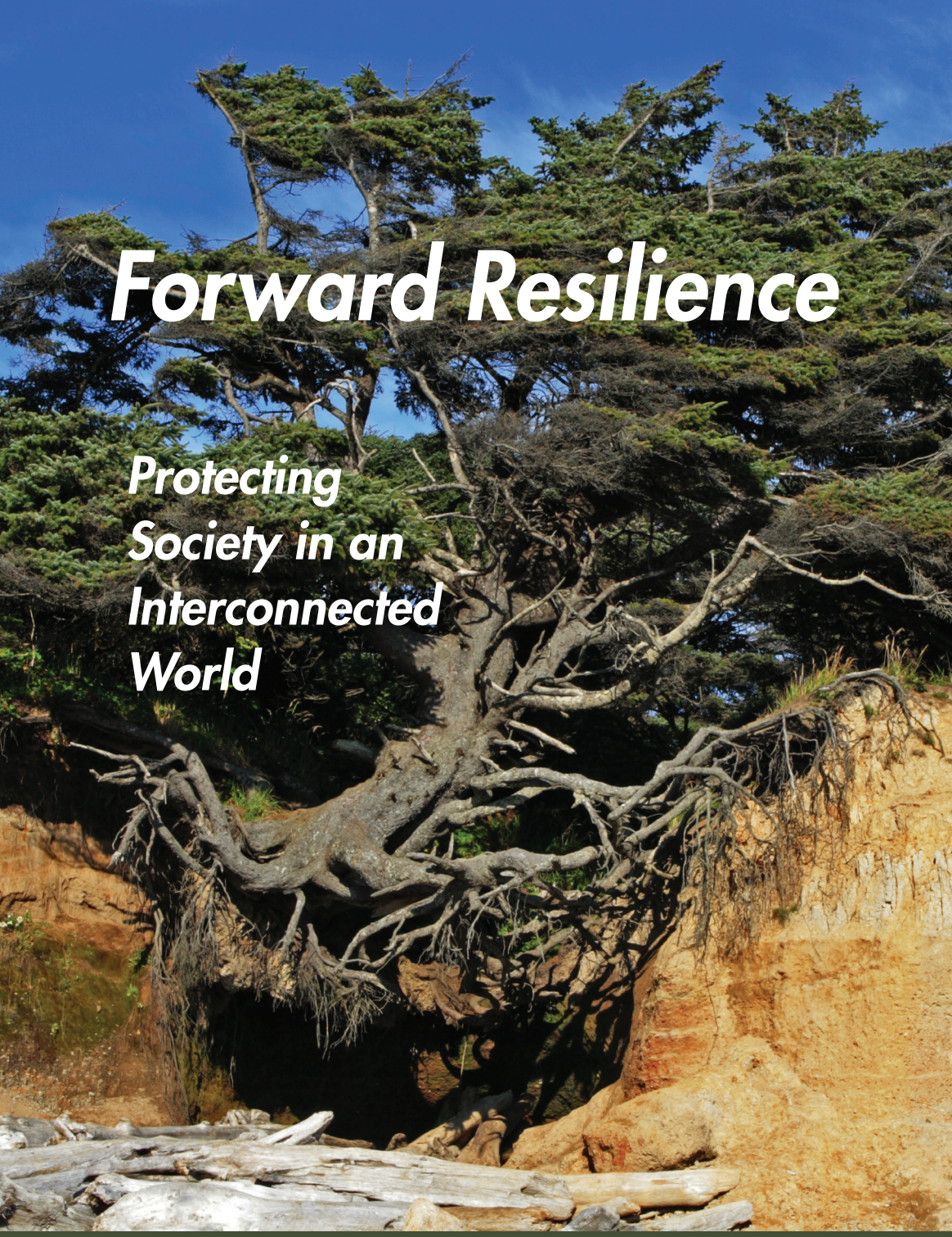


Forward Resilience

Protecting Society in an Interconnected World

Daniel S. Hamilton, Editor

Forward Resilience

Protecting Society in an Interconnected World

Daniel S. Hamilton
Editor

Center for Transatlantic Relations
Paul H. Nitze School of Advanced International Studies
Johns Hopkins University

Daniel S. Hamilton, editor, *Forward Resilience: Protecting Society in an Interconnected World*

Washington, DC: Center for Transatlantic Relations, 2016.

Center for Transatlantic Relations
The Paul H. Nitze School of Advanced International Studies
The Johns Hopkins University
1717 Massachusetts Ave., NW, 8th Floor
Washington, DC 20036
Tel: (202) 663-5880
Fax: (202) 663-5879
Email: transatlantic@jhu.edu
http://transatlantic.sais-jhu.edu

ISBN: 978-0-9907721-5-6

Cover image: Susan Ridley/shutterstock.com

Contents

Preface v

Executive Summary and Policy Recommendations vii

Chapter 1 1
Forward Resilience in Context
Tomas Ries

Chapter 2 23
Toward Greater Resilience in Uncertain Regions
David J. Kaufman and Robert L. Bach

Chapter 3 39
Going beyond Static Understandings:
Resilience Must Be Shared, and It Must Be Projected Forward
Daniel S. Hamilton

Chapter 4 53
Forward Resilience and Enhanced Cooperation:
Bringing Theory to Practice
Mark Rhinard and Bengt Sundelius

Chapter 5 67
Resilience Inside and Out: A Finnish Perspective
Axel Hagelstam

Chapter 6 75
Opening the Aperture on Resilience
Hans Binnendijk and Daniel S. Hamilton

Chapter 7 85
The Case for Forward Resilience in the Baltic States
Tomas Ries

Chapter 8 91
Resilience and Alliance Security:
The Warsaw Commitment to Enhance Resilience
Lorenz Meyer-Minnemann

Chapter 9 99
Resilience as Part of NATO's Strategy: Deterrence by Denial and Cyber Defense
Piret Pernik and Tomas Jermalavičius

Chapter 10 113
Forward Resilience in the Age of Hybrid Threats: The Role of European Intelligence
Björn Fägersten

Chapter 11 127
Temporal Projection of Societal Resilience in the EU: A Dynamic Organization Approach
Tim Prior

Chapter 12 137
How NATO and the EU Can Cooperate to Increase Partner Resilience
Anna Wieslander

Chapter 13 149
The Arguments for a Center of Excellence for Countering Hybrid Threats
Charlotta Collén

Chapter 14 157
Forward Resilience: Five Warnings
Alyson JK Bailes

About the Authors 165

Preface

The notion of resilience is gaining currency in European and Euro-Atlantic security policy discussions. The European Union, NATO, and their respective member states are each building the capacity to anticipate, pre-empt, and resolve disruptive challenges to vital societal functions. They are also exploring ways to work more effectively together in this area. But is resilience enough to deal with disruptive threats in a deeply interconnected world? In this volume our authors argue that while state-by-state approaches to resilience are important, they are likely to be insufficient in a world where few critical infrastructures are limited to national borders and where robust resilience efforts by one country may mean little if its neighbor's systems are weak. They argue not only that resilience must be *shared*, but that it must be projected *forward*, and that traditional notions of *territorial* security must be supplemented with actions to address *flow* security—protecting critical links that bind societies to one another.

This project was conducted by the Center for Transatlantic Relations at Johns Hopkins University's School of Advanced International Studies, together with the Swedish Civil Contingencies Agency, the Swedish Atlantic Council, the Finnish Ministry of Defense, and the Finnish Ministry of Foreign Affairs. Our authors engaged throughout our project with EU and NATO officials and member state experts to assess resilience efforts to date and to explore future needs, with a view to operationalizing the concept of forward resilience.

All authors write in their personal capacity. Their views do not necessarily reflect the views of any institution, organization or government. The policy recommendations do not necessarily represent the views of all authors, but distil many of their individual proposals. I am grateful to them for their contributions. I also want to express appreciation to Pål Jonson for his tireless efforts, to our many partners in Sweden, Finland and in Brussels who helped us with countless meetings, as well as my colleagues Heidi Obermeyer, Peggy Irvine, and Peter Lindeman for their help with our final volume. As always my own insights have been enriched through discussions with my colleagues at the Center for Transatlantic

Relations, and from my many conversations with Bengt Sundelius, who is not only an author in this volume but a true guide to all of us in issues of societal security and resilience.

I am particularly pleased to be able to include as our concluding chapter a contribution by the late Alyson JK Bailes, a former British career diplomat and scholar. For many years Alyson observed and reported on security developments in northern Europe as UK ambassador to Finland, as Director of the Stockholm International Peace Research Institute (SIPRI) and during her final years as a member of the faculty of the University of Iceland. She served us all well as an independent, friendly critic of regional efforts toward enhanced societal security and strengthened resilience and of the many attempts toward increased regional security cooperation among the Nordics, the Baltics and Nordic-Baltic countries together. At my request and that of Bengt Sundelius she quickly took on this critical examination role for this project. Her important chapter was delivered in February 2016, only a few months before she passed away after a long illness. Alyson is deeply missed, but her many and often sharp examinations of complex international security matters endure and continue to enlighten us.

Daniel S. Hamilton

Forward Resilience: Protecting Society in an Interconnected World

Executive Summary and Menu of Recommendations

Western countries today are focused on enhancing their resilience—building the capacity of their societies to anticipate, preempt and resolve disruptive challenges to their critical functions.

Resilience has become an important agenda item for the member states of NATO and the European Union, and a new energy is apparent in efforts to advance more effective NATO-EU cooperation in the field of resilience.

At the 2016 NATO Warsaw Summit, allies agreed to a set of baseline resilience standards and made national pledges to meet those standards; they also each made a Cyber Defense Pledge to secure their national cyber systems. EU member states have similarly approved a strategy and implementation plan to counter hybrid threats, have created a Hybrid Fusion Cell, launched contractual public-private partnerships for cybersecurity, and signed codes of conduct with platform and social media companies to prevent radicalization. Resilience also features prominently in the EU's 2016 Global Strategy document. Moreover, in a 2016 Joint Declaration NATO and the EU committed to "boost our ability to counter hybrid threats, including by bolstering resilience, working together on analysis, prevention, and early detection, through timely information sharing and, to the extent possible, intelligence sharing between staffs; and cooperating on strategic communication and response."

These are positive developments that should be encouraged and supported by publics and parliaments. But they should be understood only as first steps toward a more effective and comprehensive resilience agenda. State-by-state approaches to resilience are important, but insufficient in an deeply interconnected world. Resilience must be shared, and it must be projected forward.

Resilience begins at home, because it is as much a quality as a construct—it is not just a task for government agencies or bureaucratic planners, it must be kept alive in ways that are attuned to the characteristics and dynamics of

a particular society and sustained by the connections forged within that society.

Nonetheless, no nation is home alone in an age of potentially catastrophic terrorism, networked threats and disruptive hybrid attacks,. Few critical infrastructures that sustain the societal functions of an individual country are limited today to the national borders of that country. Social cohesion within a given country can be affected by flows of goods, services, money, data, energy, or simply people—whether refugees or radical elements who cooperate and operate across borders.

This means that traditional notions of *territorial* security must be supplemented with actions to address *flow* security—protecting critical links that bind societies to one another. Governments accustomed to protecting their territories must also focus on protecting their connectedness. This requires greater attention to *shared* resilience. None of NATO's seven baseline requirements for resilience, for instance, can be met without attention to shared resilience.

NATO and EU members also share a keen interest in projecting resilience *forward*, since robust efforts by one country may mean little if its neighbor's systems are weak. NATO and EU member states have a vested interest in sharing approaches and projecting operational resilience procedures *forward* to key neighbors.

NATO allies and EU member states should identify—very publicly—their resiliency with that of others beyond the EU and NATO, and share societal resilience approaches, operational procedures, and foresight analysis with partners to improve societal resilience to corruption, psychological and information warfare, and intentional or natural disruptions to cyber, financial and energy networks, and other critical infrastructures, with a strong focus on prevention but also response. Forward resilience should also enhance joint capacity to defend against threats to interconnected domestic economies and societies and resist Russian efforts to exploit weaknesses of these societies to disrupt them and put them under its influence.

Forward resilience should also include a temporal dimension through better shared coordination with regard to early warning and foresight analysis, as well as "bounce back" capacities well in advance so as to deter attacks or disruptions to our societies' weak links.

In sum, effective resilience should encompass a spectrum that embraces national, shared and forward strategies, and which itself is an integral part of broader full spectrum efforts at deterrence, defense, and emergency management.

