ongoing COVID-19 pandemic) as well as shifts in political dynamics and contributions to peace operations. These and other disruptive changes demand resilience, agility, and adaptability by peace operations in order to effectively deliver on their mandates while upholding their legitimacy and credibility.

[1] United Nations, *Performance Peacekeeping*, Final Report of the Expert Panel on Technology and Innovation in UN Peacekeeping, 2014, accessed August 18, 2020, 19, https://peacekeeping.un.org/sites/default/files/performance-peacekeeping_expert-panel-on-technology-and-innovation_report_2015.pdf.

[2] United Nations, *Charter of the United Nations and Statute of the International Court of Justice* (New York: United Nations Publications, 2015), 2.

[3] United Nations, Charter of the United Nations, 27, 35.

[4] The term 'peace operations' in the context of this article refers to peacekeeping and peace enforcement missions. Peace Operations entail a broader spectrum of activities ranging from conflict prevention, peacekeeping, peace enforcement, peacemaking and peacebuilding. See United Nations Peacekeeping, *Principles and Guidelines (Capstone Doctrine)* (New York: United Nations, 2008), 17-20, accessed August 18, 2020, https://peacekeeping.un.org/sites/default/files/peacekeeping/en/capstone_eng.pdf.

[5] United Nations, *Capstone Doctrine*, 7.

[6] United Nations, *Capstone Doctrine*.

[7] United Nations Peacekeeping, "Where We Operate," accessed August 1, 2020, https://peacekeeping.un.org/en/where-we-operate.

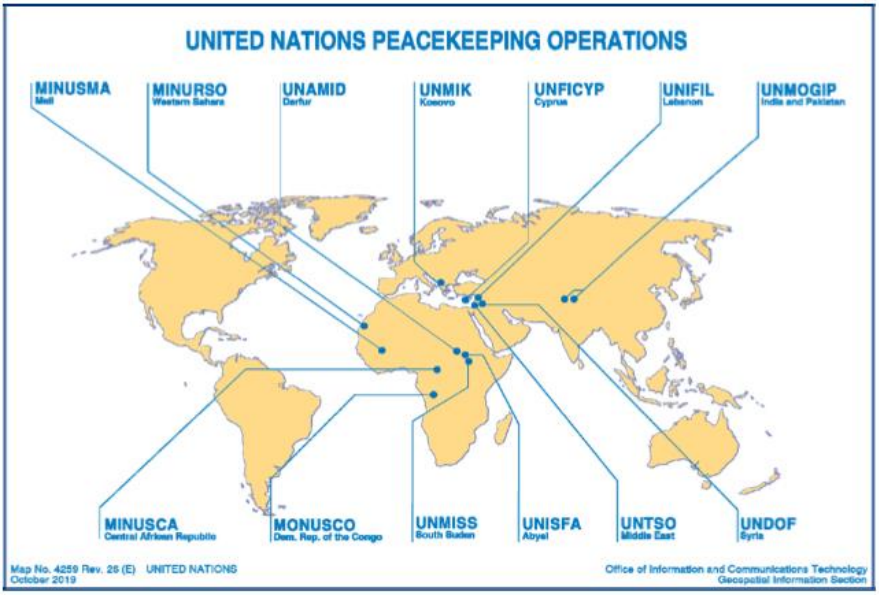


Figure 1: United Nations Peacekeeping Missions as of 31 March 2020.[8]

The world is also experiencing exponential growth in technologies and other forms of innovation from digital technologies, advanced robotics, artificial intelligence, blockchain, big data, Internet of Things (IoT), and 3D technologies, among others. In addition to the development of new technologies, their rates of diffusion, adoption, and application are also on the rise. On internet application, for instance, the International Telecommunications Union (ITU) estimates that 4.1 billion people (53.6 % of the global population) was using the Internet as of 2019, which was a significant rise from 2005's 16.8% of the global population.[9] For digital technologies, by 2018, the subscription to mobile phones per 100 people of the global population was 106; in sub-Sahara Africa, the number stood at 82; the European Union at 123; the Middle East and North Africa at 106; East Asia and the Pacific at 122; and for fragile and conflict-affected States at 77.[10]

Technology portends significant benefits for the security and defense sectors. Leveraging new technologies remains crucial to enhance the resilience of peace

[8] United Nations Peacekeeping, "Peacekeeping Operations Factsheet," accessed October 18, 2020, https://peacekeeping.un.org/sites/default/files/pk_factsheet_3_20_english.pdf.

[9] International Telecommunication Union (ITU), "Measuring Digital Development: Facts and Figures 2019," accessed August 1, 2020, https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf.

[10] World Bank, "Mobile Cellular Subscriptions (per 100 people)," International Telecommunication Union, World Telecommunication/ICT Development Report and Database, accessed August 2, 2020, https://data.worldbank.org/indicator/IT.CEL.SETS.P2.

operations by better addressing emerging security needs (such as the increasing IEDs and Vehicle-Borne Improvised Explosive Devices, VBIEDs) largely targeted at peacekeepers and civilians. New technologies can also play a significant role for both the Protection of Civilians (PoC) and force protection through enabling better observation, monitoring, surveillance and early-warning. New technologies are also becoming critical enablers and force multipliers in vast mission areas where intelligence generation, analysis and monitoring capabilities are increasingly in demand.

The Expert Panel on Technology and Innovation in UN Peacekeeping in its report 'Performance Peacekeeping' acknowledged that "UN peacekeeping remains well behind the curve" in technological adoption and application while noting that UN peacekeeping "can and must leapfrog into-at least-the current day and position itself to face the challenges of the future." [11] Acknowledging the complexity of crises that peacekeepers are deployed to manage, the Report notes the essence of technology in peacekeeping and emphasizes that "no mission can be expected to succeed in today's complex environments without an ability to innovate and make effective use of technology, and no advantage should be withheld from those working for the cause of peace." [12]

As security challenges within areas where missions operate keep evolving, the adoption of new technologies will be key in building the resilience of peace operations. For peace operations, resilience also entails strategic anticipation and mapping the transforming nature of conflict, and ensuring that responses are agile and adaptable to these changes. The High-Level Independent Panel on Peace Operations (HIPPO) in its 2015 Report notes the necessity to adapt peace operations "to new circumstances" and the need to "ensure their increased effectiveness and appropriate use in future." [13] A significant part of this change is enhancing the technological capabilities of peace operations to resonate with the present and future needs. For peace operations to enjoy legitimacy and credibility, they need to be adaptable and resilient to meet the evolving security needs of the populations they are mandated to serve and protect.

While new technologies are not a panacea in resolving all challenges peace operations face, they play a significant role in enabling peace operations reinvent themselves and implement their mandates in a more informed and effective manner amidst new challenges.

[11] United Nations, *Performance Peacekeeping*, 16.

[12] United Nations, *Performance Peacekeeping*, 3.

[13] United Nations General Assembly, *Identical letters dated 17 June 2015 from the Secretary-General addressed to the President of the General Assembly and the President of the Security Council: Comprehensive review of the whole question of peacekeeping operations in all their aspects, Comprehensive review of special political missions, Strengthening of the United Nations system* (HIPPO Report), 17 June 2015, A/70/95–S/2015/446, 9, accessed August 23, 2020, https://www.un.org/en/ga/search/view_doc.asp?symbol=S/2015/446.

The Evolution of Peace Operations

> *Clearly we cannot continue to afford to work with 20th century tools in the 21st century.*
>
> – Hervé Ladsous [14]

Technology as a resilience factor for peace operations must be framed within the evolution of peace operations and the significant transformation of peace operations, as well as their future trajectories. A number of peace operations have complex and robust mandates and operate within challenging environments. The evolution of peace operations has also been shaped by the nature of security threats to global security, particularly the evolving nature of armed conflict.

Peace operations have transitioned from "Observer Missions," whose principal responsibility was to observe activities and deployments of armed forces of conflicting states pegged on UN-mediated ceasefire agreements.[15] In its first forty years, UN peacekeeping was largely involved in the observation and supervision of ceasefires within interstate conflicts.[16]

"Interposed forces," the "second generation" of peace operations, comprised of smaller units of soldiers conducting largely monitoring, observation and supervision functions being "interposed between conflicting armed forces."[17] At times, these forces have to engage in physical separation of combatants to create conditions for monitoring of volatile areas and engage in efforts to ensure the adherence to ceasefires while ensuring parties do not gain new grounds.[18]

Multidimensional peace operations form the "third generation" of peacekeeping operations. Their role increased in the post-cold war era with the transformation of conflict to largely internal (intrastate) conflicts, rising in "both number and intensity," and thereby more involvement of UN peace operations in states' internal dynamics in the quest for sustainable peace and nation-building.[19] Since 1989, there have been more than 30 multidimensional peace operations.[20] Multidimensional peace operations comprise the majority of peace operations today. They are involved in a wider scope of functions including "disarmament, demobilization, and reintegration of former combatants," humani-

[14] Herve Ladsous is a former United Nations Under-Secretary General for Peacekeeping Operations. See "UN Peacekeeping Chief Wants More Drones," *Al Jazeera*, May 30, 2014, accessed October 18, 2020, https://www.aljazeera.com/news/africa/2014/05/un-peacekeeping-chief-wants-more-drones-201453045212978750.html.

[15] A. Walter Dorn, *Keeping Watch: Monitoring, Technology and Innovation in UN Peace Operations* (Tokyo: United Nations University Press, 2011), 10.

[16] Mateja Peter, "Peacekeeping: Resilience of an Idea," in *United Nations Peace Operations in a Changing Global Order,* ed. Cedric de Coning and Mateja Peter (Cham: Palgrave Macmillan, 2019), 25-44, quote on p. 29.

[17] Dorn, *Keeping Watch,* 11.

[18] Dorn, *Keeping Watch,* 11.

[19] Dorn, *Keeping Watch,* 12-13.

[20] Dorn, *Keeping Watch,* 13.

tarian assistance, promotion and protection of human rights, restoration of the rule of law, facilitation of political processes, the protection of civilians,[21] intelligence, analysis, investigations, and forensics.

"Transitional administrations"—the "fourth generation" of peace operations established in the late 1990s—entailed the United Nations going beyond the supervision of peace agreements to exercising governance over entire territories over transitional periods.[22] Transitional peace operations are comprehensive and involve a wide scope of activities from education, military, legal, and even sanitation functions, bringing together civilian, police, and military actors.[23]

The post-1988 period has seen a shift in peace operations both quantitively and qualitatively, with 58 of the 71 UN peace operations established in that period.[24] Qualitatively, mandates assigned to peace operations became more complex, multidimensional, and entailed addressing some internal matters of States where they were deployed, largely monitoring aspects that are non-military by nature.[25]

In the 2000s, the Protection of Civilians (POC) mandate became central in UN peacekeeping, denoting an additional shift from state-building and peacebuilding mandates to "emergency humanitarian peacekeeping."[26] Transformations within peace operations have also been defined by personnel contributors to peace operations with larger troop and police contributions from Africa and Asia.

Despite the evolution in peace operations, observation and the need for monitoring, mobility, and secure communication have been enduring. With the involvement of peace operations in volatile areas, functions such as information collection, analysis, peacekeeping intelligence, and engaging targets in hostile environments are gaining importance.

Technology as a Resilience Factor for Peace Operations

> *As the world's technological revolution proceeds, the United Nations can benefit immensely from a plethora of technologies to assist its peace operations. Missing such opportunities means missing chances for peace …*
>
> – Walter Dorn [27]

Resilience for peace operations, while enabling missions to optimally respond to evolving security needs, is essential in upholding the credibility of the wider mul-

[21] United Nations Peacekeeping, "What is Peacekeeping," accessed August 29, 2020, https://peacekeeping.un.org/en/what-is-peacekeeping.

[22] Dorn, *Keeping Watch,* 13.

[23] Dorn, *Keeping Watch,* 17.

[24] Peter, "Peacekeeping: Resilience of an Idea," 31.

[25] Peter, "Peacekeeping: Resilience of an Idea," 31-32.

[26] Peter, "Peacekeeping: Resilience of an Idea," 36.

[27] A. Walter Dorn, *Smart Peacekeeping: Toward Tech-Enabled UN Operations* (New York: International Peace Institute, 2016), 1.

tilateral system. Peacekeeping "is the activity that the UN is most visibly associated with,"[28] hence adaptability and resilience for peace operations are linked to the credibility of the wider United Nations system. A number of factors are vital to enhancing the resilience of peace operations ranging from innovative systems of operations, partnerships, and the adoption of new technologies.

Peace operations have undergone a number of transformations and technology can/is already enhancing the resilience of peace operations amidst these transformations. In the future, more changes in peace operations are going to demand further adaptation for resilience. This section focusses on how technology can/is enhancing the resilience of peace operations amidst:

i. Dynamic security environments and changing conflict patterns (with a focus on the rising IED threat)

ii. The increasing significance of the Protection of Civilians (POC) mandate.

Dynamic Security Environments and Changing Conflict Patterns (with a Focus on the Rising IED Threat)

The period from the 1990s onwards has been characterized by increased deployment of peace operations, largely reflective of the rise in conflicts, most of them intrastate, protracted, and asymmetric in nature. There is also the frequent, intense, and indiscriminate use of IEDs, and this will be a defining threat for peace operations as IEDs are increasingly becoming the "weapons of choice" for non-state armed groups,[29] including in areas with peace operations deployed. This is the case for the United Nations Multidimensional Integrated Stabilization Mission in Mali (MINUSMA) and the African Union Mission in Somalia (AMISOM).

Belligerents, mostly without access to conventional armament, exploit the use of asymmetric tactics and weapons like IEDs to gain a tactical and operational advantage over peacekeepers, which often have led to high causalities among both peacekeepers and civilians.[30] While IED attacks are not pervasive across all missions, they are nevertheless drawing a significantly high number of peacekeeper casualties.[31] They also pose significant challenges to peacekeepers' safety and mobility and restrict missions' scope of operation.[32]

In Somalia, as is the case in Mali, the IED/VBIED attacks are increasingly compounded by mortar attacks, ambushes, raids, and attacks by rebels and terrorists

[28] Peter, "Peacekeeping: Resilience of an Idea," 25.