NATO

Make resilience an integral element of NATO's core tasks, or consider making resilience a fourth core task. A key element of Russia's strategy is the use of strategic surprise and hybrid threats to take advantage of vulnerable societies. Extremist threats from the south also challenge the fabric of Western societies. Greater societal and defense resilience can be an important component of an effective response. Creating a higher degree of resilience in vulnerable societies makes it more difficult for state or nonstate actors alike to disrupt and create the instability they need for their success. Societies deemed indefensible in traditional defense terms can be rendered indigestible through resilience. Resilience has become integral to each of NATO's core tasks of collective defense, cooperative security, and crisis management, and forward resilience can be an important element of NATO partnerships. Initial activities could include the following:

- ***Conduct a survey of resilience requirements.*** NATO's newly adopted resilience guidelines provide an opportunity to survey NATO members and partners to identify how countries believe they measure up against these guidelines. The results can be used to guide further support efforts.
- ***Set priorities.*** NATO analysts might create a matrix using country vulnerability profiles and functional requirements suggested in this book along with survey results to establish a list of priority activities. For example, the matrix might show that border control is the top priority in the Baltic states but would be something different in other nations. NATO might then use the results of this matrix to identify immediate- and longer-term resilience requirements. This effort could complement the recommended survey.
- ***Identify those who can strengthen forward resilience.*** NATO's Civil Emergency Planning Committee has compiled a list of civilian experts who could be called upon to support the enhancement of resilience. But given the magnitude of the task, much greater efforts will be needed to identify others who can strengthen and project

resilience. No single organization or country has the breadth and capability to deliver on all of these requirements for enhancing resilience. This effort would include identifying those international institutions, non-governmental organizations, nations, and individuals that have a particular expertise in some element of resilience. For example, NATO's Cyber Center of Excellence and its Computer Incident Response Capability are already helping countries with their network security resilience, while OSCE and institutions such as the U.S. National Endowment for Democracy or the European Endowment for Democracy might be well suited to support societal resilience.

- ***Expand the functions of NATO's Civil Emergency Planning Committee (CEPC).*** NATO's CEPC currently has a mandate to plan for contingencies that involve civilian casualties and to provide civilian expertise in the field of terrorism preparedness, consequence management, disaster response, and protection of critical infrastructure. If the expanded scope of resilience requirements we suggest is accepted, CEPC's responsibilities need to be expanded and more resources will be required. There would be a corresponding shift in its emphasis towards enhancement of national resilience.
- ***Create Forward Resilience Advisory Support Teams.*** NATO has periodically used Advisory Support Teams for civilian emergency planning purposes. The resilience commitments made at the Warsaw Summit will require a revitalization and expansion of these Advisory Support Teams in such areas of emergency preparedness including assessments; intelligence sharing, support and analysis; border control; assistance to police and military in incident management including containing riots and other domestic disturbances; helping effectuate cross-border arrangements with other NATO members; providing protection for key critical infrastructures including energy; and, in the cyber arena, support to and enhancement of NATO's Cyber Response Team. Efforts to build these teams should be accelerated. In certain countries, such Teams could be collocated with NATO Force Integration Units, and help national responses with NATO military activities including especially special operations activities.
  - Host nations could be encouraged to establish working group-type secretariats to coordinate defense activities with overlapping civil authority and private sector key critical infrastructure func-

tions to enhance national capacity to anticipate, prevent, respond and recover from disruptive scenarios and to provide a key point of contact for Forward Resilience Advisory Support Teams.

- ***Create "Partnership Programs" for Resilience.*** This concept would be modeled on the current U.S. National Guard State Partnership Program which now operates in 22 European countries and five Middle Eastern countries. In the first instance, these U.S. National Guard programs might be expanded to focus more on resilience issues. But more ambitiously, national partnerships might be created on a framework nation basis to connect NATO members and NATO partners. For example, Italy might serve as a framework nation to develop a resilience partnership with a country in North Africa. Sweden might serve as a framework nation to develop a resilience partnership with a country in eastern Europe. This concept could help to decentralize the resilience-building effort and significantly expand its scope, while also contributing to establishment of specific trust funds and tailored training projects.
- ***Develop clear political guidance concerning which activities will be open for different partners,*** taking into consideration willingness of an individual partner to cooperate with the Alliance, as well as their maturity level. Some partners should be engaged into partnerships with industry and into various NATO's education and training efforts (cyber defense courses, cyber ranges, cyber hygiene platforms, etc.). Some partners should be engaged in planning phases of crisis management and cyber defense exercises. Engagement in these activities and in the Federated Mission Networking should be widened beyond the current range of seven partners.
- ***Establish special cyber support teams*** that can be deployed to partner countries to increase interoperability, improve information-sharing and coordinate responses to cyber crisis. Establish individually-tailored projects and expand existing projects in accordance with interests and capacities of partners to enhance their cyber security and defense. Prospective cooperation areas in cyber defense include increasing interoperability, sharing strategic and technical information and threat assessments, coordinating responses to cyber crisis, and engaging partners into NATO's education, exercises and training activities.
  - To support NATO allies' resilience in the cyber security context, cyber experts should be included within NATO Force Integration

Units (NFIU). This would help assess vulnerabilities, increase preparedness and interoperability in regards with crisis response.

- Assess the levels of the existing maturity of cyber security and defense capacity in partner countries. Coordinate and synchronize mutual training and assistance projects with the EU in order to avoid overlapping. The Partnership Review and Planning Process (PARP) should include cyber defense elements as part of broader resilience efforts, and planning should to be aligned with the NATO Defense Planning Process (NDPP).
- Partners would benefit from the development of minimal requirements for the protection of their critical infrastructure and in regards with cyber defense.

- ***Include resilience and forward resilience components in NATO exercises, training, education, and operational planning.*** Resilience events should be included especially in NATO Crisis Management Exercises (CMX) and cyber exercises such as the annual cyber coalition exercises. NATO/Partner exercises should incorporate forward resilience efforts.
- ***Pay attention to societal resilience.*** Although NATO is paying most attention to infrastructure, networks and civil preparedness, it should also include into its monitoring, assessment and support measures considerations of societal resilience, i.e., the ability of society to maintain rule of law, respect for human rights, and democratic principles in the face of disruptive challenges. This is particularly important from the perspective of maintaining the Alliance's credibility, cohesion, unity and public support to its mission.
- ***Place renewed emphasis on oversight of implementation,*** including novel compliance mechanisms. Peer-review groups (3-5 members making site visits to other member governments to report on resilience) has worked in other international organizations – NATO should consider such mechanisms of naming and shaming as well.
- ***Develop a more robust strategic communications strategy*** to address Russia's information operations, particularly where Moscow draws on social media and hidden messages that seek to exploit social and political differences in allied and partner states. The StratCom Center of Excellence in Riga could be used to plan how the EU, NATO, and partners could connect in order to ensure efficient strategic communication to counter hybrid threats. This would include suggestions for both vertical and horizontal organisation and points of

contact in individual countries, as well as NATO and the EU, and should cover the full spectrum of endeavors, from proactive efforts to crisis management.

Include Finland and Sweden as full partners in these efforts. Both countries have significant traditions of total defense and societal security, and would bring significant added value and experience to these efforts. Finnish experience with territorial defense, border guards, and whole-of-government approaches to societal security, for example, or Swedish expertise with addressing asymmetrical dependencies on external resource flows, may mean that these countries could be leaders in cooperative efforts as neighbors seek to enhance their efforts in such areas.

- ***Forward resilience should be integrated as a high-priority element of each country's Enhanced Opportunities Partnership (EOP).***
- ***NATO should also intensify work in the 28+2 format connected to Civil Emergency Planning***, which has not advanced as far as the 28+2 in the military and political arenas.

EU-NATO

Given the broad nature of the security challenges we face, and given that military means alone will often be insufficient or irrelevant to address them, there is a compelling need for improved cooperation between NATO and the EU. Synchronizing the EU's extensive civilian and small-operations military expertise with NATO's high-end military capacity and transatlantic reach would dramatically improve the tools at the disposal of the Euro-Atlantic community. Without parallel changes in course, NATO and the EU will continue to evolve separately, generating considerable waste in scarce resources, political disharmony, growing areas of overlap, and increased potential for confusion and rivalry.

Important steps have already been taken. In July 2016 both organizations pledged in a Joint Declaration to cooperate to "counter hybrid threats, including by bolstering resilience." Various areas have been identified for enhanced coordination and cooperation, including situational awareness, information sharing, strategic communications, cybersecurity/cyberdefense, crisis prevention and response, and civil-military planning. A playbook for NATO-EU cooperation, dealing with a range of hybrid-warfare scenarios, has been developed for the areas of cyber defense, strategic communications, situational awareness and crisis management.

These are all good initiatives. Still, more can be done. In addition, both NATO and EU leaders have acknowledged that they have not yet addressed in any systematic manner how both institutions could help partners become more resilient. Consideration should be given to the following steps.

Develop mechanisms for institutional cooperation, including a NATO-EU Resilience Coordinating Council. Ideally, such a Council would have an inward-looking and an outward-looking dimension.

- ***Looking inward,*** the NATO International Staff and the EU External Action Service and relevant DGs staff should develop an inter-service mechanism to engage together on a regular basis on exchange of good practice, lessons learned exercises, means to identify and address critical vulnerabilities, shared sense-making, situational and threat assessments, and early warning and early action procedures.
- ***Looking outward,*** the Council should engage both private sector actors and non-member governments who are critically involved in global and theatre networks and flows to promote networked resilience. Specifically, the Council would
  - promote public-private partnerships to facilitate wider resilience linked to NATO/EU baseline requirements;
  - engage recipients of resilience measures to ensure effective forward resilience; and
  - engage additional donors to enable the provision of resilience measures.

Pool EU and NATO resources for the Forward Resilience Advisory Support Teams outlined earlier. They might be used to address the highest priority needs in countries where both the EU and NATO are each engaged in projecting resilience beyond their borders, for example in Ukraine and in the western Balkans.

Establish a comprehensive system of national resilience indicators (Resilience Monitor/Index), covering all relevant domains, to monitor and assess the overall state of resilience in individual nations. This would provide a basis for more focused and specific measures—at the national, EU and NATO levels—to address short, medium and long-term needs. Such indicators could also encompass partner countries willing and able to participate.

Work with host nations to tailor programs. Resilience-building efforts will not work without the active cooperation of host nations. Those

who require or desire assistance with their own resilience efforts will need to take a major role in tailoring programs to fit their own needs, based in part on the recommended survey. The NATO-EU Resilience Coordinating Group, perhaps using joint EU/NATO Forward Resilience Advisory Support Teams, might take the lead in working with priority host countries through Individually Tailored Resilience Planning and Review procedures.

Encourage the establishment of regional working groups. Host nations could, in addition to creating national working groups as points of contact for Forward Resilience Advisory Support Teams, establish working groups with like-minded allies and partners in their region to facilitate shared resilience and interoperable efforts. The Nordic and Baltic states, for instance, might consider a regional approach to forward resilience efforts, somewhat similar to such regional mechanisms as Nordic Defense Cooperation (NORDEFCO) or the Southeast European Defense Ministerial.

Harness improved intelligence-sharing to enhance forward resilience both geographically with select partners and temporally in terms of training and foresight analysis. Intelligence services can address hybrid challenges by identifying and addressing vulnerabilities at home and abroad, and by monitoring hybrid threats and countering hybrid tactics. Multinational intelligence cooperation, however, remains hampered within both NATO and the EU by diverging member state interests, varying levels of trust among intelligence agencies, bureaucratic resistance, and the fact that countering hybrid tactics require intelligence agencies to cover a broad range of actors and organizations spanning the civil, cyber and military domains—a challenging task at the national level, and even more so on an international level.

NATO and the EU have each taken steps to address these challenges. At Warsaw, NATO decided to improve Joint Information Surveillance and Reconnaissance (JISR) capabilities and to create a new Assistant Secretary General for Intelligence and Security, who will run a new Division in the International Staff. The EU's new Hybrid Fusion Cell, which will receive, analyze, and share classified and open source information specifically relating to hybrid threats, is housed within the EU Intelligence and Situation Center (EU IntCen). Still, more needs to be done, and more done together, particularly with regard to forward resilience.

- ***Produce better open source intelligence output within both the NATO and EU systems***, allowing for more efficient responses against hybrid tactics.
- ***Establish genuine multilateral intelligence training.*** The EU IntCen should scale up training modules not just to new EU intelligence analysts, but also to non-intelligence offiers within the EU bureaucracy as well as NATO officials, to familiarize them with each other's systems, and to some extent, to analysts from security agencies in partner countries. Similarly, NATO should consider opening its training modules to relevant EU officials.

Hold joint crisis management exercises with a focus on forward resilience. The EU and NATO have been conducting such exercises over the past few years; it would be useful to incorporate hybrid or disruptive threats, also with partners, into such exercises.

Consider lead nation efforts for key initiatives or to accompany certain reform efforts. The fact that both Sweden and Finland are EU members and could help promote further EU-NATO cooperation has been highlighted but not yet fully explored in the EOP. Both countries are net contributors to EU crisis management and have a long tradition of involvement in neighborhood issues, particularly in the east. Thus, they can with credibility and competence assume leading roles in pursuing questions and issues of common interest. As suggested in the review of the EU's neighborhood policy, individual member states could take the role of lead partner for certain initiatives or to accompany certain reform efforts. The role of lead partner could be used to promote NATO-EU cooperation in specific projects for countries that are devoted to bridging the two organizations closer together. Sweden and Finland should put those words to action. By forming task groups open for other members, Sweden and Finland can assume the role as lead partners to strengthen EU-NATO cooperation on Baltic Sea region security and resilience to the east and in the south.