[29] United Nations Office for Disarmament Affairs, "Improvised Explosive Devices (IEDs) Publication," accessed September 12, 2020, www.un.org/disarmament/convarms/ieds2/. See also Report of the UN Secretary General on Countering the Threat Posed by Improvised Explosive Devices (2018), 3.

[30] Lisa Sharland, "Counter-IED Technology in UN Peacekeeping: Expanding Capability and Mitigating Risks," *International Peacekeeping* 22, no. 5 (2015): 587-602.

[31] Sharland, "Counter-IED Technology in UN Peacekeeping."

[32] United Nations, *Performance Peacekeeping*, 46.

on peacekeepers' bases and convoys.[33] In Somalia, the terrorist group Al Shabab is also launching attacks using Under Vehicle Improvised Explosive Devices (UVIEDs), conducting ambushes and attacks along Main Supply Routes (MSRs) amidst a host of other asymmetric tactics, particularly suicide bombings and assassinations.[34]

There are projections that future missions might be deployed to environments facing similar threats, particularly to Syria, Yemen, and Libya.[35] Although missions are not entirely similar, an element of resilience for peace operations is drawing lessons from the experience of multinational forces in both Iraq and Afghanistan on technological applications to counter IEDs.

Both high-tech and low-tech solutions can be applied in counter-IED efforts. Relatively cheaper, tethered balloons, as well as blimps, may be used for surveillance purposes.[36] Mine-protected vehicles and armored ambulances,[37] as well as helicopters, enhance force protection and mobility within hostile missions and can also be used for medical evacuation. These are key to ensuring that forces are not exposed to harm.

The Expert Panel on Technology and Innovation in UN peacekeeping recommends that within areas affected by IEDs, convoys could be equipped with "small tactical UAVs" which could be used to generate "mobile intelligence," while "surveillance and reconnaissance (ISR) platforms" could be used to survey chokepoints and other hazard spots along routes.[38] Electronic countermeasures (IED jammers) could be connected to intelligence resources to further mitigate the IED threat.[39] Smartphone applications to detect IEDs and other forms of Explosive Remnants of War (ERW) could be applied by missions in counter-IED efforts.[40] Ground Penetrating Radars (GPR) can be used to detect mines beneath the ground surface, while some hand-held devices can be used to detect explosive compositions.[41]

On identified hot spots, hazard points, or chokepoints, "tethered surveillance platforms" can be installed to improve surveillance.[42] Tethered aerostats can be

[33] Cedric De Coning, Chiyuki Aoi, and John Karlsrud, eds., *UN Peacekeeping Doctrine in a New Era: Adapting to Stabilization, Protection and New Threats* (Oxon: Routledge, 2017), 1.

[34] See the African Union, "Peace and Security Council 865th meeting: Progress Report of the Chairperson of the Commission on the Situation in Somalia/AMISOM," accessed September 12, 2020, 2 https://au.int/sites/default/files/documents/37727-doc-psc-progress-report-865-meeting-amisom-somalia-7-august-2019-eng.pdf.

[35] De Coning, Aoi, and Karlsrud, eds., *UN Peacekeeping Doctrine in a New Era,* 1.

[36] Sharland, "Counter-IED Technology in UN Peacekeeping," 594.

[37] Sharland, "Counter-IED Technology in UN Peacekeeping," 595.

[38] United Nations, *Performance Peacekeeping*, 46.

[39] United Nations, *Performance Peacekeeping*, 47.

[40] United Nations, *Performance Peacekeeping*, 47.

[41] United Nations, *Performance Peacekeeping*, 46.

[42] United Nations, *Performance Peacekeeping*, 46.

integrated with devices such as acoustic detectors, radars, electro-optical/ infrared sensors, and high-resolution video cameras to enhance their surveillance capabilities.[43] They may also be linked to a ground control station for data transmission, media storage, and system management.[44] This is useful in transmitting information to peacekeepers stationed in various mission areas or peacekeepers on the move. Mine-protected vehicles are essential in protecting troops on the move and in offering evacuation platforms during emergencies.[45]

In countering devices that could potentially trigger IEDs, technology can be applied for both electrical and mechanical disruption.[46] While technology will enhance the resilience of peace operations in counter-IED efforts, working with local communities and mounting comprehensive global efforts to disrupt both networks and their enablers are essential elements in wider counter-IED efforts in peace operations.[47] Featuring technology in the trilateral counter-IED operational approaches is key, particularly in "preparing the force, defeating the device and attacking the network."[48]

Developing inter-mission collaboration and partnerships on counter-IED technology application is key, particularly for missions facing similar challenges such as MINUSMA and AMISOM, and so is learning from NATO's International Security Assistance Force (ISAF) experience in Afghanistan and Iraq. Sharing and continuous mentorship and learning will build the resilience of peace operations against emerging threats. It will also be key in monitoring patterns and understanding the changing technological dynamics of the IED threat.

Addressing varying technological capabilities and training among troop, police, and civilian contributors to peace operations remain vital in building technological resilience of the peace operations architecture in countering IEDs.

While technology and innovation are important in mitigating threats posed by IEDs, to ensure resilient counter-IED strategies, peace operations and national armies from which the troops are generated need to understand and cope with the evolving technological dimensions in the application of IEDs by belligerent actors. The continuing ease of spread of IED production and assemblage knowledge on the Internet remains a concern. The UN Secretary-General notes the alarming development of the use of Unmanned Aerial Vehicles (UAVs) to 'air drop' IEDs.[49] The Islamic State of Iraq and the Levant (ISIL) particularly has used

[43] Space and Naval Warfare Systems Center Atlantic, "Tethered Aerostat Systems Application Note: System Assessment and Validation for Emergency Responders (SAVER)," September 2013, 1.

[44] Space and Naval Warfare Systems Center Atlantic, "Tethered Aerostat Systems," 1.

[45] United Nations, *Performance Peacekeeping*, 46.

[46] United Nations, *Performance Peacekeeping*, 3.

[47] Sharland, "Counter-IED Technology in UN Peacekeeping."

[48] Sharland, "Counter-IED Technology in UN Peacekeeping," 593.

[49] United Nations General Assembly, "Countering the Threat Posed by Improvised Explosive Devices: Report of the Secretary General," A/73/156, 12 July 2018, p. 5, accessed September 12, 2020, https://digitallibrary.un.org/record/1637474?ln=en.

"projected grenades" as "airborne improvised explosive devices."[50] The disintegration of the group and its spread to other regions is a concern, specifically in regard to the spread of the technological know-how for the production and use of IEDs.

With the increasing need for better observation and monitoring capabilities for aerial reconnaissance, UAVs equipped with cameras are useful and the UN is applying UAVs since 2013 in missions in the Democratic Republic of Congo.[51] UAVs have also been deployed in Mali, where the Dutch contingent deployed UAVs and Apache helicopters equipped with camera pods for aerial reconnaissance.[52]

Aerostats equipped with cameras are useful in observation and monitoring and the UN is now using them in Mali in distant airfields where belligerents had previously launched attacks and also planted IEDs.[53] Aerostats could also be equipped with acoustic sensors and aid troops in identification of the direction of gunfire and further direct onboard cameras in that direction, thus providing early-warning, better situational awareness, and enhancing force protection.[54]

Non-State Armed Groups operating in some areas where missions are deployed are increasingly exploiting the cover of the dark for attacks on both civilians and peacekeepers[55] and for other nefarious purposes, including smuggling of human beings and illicit arms,[56] planting mines and other forms of explosives. Technology enables peacekeepers to "break the night barrier."[57] Image intensifiers enhance visibility at night, while thermal infra-red (IR) sensors enable viewing at night heat from both human bodies and vehicles.[58] These capabilities, used with other technologies like drones with night-vision sensors, will continue enhancing the resilience of peace operations to operate both during the day and night as a conflict involving non-state actors continues to feature night tactical and operational elements. Advanced night vision goggles, as well as UAVs em-

[50] UN General Assembly, "Countering the Threat Posed by Improvised Explosive Devices," 5.

[51] Dorn, *Smart Peacekeeping: Toward Tech-Enabled UN Operations,* 6-7.

[52] Dorn, *Smart Peacekeeping: Toward Tech-Enabled UN Operations,* 7.

[53] Dorn, *Smart Peacekeeping: Toward Tech-Enabled UN Operations,* 7.

[54] Dorn, *Smart Peacekeeping: Toward Tech-Enabled UN Operations*, 8.

[55] For instance, in December 2017, in what was termed as the "worst attack on UN peacekeepers in the Organization's recent history" in a night attack, 12 UN peacekeepers lost their lives, 40 sustained injuries, while four were critically injured. See United Nations Secretary-General, "Secretary-General's Remarks on the attack on peacekeepers in the Democratic Republic of Congo," 8 December 2017, accessed October 16, 2020, https://www.un.org/sg/en/content/sg/statement/2017-12-08/secretary-general%E2%80%99s-remarks-attack-peacekeepers-democratic-republic.

[56] Dorn, *Smart Peacekeeping: Toward Tech-Enabled UN Operations*, 9.

[57] Dorn, *Smart Peacekeeping: Toward Tech-Enabled UN Operations*, 9.

[58] Dorn, *Smart Peacekeeping: Toward Tech-Enabled UN Operations*, 9.

bedded with IR sensors, are key in enabling peacekeepers to conduct more effective night time operations.[59]

Emerging powers such as China and India are also playing an increasing role in peace operations both by contributing troops and funding peace operations. With the increased number of peace operations, this "new constellation" also has technological dynamics that can enhance their technological resilience. Missions can embrace more south-south technology cooperation as well as triangular technology cooperation whereby a technologically stronger country supports a Troop and Police Contributing Countries (TCC, PCC) through the organization leading the peace operation.[60]

The acquisition of technology is a crucial element and so is the training of peacekeepers on the application of technologies/innovations on sophisticated security issues like cybersecurity. There is a need for ongoing training (at the national level) and in the field during service to enhance peace operations' resilience amidst the growing cybersecurity threats. There is also a need to address the challenge of the rotation of troops to ensure troops in the field bear the requisite technological capabilities for specific missions.

The Increasing Significance of the Protection of Civilians Mandate

> *This challenging mandate is often the yardstick by which the international community, and those whom we endeavour to protect, judge our worth as peacekeepers.*[61]

Today, more than 95 % of peacekeepers are mandated to protect civilians.[62] Increasingly since the end of the Cold War, violent conflict has been largely intrastate in nature, involving non-state actors. These conflicts have triggered massive humanitarian crises, and civilians are increasingly deliberate targets. The rising attention to the protection of civilians is to ensure that the crises and failures to protect civilians by governments and peace operations in the 1990s across Rwanda, Bosnia, and Somalia are not repeated. By itself, the drive towards incorporating the protection of civilians in the mandates of most peace operations is in resonance with the evolving dynamics of contemporary conflicts, where civilians are targets or are increasingly caught in the crossfire, which points to the resilience of peace operations.[63]

[59] Dorn, *Smart Peacekeeping: Toward Tech-Enabled UN Operations*, 9.

[60] Author's interview with Prof. Cedric De Coning, March 13, 2020.

[61] United Nations Peacekeeping, "Protecting Civilians," accessed August 23, 2020, https://peacekeeping.un.org/en/protecting-civilians.

[62] United Nations Peacekeeping, "Protecting Civilians."

[63] The idea of peacekeeping has been resilient amidst changing conflict patterns entailing "different activities" since the first peacekeeping mission in 1948. Peacekeeping is also adapting to the shifting power dynamics within the global order. For more on the *resilience of the idea of peacekeeping* see Mateja Peter, "Peacekeeping: Resilience of

The UN Secretary General in his report on the "Protection of Civilians in Armed Conflict" notes that in 2019 "more than 20,000 civilians had been killed or injured" in conflict-related attacks in 10 countries – "Afghanistan, the Central African Republic, Iraq, Libya, Nigeria, Somalia, South Sudan, Syrian Arab Republic, Ukraine, and Yemen."[64] This number is certainly higher if the number of civilian casualties and civilians injured in Cameroon, Chad, the Democratic Republic of Congo, Mali, Mozambique, Myanmar, Niger, Sudan (Darfur), and the occupied Palestinian territory is factored in.[65]

With the majority of the peace operations bearing the mandate to protect civilians, their success in this function is contingent, among other factors, upon adequate resourcing and equipping. Bellamy, Williams, and Griffins note that "well-equipped operations" that are sent out with the support of the international community bear a greater likelihood of saving lives compared to "contentious, ill-equipped and ill-conceived operations."[66]

In situations of armed conflict, timely and accurate information can save lives.[67] Digital technologies can be used in mission areas to assist civilians and peacekeepers to connect, share information and news, to conduct learning and also to take decisions.[68] This bolsters the element of "participatory peacekeeping," where there is interaction between the mission and locals and the latter share information for early warning, thereby participating in enhancing their own security which also fosters "protection through connection."[69]

The United Nations Stabilization Mission in DR Congo (MONUSCO) developed the "Community Alert Network," which capitalized on the distribution of phones to leaders within the community who would then share information with the mission in the event of any looming danger.[70] Early-warning and intelligence will continue to be key in ensuring that peacekeepers act before actual incidents and thereby avert attacks before they happen. Technology will serve a key role in providing information on both planned incidents, sharing pictures, and with advanced Global Positioning Systems (GPS) enabled devices, sharing locations where civilians can be reached.

Satellite imagery can be accessed commercially, and peace operations can profit from an almost real-time reconnaissance with prices for the imagery falling

an Idea," in *United Nations Peace Operations in a Changing Global Order,* ed. Cedric de Coning and Mateja Peter (Cham: Palgrave Macmillan, 2019), 25-44.

[64] United Nations Security Council, "Protection of Civilians in Armed Conflict. Report of the Secretary General," S/2020/366. May 6, 2020, p. 3, accessed October 17, 2020, www.unocha.org/sites/unocha/files/SG%20POC%20Report-May%202020.pdf.

[65] United Nations Security Council, "Protection of Civilians in Armed Conflict," 3.

[66] Alex J. Bellamy, Paul D. Williams, and Stuart Griffin, *Understanding Peacekeeping,* 2nd ed. (Cambridge: Polity Press. 2010), 2.

[67] UN Security Council, "Protection of Civilians in Armed Conflict," para 13, 10.