Support and Strengthen the Helsinki-based Center of Excellence for Countering Hybrid Threats. This new independent center remains outside formal NATO and EU structures while being open to both EU and NATO participation. It promises to do what the EU Fusion Cell does not—provide strategic level research, exercises and training, develop shared "sense-making," enhance interoperability, and build long-term capacity in countering hybrid threats.

- ***Second NATO and EU officials to the Center***, providing for even closer cooperation.
- ***Assign priority attention to studying and understanding what deters Moscow, how it assesses vulnerabilities of target countries and how it seeks to exploit those vulnerabilities to its strategic ends.***
- ***Engage key societal stakeholders in the Center's work.*** The Center will need to draw on clusters of expertise from government, the private sector, academia, think tanks and civil society if it is to effectively understand the vulnerabilities and gaps in vital transnational societal functions.

U.S.–EU

Create a EU-U.S. Transatlantic Resilience Council—operating at a similar level as the Transatlantic Energy Council—to integrate the discussion on societal security, justice, and freedom across all sectors and serving as a cross-sector forum for strategic deliberations about threats, vulnerabilities, and response and recovery capacities that cut across sectors and borders. This group would complement existing professional work within established but stove-piped fora. Although new institutions are not the first imperative for building resilience, some degree of structured oversight between both continents is needed to provide strategic perspective on where EU-U.S. cooperation is working and where more attention is needed.

Improve coordination among EU and U.S. operation centers, a "hot line" connection with the task of providing early warning, situational awareness, and crisis coordination support. Such centers should include the DHS National Operations Center (NOC), FEMA's National Response Coordination Center (NRCC), and the EU Emergency Response Coordination Centre (ERCC). These objectives require regular exercises between EU and U.S. officials to familiarize themselves with procedures and protocols in working together.

Use U.S-EU leadership on resilience to create an informal Multinational Resilience Policy Group to explore policy leadership issues related to supporting resilience at local, national and international levels. A study and benchmarking initiative of this type was launched among governmental and non-governmental representatives from the U.S., Canada, four EU member states, and Australia, Israel, New Zealand,

and Singapore in 2010. More such efforts are needed, in areas ranging from countering violent extremism to helping dislocated populations and communities grappling with the pressures of supporting them.

Bolster coordination with the private sector. Effective resilience requires engagement by the private sector, which owns most infrastructures—both actual facilities and networks—critical to essential societal functions, yet has its own views of protection that may differ from those of governments. A good first step would be to develop a task force that could report to EU-U.S. summits to feature private sector views on priority areas such as cyber resilience and supply-chain resilience.

- ***Consider a Global Movement Management Initiative (GMMI).*** One example where U.S.-EU leadership efforts could pioneer shared resilience with the private sector is with regard to global movement systems, which are integrally linked in today's highly networked and interconnected global economy. The drive to improve efficiency has made these global movement systems more vulnerable not only to attack by terrorists, but to cybercrime and even natural disasters and extreme weather. A EU-U.S. public-private Global Movement Management Initiative could offer an innovative governance framework to align security and resilience with commercial imperatives in global movement systems, including shipping, air transport, and even the internet. And if the EU and the United States could achieve agreement, the norms and standards that would emerge could provide a framework for global arrangements.

Chapter 1

Forward Resilience in Context

Tomas Ries

Addressing Security Needs

Resilience is one of four ways that humans address their security. They include science, strategy, resilience, and a fourth approach that I call "transcending."

Science is the quest to remove uncertainty through understanding. It does this in two ways. One is creative speculation employing logical reasoning (mathematics) to propose how things might function and thus creating hypotheses. The other is testing the hypotheses empirically for falsification, thereby transforming an hypothesis into a theory, if rigorous testing has not disproved it.

While science indicates that there is no absolute certainty (and the history of science reinforces this) we can achieve a very high level of operational certainty for all practical purposes. Our understanding of how the world around us functions, and the technologies that this has generated, has vastly expanded the domain of certainty around the human condition.

And certainty, in terms of understanding causality, confers tremendous power to manipulate our environment. However, despite the advances of science over the last four hundred years, the domains of certainty still remain very small, and beyond them hosts of challenges shrouded in various degrees of uncertainty confront us. This is where strategy and resilience come into play.

Strategy is the attempt to manage uncertainty. It operates outside the tended gardens of science, accepting and engaging uncertainty. As uncertainty still dominates the human condition, it is the most important tool we have at our disposal. It can be divided into two approaches, shaping and dancing.

Shaping is the attempt to manipulate our environment so it accords with our interests as far as possible. This requires conditions where uncertainty is limited and a degree of forecasting is possible. It thus addresses the known-knowns and the known-unknowns. Shaping can be inward-oriented, improving one's own condition, or outward-oriented, shaping the environment. It has dominated much of our strategic thinking since the 19th century. Today, as uncertainty increasingly dominates the human condition, it is being superseded by dancing.

Dancing is needed under conditions of greater uncertainty, when forecasting, planning and shaping are undermined and surprises dominate. Dancing consists of rapidly adjusting to the unexpected, responding to challenges or exploiting opportunities. It addresses the known-unknowns which may be prepared for to some extent, but which still require flexible adjustments, and the unknown-unknowns, which require a great deal of flexibility.

Shaping and dancing call for two very different mindsets. The first is based on analysis, planning, and imposing, and often entails caution and rigidity. The second is based on intuition, agility, and accommodating, and requires boldness and flexibility. Yet both depend on limiting uncertainty, permitting a degree of forecasting, and/or conditions in which the inevitable surprises are not too severe. When uncertainty becomes truly rough, both in terms of intensity and severity, resilience is required.

Resilience becomes important when both science and strategy fail, and we are confronted with a shock or pressure that threaten to significantly alter our condition or existence. It thus addresses the unknown-unknowns. It is examined closer below.

Transcending the environment is the quest for positive liberty. It may be the most effective approach, but few are attracted to it, even fewer succeed, and it is in any case an individual approach, not available to societies as a whole. Thus it is not addressed here.

The Concept of Resilience

Resilience is the response to pressures and shock that take one by complete surprise, or which one may have foreseen, but for which one neglected to prepare. These Black Swans can sneak up on you, knock you down and leave you surprised and battered, with no forewarning or reaction time. Resilience hurts. It is neither a pleasant nor an easy option. It entails accepting and absorbing the blow (and suffering the strain and pain) and

sacrificing important and dearly held things in order to preserve core essentials (and enduring the sacrifice). It does, however, offer the chance of survival.

Resilience is thus a fallback position, the next to last in line before adaptation, which I address in the next section.

Resilience involves no strategic shaping of the environment, little or no dancing, and a correspondingly greater degree of strain and potentially suffering. Under these conditions it is hard to carry out any sort of elaborate strategy. As Mike Tyson puts it: "Everyone has a plan until you punch them in the face, then they don't have a plan."[1]

Whether resilience can be considered part of the strategic approach depends upon how one defines it. Along with science it is certainly a crucial method for survival. However, it is not part of strategy understood as shaping and dancing, as it is entirely reactive. There is no proactive shaping of the incoming energy and very little reactive dancing, apart from absorbing the energy. It is essentially a fallback condition that enables a system to weather completely unexpected challenges to its function and survival. It is that which allows one to survive a completely surprising blow from behind, and then either endure whatever comes, or get back on one's feet and fight back or run. In this respect it is far removed from the strategic approach.

On the other hand, if one is concerned about cataclysmic Black Swans, one may deliberately foster a generic resilience, reinforcing one's capacity to endure unexpected and shocks—either against totally unimaginable but catastrophic surprise, or else against envisaged but remote possibilities, such as the civil defense programs during the Cold War. In either of these cases, the promotion of resilience may be considered a form of strategy, similar to that of an insurance policy. It is certainly a prudent complement to the more active forms of strategy involved in the quest for power. As Zolli and Healy put it, "If we cannot control the volatile tides of change, we can learn to build better boats. We can design . . . systems to better absorb disruption, operate under a wider variety of conditions, and shift more fluidly from one circumstance to the next. To do that we need to understand the emerging field of resilience."[2]

---

[1] Mike Tyson, quoted by Jim Messina, in Dan Balz, *Collision 2012: Obama versus Romney and the Future of Elections in America*. As cited in Edward Luce, "Of Comedy and Errors." *Life & Arts—FT Weekend*, August 10/11, 2013: p. 10.

[2] Andrew Zolli and Ann Marie Healy, *Resilience. Why Things Bounce Back* (London: Headline Publishing Group, 2012), p. 323.

Resilience can thus be considered as being partly beyond power. It confers a degree of passive power, if the objective is to avoid being eliminated and if resilience succeeds in avoiding extinction. But it is a very defensive form of power that does not, per se, influence the danger itself other than, perhaps, through exhaustion.

What: Defining Resilience

A preliminary simple definition of resilience is the ability of a system to accommodate dramatic change while retaining its essence and ability to evolve intact. I will elaborate on this below. Initially it is enough to note that the simple definition above involves three key conceptual components: a system, accommodation, and retaining its essence intact.

System implies that the resilient agent is in fact a system, that is to say a collection of dynamically interacting components, which generate a collective function—the essence of the system—which defines their existence, individually and collectively. Every system thus embodies a core function—its essence. If this essence is lost or changed the system ceases to exist. It either evolves into something else, or goes extinct. This essence, in turn, is sustained by a series of vital life systems. These are more open to change, provided they still maintain the essence, or core function of the system. Finally, the system has a variety of physical manifestations—the branches, leaves and flowers that constitute its contextual shell. These are the most open to change, without affecting the essence.

Accommodation is the key operational characteristic of resilience. It implies that resilience does not resist the incoming energy, but receives it, bends to it, or accommodates it in some other way, and yet does not break. This is the elastic operational aspect of resilience. Resilience is thus not the same as deterrence, where the stressful energy is pre-empted, or defense, where the stressful energy is resisted. From a Daoist perspective water may exemplify this sort of absorption.[3]

A second key quality of accommodation as used here is the ability to sacrifice the less important in order to preserve the essence. This can be painful and drastic. The need and ability to amputate a gangrenous wound to save the life is one example. The human body's reaction to extreme cold

[3] See Francois Jullien's chapter on the nature of the energy of water, "Images d'eau," in Francois Jullien, *Traité de l'efficacité* (Paris: Grasset, 1996), pp. 261–280.

by sacrificing the extremities (nose, ears, hands, feet, etc.) to retain heat for the vital organs is another. In the social dimension, the ability of a society to survive oppressive occupation and recover its essence once liberated is another. In all cases, accommodation to strain can hurt.

Retaining its essence and ability to evolve intact is a second operational characteristic of resilience. As Zolli and Healy put it, resilience involves the ability to "maintain its core purpose and integrity in the face of dramatically changed circumstances."[4]

This angle is important since it highlights the crucial issue of essence, or the core purpose of whatever one is considered resilient. It is crucial because it directs all one's efforts. It makes a huge difference if one sees the core purpose of a given society as being to safeguard the lives and health of all its members, or of safeguarding freedom and independence, or promoting spiritual values, future genetic base, or ecological base, and so forth. The question matters because in a severe crisis involving resilience we will not be able to offer our citizens all the nice values and services that we have built up in peacetime. We will have to make sacrifices, sometimes brutal.

This implies that even if the outer layers of the target bend to the incoming energy, or even break under its onslaught, the inner core of the system, and the critical vital life systems that sustain it, remain intact and can either continue to function while the stressful pressure is applied, or can hibernate and be revived once the extreme pressure is eased. While resilience may include a degree of superficial adaptation, affecting the system's external layers, it thus does not imply a deep adaptation, transforming its essential function or its key vital life systems. Nor is resilience the same as evolution, which ultimately involves a transformation of the essence (or extinction).

Resilience thus involves external softness and elasticity coupled with internal endurance and tenacity of the core. In this respect it cleaves to the Daoist principle of "cotton outside, steel inside. Not the other way around." It accommodates pressure and surface changes while protecting the essence and its ability to recover (if only partly) at a later time. As such it is a partial transformation, but on a sliding scale towards adaptation, which is similar but deeper, affecting a greater part of the support system and, in extremis, the essence. Evolution is an example of resilience leading to adaptation leading to deep transformation.

---

[4] Zolli and Healy, op. cit., p. 7.

A simple example of resilience could be bamboo bending to the wind. A good example of a more elaborate and sophisticated form of resilience is the practice of *tuishou* in the Chinese martial art of *Taijiquan*. *Tuishou* is generally translated as "push hands," but since it in fact is anything but pushy, it might be better translated as "sticky hands" or, better still, as "transforming energy."

Other Definitions

To refine the concept of resilience further we may examine some other definitions of the concept.[5] For example, one loose definition by Carl Folke is "Resilience is the long-term capacity of a system to deal with change and continue to develop."[6] This definition is valuable in that it notes that the resilient agent is a system. As we shall see below this has important operational implications. Beyond that, however, the definition is too loose to be useful. First, our environment is constantly changing, and all objects and systems in it constantly deal with change, and most continue to develop. Folke's definition would thus include almost everything almost all the time. What is missing is the element of dramatic change. It may thus serve as a very general definition of functioning, but not resilience. The second reason it is inadequate is because resilience also involves a short-term capacity to deal with change, such as for instance a sudden shock.

One of the best books on resilience has been written by Andrew Zolli and Ann Marie Healy. They offer a better definition which elegantly covers these deficiencies: "We frame resilience in terms borrowed from both ecology and sociology as *the capacity of a system, enterprise, or a person to maintain its core purpose and integrity in the face of dramatically changed circumstances*."[7]

This nicely generic definition includes two key elements missing in the Folke definition. First, the dramatically changed circumstances, which specify that resilience is more than merely dealing with change. It is the capacity to deal with dramatic, or disruptive, change. This is fairly obvious.

---

[5] Like all concepts, resilience is contested. For a short but very good overview of some of the fracture lines see Michael Hanisch, "What is Resilience? Ambiguities of a Key Term," *Security Policy Working Paper* No. 19/2016 (Berlin: Federal Academy for Security Policy), p. 4. Here I will only examine two particularly clear and useful studies of resilience.

[6] Carl Folke, Director of the Stockholm Resilience Centre. SRC webpage 4.4.2011, text accompanying small lecture video.

[7] Zolli and Healy, op. cit., p. 7 (italics in original).

The second point is deeper, and that is the capacity to maintain core purpose. As we shall see, this is crucial, for that is really what resilience is all about. When disruptive change strikes one must generally sacrifice something. What counts is keeping the essence of the system intact, as well as the minimum vital life systems that support it. As we shall see it also has crucial operational implications for any deliberate attempts to promote resilience, since it forces one to focus and prioritize.

Southwick and Charner offer a narrower, context-bound definition of resilience that largely echoes the core message of Zolli and Healy:

> In the physical sciences, materials and objects are termed resilient if they resume their original shape upon being bent or stretched. In people, resilience refers to the ability to bounce back after encountering difficulty. The American Psychological Association (APA) defines it as the "process of adapting well in the face of adversity, trauma, tragedy, threats and even significant sources of stress—such as family and relationship problems, serious health problems, or workplace and financial stresses. In his book, *Aging Well*, Harvard University psychologist George Vaillant (2002) describes resilient individuals as resembling "a twig with a fresh, green living core. When twisted out of shape, such a twig bends, but it does not break; instead, it springs back and continues growing."[8]

The APA definition mixes resilience with adaptation. Some such as Folke and Zolli/Healy define resilience as the ability to return to a state preceding the shock, which is reconstitution, not adaptation. On the other hand, it all depends on what one considers the preceding state to be. In fact most conditions entail several layers, from the most superficial context-bound to the deep enduring essence. In the face of severe shocks, which make it impossible to restore previous contextual conditions, one must adapt at that level while maintaining or restoring the deeper essential levels. In this sense resilience would include both adaptation to the inevitable at the superficial levels but maintenance or restoration at the core. The twig may bend out of shape, but it still grows and functions as a twig. Ideally, resilience involves full restoration, in which case no adaptation is needed. But when necessary, it involves a mix of adaptation and restoration, provided the essence is restored.

---

[8] Steven M. Southwick and Dennis S. Charney, *Resilience. The Science of Mastering Life's Greatest Challenges* (Cambridge: Cambridge University Press, 2012), p. 7.

Zolli and Healy also make a number of important distinctions concerning resilience. One is that resilience is not always the same as robustness: "resiliency is not *robustness*, which is typically achieved by hardening the assets of a system. The Pyramids . . . are remarkably robust structures . . . but knock them over and they won't put themselves back together."[9] Another is that resilience is not redundancy: "The same holds true for *redundancy* . . . Highly resilient systems are frequently *also* highly redundant systems. But backups are costly . . . Worse still, these backups may become of little or no use when circumstances change dramatically."[10]

This is a particularly apt observation for our present condition. In an age of austerity, most states do not have the money to subsidize agriculture (providing a partial domestic source of food) nor maintain large stocks of oil and grain, or huge shelters for the population. And yet all these could still be needed.

Finally, they note that resilience does not imply returning to an identical state: "resilience does not always equate with the recovery of a system to its initial state. . . . In their purest expression, resilient systems may have no baseline to return to—they may reconfigure themselves continuously and fluidly to adapt to ever changing circumstances, while continuing to fulfill their purpose."[11]

The question is whether such fluidity permits any significant transformative core purpose. If one only reacts, then any shaping of the surroundings would be very limited and shallow. There is a price to be paid for such a degree of resilience. Thus there is probably an optimal equilibrium between stasis and fluidity that permits one both to shape the external environment and adapt to it (an enduring core and adapting surfaces). Go too far either way and one either ends up either as the Pyramids or as a virus.

The Nature of That Which Can Be Resilient

To get an even better grasp of resilience it helps also to understand the nature of that which is resilient. Whether it is a virus, or a global ecosystem, it can be described as a system with three core abilities. The first is the ability to survive a sudden shock to its normal condition. This could include

---

[9] Zolli and Healy, op. cit., p. 13 (italics in original).

[10] Ibid.

[11] Ibid.

the ability to protect the vital core of the system while sacrificing system peripherals. The second is the ability to return to its original state after the shock. The third is the ability to adjust itself to new conditions if they do not permit a return to the original state, but without losing its essence and vitality. This third feature distinguishes a resilient ecosystem from an elastic rubber band. Elasticity is a crucial component of resilience, but it is not enough. A resilient system must also be able to alter itself if survival so demands, yet without losing its essence.

These three abilities are, in a sense, the physiology of resilience. They imply that resilience must be a fairly complex dynamic system, similar to a living organism in the sense that it has a dynamic function, seeks the survival of that function (in other words, of itself), and has the ability to make complex adjustments in that effort. This description thus considers ecosystems, states, societies or cities as living beings, alongside such obviously living organisms such as viruses, plants and animals. One day it could include machines imbued with artificial intelligence, if indeed we could still call such things machines.

In addition to the physiology of resilience, we may also describe the morphology of resilience. From this perspective a resilient system can be divided into three functional parts. The first is the essence, or its core function: that which makes the system what it is, animates it and gives it an evolutionary purpose, even if this is not a conscious purpose. The second encompasses the vital life systems that sustain the essence. The third consists of the outer trappings, including all sorts of more or less redundant or replaceable supporting elements. These are important under normal circumstances, but may be sacrificed in a catastrophe.

Both the physiology and morphology of resilience have implications for how resilience works. We may thus turn to a short outline of how resilience may occur.

How: Promoting Resilience

The definition of resilience includes the three core functions outlined above: surviving the initial shock (preserving the essence) even as peripheral components are buffeted; recovering sufficient vital life systems to sustain the essence, while the storm rages; and finally, adjusting external trappings and vital life systems, if necessary, to sustain the core essence. This last element implies that a resilient system may look very different superficially

after being subjected to trauma, but that its essence remains largely the same. If the essence is no longer the same, then the victim will either have become extinct or been transformed into something radically different.

To survive the initial shock, resiliency needs at least three overlapping qualities. First is the ability to absorb incoming energy. The key quality here is redundancy, whether in terms of space and time, or reserves and alternatives. It needs all those things a hyper-efficient system weeds out. They offer hyper-efficiency, and thus better everything, under normal conditions. But hyper-efficient systems become fatal as soon as conditions become abnormal. Under these conditions we need fat and we need slack, because they permit us to absorb shock. Of course a fine balance is necessary here. Too much slack and fat and the system will not survive the initial blow. Too little slack and fat and it will not have enough reserves to sustain the initial blow.

Nevertheless, one of the key lessons from a resilient perspective is that hyper-efficiency is the enemy of resilience. It makes it, and our entire system, frighteningly vulnerable. We need to get back some fat. The problem for societies living in the age of austerity is that systemic fat costs money. We can no longer subsidize national agriculture to maintain a degree of nutritional self-sufficiency, we can no longer afford the luxury of extra manpower or goods stored in warehouses.

The second quality is the ability to adjust to the incoming pressure, both in terms of avoiding meeting the incoming force head-on, and in terms of modifying its own normal way of functioning. The key quality here is agility and flexibility, dodging the blow and improvising its response. Here too there is a fine balance between giving way so much that one is crushed, and resisting a force that one cannot defeat.

The third quality is the ability to protect its essence even as it its external trappings, and even some vital life systems, bend and crack under the pressure. This calls for an ability to conceal, shield or even remove the vital essence from the incoming force. Here there is no fine equilibrium. All else may be modified or sacrificed, but the core essence must be preserved at all costs, lest one go extinct.

To endure and recover the ability to sustain the essence over time, resiliency requires at least three overlapping qualities:

- First, the ability to endure external pressures by reducing them. This can be done by deflecting them, by returning them against their sources, or by absorbing them.
- Second, the ability to adjust sufficiently to permit survival. This can be done by compromising on non-essential functions, or even discarding them, as for instance in an amputation.
- Third, the ability to sustain essence over time and under the new pressures. This requires ensuring that the minimum of vital life systems needed for the survival of the essence remain functional. Under extreme stress this may be complemented by shutting down the active functioning of the essence, but retaining the minimum needed to allow it to be reanimated at a later time when conditions are more clement. Examples are hibernation or going comatose.

These qualities are in turn facilitated by a degree of measured creative destruction. Thus:

> Regular, modest failures are actually *essential* to many forms of resilience—they allow a system to release and then reorganize some of its resources. Moderate forest fires, for example, redistribute nutrients and create opportunities for new growth without destroying the system as a whole. . . .
>
> More broadly, resilient systems fail gracefully—they employ strategies for avoiding dangerous circumstances, detecting intrusions, minimizing and isolating component damage, diversifying the resources they consume, operating in a reduced state if necessary, and self-organizing to heal in the wake of a breach. No such system is ever perfect, indeed just the opposite: A seemingly perfect system is often the most fragile, while a dynamic system, subject to occasional failure, can be the most robust. Resilience is, like life itself, messy, imperfect, and inefficient. But it survives.[12]

The interesting point here is that what may appear to be ideal conditions to postindustrial humans—safety and security, hyper-efficiency, constant smooth functioning and comfort—reduce resilience. The more just-in-time delivery, the less resilience. From this perspective, a degree of slack, redundance and fat are good. Cars made in the 1960s are highly resilient. Today's cars are wonderful but offer extremely low resilience.

---

[12] Zolli and Healy, op. cit., pp. 13–14.

More operationally, Zolli and Healy identify five ways to promote resilience: ". . . sufficient reserves available to any given system; or diversifying its inputs; or collecting better, real-time data about its operations and performance; or enabling greater autonomy for its constituent parts; or designing firebreaks so that a disturbance in one part does not disrupt the whole. . . ."[13]

They miss out on one crucial element to which they refer later on in their book: allowing smaller sustainable disruptions to take place, which both strengthen the system itself and help reduce the likelihood of big cataclysmic disruptions. A typical example (to which they refer) would be regular but small forest fires as opposed to rare but massively destructive forest fires. Another example would be allowing children to learn from small experiences (hammer on the thumb) rather than shielding them from all harm, leaving them unprepared to deal with the world. In fact the difference lies in accepting flow and realizing that excessive safety and comfort is as damaging as excessive danger and hardship. The balance is crucial.[14]

Finally there are recipes for resilience. The psychologists Southwick and Charney identify ten coping mechanisms that have proved effective for dealing with stress and trauma, which they refer to as "Resilience Factors." All resilient individuals they interviewed:

1. Face reality: Confront their fears
2. Maintain energy: Maintain an optimistic but realistic outlook
3. Are open to support: Seek and accept social support
4. Have guides: Imitate sturdy role models
5. Manage themselves: Accept responsibility for their own emotional well-being

Most also:

6. Have an anchor: Rely on an inner moral compass
7. Find an anchorage: Turn to religious or spiritual practices
8. Are stoic: Find a way to accept that which they could not change

---

[13] Ibid, p. 6.

[14] For a useful take on this see Greg Ip, *Foolproof: Why Safety Can Be Dangerous and How Danger Makes Us Safe* (London: Headline Publishing Group, 2015), p. 326.

9. Are robust: Are active problem-solvers who look for meaning and opportunity in the midst of adversity and even find humor in the darkness.