[68] UN Security Council, "Protection of Civilians in Armed Conflict," para 13, 10.

[69] Dorn, *Smart Peacekeeping: Toward Tech-Enabled UN Operations,* 12-13.

[70] Dorn, *Smart Peacekeeping: Toward Tech-Enabled UN Operations,* 13.

along with latency periods and time of delivery.[71] Satellite imagery is useful in monitoring large distant areas, particularly where missions are mandated to protect civilians.

Missions can also use the Internet, SMS alert networks, television, radio, and social media to share information with civilians [72] as part of the technology for protection initiatives. In addition to SMS, technology-based Community Alert Networks (CANs) can use mobile phones, free hotline numbers, high-frequency (HF) radios, and satellite phones.[73] The use of technology for protection should be accompanied by safeguarding sensitive personal data to ensure that the privacy of vulnerable people under protection is adhered to.[74] There is a need to also watch out to ensure that belligerent actors do not exploit social media to spread disinformation, incite violence, and promote hatred, which entrenches divisiveness and exacerbates violence.[75]

Resilience will also ensure that missions continue to dedicate efforts towards social media monitoring, detection, and threat assessment as part of conflict mapping, considering that non-state armed groups and other belligerent groups are maliciously leveraging tools like social media for enticement, manipulation, recruitment and coordination.[76]

Since 2019, the Unite Aware (formerly referred to as the "Situational Awareness Programme")—an IT applications platform—is being applied in peacekeeping missions for situational awareness.[77] The platform is comprised of applications such as the "Unite Aware Incidents" aiding the protection of civilians through tracking POC incidents and depositing them in a "central database repository," the "Unite Aware Maps" which offer visual, geospatial mission data on both fixed and variables such as patrol plans as well as location of critical infrastructure and incidents, and the "Unite Aware Dashboards," which offer customized views of data on POC issues such as number of rape incidents, killings and other incidents which can be further aggregated into specific locations, gender, and age.[78]

With the transformation of warfare and belligerents increasingly operating within communities both in urban and rural settings, empowering civilians with secure energy-saving communication technologies, particularly for areas with-

[71] Dorn, *Smart Peacekeeping: Toward Tech-Enabled UN Operations,* 5.

[72] Dorn, *Smart Peacekeeping: Toward Tech-Enabled UN Operations,* 13.

[73] United Nations Department of Peace Operations, "The Protection of Civilians in United Nations Peacekeeping Handbook," 97

[74] United Nations, Performance Peacekeeping, 118; See also John Karlsrud, *The UN at War: Peace Operations in a New Era* (Cham: Palgrave Macmillan, 2018), 75.

[75] United Nations Security Council, "Protection of Civilians in Armed Conflict," Report of the Secretary General S/2020/366, May 6, 2020, para. 39, 10, accessed October 17, 2020, www.unocha.org/sites/unocha/files/SG%20POC%20Report-May%202020.pdf.

[76] UN Security Council, "Protection of Civilians in Armed Conflict," para. 39, 10.

[77] United Nations Department of Peace Operations, "The Protection of Civilian," 104.

[78] United Nations Department of Peace Operations, "The Protection of Civilians," 104.

out reliable electricity, is key for active engagement with the mission to communicate on any planned attacks and other nefarious activities being planned at the community level. This in turn, will enhance the security of both the civilians and the forces and enhance the resilience of peace operations amidst changing conflict dynamics. Photos taken by civilians can be used as evidence in legal proceedings addressing possible atrocities and violence against civilians.

UAVs used in mission areas equipped with capabilities such as thermal imaging cameras are crucial in capturing high-resolution and detailed imagery that is useful in locating objects, analyzing terrain, measuring distance and areas and, where there are incidents, UAVs can be used to obtain the exact location.[79] Noting the expansive terrain most missions cover, UAVs can play a crucial multiplier effect enabling the mission to "see and gather information" from locations that are either difficult or hostile to reach, thus enabling wider presence of the mission as well as advancing the protection of both civilians and the Force.[80] The information generated provides situational awareness, monitoring movements of violent armed groups as well as displaced civilian populations, and can be used later in the investigation of incidents related to the protection of civilians (POC).[81]

Technology will undoubtedly play a significant role in the protection of civilians. However, as peace operations harness technological opportunities as a resilience factor to enhance civilians' protection, it is also important to plan for and address the gendered dynamics of technological divides, particularly on technological access and application. This will ensure peace operations are resilient in harnessing technology to protect *all* while "leaving no one behind." In most of the societies where violent conflict is occurring, women are also culturally responsible for raising children and maintaining homesteads. Hence, the protection of children is largely tied to the protection of women. And if women do not have access to digital technologies and the Internet, which can be used in protection, that leaves children, and the elderly (for whom women are also carers) exposed and vulnerable.

Part of the foresight and resilience measures to ensure that the Internet can be used to communicate and enhance protection is planning on addressing the internet connectivity divide. Out of the current 13 UN-led peacekeeping operations, seven are in Africa, 3 in the Middle East, and 2 in Europe.[82] However, internet connectivity as of 2019 was 28.2 % in Africa, 51.6 % for the Arab States, 48.4 % for Asia and Pacific, and 82.5 % in Europe (Figure 2).[83]

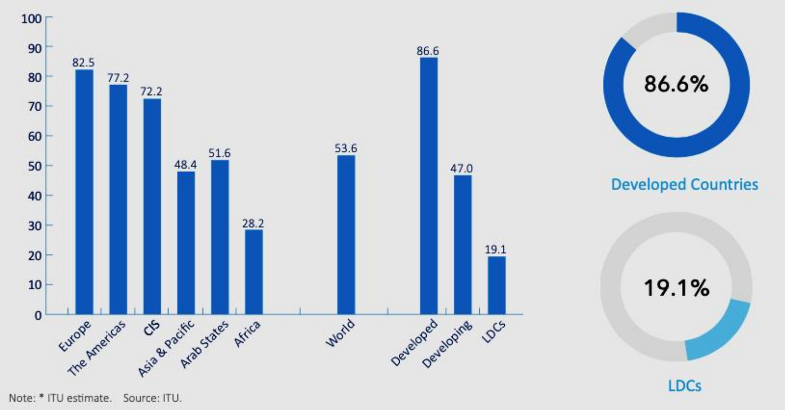
[79] United Nations Department of Peace Operations, "The Protection of Civilians," 104.

[80] United Nations Department of Peace Operations, "The Protection of Civilians," 104.

[81] United Nations Department of Peace Operations, "The Protection of Civilians," 104.

[82] United Nations Peacekeeping, "Where we operate."

[83] International Telecommunication Union (ITU), "Measuring Digital Development: Facts and Figures 2019," accessed August 1, 2020, https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf.



Note: * ITU estimate. Source: ITU.

Figure 2: Percentage of Individuals using the Internet, by Region and Development Status, 2019.[84]

Future missions may need device mechanisms to lower cost and field appropriate internet connectivity for populations-at-risk if they are to tap into the Internet for protection. This is an aspect that will require more cooperation and partnership with the private sector.

Part of technological resilience will entail the *protection of the minds* in as much as peace operations focus on *protecting the body*. The *battle for the minds* of civilians is increasingly becoming one of the spaces contested by non-state armed groups who seek to influence civilians using the Internet and digital technologies. Protection of the minds will only gain greater importance amidst the great scope of protection. Strategic communication will become even more important; hence, in some missions such as Somalia, the UN is already engaging in strategic communication campaigns to counter the radicalizing messaging and effect from the Al Shabab terrorist group.[85]

Protection of civilians' taping into digital technologies, particularly mobile phones, should factor in the adoption and use of mobile phones in the areas where peace operations are deployed. Mobile phones enable community members to alert peacekeepers of any danger (ongoing or impending) or even reporting on any irregular activities – this is, particularly, when belligerents are embedded within civilian populations. Part of resilience entails asking how these new threat dynamics can be mitigated and also how affordable mobile phones can be to the wider population for protection. While the subscription of mobile phones "per 100 people" stood at 106 in 2018, the numbers seem to be grim when it comes to conflict-affected countries, particularly those with active peace operations and most in need, as indicated in the next table.[86]

[84] ITU, "Measuring Digital Development: Facts and Figures 2019."

[85] Peter, "Peacekeeping: Resilience of an Idea," 38.

[86] World Bank, "Mobile Cellular Subscriptions (per 100 people)."

Table 1. Countries Experiencing Violent Conflict (All Apart from Yemen with Active Peace Operations) and Subscription of Mobile Phones per 100 People, 2018.

Country	Mobile phone subscription per 100 people
Afghanistan	59
Central African Republic	27
Democratic Republic of Congo	43
Mali	115
Somalia	51
South Sudan	33
Sudan	72
Yemen	54

Conclusion

Technological adoption remains a significant step in bolstering the resilience of peace operations. Mapping and conducting strategic foresight are crucial for peace operations in order to anticipate, plan, and prepare for future threats. This is no small feat for peace operations that are constituted of forces from across the world with different military cultures, training, and capabilities. Incorporating strategic anticipation in peace operations is an important element to identify the tools, equipment, innovations, and technologies necessary to contribute to the resilience of peace operations.

Cooperation and complementarity will continue to be important, noting the different capabilities of States within the international system and the contributions they can make to peace operations. Technological resilience for peace operations entails the resilience of the key actors in the peace operations, particularly the TCCs, PCCs, and increasingly the Technology Contributing Countries (TechCCs).[87] For the TechCCs, it is important to explore longer-term partnerships. The resilience of the militaries of the individual TCCs will largely impact the resilience of the wider peace operations architecture in relation to technology and innovation.

Peace operations are likely to be impacted by the dynamic changes and trends impacting the global security, political and economic spaces. Transformations in conflict are generating new needs and shifting the focus of mandates to non-traditional aspects such as stabilization amidst threats such as pandemics (as is the case currently with the ongoing COVID-19 pandemic) as well as adverse climate-change-related incidents such as flooding, droughts, and the attendant humanitarian needs they generate.

While the rapid development of technologies presents new opportunities for peace operations in implementing their mandates, technology adoption needs to consider potential unintended and undesired impacts associated with new

[87] Dorn, *Smart Peacekeeping: Toward Tech-Enabled UN Operations,* 1.

technologies. Among these are dual-use technologies and the potential application of technologies for violent purposes, cyber intrusions into crucial mission data, and the hostile use of new technologies by belligerent actors.

Amidst changes that are ambiguous, uncertain, and complex,[88] while bearing very significant disruptions, peace operations will need to be agile, innovative, and adaptative to mitigate the threats while delivering on their mandates. Adopting technology and other innovations are opportunities for peace operations to navigate these changes more effectively.

Technology adoption must also be matched with agility and other resilience factors, among them strategic anticipation, foresight and innovation to adapt specific responses to mission needs as they emerge; the updating of manuals (such as the contingent owned equipment manual) to reflect the evolving needs for peace operations; continuous education and skills development for the end-users of the new technologies in mission areas; partnerships to strengthen the capabilities of the different personnel contributors; and continuous learning at the intra-mission level and inter-mission level on technology trends, mission needs and suitability.

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

Veronica Waeni **Nzioki** is a Foreign Service Officer in Kenya's Ministry of Foreign Affairs and a researcher on peace and security. Her research interests focus on new technologies, innovation, peace operations, armed conflict, and warfare transformation. Veronica previously worked with the International Labor Organization (Employment Program) at the Central and Eastern Europe office in Budapest, Hungary. She also worked with the Jesuit Refugee Services in Northern Uganda, as well as the University of Nairobi as an academic programs coordinator and policy researcher. Veronica holds a Master of Advanced Studies in International and European Security jointly offered by the University of Geneva and the Geneva Centre for Security Policy (GCSP), Switzerland, a Master's degree in International Relations from Corvinus University of Budapest, Hungary, and a Bachelor's degree in Political Science and Sociology (Double Major) from the University of Nairobi, Kenya. She undertook Gender studies at the Abo Akademi University in Finland under the North-South-South Exchange Program. Veronica is a GCSP alumna under its Leadership in International Security Course (LISC).
E-mail: nziokiveronique@gmail.com

[88] Hassan Abul-Enein, "Resilience and Agility: Managing and Mitigating Evolving Threats in a Hyperconnected World," *Strategic Security Analysis*, no. 13 (Geneva Centre for Security Policy, August 2020), 3, https://www.gcsp.ch/publications/resilience-and-agility-managing-and-mitigating-evolving-threats-hyperconnected-world.

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

María Julia Moreyra, *Connections QJ* 19, no. 4 (2020): 87-96
https://doi.org/10.11610/Connections.19.4.06

Research Article

The Importance of Resilience in the Women, Peace and Security Agenda, Particularly during the Covid-19 Pandemic

María Julia Moreyra

PeaceWomen Across the Globe, http://www.1000peacewomen.org/

Abstract: Women have taught different ways of resilience through their actions in their communities. They have developed resilience and leadership. 2020 is an outstanding year regarding gender equality and women's empowerment, as it marks the anniversary of unprecedented policy commitments and practical action frameworks. COVID-19 has dramatically changed the lives of women, girls, and adolescents all over the world. Many women in charge of their communities are at the front line protecting their people and are the backbone of society's resilience. Even though most of them are affected by the virus, they go on working hard, trying to do their best for their people. It is pivotal to apply a feminist lens into foreign policies, and when implementing the Women, Peace and Security Agenda, it is extremely important to take into account that women are key actors in building resilient democratic societies.

Keywords: resilience, refugee women, displaced women, Covid-19, UNSCR 1325, actors of change, gender equality, women's empowerment, crisis.

To my mother, the best example of resilience

Introduction

The present article deals with an important topic, particularly facing humanity as a consequence of COVID-19. Resilience is pivotal in the Women, Peace and Security Agenda, which celebrates its 20th anniversary this year. As will be developed in the article, women are at the front line, protecting their communities from the threat of the pandemic. Throughout six sections, the main contents of the agenda will be analyzed, emphasizing women's resilience to which Resolution 1325 and subsequent resolutions are directed.

It is of great importance to analyze the evolution of the concept of resilience to know what lessons have been learned and how good practices are applied in the implementation of the concept of resilience in this complex moment. Special mention will be made of two groups of women, refugees, and displaced women, who are included in Resolution 1325 and who have demonstrated throughout their hard living conditions to be resilient. Finally, we will address the resilience developed by women worldwide in the wake of the pandemic and how they prioritize their communities at all times.