Many:

10. Generate robustness: Attend to their health and well-being and train intensively to stay physically fit, mentally sharp and emotionally strong.[15]

Zolli and Healy again identify seven core qualities that promote resilience on a more generic level:

> . . . virtually all resilient systems employ tight *feedback mechanisms* to determine when an abrupt change or critical threshold is nearing. . . .
>
> When such sensors suggest a critical threshold is nearing or breached, a truly resilient system is able to ensure continuity by *dynamically reorganizing* both the way in which it serves its purpose and the scale at which it operates. Many resilient systems achieve this with embedded counter mechanisms, which lie dormant until a crisis occurs. . . .
>
> Another way to bolster a system's resilience is to *de-intensify* or *decouple* the system from its underlying material requirements or to diversify the resources that can be used to accomplish a given task. . . .
>
> This . . . is made feasible by certain structural features of resilient systems. While these . . . may appear outwardly complex, they often have a simpler internal *modular structure* with components that plug into one another . . . This modularity allows a system to be reconfigured on the fly when disruption strikes, prevents failures in one part of the system from cascading through the larger whole, and ensures that the system can scale up or scale down when the time is right. . . .
>
> To encourage this modularity, many resilient systems are *diverse at their edges* but *simple at their core*. . . . .
>
> This modularity, simplicity, and interoperability enable the components of many resilient systems to *flock* or *swarm* . . . and to break into islands when under duress. . . .
>
> Yet this . . . is only part of the story. Paradoxically, resilience is often also enhanced by the right kind of *clustering*—bringing resources into close proximity with one another. But it's a special

[15] Southwick and Charney, op. cit., p. 13.

> kind of clustering, one whose hallmarks is density and diversity—of talent, resources, tools, models, and ideas.[16]

Finally they also make the important point that resilience is always uncertain, and must be nourished: "Resilience is always, perhaps maddeningly, provisional, and its insistence towards holism, longer-term thinking, and less-than-peak efficiency represent real political challenges. . . . Resilience must continuously be refreshed and recommitted to. Every effort at resilience buys us not certainty, but another day, another chance."[17]

When: Conditions Under Which Resilience Comes into Play

Zolli and Healy provide a good summary of the conditions in which resilience comes into play:

> . . . sudden and serious disruptions . . . cause you to be flipped over the threshold separating your present context and a new one. . . . Unfortunately, many of these thresholds may be crossed only in one direction. Once forces have compelled you into a new circumstance it may be impossible for you to return to your prior environment. You'll have entered a new normal.
>
> To improve your resilience is to enhance your ability to resist being pushed from your preferred valley, while expanding the range of alternatives that you can embrace if you need to. That is what resilience researchers call *preserving adaptive capacity*—the ability to adapt to changed circumstances while fulfilling one's core purpose—and it's an essential skill in an age of unforeseeable disruption and volatility. . . .
>
> Enhancing the resilience of an ecosystem, an economy, or a community may be achieved in two ways: by improving its ability to resist being pushed past these kinds of critical, sometimes permanently damaging thresholds, and by preserving and expanding the range of niches to which a system can healthily adapt if it is pushed past such thresholds.[18]

One might ask if the first solution actually is resilience. Resisting being pushed into a new valley is not resilience but resistance. However the sec-

---

[16] Zolli and Healy, op. cit., pp. 12–14 (italics in original).

[17] Ibid, p. 276.

[18] Ibid., pp. 7–9.

ond part gets to the core of resilience: preserving the essence while adjusting to a new context. There is a nuanced difference from adapting, in which case the degree of adjustment is far greater. The difference is one of degree, both resilience and adapting involve degrees of submitting to the environment by changing oneself while preserving one's essence, but adaptation as defined here involves a greater degree of self-change. On the other hand one might say that adaptation requires a degree of resilience as the alternative would be to either to resist any significant change, or to snap and break under the forces of change.

Under such conditions of great and sustained pressure the resilient may need to adapt deeply, by changing its trappings and even its vital life systems in order to retain its essence. In this case the first step towards evolutionary change is underway. If successful the system may continue in another form, including a shift of essence. If unsuccessful it will go extinct.

Key Terms

The essence of resilience consists of three core functions: survive, endure and return.

- Survival is the capacity of a system to avoid total collapse when subjected to abnormal and existential pressure or shock.
- Enduring is the ability of a system to maintain its vital core (core function and those vital life systems that sustain it) alive should abnormal conditions prevail and prevent the full functioning of the system.
- Returning is the ability of the dormant system to reanimate itself once conditions permit, either fully or partially.

A partial reanimation always involves adaptation and may include mutation. Both of these are part of evolution. Adaptation implies that the system evolves partially by degrees, mutation involves much deeper change and evolution by transformation. If a system is unable to survive, endure and return from pressure or shock it goes extinct.

The components of the above conceptual scaffold are outlined below.

System: Every living thing, from an amoeba to the global ecosystem, is in fact a dynamic system of systems of interacting energies serving a particular core function. A system thus consists of a core function, the vital

life systems that compose and sustain that core function, and a host of peripheral components and dynamics that serve the system. The more complex a system is, the more vital life systems and peripherals it has. When considering security we must always take into account that that which we are trying to protect is in fact a system. Thus we must also be able to distinguish between the core function and vital life systems that are central to the survival of the system, and the peripherals which may be sacrificed when the system is subjected to existential stress.

Total Collapse: Under ideal conditions we seek total protection. Under extreme conditions we can no longer do so, but must focus on preserving core functions and their vital life systems, while sacrificing whatever is needed to do so.

Abnormal: An event that either is totally unforeseen (a Black Swan which takes a system totally by surprise and for which it is entirely unprepared), or an event that is foreseen but is considered so unlikely that one invests little or nothing to prepare for it specifically, or an event for which one is only partially prepared.

Existential: An event that may lead to systemic collapse. Systemic collapse is when the vital core (see below) of a system is destroyed, leading to total systemic collapse, as opposed to secondary threats, which only challenge the peripheral parts of a system. Systemic collapse is the same as extinction. Peripheral damage can be survived.

Avoiding extinction and retaining the ability for continued adaptation is the highest priority of any system engaged in evolution. The default setting of all natural systems, from plants to the human body to the global ecosystem, is to protect the vital core by sacrificing the peripherals when necessary. Human intent combined with power may interfere with this default setting temporarily (for instance political decisions) but if the pressure is intense enough the core principle always kicks in and wins out. A perfect example is the reaction of the Swedish government and society to the flood of asylum seekers in the fall of 2015.

Pressure or Shock: Pressure and shock differ in degree but both can present existential threats. They are a function of three variables: surprise, speed and severity. If an event comes as a total surprise (unknown unknowns), at great speed, and with great intensity (extreme systemic challenge) then it is a shock. If the severity is high but if there are warning signs (known unknowns), the evolution is gradual.

Vital Core: Essence, consisting of core function and the minimum vital life systems needed to sustain it. Examples are seeds that can survive forest fires. One may thus distinguish between a vital core that is essential for the survival of a system, and its individual and/or peripheral components and attributes, which are generated by the core and which play complementary roles in the full system, but are not essential for the survival of the system as a whole.

The distinction is crucial both for the security analyst and the leadership. Under normal conditions, when all is going well, we tend to take the functioning of our vital life systems for granted and focus on peripheral attributes, such as saving human lives, protecting property, respecting laws and regulations, etc. However in a catastrophe one may have to sacrifice one or more of these in order to safeguard the vital core upon which society as a whole depends for its very survival. This means that in a catastrophe we will have to make sacrifices, and sometimes extremely severe sacrifices for which a political leadership and state institutions used to operating only under normal circumstances will be totally unprepared.

It is also crucial to note that one of the fundamental principles of ecosecurity (the ways in which ecosystems safeguard their security) is that the individual component counts for nothing, the collective vitality counts for all. Thus individual components are constantly sacrificed for the system as a whole to flourish. And to flourish means to evolve, which always involves change. From this perspective the Daoist worldview and perspectives on security are a crucial complement to our Aristotelian worldview, and absolutely essential for any attempt to understand and develop resilience. Colin Gray has hinted at the importance of the Daoist perspective,[19] but the one Western author who has truly examined this in depth is the French philosopher Francois Jullien. His books on this topic are brilliant.[20] He is required reading for anyone interested in strategy in general and in resilience in particular.

---

[19] Colin S. Gray, *Strategy and Defence Planning. Meeting the Challenge of Uncertainty* (Oxford: Oxford University Press, 2014), p. 325.

[20] For a deep, original and important analysis of the essence of strategy, see Francois Jullien, *A Treatise on Efficacy* (translated by Janet Lloyd) (Honolulu: University of Hawaii Press, 2004).

Developing Forward (Networked) Resilience

Forward resilience is crucial in a world dominated by and depending upon global flows. The concept of forward resilience applies mainly to the functional security dimension, i.e., the global networks and nodes upon which our economies and technical infrastructure depend.[21] But in such a world there is actually no forward. With all nodes and flows interlinked, they all become critical to varying degrees. Thus a better term would be Functional Resilience, or Networked Resilience, though I will continue to use Forward Resilience here.

This view of security is important because our societies no longer function as national islands and cannot do so in future. We all depend entirely on complex transnational technical and economic flows. Hence forward resilience, understood as ensuring that nodes and flows beyond national and regional borders can function under pressure, is crucial both for sheer survival and as the optimal remedy against disruptions.

Forward resilience is thus understood here as two things: first, networked resilience across borders, or transnational resilience; and second, resilience in the domain of functional security, or functional resilience.

The functional dimension is one of three security dimensions on which humanity depends. The foundation upon which all else rests is the ecological dimension. When healthy, it offers a livable habitat and natural resources. Resting on this is the functional dimension, consisting of science, technology and economic activity. It provides the practical understanding, tools and products that humanity needs and enjoys. Finally, at the very top, is the social dimension, consisting of human societies and their governance. This is the domain of politics, or the distribution of goods and the quest for influence that goes with it. Their functioning, and their interaction, determine humanity's security.

The functional dimension of security is crucial in its own right. It contains a host of specific threats from within this dimension, such as design (Y2K), management (2008 financial crisis), maintenance (national infrastructure), etc. However today it is also becoming increasingly vulnerable to extra-dimensional factors. These include ecological dimension challenges such as pandemics, storms and so forth, and antagonistic challenges

---

[21] The concept of functional security was first encapsulated by Bengt Sundelius, "Functional Security," in *Functional Security* (Stockholm: Swedish National Defence College—Acta B30, 2004), pp. 17–22.

from the social dimension, emanating from global organized crime, transnational revolutionary movements, and hostile state actors. The last are a particular challenge since they have the resources to deliver truly existential blows against another state's functional survival. We also see continuous signs of preparations to disrupt our functional systems.

We also know from Russian official documents and actions that Russian grand strategy emphasizes waging what we could call functional war against our functional life systems, in order to prepare for, support or even replace military warfare. This is nothing new, it is a clear continuation of the Soviet correlation of forces concept, but it is now being prepared intensively. There are also indications that Russia believes that the West is engaging in a similar sort of warfare against the Russian Federation.

To develop forward resilience two things are necessary. The first is mapping and understanding the challenge. The second is establishing the capabilities needed to strengthen our resilience.

Understanding and Mapping

Our knowledge and understanding of the problem is limited. We must start to understand four areas:

- our transnational functional vital life systems;
- their vulnerabilities and gaps;
- activities and preparations undertaken by others, whether state or non-state actors, to disrupt our systems; and
- how we may develop a networked resilience that can reduce our vulnerabilities.

This is essentially a research task that can be carried out by a policy-oriented central tasking group that could outsource research to clusters of expertise from government, the private sector, academia and civil society. See for instance the the Development, Concepts and Doctrine Centre (DCDC) of the British Ministry of Defense.

Implementing

With a clearer idea of the terrain and requirements, we can begin implementing measures for networked resilience. This task is essentially the same as NATO's military role, but focused on functional security rather

than military defense, and hence at a lower level of political intensity. The operational principles and requirements, however, are the same.

For this we need an agency that can promote transnational functional resilience. Whether this would act under the aegis of NATO, the EU, or another entity entirely is a minefield I will not enter here. Such an agency would need to carry out three core functions:

- ***Act as a forum for political decisions*** needed to implement networked resilience. This is in essence similar to NATO's civil-political role, but less politically charged than defense, though highly relevant for economic and technological interests and the private sector.
- ***Carry out studies of the overall situation and specific challenges***, providing expert support for the political forum on measures to enhance networked resilience. This includes at least three tasks:
  - overview scanning of the state and evolution of the functional landscape (including the functional networks, their vulnerabilities and related Russian activities;
  - suggesting to the political forum how networked resilience may be enhanced;
  - overseeing the civil-military overlap.
- ***Implement or oversee measures agreed upon in the political forum*** to enhance networked resilience. This includes interacting with at least four types of overlapping tasks.
  - First, to engage major actors involved in global and theatre networks and flows (governments and business), in order to enable global resilience, in this case linked to NATO requirements;
  - Second, linking government and private sectors in order to promote public-private partnership for resilience;
  - Third, engaging the recipients of resilience measures, to enable the implementation of such measures;
  - Fourth, engaging donors to enable the provision of resilience measures.

Implementing this sort of agency would be a first step towards protecting our functional security not only nationally but also transnationally. This can only be done multinationally and through public–private partnerships.

Developing this sort of forward resilience is crucial and highly overdue. A major challenge will be to bridge the gap between two contrasting interests: the focus on cost-efficiency, which favors vulnerable hyper-efficiency; and the need for redundancy and slack, which can promote resilience, especially against the unforeseen.