Women, Peace, and Security

Unanimously adopted on October 31, 2000, Resolution 1325 is the first ever resolution passed by the United Nations Security Council acknowledging the need for and contributions of half the world's population—women—to international peace and security.

Women and men experience violent conflicts as gross human tragedies. But the roles, experiences, needs, and interests of women, girls, men, and boys are very different. Women are more severely affected by sexual abuse and domestic violence, displacement, and social discrimination, and they need to be very resilient to sustain themselves and their communities. They carry heavy burdens.

PeaceWomen Across the Globe (PWAG), a Swiss organization that came into existence after the nomination of 1000 women to the Nobel Peace Prize in 2005, recognized 5 Ps for peace taken from the Resolution:

- **P**articipation: greater inclusion of women in peacebuilding
- **P**revention of conflict and gender-based violence
- **P**rotection of the rights and needs of women and girls during and after armed conflicts
- **P**eacekeeping and **P**eacebuilding: gender mainstreaming in all activities and phases.[1]

The most important aspect of UNSCR 1325 is that it recognizes thousands of peace women across the globe as "actors of change." When women are better, whole communities benefit.

Women from the Balkans, Burundi, Cote d' Ivoire, Democratic Republic of Congo, Guinea-Bissau, Haiti, and Iraq, among others, who held meetings with representatives of the General Secretary of the United Nations on the occasion of the 10th anniversary of UNSCR 1325, showed great resilience before the obstacles and challenges they faced.

In its last paragraph, UNSCR 1325 established that the Security Council "Decides to remain actively seized of the matter." Following this commitment, the

[1] *No Women – No Peace: 10 Years UN Resolution 1325* (Switzerland: PeaceWomen Across the Globe, 2010), 2.

Security Council adopted these Resolutions: 1820 (2008); 1888 (2009); 1889 (2009); 1960 (2010); 2106 (2013); 2242 (2015); 2250 (2015). UNSCR 1820 condemns the use of sexual violence as a tool of war and declares that "rape and other forms of sexual violence can constitute war crimes, crimes against humanity or a constitutive act with respect to genocide." Through UNSCR 1888, the Security Council decided to specifically mandate peacekeeping missions to protect women and children from rampant sexual violence during armed conflict, as it requested the Secretary-General to appoint a special representative to coordinate a range of mechanisms to fight crime. In UNSCR 1889, the Security Council called for a wide range of measures to strengthen women's participation at all stages of peace processes, focusing on the period after peace agreements have been reached, as it began an intensive day-long discussion on the topic. In UNSCR 1960, the Council requested information on parties suspected of patterns of sexual violence during armed conflict to be made available to it. UNSCR 2106 reiterates that all actors, including not only the Security Council and parties to armed conflict but all member states and United Nations entities, must do more to implement previous mandates and combat impunity for these crimes. With UNSCR 2242, the Council decided to integrate women, peace, and security concerns across all country-specific situations on its agenda. In UNSCR 2250, the Security Council urged member states to consider ways to increase the inclusive representation of youth in decision-making at all levels in local, national, regional and international institutions and mechanisms for the prevention and resolution of conflict, countering violent extremism, other activities conducive to terrorism and, as appropriate, to consider establishing integrated mechanisms for meaningful participation of youth in peace processes and dispute resolution.

Resilience: and the Women, Peace, and Security Agenda in Times of Covid-19

2020 is a significant milestone for gender equality and women's empowerment as it marks the anniversary of unprecedented policy commitments and practical action frameworks. The COVID 19 pandemic has abruptly disrupted plans to assess the progress towards these milestones, celebrate the achievements and set new objectives or goals.[2]

The pandemic has profoundly affected people's lives. Women and girls have been particularly affected by the virus and the measures taken to prevent its spread. Once again, women have shown that they are the backbone of community resilience. The Women, Peace and Security (WPS) movement has shown its strengths, weaknesses, and resilience in this crisis. UN Women also responded

[2] Palvina Makan-Lakha and Molly Hamilton, "Resilience and Determination: Women, Peace and Security in the Time of COVID–19," ACCORD (African Centre for the Reconstructive Resolution of Disputes), July 22, 2020, accessed September 17, 2020, https://www.accord.org.za/analysis/resilience-and-determination-women-peace-and-security-in-the-time-of-covid-19/.

swiftly to the gendered impact of the pandemic. Framing its response, UN Women outlined five priorities: gender-based violence, including domestic violence; social protection and economic stimulus packages to serve women and girls; people support and practical equal sharing of care work; women and girls leading and participating in COVID-19 response planning and decision-making; and data and coordination mechanism to include gender perspectives.[3]

The WPS agenda is relevant in this difficult time. As it was said, women are the backbone of resilient communities, as they themselves are resilient and teach their societies how to face serious challenges. They work with local radio broadcasters to spread messages about the threat of the virus and the appropriate hygiene measures. They educate other women and girls to comply with measures to avoid contracting the virus. In short, they protect their communities. Even in the midst of chaos, women have a powerful voice, and they seek to make their societies more peaceful and resilient.

It is important to apply a feminist lens to the women's peace and security agenda, considering that women are key actors in building resilient democratic societies. Therefore, their rights and voices need to be kept alive and intact. During these uncertain and difficult times, it is pivotal to turn to women leaders from around the world for inspiration. They have forged peace when ravaged by war; they have driven innovation despite all odds; and they persisted in the face of challenges and insisted on building a better future.[4] Their messages are perseverance, hope, resilience, strength, fight against discrimination, not giving up, and being together.

The Concept of Resilience

Resilience is a scientific term that applies to materials that have the capacity to return to their original shape after being bent or stretched. Over time, however, the term got to be applied to people as well – people who have the ability to recover readily from illness, depression, defeat, or other kinds of adversity.[5]

Gender is pivotal in this analysis because this article deals with women and because the wider social environments are clearly gendered. Vulnerability and resilience are shaped by gender in various and complex ways. People who suffer marginalization and discrimination are most vulnerable to their negative impact.

It is well documented in the literature how the life-cycle (from infancy to old age) intersects with the different structural vulnerabilities with a particular individual face. Throughout human societies, gender identity dictates a woman's or

[3] Makan-Lakha and Hamilton, "Resilience and Determination."

[4] "Ten Things You Can Learn from Women's Resilience that Help You Stay Strong in the Time of Covid-19," *UN Women*, May 19, 2020, accessed September 17, 2020, www.unwomen.org/en/news/stories/2020/5/compilation-ten-things-you-can-learn-from-womens-resilience.

[5] Rose Gantner, "Women and Resilience," in *Guide to Good Health* (Summer 2012): 7, www.guidetogoodhealth.com/PDF/ArchivedIssues/GGH%20Sum12.pdf.

man's role in the family and wider society. Other aspects of identity with a profound impact on resilience include ethnicity, race, disability, age, or social status.[6]

For many women, resilience is an instrumental strength. Both women and men need resilience to deal with difficulties in life. But women often need to be more resilient than men to overcome traditional obstacles placed in their way in order to advance in the business world. Too many women, however, are not aware of the amount of resilience they do possess.

Dr. Gail M. Wagnild is the founder of the Resilience Center and an expert on resilience, and she says that when you know your capacity for resilience, it gives you the confidence to deal with whatever life throws at you. Being resilient helps you cope in various ways, be they personal, professional, or social.[7]

Indeed, people do not have control over certain aspects of their lives, such as accidents, natural disasters, and illness, among others, but they have the power to respond to such events and choose to do so with resilience. Themes related to resilience include social connectedness, extending self to others, moving forward with life; curiosity/ever-seeking; "head-on" approach to challenge; "maverick"; and spiritual grounding.[8]

During the past few decades, there has been a proliferation of research on resilience, and the concept has been well-researched in the literature. Yet, in terms of defining resilience, there is controversy in the literature as to whether resilience is a characteristic/personal quality, a process, or an outcome.[9] In defining resilience as a personal quality, Ahern, Ark, and Byers argue that resilience is an "adaptive stress resistant personal quality,"[10] whereas resilience is defined as "a dynamic process that is influenced by both neural and psychological self-organizations, as well as the transaction between the ecological context and the developing organism."[11] However, when defined as an outcome, resilience is

[6] Julie Drolet, Lena Dominelli, Margaret Alston, Robin Ersing, Golam Mathbor, and Hauriu Wu, "Women Rebuilding Lives Post-Disaster: Innovative Community Practices for Building Resilience and Promoting Sustainable Development," *Gender & Development* 23, no. 3 (2015): 433-448, quote on p. 438, https://doi.org/10.1080/13552074.2015.1096040.

[7] Gantner, "Women and Resilience."

[8] Beth I. Kinsel, *Older Women and Resilience: A Qualitative Study of Adaptation*, PhD Dissertation (Columbus, OH: Graduate School, Ohio State University, 2004).

[9] Nancy R. Ahern, Pamela Ark, and Jacqueline Byers, "Resilience and Coping Strategies in Adolescents," *Paediatric Nursing* 20, no. 10 (2008):32-36, https://doi.org/10.7748/paed2008.12.20.10.32.c6903.

[10] Ahern, Ark, and Byers, "Resilience and Coping Strategies in Adolescents," p. 32.

[11] W. John Curtis and Dante Cicchetti, "Emotion and Resilience: A Multilevel Investigation of Hemispheric Electroencephalogram Asymmetry and Emotion Regulation in Maltreated and Nonmaltreated Children," *Development and Psychopathology* 19, no. 3 (2007): 811-840, quote on p. 811, https://doi.org/10.1017/S0954579407000405.

thought of as "a class of phenomena characterized by good outcomes in spite of serious threats to adaptation or development."[12]

It is important to cite different concepts of resilience. According to Ungar "resilience is both the capacity of individuals to navigate their way to the psychological, social, cultural and physical resources that build and sustain their well being and their individual and collective capacity to negotiate for these resources to be provided in culturally meaningful ways."[13] This understanding of resilience goes beyond an individual notion to a more relational and holistic approach.[14]

Nevertheless, despite the vast range of definitions, there is some agreement in the field to determine if someone is displaying a resilient profile/ resilience. Two elements must be present: namely, adversity (i.e., a high-risk situation or threat) and successful adaptation/competence.[15] Adversity is evaluated according to negative life circumstances[16] , and adaptation is defined as successful performance on age-developmental tasks.[17]

Women and Resilience

Women face a variety of advantages and adversities in their lives. They go on realizing a strong investment in and positive orientation toward life regardless of the challenges and losses they experience, particularly in difficult times, such as the one produced by Covid-19. They face common challenges, and there is potential to work with them collectively and to lessen their vulnerability. If they see a need, they respond.

Women can name their experiences, reactions, advantage, and adversity. This means that women are resilient. When are they resilient? When they are faced with many challenges and changes in their lives, such as conflict childhood, unhappy marriages, physical illnesses, the loss of their husbands, to name just a few examples. At present, they make great efforts in order to protect their communities in the face of the pandemic threat. In addition, other political, economic, and social factors impact women. These impacts could not be ignored. For this reason, it is pivotal that women could share their experiences and stories and that they are listened to.

[12] Ann S. Masten, "Ordinary Magic: Resilience Processes in Development," *American Psychologist* 56, no. 3 (2001): 227–238, https://doi.org/10.1037/0003-066X.56.3.227.

[13] Michael Ungar, Mehdi Ghazinour, and Jörg Richter, "Annual Research Review: What is Resilience within the Social Ecology of Human Development?," *Journal of Child Psychology and Psychiatry* 54, no. 4 (2013): 348-366, https://doi.org/10.1111/jcpp.12025.

[14] Drolet, et al., "Women Rebuilding Lives Post-Disaster," 435-436.

[15] See, for example, Masten, "Ordinary Magic: Resilience Processes in Development."

[16] Tammy A. Schilling, "An Examination of Resilience Processes in Context: The Case of Tasha," *Urban Review* 40, no. 3 (2008): 296-316, https://doi.org/10.1007/s11256-007-0080-8.

[17] Julie A. Pooley and Lynne Cohen, "Resilience: A Definition in Context," *Australian Community Psychologist* 22, no. 1 (2010): 30-37, 30-31.

Examples of Resilience

Women Suffering Great Trauma

Many women who are survivors of sexual abuse or assault are very resilient. If they have an environment that contains them, they are more likely to recover from this traumatic experience with profound effects on their lives. They have a sense of hope, the ability to turn a disadvantage into an advantage and transcend adversities in their lives.

These facts affect women and men differently according to the particular gender roles and relations within a specific community. Other aspects of identity make individual women's experiences vary markedly from others. In many countries of the world, women are more likely to be numbered amongst the poor, landless, and malnourished, and these existing vulnerabilities are enhanced when traumatic events happen.

They could see their strengths in painful experiences. In some cases, their faith adds meaning to life. Besides, if they share their experiences of challenge and adversity, they will be empowered to go on and be an example to other women who face the same traumatic experiences.

Optimism, independence, and the ability to overcome obstacles are characteristics of resilient women who consider and acknowledge life as a series of challenges. They also express the belief that one should make plans and not wait for something to happen. This behavior helps them in difficult times and fosters the belief that they could take care of themselves.

Positive or negative events that occur at a particular time in the individual's life can affect resilience development. In the case of girls, if they were resilient in this stage of their lives, they are resilient in their adulthood. The early years of life comprise the beginning of the accumulation of advantage and adversity. From this perspective, persons who overcome adversity early in life attain confidence and self-efficacy from that experience; thus, they accumulate resources that would be available in the event of a subsequent challenge.

In some cases, young girls are particularly vulnerable to being withdrawn from education to assist with the workload, forced child marriages, and trafficking.[18]

The recollection of their experiences reflects their ability to adapt from childhood and influences their longitudinal adaptive coping process. There is recognition of support within their childhood contexts that enabled them to survive, as well as recognition for the individual characteristics they possessed. Understanding these internal characteristics gave them the confidence to find coping strategies as a child but also as an adult.[19] Women find their own ways of facing

[18] Margaret Alston, *Women and Climate Change in Bangladesh* (London and New York: Routledge, 2015).

[19] Pooley and Cohen, "Resilience: A Definition in Context," 33-34.

adversity, often by being open to risk-taking, creative problem-solving, or joining other women in mutual support.

Refugee and Displaced Women

> *Women know about the misery of refugees and the fate of those who were displaced.*
>
> – Activist Safaa Elagib Adam, Sudan/Darfour [20]

Resilience is applied to refugees since they have experienced major life upheavals and frequently attempt to rebuild individual, family, and the whole of community trajectories.[21] The same is applied to displaced women.

It is very important to apply the resilience 'lens' to understand the experience of refugee and displaced women, who in general, are single mothers and have to face many difficulties, which increases their vulnerability. Several studies established that within the category of internally displaced people (IDP), women are the vulnerable within the vulnerable. They face and resist all types of shocks, for example, conflict and natural disaster, among others. The aforementioned studies account for displacement-related vulnerabilities such as access to employment, housing, land and property, and food and highlight higher poverty rates of urban IDPs than the rest of the urban poor.[22] Refugee and displaced women put their children's welfare in the first place to provide them with better opportunities in the social, cultural, linguistic, economic, and political environment.

From the standpoint of privileged "first world" lives, the question of exploring the wellbeing of refugee women is in danger of being reduced to a simplistic dichotomy of either pathologizing in relation to trauma or valorizing with regard to resilience.[23]

We emphasize these matters within the context of managing everyday life, where the daily routine is not simply the vessel in which lives are lived; rather, it is the milieu in which the social processes of resilience are continuously enacted. The women's resilience embedded in daily routines challenges the focus of much of the resilience discourse on 'extraordinary' events, while the social dimension of resilience is situated in person-environment interactions acknowledges resilience as an ongoing process achieved over time and, according to contexts, rather than an atypical static inner trait.

[20] *No Women – No Peace*, 17.

[21] Caroline Lenette, Mark Brough, and Leoni Cox, "Everyday Resilience: Narratives of Single Refugee Women with Children," *Qualitative Social Work* 12, no. 5 (2013): 637-653.

[22] Nassim Majidi and Camille Hennion, "Resilience in Displacement? Building the Potential of Afghan Displaced Women," *Journal of Internal Displacement* 4, no. 1 (January 2014): 78-91.

[23] Lenette, Brough, and Cox, "Everyday Resilience," 638.

Despite the fact that many refugee women are isolated and experience significant emotional, financial, and physical risks post-resettlement, they show strengths in their daily lives. Regarding IDP women, the concept of resilience has been increasingly used to describe their abilities to adapt to new environments after the shock of displacement, based on the development of specific coping mechanisms.

Be Resilient in Times of Covid-19

Having come through this pandemic hardship contributes to women's feelings of self-worth and control. When women share their struggles, they teach how they have managed, talking heart-to-heart about their concerns. Dialogue and sharing of experience are important indicators of building resilience and can be applied to the pandemic.

COVID-19 has shown that women have the capacity to gain social competence, the capacity to be flexible, empathetic, and have the ability to plan and think critically and reflectively. Women are rebuilding their lives in the middle of this complex event and promoting sustainable development. Women perfectly know that building resilience requires more than reducing vulnerability. It needs empowering responses to disasters and trauma, which aim to support and foster women's resilience, enhancing their ability to answer to traumatic episodes.

It is pivotal that governments increase resilience capacity by focusing on women (the protagonists of this article) and link this to the Sustainable Development Goals, in which they are engaged. While the vulnerabilities of women in difficult times, as the one humanity is facing at present because of the pandemic, are evident, so too is their resilience. It is important to acknowledge women's capacities to care for their children and family members while, depending upon the social context, women are engaged in multiple activities and tasks in the productive, reproductive, and community spheres.

The need to address the diverse challenges women face is integral to a more holistic approach to building resilience and sustainable development in communities that are devastated. This pandemic shows that resilience empowers women, ceasing to be a silent group in the community, which has a profound effect in their visions about right, justice, and human dignity. Their skills and leadership are instrumental in order to build resilience. It is fundamental that international agreements must promote gender equality and human rights to build the resilience of women and girls in their communities. The Pandemic confronts women and all humanity with the need to promote a sense of purpose, perseverance, equanimity, balance, and self-reliance.

Conclusion

As we could appreciate in the present article, some important considerations as regards resilience begin to emerge. Certain pivotal internal resources contribute to resilience such as self-efficacy, coping, and sense of belonging. After studying the subject in-depth, resilience represents the interaction between risk factors (vulnerability) and protective resources (protection). Resilience is built from the foundation of economic and social security. Living in poverty as part of a marginalized group creates few opportunities to build up the resources needed to fall back on at a time of disaster. Social protection initiatives that provide access to essential services and income, including protection from the risks of disasters, are a universal human right and contribute to building resilience by improving economic security, health, and wellbeing.[24]

Without any doubt, women are actors of change since they cope with different strategies. Resilience is a key factor for women who has experienced traumatic events in their lives. They give us the following message: "*Believe and trust in yourself.*"

Two final considerations, taking into account that much more remains to be done. As Eleanor Roosevelt, former US Delegate to the United Nations, said: "We call on the governments of the world to encourage women everywhere to take a more conscious part in national and international affairs, and on women to come forward and share in the work of peace and reconstruction as they did in the war and resistance." These words apply more than ever to the moment humanity goes through due to COVID-19. Resilience is that wound through which the light enters and which becomes present after having faced adverse facts.

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

María Julia **Moreyra** is an Argentinian Lawyer. She holds a Master's Degree in International Relations (FLACSO, Argentina). At present, she is a Member of the Ministry of Women, Gender Policies and Sexual Diversity of the Province of Buenos Aires, Argentina. Since 2009 she is Regional Coordinator for Latin America and the Caribbean of the Swiss organization PeaceWomen Across the Globe (PWAG). Ms. Moreyra is Peace Fellow 2016 (Rotary Peace Center, Chulalongkorn University, Thailand), Activator of Positive Peace (Latin America), and Ambassador of the Institute of Economics and Peace (Sidney, Australia). She is a trainer of the Course "Prevention of Human Trafficking with Sexual Purposes," aimed to high-school teachers in Uruguay, invited by the Rotary Club of Montevideo due to her expertise on the topic. She has specialized in "Women, Peace and Security," is a regular speaker at national and international conferences with a number of published books and articles in the areas of her specialty.
E-mail: mujeresdepazenelmundo@gmail.com

[24] Drolet, et al., "Women Rebuilding Lives Post-Disaster," 445.

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

Giulia Ferraro, *Connections QJ* 19, no. 4 (2020): 97-107
https://doi.org/10.11610/Connections.19.4.07

Research Article

After the Crisis: The Role of Resilience in Coming Back Stronger

Giulia Ferraro

Geneva Centre for Security Policy, https://www.gcsp.ch/

Abstract: The world has entered a period of increased tension marked by larger and more frequent disasters, a widespread socio-economic crisis, and a growing sense of mistrust towards institutions and international legal frameworks. In the midst of these challenging times, the idea of resilience has caught the attention, especially that of the western world, which has been shocked by the COVID-19 pandemic. The purpose of this article is to place the word resilience within the context of contemporary crises so that the international community is not tempted to redirect some of their funds reserved for prevention and preparedness toward something 'new.' Specifically, the article makes three arguments. First, the concept of resilience ought to be understood rightly as a sign of elasticity. Second, resilience is not an alternative to prevention and preparedness but, rather, their result as properly identified in the Sendai Framework. Third, modern crises and the challenges they pose are an opportunity to improve the way we work, reinvigorate international and domestic systems and relations, and ultimately move forward.

Keywords: resilience, crisis management, Sendai Framework.

Introduction

There is widespread confusion about the term resilience. The starting point is that its meaning changes depending on whether one speaks in a technical or non-technical sense. Thus, the idea of resilience discussed in engineering is different from the one conveyed in social science. In this article, the author carries out an analysis based on the latter meaning and discusses resilience in the context of global crises and emergencies. The author explains how this term is often used vaguely in crisis management, probably due to poor discrimination between the phases of crisis management cycles. Resilience is not a 'blanket' concept that covers the before, during and after of dramatic events; instead, it belongs to the final stage of crisis management cycles. Such a rough interpretation of the term has important practical consequences as funds and resources that should be earmarked for prevention and preparedness can be ineffectively and prematurely redirected to strengthening or building resilience. Lastly, the author concludes that resilience is an important concept as it prompts us to take a reality check. In other words, through the pretext of building or enhancing our ability to adapt to and survive difficult situations, we offer ourselves an opportunity to take a moment to reflect on our condition and how we wish to move forward.

As a general overview, the article is structured in three parts. First, the concept of resilience is presented through an explanation of its meaning and the reason why it has seized so much attention. Second, resilience is placed in the context of crisis management, and it is argued that the Sendai Framework might be an interesting base for further work on this topic. The third part reflects on where we are and where we are going as an interconnected and interdependent society, and the conclusion includes some final remarks.

Elasticity and Crisis

Resilience is a skill. Though we all have different levels of aptitude for it, nobody is born resilient. Instead, it is something that we acquire through time and experience. Thus, faced with the difficulty of living in crisis-prone times, the international community has decided to look into resilience and elected it as an indispensable tool for our survival.

The Quality of Elasticity

The word resilience derives from the Latin verb *resilire* – *re* being the prefix and *salire* the verb to jump, which means to leap, spring back, or recoil.[1] With the scientific progress of the XVII century, the Latin adjective *resiliens* began to indicate not only what bounces but also something that can stretch and resume its shapes.[2] Thus, in its original connotation—which still applies in technical fields such as engineering—resilience represents a body's ability to absorb energy from an impact with another body, bend or contract, and then return to its original physical structure.[3] However, with time, the word resilience transited to other non-scientific fields, eventually turning into something more than the innate quality of elasticity of inanimate objects. Specifically, it started to symbolize

[1] James Morwood, *The Pocket Oxford Latin Dictionary* (Oxford: Oxford University Press, 2012).

[2] "L'elasticità di Resilienza," Risposta ai Questiti, Accademia della Crusca, last modified December 14, 2014, https://accademiadellacrusca.it/it/consulenza/lelasticit%C3%A0-di-resilienza/928.

[3] Krista S. Langeland, David Manheim, Gary W. McLeod, and George Nacouzi, *How Civil Institutions Build Resilience: Organizational Practices Derived from Academic Literature and Case Studies* (Santa Monica, CA: RAND Corporation, 2016), 5-9.

the quality of preserving one's integrity and purpose despite the occurrence of dramatic events. In corporate governance, resilience became "the intrinsic ability of an organization (system) to maintain or regain a dynamically stable state, which allows it to continue operations after a major mishap and/or in the presence of a continuous stress"[4]; in ecology, "the capacity of a system, enterprise, or person to maintain its core purpose and integrity in the face of dramatically changed circumstances."[5] However, one of the most interesting perspectives is presented in psychology, where resilience has been identified as something more than the quality to repair and renovate in the face of adversities. Here, resilient entities are expected to maintain their integrity and return to their original state, *at least* as strong as they were before the significant event occurred.[6] This interpretation carries an aspect of potentiality for enhancement—*growing better and stronger*—through the capacity of individuals to take advantage of negative events and foster positive and enduring developments within and around them.

Regardless of the field, the quality of elasticity remains the fundamental ingredient whenever we talk about resilience. Thus, it is important to set a clear distinction between resilience and resistance, which are often used as synonyms, although they carry different meanings. The latter indicates flexibility. It presumes the application of force against an object which resists this force, like a tree that bends to withstand strong winds. If the pressure is too great, however, the body can break. The former, as explained above, is a form of elasticity. The body does not fight the impact but rather absorbs the energy, dampens it, and ultimately resumes its original shape. Another important consideration regards the interpretation of resilience as applied to non-inanimate objects such as people and all entities that are intrinsically connected to and dependent on human beings like organizations and governments. In this context, resilience becomes the skill that allows us to adapt to challenging situations and come back from them enhanced. This is not a consideration of a body that can physically bend and then bounce back; rather, it implies a more abstract idea of elasticity. It is the ability to maintain core integrity and purpose, take stock of and adapt to the situation, reorganize, and then start again. This is not something innate for humans nor human-led entities. Instead, it is contingent on the amount of work and effort that is devoted to it. This is also confirmed by the language usually associated with resilience: you do not unleash resilience; you *build* or *enhance* it. Thus, resilience allows us to move forward from disruptive events as improved entities, provided we invest in it. Resilience needs work and dedication, so we have to strive for it. If no hard work is put in to attain it, then there is no becom-

[4] Karl E. Weick and Kathleen M. Sutcliffe, *Managing the Unexpected, Resilient Performance in an Age of Uncertainty* (San Francisco, CA: John Wiley, 2001), 14, citing Constance Perin, *Shouldering Risks: The Culture of Control in the Nuclear Power Industry* (Princeton: Princeton University Press, 2006), 267.

[5] Langeland, et al., *How Civil Institutions Build Resilience*, 5.

[6] "L'elasticità di Resilienza."

ing stronger, and we remain at the same point we were at before the dramatic event hit us.

The Discovery of Resilience in Times of Crisis

News headlines have been fiercely drawing our attention to the growing number of crises, emergencies, and threats that we are facing. Significant disrupting events are occurring more frequently, with greater strength, and often concurrently.[7] In such a complex landscape, the call for resilience has inevitably reached the realm of social science.[8] In 2016, the members of the North Atlantic Treaty Organization (NATO) agreed on a resilience-focused approach to resist and recover from major shocks and threats.[9] They signed the Commitment to Enhance Resilience, where resilience is identified in Paragraph 1 as "the basis for credible deterrence and the effective fulfilment of the Alliance's core tasks."[10] The United Nations (UN) has also become fascinated by the idea of resilience. In 2013, the United Nations Central Emergency Response Fund published a position paper where resilience is described as an "end state" for communities and households to endure stresses and shocks,[11] and in 2011 the UN Development Program published a report to discuss the role of resilience to ensure sustainable economies in developing countries.[12] The European Union (EU) has also embraced resilience in its 2016 European Union Global Strategy, with resilience promoted to the status of guiding principle for the EU's external action.[13]

These are only a few of the many examples of how the concept of resilience has made it into the work of the international community. Unfortunately, such a great proliferation of ideas and commitments has also fostered great confusion. That is because the way the term resilience is interpreted and what it is supposed

[7] United Nations Office for the Coordination of Humanitarian Affairs, *Global Humanitarian Overview 2020* (Geneva: OCHA Geneva, 2019), 17-19.