Chapter 2

Toward Greater Resilience in Uncertain Regions

David J. Kaufman and Robert L. Bach[1]

On October 4, 2016, while Hurricane Matthew battered Haiti some 1,000 miles and four days away from a position where it could threaten U.S. coastal communities, Governor Nikki Haley of South Carolina ordered an evacuation. She described her state as being within a "cone of uncertainty" in terms of the potential path of the storm and decided to get ahead of it. "We can always pull back, but you can't get that time back if you wait too long," she reportedly said.[2]

It was a wise, if controversial, decision. Even with thousands evacuated, the hurricane caused at least 22 deaths and left thousands with flooded homes and many more without electricity.[3] The damage would have been greater if she had waited.

Governor Haley's dilemma and the decisions she made are just small examples of the challenges and choices the world community must increasingly face. After decades of warning about emerging trends that could have devastating impacts on human communities, the world is now experiencing those impacts. The risks have become greater and more uncertain, and as events and information move more rapidly, the time available to formulate action and response has become increasingly compressed. Climate change, population growth, urbanization, mobility, technology, and the forces of globalization have created an interconnected set of risks that are exerting increasing pressures on developed and developing nations alike.

---

[1] The views represented in this paper are those of the authors, and do not represent the views of any organization.

[2] Jamie Self, "Did They All Get Out? Gov. Haley Reflects on Hurricane Matthew," *The State*, October 15, 2016. Emergency Management. http://www.emergencymgmt.com/disaster/Did-they-all-get-out-Gov-Haley-reflects-on-Hurricane-Matthew.html.

[3] NOAA National Centers for Environmental Information, "Billion-Dollar Weather and Climate Disasters: Table of Events." See https://www.theguardian.com/environment/2016/oct/11/hurricane-flooding-us-climate-change.

Disaster patterns are changing. For example, in the year 1800 the frequency of super storms the size of hurricanes Katrina and Sandy was nearly one every 400 years. By the year 2100, warming oceans and increased atmospheric moisture will produce one such storm every 90 years.[4] As average temperatures in the western parts of North America have risen by a full degree Celsius over the last 30 years, the area damaged by forest fires has doubled in size and is larger now than the states of Massachusetts and Connecticut combined.

Chronic drought has produced rising death tolls and contributed to increased urban migration and social conflict in Syria, Sudan, and elsewhere as water and resource shortages exacerbate ethnic and national tensions. In 2011 and 2012, more than 12 million people in the Horn of Africa were severely affected by what has been called the worst drought in 60 years. The United Nations projects that by 2025 half of countries worldwide will face water stress or outright shortages, and that by 2050 as many as three out of four people around the globe could be affected by water scarcity.

According to the World Disaster Report 2016,[5] since at least 2004 the forced upheaval and displacement of populations has represented the greatest source of disaster impacts globally. In 2014, for example, 59.5 million people were forcibly displaced in the world. Moreover, displaced persons are staying in host countries longer than in the past, challenging the capacities of the global humanitarian architecture.[6] More than 11 million persons have been forcibly displaced from the war in Syria alone, and estimates of the potential for additional forced migrations range as high as 1 billion persons by 2050.

The Zika and Ebola outbreaks highlight the evolving public health risks that globalization poses. The Ebola outbreak in West Africa, which began in 2014 and led to 11,310 deaths in Liberia, Sierra Leone, and Guinea, spread as far as the United States.[7] The Zika virus quickly connected to other disease vectors and spread throughout the Americas. Destruction of wilderness areas will continue to combine with climate

---

[4] https://www.theguardian.com/environment/2016/oct/11/hurricane-flooding-us-climate-change.

[5] International Federation of the Red Cross and Red Crescent Societies, *World Disasters Report 2016. Resilience: Saving Lives Today, Investing for Tomorrow.* Geneva: Switzerland, www.ifrc.org, 2016.

[6] World Economic Forum, *The Global Risks Report 2016*, Geneva. http://wef.ch/risks2016.

[7] World Health Organization, 2016, as cited in IFRC, 2016, *op. cit.*

change, urbanization, and modern transportation to expand the spread of new diseases, facilitate the movement of known diseases to new areas, and contribute to the re-emergence of previously eradicated diseases.

The global spread of risk and uncertainty also includes vulnerabilities associated with transnational criminal networks, sophisticated human trafficking, terrorism and, increasingly, cyber insecurities. Information flows are revolutionizing change cycles, and social networks are shifting the ways in which people self-organize and mobilize. Increasingly, individuals and small groups of motivated actors are able to have impact, for both good and ill, at scale and speeds not previously possible. This can result in both immediate and long-term damages caused by direct human behavior. The shift we are witnessing in the nature of the transnational terrorism threat toward inspired, independent attacks offers a clear example of how these risks can tear at the social fabric of communities around the world, undermining institutional strengths and exacerbating the frailties of vulnerable people. The extraordinary rise of cybercrime as the world's most lucrative criminal activity offers another example.

These and other global drivers of change are troubling as separate trends, but of greater concern are the ways in which they increasingly overlap, interact, and become interdependent and mutually reinforcing. In combination, they can create unanticipated crises that are so complex that existing strategies and policies are no longer sufficient to afford protection or adapt to cascading consequences. Japan's 3/11 triple disaster devastated that country, killing more than 15,000 and leaving over 200,000 homeless, 4.5 million without power, and 1.5 million without access to public water systems. It also shut down truck production in Louisiana, caused a run on potassium iodide across the west coast of the United States, and affected energy policy in Germany. In Haiti, the damages from Hurricane Matthew added to the struggle to recover from an earthquake six years earlier that killed hundreds of thousands and nearly destroyed the nation's government. Like the earthquake, Matthew struck on the eve of a national election and disrupted hopes of ending pervasive violence and political turmoil. Today, Haiti suffers not only from chronic poverty and devastated infrastructure, but also a widespread cholera epidemic, and its citizens leave in large numbers for the United States, where many resettle permanently.

In 2010 the United States issued a new National Security Strategy that embraced the reality that even "as we do everything within our power to prevent these dangers, we also recognize that we will not be able to deter

or prevent every single threat." The United States set forth the explicit goal of strengthening national resilience, defined as "the ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption." Six years later, bearing witness to the Christchurch earthquake, east African drought, Hurricane Sandy, Japan's 3/11, the Syrian crisis, Ebola outbreak, and many other crises, the need to focus on enhancing the resilience of our communities and of nations is more important than ever.

This chapter calls attention to several priority areas in this quest for future resilience. In particular, it focuses on the uncertainties and risks of the emergent global environment and on the strategic urgency that the compression of time has created. We focus on three overlapping issues. They are (1) the primary significance of resilience in global supply chains; (2) the transformation of regions and communities as the strategic focal points for resilience efforts; and, (3) the urgency of developing new forms of governance to lead resilience efforts.

Our core argument is that future resilience depends on the strength of physical, social, and political connectedness, whether in local communities or on the broader international stage. The complexity of overlapping trends and recurring disruptions of environmental, economic, and human conditions needs to be met with a level of organization—institutional and social—that matches the risks that arise. Economic complexity in the form of vast global supply chains, for instance, calls for strategies of collaboration among diverse participants at each stage in the interlinked production, distribution, and service phases. No one entity can sufficiently control or protect the entire interdependent set of activities.

Local community resilience similarly requires a deeper level of connectedness, focused especially on including more, and more diverse, members. Stronger connectedness can strengthen social cohesion within and across communities, overcome the alarming decline in trust in government, and facilitate operational relationships among government, business, and civic actors that can meaningfully change outcomes in crises.

Acts of willful opposition and antagonism, whether by state actors or non-state actors, can pose direct threats to the security and resilience of communities, nations, and entire regions. The explicit motive of most terrorist attacks is, of course, to undermine faith and confidence of a population in its government—these are first and foremost an attack on social trust. Similarly, the activities of transnational criminal networks and blatant

state-sponsored misinformation campaigns can directly undermine social cohesion within neighboring nations and communities and put vulnerable populations at risk.

Expanding and deepening economic, social and political connectedness is key to anticipating these and other future complexities and to strengthening the social resilience of communities and nations in the face of them. But this effort will require new forms of leadership and governance. Regional governance and cooperation mechanisms will likely be increasingly important. Nongovernmental groups, working across local jurisdictional borders and cultural boundaries, will likely be more effective than entrenched governments, both in mobilizing the actions needed to prepare and recover from emergencies, and in motivating citizens to act before it is too late.

Supply Chains and their Disruptions

In 2008, for the first time in human history, more people lived in urban centers than in rural areas; global urban population is expected to reach 6.2 billion by 2050. Advances in transportation and communications technologies have made this shift toward geographical concentration possible, enabling the massive movements of energy, food, water, waste, and commodities required by dense urban populations– often over long distances. In 1975, there were three megacities (cities with a population over 10 million); today there are thirty-five. The largest, Tokyo and Jakarta, each exceed 30 million residents. Megacities also comprise 42 of the 100 largest economic entities in the world, according to the Chicago Council on Global Affairs, up from 34 just six years ago.[8]

The density and complexity of supply chain networks that have emerged to support this growth defies measure. According to a Chatham House report on the 2010 eruption of Iceland's Eyjafjallajökull volcano, the globalization of supply chains has raised the likelihood of second or third order impacts that are hard or impossible to predict. Business interruption and supply chain risks consistently rank among the top global business risks, according to the Allianz Risk Barometer, and just-in-time delivery models for many key lifeline commodities (e.g., food, pharmaceuticals, medical

[8] Noah Toly, "In the Future, Cities May Finally Solve Problems That Have Stumped the World's Biggest Nations," *Quartz*, October 13, 2016.

supplies) have led to significant concentration in the distribution level of supply chains.

This organizational and geographical concentration represents a strategic capacity that, in many circumstances, dwarfs the capacity of even the largest government organizations. For example, the Washington, D.C. metropolitan area consumes more gross tonnage of dry and frozen food every year than all non-fuel material moved by the U.S. military into Afghanistan and Iraq over thirty months between 2001 and 2004.[9]

Significant attention has been paid to issues concerning the security and integrity of multi-layered supply chains, and progress is being made. The most notable efforts seek to guard against the introduction of illicit and counterfeit materials into the supply chain, whether criminal or terrorist in nature. But comparatively less attention has been paid to how greater resilience can be fostered within these supply chains. For instance, the grocery supply chain in Japan's Tohoku region demonstrated considerable resilience after its March 2011 earthquake. But with a population over 9 million, the region benefits from its proximity to much larger food networks that primarily serviced the greater Tokyo and Osaka areas, with populations exceeding 42 and 22 million respectively. Precious little is understood about how these networks would have withstood a scenario in which the tsunami spawned by the earthquake had hit Tokyo instead of Tohoku.[10]

Supply chains are not bound by international or intra-state boundaries. They often operate in large regional networks surrounding dense urban areas that bear little relationship to governmental structures and jurisdictional boundaries. The density and interdependence of these networks, while facilitating resilience in the face of many risks, also gives rise to the potential for catastrophic degradation or failure of the lifeline supply chains that support these large populations. For government actors, replacing broken supply chains in the aftermath of crisis will be essentially impossible. A new focus is needed to better understand how government can mobilize support to, and work cooperatively with, private owners and operators of lifeline supply chains to redirect and restore capacity in the system in the aftermath of crises.

---

[9] "Considering Catastrophe," Mid-Atlantic Supply Chain Resilience Project, 2014, pp. 31.

[10] "The Role of Groceries in Response to Catastrophes," CNA, 2016.

Regional and Community Resilience

Whether supporting new forms of cooperation around supply chains or creating more localized efforts, resilience strategies will need to tackle a fundamental misalignment of established government jurisdictions and authorities and the shape and scale of complex risks. Hazards, for instance, clearly reach beyond regulatory boundaries and the purview of specific governmental authorities. Reflecting on the damage done from Hurricane Sandy in the United States, the U.S. Secretary of Housing and Urban Development acknowledged that "Natural disasters do not respect State or local boundaries, thus rebuilding plans cannot be bound by jurisdictional lines. . . . A series of uncoordinated hazard mitigation measures may yield unintended consequences and could ultimately decrease resilience in the long-term."[11]

New forms of cooperation will also need to reach deeply into the social structure and composition of local communities, reenergizing connections and even forming new networks that include more diverse members. These social connections may be at least as important as the large physical infrastructural investments that draw most public and private attention. Research on the earthquakes in Kobe, Japan and Christchurch, New Zealand shows that focusing first on social connections in local communities to quickly reestablish social activity, including small businesses, schools, recreation and social life, sparks other forms of recovery and improves longer-term efforts.

Local social connectedness is also essential to anticipating how residents will step forward and mobilize before and in the aftermath of disasters, as both formal volunteers and informal, spontaneous supporters. In New Zealand, some of the volunteers who mobilized the "student army" were driven both by the immediate impact of an earthquake, and from a long-standing desire to contribute to their local communities. In the New York area, another spontaneous group formed out of the Occupy movement to turn the energy of earlier political protests into offers of valuable help to local communities hit hard by Hurricane Sandy.