[8] Eugenio Cusumano and Stefan Hofmaier, *Projecting Resilience Across the Mediterranean* (Cham: Palgrave Macmillan, 2020), 5.

[9] "Commitment to Enhance Resilience," *E-Library*, NATO, last modified July 8, 2016, https://www.nato.int/cps/en/natohq/official_texts_133180.htm.

[10] "Commitment to Enhance Resilience."

[11] "Position Paper on Resilience," *United Nations Office for the Coordination of Humanitarian Affairs,* last modified May 11, 2013, https://cerf.un.org/sites/default/files/resources/OCHA%20Position%20Paper%20Resilience%20FINAL_0.pdf.

[12] "Towards Human Resilience: Sustaining MDG Progress in an Age of Economic Uncertainty," *United Nations Development Programme,* last modified November 3, 2015, www.undp.org/content/undp/en/home/librarypage/poverty-reduction/inclusi ve_development/towards_human_resiliencesustainingmdgprogressinanageofecono micun.html.

[13] "Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy," European External Action Service, EUGS, last modified June, 2016, https://eeas.europa.eu/sites/eeas/files/eugs_review_web_0.pdf.

to achieve differ from one entity to another.[14] For NATO, resilience serves the purpose of ensuring that the capacity of its members to resist attacks is preserved, thus fulfilling Article 3 of the Washington Treaty.[15] Understood in this way, resilience is about pliability and flexibility rather than elasticity, thus losing its core characteristics of absorbing and dampening energy.

Moreover, such an interpretation does not carry the idea of an opportunity for positive growth in the face of adversities, remaining fixated on a rigid guarantee for defense. The EU and UN seem to be on a different mission. They have welcomed a wider notion of resilience, raising some questions as to whether this word might carry different meanings depending on the context in which it is used.[16] It is also worth noting that both the UN and EU have pledged to implement resilience across all societies and regions, which is a very ambitious goal.

Resilience after Crises

There is a strong connection between preparedness and resilience. Respectively, they define the beginning and end of crisis management cycles. However, resilience is often misinterpreted as a "blanket" concept for all phases. This lapse means that resources are wasted while we are also missing out on an opportunity for enhancement. Though no perfect schemas are available yet, the Sendai Framework might be an interesting step in the right direction.

Crisis Management Cycles and Resilience

There is a crisis when there are three elements.[17] First, there must be a threat to the integrity/scope of an entity. Second, the time for decision-making is limited. Third, the amount of information produced is so significant that processing it systematically proves challenging. Time *per se*, however, does not determine whether there is a crisis.[18] Both sudden (e.g., cyberattacks) and protracted (e.g., climate change) events can still satisfy the elements mentioned above and give rise to disruptive circumstances. In order to address these situations in an organized and effective manner, blueprints of crisis management can be employed. The idea is to divide the tasks according to three timeframes: the "before," "during," and "after" of the crisis.[19] It should go without saying that the allocation of time and tasks is not set but relies greatly on the judgment and sensibility of those involved in implementing these cycles. That is, you move forward to the next phase of a crisis management plan whenever it is appropriate based on the

[14] Cusumano and Hofmaier, *Projecting Resilience Across the Mediterranean*, 5.

[15] "In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack." North Atlantic Treaty art 3, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243.

[16] Cusumano and Hofmaier, *Projecting Resilience Across the Mediterranean*, 7.

[17] Christer Pursiainen, *The Crisis Management Cycle* (London: Routledge, 2017), 2.

[18] Pursiainen, *The Crisis Management Cycle*.

[19] Pursiainen, *The Crisis Management Cycle*.

specific circumstances of the case at hand. Though this statement could appear to be vague and not necessarily useful, it gives us the opportunity to reflect on the fact that crises like those that are testing the scope and integrity of governments and populations are exceptional circumstances that require high-level leaders and professionals in order to be appropriately addressed.

The pre-crisis phase begins with prevention and preparedness and ends with the alert of a crisis.[20] This is a phase of foresight that is often neglected as there is a widespread perception that it is better to hold back on intervention until any potential situations arise.[21] Although everyone certainly has the right to organize their resources as they see fit, and there is wisdom in the idiom *I'll cross that bridge when I get there*; the decision not to invest in forward-thinking planning is a costly one. A serious approach to prevention and preparedness can significantly mitigate the immediate impact and subsequent consequences of dramatic events.

The second phase is about the response.[22] This can develop very quickly, and it ranges from early warning to action to recovery. While some decisions can be based on previous prevention and preparedness findings (e.g., activating business continuity plans), most critical decision-making occurs in this phase. It is very burdensome to make the call on many important matters at the same time (i.e., set strategic objectives, allocate and re-allocate resources, lead teams, learn about changing interests and adjust the response accordingly), and that is probably the reason why this phase is the one that attracts more attention. Then there is the third phase, which is devoted to recovery and learning.[23] As opposed to the previous dynamic phase, this is the moment of adaptation to the new conditions, when communication flow restarts and lessons learned are drawn out. It is in the context of this last phase that we find resilience. Indeed, there can only be elasticity, and a return to the original form after the event has occurred.

Nevertheless, if it is true that resilience is the ability to "dampen the energy and bounce back" from challenging circumstances, that is only one part of the picture. As seen in the previous chapter, resilience in non-inanimate entities also entails the idea of coming back stronger than before. To gain such strength, the entity needs to pause, take stock of the situation, adapt to the new reality, and appreciate how things can be transformed for the better. Thus, resilience is a quality that needs time and awareness to be developed, preconditions that are very hard to get during a crisis. Furthermore, waiting too long to do such an exercise of self-reflection and renovation usually leads to not doing it at all. For these particular reasons, it would be inefficient to place resilience anywhere but at the end of a crisis management cycle. Resilience is something we can and

[20] Pursiainen, *The Crisis Management Cycle*.

[21] Patric Lagadec and Benjamin Topper, "How Crises Model the Modern World," *Journal of Risk Analysis and Crisis Response* 2, no. 1 (2012): 21-33.

[22] Lagadec and Topper, "How Crises Model the Modern World."

[23] Lagadec and Topper, "How Crises Model the Modern World."

should work for, but we need to invest in it at the right time. It would be unfortunate to allocate and spend resources for projects on resilience at a time when we are engrossed in other equally important tasks.

Sendai Framework

In 2015, the United Nations adopted the Sendai Framework for Disaster Risk Reduction 2015–2030.[24] The agreement, composed of seven global targets [25] and four priorities for action,[26] calls for a more inclusive and coherent way of dealing with crises. The objective is twofold. On the one hand, it seeks to shift the attention from the emergency response (phase two) to reducing and managing risks (phase one). On the other hand, it seeks to ensure a global alignment in the way crises are managed. In other words, the Sendai Framework aims at fostering a universal approach where the drivers of crises ("hazards, exposures and vulnerabilities") [27] are identified, prevented, and reduced before the occurrence of severe events. The argument is that crises can be avoided, precluded, or at least limited by paying more attention to their root causes, requiring all actors to join forces.

In the context of the Sendai Framework, resilience is mentioned as the third Priority for Action, *Investing in disaster risk reduction for resilience*.[28] The idea is that it is essential to invest in work that seeks to address the drivers of crises to enhance the strength and ability of "persons, communities, countries and their assets, as well as the environment" to recover from disasters.[29] Thus interpreted, resilience is not an alternative to prevention and preparedness, but their result. Resilience is the "end game," and how well those affected will be able to move forward after crises hit greatly depends on the work done before the event even occurred. Unfortunately, the Sendai Framework wording is vague when it comes to resilience, likely because the core of the agreement is risk management rather than resilience *per se*.

Further, the Sendai Framework does not suggest direct investment for resilience; rather, funds would have to be directed toward preparedness and prevention activities and from there flow down to projects engaged in resilience. In a

[24] "Sendai Framework for Disaster Risk Reduction 2015-2030," United Nations Office for Disaster Risk Reduction, last modified March 18, 2015, www.undrr.org/publication/sendai-framework-disaster-risk-reduction-2015-2030.

[25] i) Lower disaster mortality by 2030; ii) reduce the number of people affected by 2030; iii) reduce economic loss; iv) reduce disaster damage to fundamental goods and services; v) increase the number of states with risk reduction strategies; vi) enhance international cooperation; vii) increase and improve early warnings.

[26] i) Understand disaster risk; ii) strengthen disaster risk governance to manage disaster risk; iii) invest in disaster risk reduction for resilience; iv) enhance disaster preparedness for effective response and recovery.

[27] "Sendai Framework."

[28] "Sendai Framework."

[29] "Sendai Framework."

global financial crisis like the one we are experiencing, one might legitimately question whether it is realistic to believe that any investments will make it all the way to the final stage of crisis management and fulfill the third Priority for Action.[30] Moreover, it is foreseeable that at least some of those criticizing the Sendai Framework for failing to deliver on its promise to address the root causes of disasters will also develop skepticism about resilience.[31] Nevertheless, the ability of the Sendai Framework to raise attention on the broader spectrum of crisis management represents a valuable step forward and could be promoted as the basis for more work on resilience-centered approaches.

The Opportunity

Though crises are a constant of human societies, we are witnessing an increasing number of black swan disasters that challenge our systems and ability to respond. Over the last decade, we have been engrossed by the task of refining our understanding of crises and their risks. Today, we have the opportunity to complete the picture by carving a space for resilience. If not for the sake of becoming stronger, we should do that because it is a good exercise of awareness.

"Black Swans" Are the New Normal

In the past, the view was that crises were seldom unpredictable, and "black swans" remained the exception.[32] Then, ten years ago, we realized that things have been changing, and black swans are occurring at a higher rate than expected. Thus, we have witnessed wars, incidences of social unrest, financial crises, health crises, natural disasters, technological disasters, and industrial disasters even coinciding with one another. A major factor that has to be considered when thinking about this change of trends is the interconnected and interdependent nature of the complex society in which we live. As a result, the effects of crises occurring anywhere tend to spill over geographical and political borders.[33] COVID-19 pandemic is a good example. The outbreak of an unknown disease in China at the end of 2019 spread across the world in a matter of months, reaching everybody from remote communities to those in the most accessible countries. This health crisis has also brought humanitarian and economic challenges while exacerbating the already precarious situation of many vulnerable people. Moreover, the crisis has been unfolding in conjunction with other emergencies such as an above-normal Atlantic hurricane season, endemic social unrest, and systematic cyberattacks, just to name a few.

[30] Mami Mizutori, "Reflections on the Sendai Framework for Disaster Risk Reduction," *International Journal of Disaster Risk Science* 11 (2020): 147–151.

[31] Ben Wisner, "Five Years Beyond Sendai—Can We Get Beyond Frameworks?" *International Journal of Disaster Risk Science* 11 (2020): 239–249.

[32] Lagadec and Topper, "How Crises Model the Modern World," 23.

[33] Daniel S. Hamilton, ed., *Forward Resilience: Protecting Society in an Interconnected World* (Washington, D.C.: Center for Transatlantic Relations, 2016).

The bottom line is that we feel fragile.[34] We understand that exceptional events will occur and have a transformative impact on our lives and integrity of our societies. To limit any sense of dizziness from feeling at the mercy of the unexpected, we have resolved to change our mindset and invest in preparedness and prevention approaches. Unfortunately, it appears that predicting risks and addressing drivers is not enough. So, to foster more reassurance, we have turned to resilience. Indeed, there is comfort in thinking that we will survive whatever emergency happens, we will make the best out of the situation, and that we will come out of it even stronger. Thus, presented and contextualized in our global society, resilience becomes the exercise of enhancing countries' communication systems,[35] organizations, and alliances' agreements,[36] and communities' readiness.[37] These are undoubtedly important kick-offs, but how serious are we about fostering resilience?

Have We Forgotten Something?

Too often, we recycle data, news and information for our conversations on resilience. We also do it with time and resources. That is, we are not yet convinced that resilience deserves its own space. Certainly, we talk about it, but between the response to crisis A and the prevention/preparedness for crisis B we seldom allocate meaningful time to reflect on how our condition and the environment around us have changed and how we wish to move forward. Instead, we take some of the funds from the next prevention and preparedness programs, we book in some time whenever possible, we come out with lessons learned, and that is the end of the current resilience-centered approaches. The author argues that this is not enough and, even worse, it is a missed opportunity. To set aside time for building or enhancing resilience means to find a space where we can work on those skills that help us regain our stability after the recoil from the dramatic event. This is not space where you do the planning for the next crisis, but it is the one where the organization, system, individual, or community take a deep breath and thoroughly reflect on what has happened and how it wishes to move forward.

Meanwhile, crises will continue to happen. If we do not make a conscious effort to include resilience in our routine of crisis management, then we will still

[34] Arjen Boin, Louise K. Comfort, and Chris C. Demchak, "The Rise of Resilience," in *Designing Resilience: Preparing for Extreme Events* (Pittsburgh, PA: University of Pittsburgh Press, 2020), 1-12.

[35] P.H. Longstaff and Sung-Un Yang, "Communication Management and Trust: Their Role in Building Resilience to "Surprises" Such as Natural Disasters, Pandemic Flu, and Terrorism," *Ecology and Society* 13, no. 1 (2008): 3, https://doi.org/10.5751/ES-02232-130103.

[36] Anna Wieslander, "How NATO and the EU Can Cooperate to Increase Partner Resilience," in *Forward Resilience: Protecting Society in an Interconnected World,* ed. Daniel S. Hamilton (Washington: Center for Transatlantic Relations, 2016), 137-148.

[37] "Sendai Framework."

move forward, just a little blinder and weaker. However, it is unfortunate that we are not ready yet to take this potential for enhancement seriously. Of course, even if we invest more in resilience, we still have to deal with black swans and predicted crises. However, if we embrace this, we will have the capacity to take advantage of these negative events and foster positive and enduring developments within and around our systems. In particular, we could come to approach modern crises and the challenges they pose as an opportunity to improve and reinvigorate international and domestic systems and relations. We have to move beyond our backyards and work together as an international community to develop transnational channels of exchange and support to prevent, prepare for, and ultimately emerge stronger from the complex crises we face. Until we recognize that resilience plays a pivotal goal in delivering meaningful and overarching crisis management cycles, our planning for and responses to crises will be regrettably incomplete.

Conclusion

The word resilience has gained a lot of traction in the last decade. Applied to different fields, it assumes nuances that time and again give it slightly different meanings. Nevertheless, the idea at the core of resilience remains the same whenever applied, and it can be summarized in the word "elasticity." In this article, the author focused on the idea of resilience as applied to global crises and asked what exactly it means and whether it is really needed in this context. While recognizing the hard work required to achieve it, the author concluded that resilience is indispensable and should be strived for, as it would be regrettable if we were to emerge from ongoing and future crises unchanged.

It is promising that we care enough to continue engaging in this conversation. This is not just a matter of wording or abstract thinking. How we decide to interpret and pursue resilience has a real impact on the lives of many people, the integrity of many systems, the plans for distribution of funds and, most importantly, the global security landscape at large. We ought to exchange ideas, seek feedback, and hear what others have to say as that is the way to sharpen our critical thinking and make the right adjustments to foster progress as a global and strongly interlinked community.

In the author's opinion, the Sendai Framework represents an interesting opportunity for setting the record straight about resilience. Though it could be argued that it has not yet achieved its own goals and that the idea of resilience therein is somewhat vague, the Sendai Framework is one of the few instruments available that presents an overarching approach to crises. Through the medium of the framework, greater emphasis could be placed on the difference between the before (prevention and preparedness) and after (resilience) of crisis management priorities. In turn, this could help to more meaningfully respond to at least some issues related to crises, such as the allocation of resources and the need for more enduring solutions.

Acknowledgment

The author wishes to thank the members of the editorial board of *Connections: The Quarterly Journal* as well as Dr. Matteo Tondini, Colonel (GS) Laurent Currit, don Riccardo Battocchio, and Mr. Dom Johnson for their valuable and always highly appreciated support.

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

Giulia Ferraro has an international legal background. She began her career in the private sector and worked for a commercial law firm in Melbourne, Australia, until 2018, when she transitioned to the humanitarian field. Since then, she has worked on peace and security issues in Sri Lanka, Colombia, and Switzerland. At the time of writing, Giulia is a fellow at the Geneva Centre for Security Policy in Switzerland, where she is collaborating on a project on sustainability and security as well as pursuing new partnerships and opportunities. Giulia holds a Master of Laws from the University of Melbourne, Australia and an Integrated Master's Degree from the Università Cattolica del Sacro Cuore di Milano, Italy. She also studied law in the UK and Lithuania. Giulia speaks Italian, English, a good level of Spanish, and she is now learning French. *E-mail*: fg.ferrarogiulia@gmail.com

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

Borislava Manojlovic, *Connections QJ* 19, no. 4 (2020): 109-120
https://doi.org/10.11610/Connections.19.4.08

Research Article

Conflict Resilience and the Image of the Other among North and South Koreans

Borislava Manojlovic

The Carter School for Peace and Conflict Resolution, George Mason University, https://carterschool.gmu.edu/

Abstract: The article aims to articulate key micro-level factors that contribute to the resilience to conflict of South and North Korean communities living in the Seoul metropolitan area. The concept of resilience at the micro-level is defined as having three aspects: recognition of communal and individual interdependence, quality of interaction, and perceptions promoting cooperation and trust. The problem-solving workshop conducted with North Korean diaspora members and their South Korean counterparts served as an opportunity to assess communal resilience to conflict. The findings show that resilience may improve by enabling quality interaction among community members and the introduction of education that promotes understanding, tolerance, and respect.

Keywords: conflict resilience, problem-solving, North Korea, South Korea.

Introduction

The article aims to articulate key micro-level factors that contribute to the resilience to conflict of South and North Korean communities living in the Seoul metropolitan area. The ideologically, socially and economically diverse communities represent a microcosm of the challenges and opportunities that may emerge with the integration of the two Koreas. The concept of resilience to conflict is observed through a dynamical systems lens. Specifically, the nested model of components of sustainable peace [1] is used to look at micro-level factors for resilience to destructive conflicts. The concept of resilience at the micro-level is de-

[1] Robin R. Vallacher, Peter T. Coleman, Andrzej Nowak, Lan Bui Wrzosinska, Larry Liebovitch, Katharina Kugler, and Andrea Bartoli, *Attracted to Conflict: Dynamic Foundations of Destructive Social Relations* (New York: Springer, 2014).

Partnership for Peace Consortium of Defense
Academies and Security Studies Institutes

fined as having three aspects: 1) recognition of communal and individual interdependence; 2) quality of interaction; and 3) perceptions promoting cooperation and trust. The problem-solving workshop (PSW) conducted with North Korean diaspora members, and their South Korean counterparts served as an opportunity to assess communal resilience. The exercises and survey of the participants during the problem-solving workshop provided insights into the communal resilience of the two communities that are facing challenges of socio-economic integration and negative perceptions towards each other.

The workshop took place in Songdo, South Korea, with 14 participants that belonged to North and South Korean communities living in South Korea. Although communal resilience requires a longitudinal and multi-level study, this article offers a glimpse into the participants' perceptions generated via survey and problem-solving exercises. The problem-solving workshop focused on identifying issues that communities faced in their everyday interaction, how they dealt with differences, and addressed the problems. The findings show some preliminary insights into the ways communities could become more resilient to conflict through quality interaction among community members and the introduction of education that promotes understanding, tolerance, and respect.

Problem-Solving Workshops

From September 28-29, 2019, the Peace and Conflict Studies Center Asia (PACSC Asia) hosted a two-day problem-solving workshop (PSW) on the IGC Korea Campus in Songdo with 14 members of South and North Korean communities living in South Korea. The workshop is a well-established practice in peacebuilding and conflict resolution that provides an informal, low-risk, noncommittal forum in which unofficial representatives can privately analyze different issues, identify problems, and engage in active problem-solving processes.[2] The purpose of the workshop was to generate key insights and perspectives from North and South Koreans living in South Korea on the best ways to deal with integration and coexistence issues as the process of reunification moves forward. The workshop offered a safe place for North Korean diaspora members to share their experiences and to connect with others who have faced similar challenges while adapting to South Korean society. The participants discussed relevant issues in an informal, discreet, safe, and low-profile context.

The PSW was hosted over a period of two days. It consisted of lectures, group work, and structured exercises and discussions that provided concrete ideas on the major issues and strategies of problem-solving that could serve to inform policy of future peacebuilding efforts and contribute to communal resilience to conflict. Together with colleagues and students, the workshop was facilitated by Dr. Borislava Manojlovic, who created specific program activities to help the participants analyze and identify problems, generate solutions, build teams, and use

[2] Dean Pruitt, Sung Hee Kim, and Jeffrey Z, Rubin, *Social Conflict: Escalation, Stalemate, and Settlement* (Boston, MA: McGraw-Hill, 2004).

conflict resolution skills to gain deeper insights into the core issues and propose creative ideas. George Mason students from PACSC Asia worked as translators, discussion leaders, note-takers, and logistics staff during the workshop.

A bigger pool of workshop participants would be necessary to claim the statistical significance of the results. However, this study's contribution is in its preliminary findings, generated through a unique venue—problem-solving workshops—in which participants from both communities have been able to interact face-to-face and lead an in-depth discussion about key issues. The venue for free and open discussions between the two communities in Koreas has been almost non-existent. Therefore, PSWs provided a unique and safe locale to generate both the qualitative and quantitative data on a smaller sample, which offered the initial insight into the communally identified issues. While the sample has been limited, the scope and depth of the collected data have been substantial. This study's findings show that people's perceptions towards the other are primarily shaped through intercommunal interaction and quality contact can significantly impact future relations in communities.

Literature Review

Before delving into the data collected during the PSW, it is important to discuss research that has already been done on the relationship and attitudes of North and South Koreans towards each other and the possibility of integration. Kim and Jang bring insights into the increasing apathy South Koreans feel towards North Koreans living in the South.[3] The national poll of the Korean Institute for National Unification in 2005 indicated that South Koreans were experiencing lower degrees of compatriotism and animosity towards North Korean refugees compared to previous years' results. Most of them reported having "no particular emotion" towards the other. On the other hand, North Koreans living in South Korean society reported feeling "emotionally distant" from their South Korean neighbors. The authors explained that such indifference towards one another could often bring about mutual distrust, and cases where South Koreans have committed fraud against North Koreans, have only reinforced North Koreans' negative image.

Cho's article analyzes South Korea from the North Korean perspective in three ways. First, South Korea's "imagined self" is seen as inseparable from North Korea.[4] The phrase "We, the same Korean" summarizes the view that North Koreans emphasize the historical roots shared with the South Koreans. The second image of South Korea is the "tainted but strong self," in which South Korea is looked upon as a society that needs to be rescued from the U.S. imperi-

[3] Jihun Kim and Dongjin Jang, "Aliens among Brothers? The Status and Perception of North Korean Refugees in South Korea," *Asian Perspective* 31, no. 2 (2007): 5-22.

[4] Young Chul Cho, "North Korea's Nationalistic Discourse: A Critical Interpretation," *Korea Observer* 42, no. 2 (Summer 2011): 311–43.

alism. North Korean media often describes South Korea as being a colony of the Western world.

Consequently, the people of the South are viewed as naive and oblivious. Lastly, South Korea is considered to be the "threatening other" that possesses dangerous and hostile qualities that challenge the North Korean regime. It is important to keep in mind that the images North Korea portrays about the South have been communicated and censored by the North Korean government, but there is a gap in knowledge about the views of the people of North Korea themselves about their Southern counterparts.

According to data from public opinion surveys conducted by the Asian Institute for Public Studies, there seem to be different generational perceptions among South Koreans towards North Koreans.[5] More negative perceptions were reported to be stronger among those in the 20s and the elderly (60s and over). The in-between age groups generally saw North Koreans as "neighbors" and "one of us," while the younger and older generations perceived them as "enemies" or "strangers." A closer look at the survey results revealed that many young people in South Korea oppose the government's funding to North Korea and do not feel empathy for the socio-economic situation of the majority of the people there. Moreover, there is a general fear among those in the 20s and the elderly that a war could break out at any time between the two Koreas. Based on that belief, their image of the other has been primarily shaped by mistrust and apprehension.

The mistrust among the two communities has also been portrayed on some popular television shows. For example, *On Our Way to Meet You* is a television program in South Korea in which North Korean refugees are invited to speak about their experiences living and adjusting in the South. In an episode titled, "South Korean Stereotypes towards North Koreans,"[6] former North Koreans emphasized that they were often perceived as the Kim regime's supporters. One of the interviewees shared that whenever news headlines about the North Korean missile tests were released, his neighbors would criticize and shun him just because he was from the North. However, he pointed out that the regime and the people were not "one." From their testimonies, it seemed that the South Korean image of the North Koreans has been heavily dependent on how they felt about the Kim regime and their behavior fluctuated from extremely bellicose to mildly aggressive. In contrast to the South Korean belief that everyone in the North had some degree of loyalty to the Kim regime, North Koreans wished to be perceived as individuals with their own views and stance.

The literature review shows that much of the intercommunal perceptions have been affected by the daily events and public discourse coming from the

[5] Ji-yoon Kim, Chung-ku Kang, and Kil-dong Kim, "To South Korean Youth, North Korea Is Not 'One of Us'," *The Korea Times*, May 1, 2018, www.koreatimes.co.kr/www/nation/2018/05/103_248242.html.

[6] "South Korean Stereotypes towards North Koreans," *On Our Way to Meet You*, Channel A, September 10, 2017. https://tv.naver.com/v/2048839.

media, news, and other public platforms rather than through face-to-face interaction. However, this study's findings show that the perceptions of people towards the other are primarily shaped through interaction rather than media. Although the current political situation makes it difficult for interaction to take place between North and South Koreans across the state borders, efforts towards a peaceful integration can begin through interaction with North Korean diaspora members that are already in South Korea. As findings of this study demonstrate, the high levels of uncertainty and distrust about the other could be addressed by increased quality contact and education that promotes understanding, tolerance, and respect.

Participants

There were fourteen participants in the workshop. The majority of participants, ten, belonged to the North Korean diaspora, while four were members of the host South Korean community. The participants were recruited through contacts with non-governmental organizations, educational institutions, and ads posted on social media platforms. Since the participants had varying degrees of fluency in English, simultaneous translations were provided by GMU Korea students throughout the sessions. In terms of gender and age, there were ten women and four men; eight participants belonged to the 18-35 age group, while 6 participants belonged to the 36-60 age group. In terms of educational level, the majority of participants had a Bachelor's degree.

Data Collection

The problem-solving workshop with North Korean diaspora members and their South Korean counterparts served as an opportunity for the two communities to engage actively and to assess communal resilience to conflict. The PSWs focused on identifying issues that communities face in their everyday interaction and how they dealt with differences. The data was collected via a survey and through problem-solving exercises. To elicit more detailed, qualitative responses, the participants were divided into three groups, with approximately five members who participated in the "problem-solving tree" exercises. Each group created its own tree identifying major issues that they placed on the tree trunk. Then they listed the causes, and finally, they linked the issues to the outcomes in the tree branches.

The participants were given an ample amount of time to construct a tree on the topic of conflict resilience and integration as a group, and the results were shared with the participants the next day. The collected data was analyzed by examining the indicators of the three aspects of resilience at the micro-level: 1) recognition of communal and individual interdependence and integration, 2) quality of interaction, and 3) perceptions promoting cooperation and trust.

Data Analysis

Problem Solving Exercises

In this section, I examine the issues, root causes, and outcomes identified by the participants in the problem-solving exercises. Many of the issues related to difficulties in achieving peaceful co-existence and integration have to do with cultural differences between North and South Koreans. Although the two communities share a common history and ethnic tradition, the 70-year long separation under very different governing systems has resulted in a cultural divide. The differences in communication styles have been cited as one of the important challenges that the communities faced. For instance, North Koreans tend to be more direct, and they tend to speak with candor, while South Koreans are more indirect and use high-context language, which shows their socio-economic status, position, and age group.