The Dutch, Australian, and U.S. governments, among others, have sought to incorporate resilience activities directly into the mainstream of

---

[11] U.S. Department of Housing and Urban Development, *Hurricane Sandy Rebuilding Strategy: Strong Communities, A Resilient Region*. Report to the President of the United States, August 2013.

community life. The Dutch social investment strategy, for instance, emphasizes public-private partnerships in building flood preparations and cybersecurity protections within local communities. The U.S. "Whole Community" emergency management doctrine explicitly calls for establishing connectivity among different organizations, sectors, and activities within a region. In the aftermath of Hurricane Sandy, for instance, New Jersey's Local Resilience Partnerships sought cross-jurisdictional collaboration with the New Jersey Recovery Fund as part of the effort of small voluntary associations from adjacent communities to build a bottom-up structure to share resources but also retain local control over land use decisions.[12]

The significance of these efforts is that they form the social infrastructure of resilience that serves as a necessary complement to the more familiar focus on physical infrastructure.[13] While governments and international organization direct their attention to large infrastructure projects, the social conditions associated with physical infrastructure often represent more challenging policy dilemmas. For example, population displacement is considered a high risk to security and stability not only because of the sheer size and pressure on resources, but also because it severely weakens long established social connections upon which communities, families, and groups rely for stability and survival. Population displacement may also raise unexpected risks to global supply chains and other economic activities.

The upheaval of millions of people from Syria is a case in point.[14] As many fled to Turkey to find a source of support and stability, large numbers, including children, found illegal work at various points in the garment industry production and distribution chains. According to various reports, garment production often begins with difficult and abusive conditions involving illegal hand labor. Products made in these circumstances eventually reach top retail stories in London, Berlin, and elsewhere and can threaten brand reputational risk.

The displaced also are vulnerable to human trafficking, which according to recent investigations is deeply embedded in many supply chains. Indus-

---

[12] Ibid.

[13] Robert L. Bach and David J. Kaufman, "A Social Infrastructure for Hometown Security: Advancing the Homeland Security Paradigm," *Homeland Security Affairs*, Vol. V (No. 2), May 2009.

[14] http://www.middleeasteye.net/news/fashion-brands-should-do-more-protect-syrian-refugees-turkey-factories-watchdog-414513207.

try estimates reach billions of dollars that may be linked directly and indirectly from activities connected with traffickers, illegal profiteers, and organized crime syndicates operating in otherwise legitimate supply chains. Until recently, the dominant approaches to combating human trafficking have relied almost exclusively on governments and social service organizations to eliminate these risks. Little has been asked of the private sector, but this is changing. Legislative actions in California and elsewhere are refocusing on corporate behavior and their responsibilities for the safety and security of their employees, including the vulnerabilities of workers displaced by disasters and conflict. Risk from these illegal activities now threatens some of the largest global companies.

Governance

Innovations are clearly needed to find new approaches to working within and across jurisdictional and national boundaries to foster resilience in the face of today's global risks. New mechanisms, for instance, may involve regional, crossborder partnerships that combine authorities from different organizations, including governments, to operate more flexibly against widely distributed risks, including those from antagonistic actors, whether power-based, ideological, or criminal in intent. Regional capabilities could be invaluable to building resilience in the eastern Caribbean-Eastern U.S. coastal areas that now appear at severe risk of recurring super storms, sustained droughts, and new disease vectors. They are already indispensable to combatting the aggressive actions of criminal networks dedicated to exerting force against the legitimate authorities of the states through which their criminal activities pass.

Multilateral frameworks for regional governance represent one likely approach. For centuries nations have grappled with the complex and shifting challenges of conflict and national interests in an effort to manage shared risks and to pursue potential opportunities. Regional approaches to resilience have already taken form in Europe, organized by the European Union and NATO, and in the Caribbean region as a whole. For decades the United States used its regional alliances to counter Cuban opposition and expansionism, and in changing policy course, returned to a hemispheric-wide mechanism, The Summit of the Americas, to gain support. Much can be learned from these experiences, including their shortcomings.

In the United States, federal efforts to encourage state governments to use applications for grant assistance to align programs with the scale and

scope risk profiles still stumble across jurisdictional requirements. Renewed efforts to encourage risk-based planning and collaborative program development are needed to expand capacities and strengthen future responses. Within U.S. cities, new approaches are also needed to reach more deeply into local communities to mobilize diverse groups. Recent research on the collective efficacy of neighborhoods underscores this need. Public safety, for example, is enhanced significantly when community members are able to organize more inclusively, strengthen social cohesion, and assume collective ownership over neighborhood activities.[15]

A critical component of these local and regional innovations is an ability to turn recognition of shared risks into the social trust needed to bond residents and local institutions with governments, and bond governments with one another. Given the historically low levels of social trust in many nations, the governance challenge is clearly to build and maintain sufficient legitimacy with local residents to foster a willingness to work together. Fundamentally, resilience *happens* at the community scale, and the work to strengthen social trust and community capacity that can give rise to greater resilience happens at that scale as well.

Success in building resilience requires a shift in perspective toward consciously designing integrative policies that strengthen community values, vitality, and cohesion under stress through larger discussions of future opportunity, investment, and comprehensive governance. The instruments to achieve this shift already exist—they include strategic investment decisions, master planning, community development, social service delivery, and capital investment and infrastructure engineering, to name only a few areas. Most of these policy issues, of course, are rarely thought of first and foremost as resilience issues, instead they are often framed in the context of economic growth and job creation. Policy leaders will increasingly need to see the connections among, and comparative value in, these issue areas in ways that can reconceptualize how the existing pieces fit together and support one another. Becoming more integrated with wider policy agendas will require integration of natural hazards risk reduction with economic development policies, poverty reduction programs, and climate change initiatives.[16] Aggressive actions against a region also demand collective

---

[15] U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, *Neighborhoods and Crime: Collective Efficacy and Social Cohesion in Miami-Dade County*. NIJ grant 2009-IJ-CX-0039, www.nij.gov.

[16] This discussion is taken from the authors' contributions to Robert Bach, ed., *Strategies for Supporting Community Resilience: Multinational Experiences* (Stockholm: CRISMART 2015).

responses forged through greater cooperation and a recognition of shared responsibilities.

Future Resilience

Although the concept of resilience often generates debates over definitions, it succeeds as a mobilizing idea. It has brought people and organizations together that do not normally interact, especially from diverse sectors, and connected them through a shared sense of interdependency. New players and organizations that have not typically been involved in security, emergency, and disaster policy and planning discussions are now at the table, and new thinking and activities are possible because of it.[17] This mobilization is effective because it enables diverse participants to organize, build strategies, and make plans at the same level of complexity found within natural and man-made risks.

However, in a world of disruptive challenges that have cascading impacts across increasingly interdependent networks, effectiveness also demands leadership skills that reveal an ability and a willingness to embrace complexities and foster adaptive strategies. As the Secretary of the U.S. Interior Department recently noted, "We can see that climate change is already impacting our nation's national parks . . . It's clear that one of the biggest challenges our national parks face in their second century will be adaptive management in the face of a changing climate."[18] This same challenge exists in the face of dealing with willful opposition and antagonistic actors seeking to foment discord and disruption.

New efforts are needed to strengthen adaptive leadership abilities and institutional mechanisms to face the apparent chaos as these complexities unfold. The disruptions occurring simultaneously across the globe, and the growing connectedness between local challenges and distant events, may appear ungovernable. The rise of geographically dispersed nonstate groups with sufficient power and interest to attack innocents and affect nations, large pockets of chronic catastrophes, and the emergence of routine disasters out of supposedly rare events, to name just a few challenges, call for leadership perspectives that are both grand in vision and sensitively

---

[17] Ibid.

[18] Sally Jewell, quoted in https://www.theguardian.com/environment/2016/oct/11/hurricane-flooding-us-climate-change.

focused in local implementation. These new demands on leadership may be the greatest challenge to future resilience.

Much more attention is needed in both the public and private sectors to create greater institutional ability to recognize complex situations, flexibly pivot among different leadership approaches to match the context, and actively engage and support emergent groups and collective action. By and large, governments and aid organizations still rely on centralized, top-down, orders-driven operations. While such approaches work well for many day-to-day functions, they are unlikely to prevail in the chaos of future complex crises. Increasingly, public and private authorities will need to operate in areas where resource deployment must cover noncontiguous territories and the service and logistic delivery systems will involve dispersed uncontrolled activities. Supply chains will not be easily connected or reconnected, resources and responders will not be grouped together, and the groups needed to be involved may not be formed and may even contest the authorities of established organizations.

In this context, effective leaders will need to be self-starters with superlative critical thinking skills and a huge capacity for moral and ethical reasoning and decision-making. Many will operate in the absence of supervision and under intense pressures. Most of all, they will need to have the capability to establish and sustain trust. Recent criticisms of large aid organizations in recovery operations in Haiti and elsewhere demonstrate that even well-established organizations face leadership and trust challenges. The source of such criticism in the future will increasingly result more from the challenges posed by a restructuring of systemic risks, the limits of established authorities and the failure of leaders to adapt to innovative opportunities than by any specific individual or institutional mistake.

Recommendations

Resilience offers a powerful organizing framework for knitting together disparate activities in a manner that can enhance social cohesion, vitality, and regional security. This is as important at the community level to grapple with the challenges of demographic change, population relocation, or disaster recovery as it is at the regional level to counter antagonistic actors seeking criminal gain or to foment discord, or to combat the spread of disease.

Although much needs to be done, several modest first steps would help push forward a discussion of strategies to support future resilience. They revolve around a core proposition: New forms of leadership and governance mechanisms are needed to overcome the limits that established institutions and government agencies face in supporting a future resilience agenda. The following three examples offer thematic illustrations of a new leadership discussion.

A first example calls for a discussion of innovative mutual assistance mechanisms that cross national, state, and organizational boundaries. In the future, the familiar refrain that "disasters know no borders" must be met with effective arrangements to support resource sharing across borders. As discussed earlier, even the most developed nations are not immune to increasing risks and their interdependencies and, despite their considerable capabilities, will need direct assistance from neighbors, allies, and sectors unused to cooperation. In the United States, for example, the projected impacts of a severe earthquake in the New Madrid Zone, or in the Cascadian Subduction Zone, will require operational responses that rapidly exceed available resources—especially for highly specialized capabilities such as urban search and rescue.

Currently, the primary international mechanism to support resource sharing across borders is the United Nations' humanitarian system, which operates as a supply-driven mechanism to channel aid from developed nations to less developed nations struggling with a disaster response. The system contrasts starkly with mutual aid agreements in place within the United States and between individual U.S. states and their cross-border counterparts in Mexico and Canada. In those cases, disaster-affected areas can request the support of specific assets and capabilities (such as search and rescue) without political stigma and the typical jurisdictional barriers associated with legal liabilities and compensation rules. These are worked out in advance as part of a formal mutual aid framework.

Leaders need to come together across various sectors and jurisdictions to work on mutual assistance agreements that establish regional or global standards and shared best practices. Although governments will undoubtedly be part of such regional agreements, they may operate best as partners and supporters of non-governmental lead organizations. Leaders must also reach and mobilize new communities that need to be part of resilience efforts but who have been absent in previous planning activities. Precedent exists for such agreements. For instance, the International Radiological Information Exchange standard established by the International Atomic

Energy Agency might serve as a foundational brick in a new international mutual aid system for disaster response.

A second example calls for leaders to focus on regional planning frameworks that are needed to create shared approaches to resilience planning. As risks emerge in new ways and with greater intensity, existing international mechanisms do not match the scale and scope of resilience planning. The sustained nature of population displacement, for instance, and its connections to climate change and distribution of disease risks, challenge current international policy arrangements. Diaspora communities need opportunities to discuss their interests with a full range of leaders from regional organizations offering their assistance. Corporate leaders also need to plan how best to maintain connections with their workforce and support their well being, both for humanitarian reasons and to prevent risks to production or service stability. New or strengthened regional mechanisms for information-sharing, cooperative planning and capacity-building, and coordinated efforts to tackle transboundary issues such as human trafficking, can be powerful instruments for advancing the ability of nations to confront and persevere in the face of complex risks.

A third example focuses on the heightened pressures on new leaders and their skills. New opportunities are needed to create informal networks and learning exchanges that encourage participants to pursue ideas outside of their routine institutional frameworks. Government leaders need opportunities to speak directly with groups and individuals to pursue perspectives potentially inconsistent with current policies or the constraints of budget concerns. Leaders of aid organizations need opportunities to have informal, protected space to discuss opportunities and difficult choices with community members that may have very different interests and experiences. Private sector leaders need to be able to meet with colleagues who face similar issues but who may operate in different supply chain realities, with different government agencies, and various contexts of systemic risk.

In 2010, a group of governmental and non-governmental representatives from six countries met to begin an informal, unstructured dialogue seeking to understand how central governments can support greater community resilience. During six years of meetings, discussions, and community visits, participants from ten countries organized an informal Multinational Resilience Policy Group to explore a wide range of policy leadership issues related to supporting local resilience. They witnessed recovery in action, discussed local preparedness, and debated how national strategies and policies with dozens of community leaders and local officials

in more than half a dozen countries. Participating countries included Australia, Canada, Germany, Israel, New Zealand, the Netherlands, Singapore, Sweden, the United Kingdom, and the United States. The insights and lessons derived by this group manifested themselves in multiple nations' national resilience strategies and doctrinal frameworks. More such efforts are needed, in areas ranging from countering violent extremism to helping dislocated populations and communities grappling with the pressures of supporting them.