Another issue indicating cultural differences was the sharing and cavalier attitude among North Koreans. For North Koreans, "going Dutch" seems rather "cold-hearted," detached, and even rude. While it is common among South Koreans to settle their bills by paying separately or splitting the amount owed, the North Koreans are more used to taking turns to buy meals or repaying someone through other means. The "culture shock" North Koreans experience upon arriving in South Korea is similar to the experience of a foreigner coming to Korea. One participant points out that "The mental and emotional challenges we experience resemble the types of trouble third culture kids (TCKs), like missionary kids, go through upon repatriation." The different cultural, communication and language practices in communities' daily lives reveal a lack of communal and individual interdependence and integration, which may negatively affect communal resilience to conflict.

Other issues that were brought up by participants revealed the lack of trust that both communities face at the personal and relational level. For instance, North Koreans pointed out that they have interacted and engaged in conversations with their South Korean neighbors daily, yet they felt as if there was still a 'wall' between them that they could not overcome. One North Korean participant used the term 'orientalism' to explain South Korean attitudes towards him when they first learned that he had "defected from the North." The North Korean participants pointed out that there was a perception about them being 'uncivilized,' 'uneducated,' 'unrefined' or even that they were "the recipients of too much sympathy" because of the intense trauma they must have acquired living under the Kim regime. By contrast, most of the North Korean participants in the workshop possessed at least Bachelor's degrees, and many of them were studying to earn a Master's degree in South Korea. Furthermore, some came from rather wealthy backgrounds and did not describe their lives in North Korea as 'traumatic.' As one participant pointed out, "North Korean collectivism is stronger than South Korean collectivism." By this, he meant that North Korean attitude towards the Korean culture and identity was more conservative and oldfashioned. He also spoke of North Koreans' need to belong to the ingroup, which provided safety, while outsiders were generally distrusted not only because they have lived in isolation before coming to the South, but also because they saw South Koreans as more Westernized and therefore by default less trustworthy.

According to the participants, the root causes that have created the conditions for inter-communal distrust and stereotypes include North Korea's isolation from the rest of the world and the generational gap that prevents South and North Koreans from having a consistent attitude or knowledge about the other. An important finding was that the perceptions of South Koreans toward the North Korean diaspora were based on the lack of information and knowledge that can only come from face-to-face interactions. This led to the formation of stereotypes and distrust, which can pose a challenge to communal resilience and sustainable peace.

The language spoken in South Korea is full of recently adopted westernized words, which North Koreans find not only difficult to understand but also difficult to accept. For example, some of the everyday South Korean words adopted from English, such as 'nickname,' 'personality,' and 'tour' have their equivalents in Korean, but people in South Korea prefer using the westernized version. As mentioned in the literature review, South Koreans' young generation showed very little interest in co-existence and living together with their North Korean counterparts. The participants argued that the lack of interest was connected to poor education with regards to integration among youth. As one participant pointed out:

> … the voices on the coexistence and integration of the Two Koreas that are constantly heard are the voices of the international bodies and South Korea, but voices and perspectives that come from North Koreans or young people are not heard.

Therefore, an eventual peaceful solution and reunification cannot become a reality until all current and future stakeholders are given a voice on the matter.

Due to the social, economic, and cultural differences of being raised in different systems, there has been an acute lack of understanding among community members that often resulted in negative perceptions and distrust towards the other. However, individual members of both communities have constantly been trying to balance their personal and collective selves, especially when facing a perceived threat. They had needed to differentiate from the group to preserve parts of their individual uniqueness and identity, especially when their group identity was not considered advantageous. As one of the participants expressed, "North Koreans are not all the same. We want to be seen as different entities from our leader and his regime." In other words, the South Koreans' perception that all North Koreans were "the children of Kim Jong-un" and the North Koreans' perception that all South Koreans were "cocky, selfish, and passive" have been a hindrance towards improving the relationship between the two groups. This phenomenon is called a 'unitary trap,' which refers to the tendency of putting a whole group of people in one box that locks the communities in an identity struggle. The way out of the unitary trap is by exposing stereotypes, inaccuracies, and rumors, which is the key step towards achieving conflict resilience.

Survey

Survey data provided some additional insight into the perceptions of North and South Koreans about each other. The finding from the PSW exercises that personal interaction was the key factor that shaped participants' attitudes towards the other was confirmed in the survey by most participants (see Table 1).

Table 1. What Shaped Your Attitude towards South/North Koreans?

#	Answer	%	Count
1	Personal interaction with them	50	8
2	News and documentaries	18.75	3
3	Political ideology	12.5	2
4	Entertainment media (movies, music, arts, sports, etc.)	6.25	1
	Total	100	14

The majority of both South and North Korean participants (82 %) pointed out that the words that best describe their perception about the other group were "one of us" and 'neighbor,' while 16 % of the participants perceived the members of the other group as 'strangers' (see Table 2).

Table 2. Which Word Best Describes Your Perception towards South/ North Koreans?

#	Answer	%	Count
1	One of us	41.67	5
2	Neighbor	41.67	5
3	Stranger	16.67	2
4	Enemy	0	0
5	Not applicable (neutral)	0	0
	Total	100	12

The participants identified the others as 'strangers' because there were differences in language, culture, and background, while the majority stressed that because they all currently lived in the South, it was natural to think that "we were one." South Korean participants pointed out the difference between North Koreans living in the South and those in the North:

> Because of the personal interactions I have had with the North Korean diaspora, I feel as if we are one. However, I only feel that towards the North Koreans who are in South Korea. For those who are in the North, I would consider them foreigners.

When asked about the future life together and co-existence, 50 % of the participants were neutral, and 50 % agreed that the future together was possible (Table 3). This is an interesting finding that points to the ambiguity about the status of their nations and distrust that exists among communities. According to the participants, the main obstacles to integration and life together have been the regime in North Korea, failed negotiations, access to information about each country, and cultural differences. The positive aspects of integration have been the same – language, the same national roots, Confucian cultural practices, and history that bound the Korean Peninsula people for centuries.

Table 3. In the Future, Is It Possible for North and South Korea to Peacefully Coexist?

#	Answer	%	Count
8	Strongly agree	7.14	1
9	Agree	42.86	6
10	Neutral	50	7
11	Disagree	0	0
12	Strongly disagree	0	0
	Total	100	14

However, common national and ethnic identity has not been strong enough an incentive for participants to agree on the possibility of peaceful co-existence of the two states. While most of the participants considered North and South Koreans the same nation (See Table 4), both communities are ambiguous and unsure if the two nation-states could coexist.

Table 4. Do You Think North and South Koreans Are the Same Nation?

#	Answer	%	Count
1	Strongly agree	50	7
2	Agree	42.86	6
8	Neutral	7.14	1
9	Disagree	0	0
10	Strongly disagree	0	0
11	Other	0	0
	Total	100%	14

The participants' qualitative responses showed that the nature of the two states was so different that even the people who belonged to the same ethnic and cultural background could not see the two systems working either side by side or unified unless there was a major ideological change.

Another interesting finding from the survey was that the majority of the North Korean defectors felt that they were discriminated against in South Korea (see Table 5).[7]

Table 5. Have You Ever Experienced Discrimination in South Korea as a North Korean?

#	Answer	%	Count
1	Strongly agree	12.5	1
2	Agree	50	4
3	Neutral	25	2
6	Disagree	0	0
7	Strongly disagree	12.5	1
	Total	100	8

Misunderstanding was often due to the difference between Hangul language in South Korea, with its large influx of the Western vocabulary, and the North Korean dialect, which emphasized the purity of language. One participant argued:

> I have constantly heard them talk about North Korean defectors in derogatory terms and question our true motives of coming down to the South. People's tone of voice changes when they realize they are talking to a North Korean defector which immediately puts us in a disadvantaged position during job interviews and public engagements.

Another participant confirmed the previous point by stating: "When I told the principal of my child's kindergarten that I am a North Korean defector, her attitude changed. She became cold and unkind."

When asked about their hopes and goals for the future, the North Korean participants mentioned the importance of non-discrimination and living freely in South Korea. While the hopes of the South Koreans were broader and more general, North Koreans seemed to have more specific hopes and dreams that ranged from better care for their elderly and building the unification education system

[7] Note that the overall number of responses for different questions is different because the participants skipped some questions in the survey. For example, despite there being 14 participants, only 8 or 12 responded to a certain question. Moreover, some questions (Table 5) were only directed to the particular community, e.g., North Koreans.

in South Korea to visiting their hometowns and families in North Korea. Both groups had great hopes that the pain of division and parted families would be addressed in the near future.

Findings and Conclusions

Conversations on co-existence, resilience, and integration are limited to very few spaces in the current South Korean society. Despite having the same ethnic and cultural background, North and South Koreans cannot see the two political systems working either side by side or unified unless there is a major political and social change, especially in North Korea. Over 30,000 North Korean defectors currently living in South Korea have been a constant reminder that there was the other society just a few miles from Seoul that has driven those defectors out and compelled them to the life of refugees. In the new society, the North Koreans often face difficulties as they try to be accepted and understood by their hosts. The different cultural, communication, and language practices in the daily life of communities reveal that there is a lack of interdependence and integration.

This study also shows that the perceptions of people towards the other are primarily shaped through interaction. Quality interaction is much needed to promote equity and unbiased attitudes. Increased contact and cooperation among North and South Korean communities through platforms such as the PSWs can strengthen the capacity for collaboration and conflict resilience at the communal level, which is a pre-condition for the larger process of integration. As stated by Allport's Contact Hypothesis,[8] intergroup relations can be improved through quality contact under appropriate circumstances. Quality contact may challenge the initial prejudice that has been creating misunderstanding, miscommunication, and irrational fear of the other.[9]

Since conflict resolution practice is still relatively new to Korea, there is a need for more experts and activists who are willing to engage communities and do the work at the grassroots level. Having expert facilitators who understand the local needs, context, and situations to conduct future workshops and dialogues should remain a priority. Although the current political situation makes it difficult for interaction to take place between North and South Koreans across the state borders, efforts towards a peaceful co-existence can begin through interaction with North Korean diaspora members that are already in South Korea. As findings of this study show, the high levels of uncertainty and mistrust about the other could be addressed by increased quality contact and grassroots education that promotes understanding of cultural differences, tolerance, and respect.

[8] Gordon W. Allport, *The Nature of Prejudice: 25th Anniversary Edition*, Unabridged (New York: Basic Books, 1979).

[9] Buhle Zuma, "Contact Theory and the Concept of Prejudice: Metaphysical and Moral Explorations and an Epistemological Question," *Theory & Psychology* 24, no.1 (2014): 40-57.

Apart from quality interaction, the education system would benefit from incorporating a new curriculum on reunification to primary and secondary schools in South Korea. The purpose of the reunification education is not to force students to think that reunification is necessary and must happen at all cost, but to encourage them to think for themselves about the future and the role they might want to play in the process of building peace.

One of the most interesting aspects of the workshop was the impassioned participation of both South and North Koreans in the discussions. People were eager to express their views and they ardently communicated their thoughts. Moreover, they were not afraid to ask questions to others and the facilitators. The participants did not seem intimidated or uncomfortable in a new setting, and they were happy to share their stories openly. Although the overall impact of the PSW could not be measured at this point, the participants found this format empowering. Talking about their experiences, the participants exemplified resilience, strong will, and perseverance. In this way, they were able to organize their memories, process emotions, and make sense of who they are.[10] Since the goal of the PSW was not to come up with direct solutions or answers but to foster understanding and recognize the key issues, the workshop empowered the participants by providing a safe space for them to share their stories.

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

Borislava Manojlovic, PhD, is the Assistant Professor at the Carter School for Peace and Conflict Resolution, George Mason University. She is an expert in peacebuilding, transitional justice, dealing with the past, peace education, and atrocities prevention. Before joining academia, she worked on minority and reconciliation-related issues with the United Nations and the Organization for Security and Cooperation in Europe in both Croatia and Kosovo for over seven years. Her book *Education for Sustainable Peace and Conflict Resilient Communities,* was published by Palgrave Macmillan in 2018. Prof. Manojlovic received her master's degree from Brandeis University and her doctorate from George Mason University's Jimmy and Rosalynn Carter School for Peace and Conflict Resolution.
E-mail: bmanojlo@gmu.edu

[10] Nader Amir, Jane Stafford, Melinda S. Freshman, and Edna B. Foa, "Relationship Between Trauma Narratives and Trauma Pathology," *Journal of Traumatic Stress* 11, no. 2 (1998): 385-392.

Connections: The Quarterly Journal
Submission and Style Guidelines

Connections accepts manuscripts in the range of 2,000 to 5,000 words, written in a lucid style for a target audience of informed defense and security affairs practitioners and academics. All manuscripts should be submitted to the *Connections* editorial office electronically at PfPCpublications2@marshallcenter.org or uploaded to the journal website via https://connections-qj.org. They should feature the author's name, current institutional affiliation, and a provisional title at the top of the first page, and should include footnotes where necessary. Additionally, authors should provide a manuscript abstract and keywords.

Preferred themes for journal future editions include:

Arctic Exploitation and Security
Arms Control and European Rearmament
Challenges and Opportunities in Intelligence Sharing
Countering and Preventing Violent Extremism
Cybersecurity
Defense Institution Building
Future Security Scenarios
Hybrid Warfare
Limitations of Naval Power
Migration and Refugees
NATO's Unstable Periphery
Putin's Russia: A Threat to Peace or a Threat to Itself?
Terrorism and Foreign Fighters
Trends in Organized Crime

For questions on footnotes and references, please refer to the Chicago Manual of Style, at http://www.chicagomanualofstyle.org/tools_citationguide.html.

Unsolicited manuscripts are accepted on a rolling basis at the discretion of the PfPC Editorial Board.

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

The Operations Staff of the PfP Consortium of Defense Academies and Security Studies Institutes is located at the George C. Marshall European Center for Security Studies.

For all information regarding
CONNECTIONS, please contact:

Partnership for Peace – Consortium
Managing Editor – LTC Torsten Stauffer
Gernackerstrasse 2
82467 Garmisch-Partenkirchen, Germany
Phone: +49 8821 750 2333
E-Mail: PfPCpublications2@marshallcenter.org

ISSN 1812-1098
e-ISSN 1812-2973