These three examples highlight the implications of a future resilience agenda on leaders. They will be involved much more than before in supporting creative physical investments and the technological advances that have become so valuable to how the world organizes against both manmade and natural risks. But in the end, they must also be deeply involved with people and the institutions and affiliations they form, including regional groupings that involve different traditions, interests, and needs. Effective leadership at this scale hinges on social trust. Building and sustaining such trust requires informal governance and leadership efforts to strengthen social cohesion where it may be possible and to create connections where they do not exist. Only then will future generations have a fighting chance to thrive in a complex and risk-filled world.

Chapter 3

Going beyond Static Understandings: Resilience Must Be Shared, and It Must Be Projected Forward

Daniel S. Hamilton

In this age of accelerating globalization, the true security of our societies, or its citizens, economy and state institutions, is to a very large extent a function of the security of the flows across borders, of the securities of all of those flows of persons, goods, capital, energy, information, whether it be digital or otherwise, that flows across nations, regions and the globe; that is the core of the process of globalization. To secure all of these flows all the way naturally requires a high degree of collaboration; national security is no longer enough.

—Carl Bildt, former Foreign Minister of Sweden, speech at the IISS, London, December 1, 2010

Critical economic, technological, and human flows upon which our societies depend are diffusing and spreading, so that for the first time they now transcend the state on a significant scale, in terms of both volume and power; and global ecological flows for the first time are critically affected by human activity. The scale and complexity of "critical flows," as well as the dependence of many societies on such flows, have increased dramatically. Securing these global flows is emerging as the primary existential interest of all major globalizing actors, be they state or non-state. Transnational actors who direct or influence these flows are emerging as new power brokers—transnational corporations, civil society, organized crime, and transnational revolutionary networks. As long as global flows function and major state actors not only benefit but also depend on them (and realize this dependence), there is a good chance that the focus of security policy could shift from protecting and promoting state sovereignty to protecting and promoting shared critical transnational flows. But we are not yet there. "Territory"-oriented security and "flow" security agendas coexist uneasily.[1]

[1] See Erik Brattberg and Daniel S. Hamilton, eds., *Global Flow Security: A New Security Agenda for the Transatlantic Community in 2030 (*Washington, DC: Center for Transatlantic Relations, 2014), especially the chapter by Tomas Ries, "Global Flow Security: A Conceptual Framework."

Transboundary arteries crisscrossing countries to connect people, data, ideas, money, food, energy, goods, and services are essential sinews of open societies, daily communications, and the global economy. Yet they are also vulnerable to intentional or accidental disruption. Terrorists, energy cartels, illicit traffickers, cyber-hackers, internet trolls, and so-called "little green men" each seek, in their own way, to use the arteries and instruments of free societies to attack or disrupt those societies.

Governments accustomed to protecting their territories must now also focus on protecting their connectedness. New approaches are needed that blend traditional efforts at deterrence and defense with modern approaches to resilience—building the capacity of societies to anticipate, preempt, and resolve disruptive challenges to their critical functions, the networks that sustain them, and the connections those networks bring with other societies. Creating a higher degree of resilience in vulnerable societies makes it more difficult for adversaries to disrupt and create the instability they need for their success.[2]

Ensuring the resilience of one's society is foremost a task for national governments. Resilience begins at home. Yet in an age of potentially catastrophic terrorism, networked threats, and disruptive hybrid attacks, no nation is home alone. Emerging challenges will require even greater shared resilience.[3] Moreover, national resilience and collective defense must be understood as mutually reinforcing elements of the same overall effort to enhance deterrence.

NATO's Role

While resilience requires a broad approach with significant civilian political and economic aspects, it also has major military components. NATO military forces, even in small number, can be effective to back up local border forces or special operations forces to detect and neutralize foreign insurgents. National forces should be primary, in keeping with Article 3 of the Washington Treaty. But NATO allies can assist where requested, for example, for protection of key industrial, commercial, and

---

[2] See Hans Binnendijk, Daniel S. Hamilton and Charles L. Barry, *Alliance Revitalized: NATO for a New Era* (Washington, DC: The Washington NATO Project, 2016).

[3] Franklin D. Kramer, Hans Binnendijk and Daniel S. Hamilton, *NATO's New Strategy: Stability Generation*. (Washington, DC: Atlantic Council of the United States/Center for Transatlantic Relations, October 2015).

transportation nodes (especially those intended for use in reception of reinforcements), counter insurgency operations and para-military police functions, responses to civil emergencies and covert operations, and crisis response management.

NATO and its members already possess noteworthy capabilities in these areas, but their ability to act as a fully organized, capable alliance is not well-developed. NATO will need improved physical assets, strengthened strategic planning and operating capacities. It will need to coordinate closely with national governments, many of which view control of societal security resources as vital manifestations of their sovereignty, and have diverse constitutional approaches to domestic uses of their military and to civil-military cooperation in crisis situations.

Moreover, NATO engagement in this area will require a fundamentally different relationship with the EU, which has undertaken a range of activities and initiatives aimed at improving its military and civilian capabilities and structures to respond to crises spanning both societal defense and societal security, including cross-border cooperation on consequence management after natural and manmade disasters.

In short, resilience is a job for NATO, but it is not a job for NATO alone. In many instances it may require national or EU authorities to play a lead role. The issue for NATO is not just what it should do, but how it fits within an array of necessary Western efforts to bolster transatlantic resilience. In such instances, NATO may play a support role. Hybrid challenges, for instance, may include but are not limited to military elements and must be addressed in more comprehensive ways.[4]

At the July 2016 Warsaw Summit, NATO allies agreed to set resilience standards and each made a pledge to bolster its own national resilience under Article 3 of the North Atlantic Treaty, according to which allies commit to "maintain and develop their individual and collective capacity to resist armed attack." This is an important step. But more will need to be done.

Make resilience an integral element of NATO's core tasks, or consider making resilience a fourth core task. A key element of Russia's strategy is the use of strategic surprise and hybrid threats to take advantage of weak states. Extremist threats from the south also challenge the fabric

[4] Alexandra de Hoop Scheffer, Martin Quencez, and Martin Michelot, "The Five Most Contentious Issues on the Road to Warsaw," GMF Policy Brief, December 2015.

of Western societies. Greater societal and defense resilience can be an important component of an effective response. Creating a higher degree of resilience in vulnerable societies makes it more difficult for state or non-state actors alike to disrupt and create the instability they need for their success. Societies deemed indefensible in traditional defense terms can be rendered indigestible through resilience. Resilience has become integral to each of NATO's current core tasks of collective defense, cooperative security, and crisis management. Initial activities could include the following:

- ***Develop civil-military Resilience Support Teams*,** small operational units that could offer support to NATO member national authorities in such areas of emergency preparedness including assessments; intelligence sharing, support and analysis; border control; assistance to police and military in incident management including containing riots and other domestic disturbances; helping effectuate cross-border arrangements with other NATO members; providing protection for key critical infrastructures including energy; and, in the cyber arena, support and enhancement of NATO's Cyber Response Team.

  NATO is moving forward with such Advisory Support Teams. It should consider that these NATO teams could work in parallel with similar EU groups using the same playbook. In certain countries, Resilience Support Teams could be collocated with NATO Force Integration Units, and help national responses with NATO military activities including especially special operations activities.[5]
- ***Create "National Resilience Working Groups."*** Encourage relevant nations to establish working group-type secretariats to coordinate defense activities with overlapping civil authority and private sector key critical infrastructure functions to enhance national capacity to anticipate, prevent, respond and recover from disruptive scenarios and to provide a key point of contact for outside assistance, including NATO Resilience Support Teams in the east, focused on the development of resilience and response to hybrid threats; in the south, focused on resilience and humanitarian requirements; and throughout the Alliance, focused on cyber and particularly its support to the electric grid and finance. Such a group should also have continuous situational awareness of a state's hybrid risk assessment. Coordina-

[5] Kramer, Binnendijk, and Hamilton, *op. cit*.

tion, integration, and exercises at the national level will make outside support from NATO and other organizations most useful.

- ***Encourage the establishment of regional working groups.*** In addition to national working groups, concerned nations could establish working groups with overlapping issues—one approach would be to look to the nations in the framework arrangements for the east and for the south—with invitations later for others to join as they deem desirable. This would be somewhat similar to such regional mechanisms as Nordic Defense Cooperation (NORDEFCO) or the Southeast European Defense Ministerial.
- ***Include resilience events in NATO exercises, training, education and operational planning.*** Resilience events should be included especially in NATO Crisis Management Exercises (CMX) and cyber exercises such as the annual cyber coalition exercises.

Bolster coordination with the private sector. Effective resilience requires engagement by the private sector, which owns most infrastructures critical to essential societal functions. A good first step would be to develop mechanisms to coordinate with private institutions and entities on key security issues focused on the development of resilience, with cyber as the initial arena.

Enhance counterterrorism cooperation. Counterterrorism within the NATO region remains primarily the responsibility of national intelligence, interior, and police authorities. NATO's counterterrorism activities since 2001 have consisted primarily of safeguarding allied airspace and maritime approaches and intelligence sharing, i.e., guarding the approaches to NATO territory. NATO should consider options for expanding intelligence sharing and its capabilities to support the protection of critical infrastructure, especially infrastructure essential to the performance of NATO core tasks. This should include the development of procedures and plans to ensure the prompt deployment of special operations forces—useful in disrupting some kinds of terrorist attacks—if national authorities ask NATO for this type of assistance. NATO should apply its plans for securing pipelines, offshore oil platforms, and ports to insure energy supplies in wartime to the challenge of anti-terrorist protection of such critical infrastructure.

Develop a more robust strategic communications strategy to address Russia's information operations, particularly where Moscow seeks

to exploit social and political differences in allied states, including those with sizable ethnic Russian or Russian-speaking populations.

The Cyber Dimension

The responsibility to deter, detect, defend against, and defeat a cyber attack rests primarily with nations and their private sectors. But the severe impact a cyber attack can have on a nation's critical information infrastructure, and its use in recent military operations and intimidation campaigns, has implications for Alliance security.

NATO and the defense establishments of its members are under constant attack from cyber hackers seeking to penetrate their information systems, extract data, and plant viruses that could be eventually be used against allies. NATO officials have deemed these attacks to be a tier 1 threat. Attacks are aimed against NATO systems used to develop defense policies and plans, but also more dangerously against operational cyber networks needed to execute military missions.

NATO has taken the threat of cyber attacks very seriously. It has created a high level Cyber Defense Committee that reports directly to the NAC, a working level NATO Cyber Defense Management Board, a NATO Computer Incident Response Capability (NCIRC), a Cyber Defense Center of Excellence in Tallinn, and more recently a NATO Industry Cyber Partnership. The Wales Summit endorsed an Enhanced Cyber Defense Policy which further strengthened NATO's efforts in this area. Yet more must be done.

Recognize cyber as an operational domain and launch a voluntary NATO Cyber Operations Coordination Center (NCOCC). The NCOCC would report to Allied Command Operations and would be funded and manned by participating members. Ideally the United States should take the lead. Participating members should be those countries with cyber operations forces. The primary purposes of the NCOCC would be to share information among the cyber operational forces of members, conduct training and education in conjunction with the Cooperative Cyber Defense Center of Excellence (CCD COE), help Allied Command Operations and Allied Command Transformation plan cyber exercise events, and ensure deployable cyber elements are forces listed with the Enhanced NRF and VJTF.

In due course, if the NCOCC proves a success, it should transition into a permanent NATO Cyber Operations Headquarters similar to the NATO SOF HQ. Such a headquarters should generate the necessary arrangements and readiness to allow nations to pool their capabilities and produce cyber effects should there be a collective decision to do so. It should also act to achieve consensus on issues of cyber deterrence, particularly whether individual Alliance cyber defense capabilities alone are adequate, or whether capabilities are needed to effectively deter major strikes against NATO networks, the networks of individual nations, or against the critical infrastructures of Allied nations—especially the infrastructure identified as essential to NATO's core tasks. While NATO's ability to acquire capabilities to respond to such attacks is not a practical near-term consideration, individual Allies are already taking on this mission and could do the same for the Alliance in certain scenarios.

- ***Establish the means to allow SACEUR to plan for, integrate and employ the contributions of members' cyber forces for defensive, offensive and exploitative cyber operations.*** While NATO is unlikely to agree to establishing offensive cyber capabilities for the Alliance itself, individual Allies do possess these capabilities and those capabilities may need to be coordinated in time of crisis or conflict.
- ***Consider Mutual Cyber Standards Pledges.*** National networks that connect to the NATO network can be weak, creating potential vulnerabilities for the entire system. The Alliance might address this problem via a "mutual cyber pledge," grounded in an Alliance-wide certification system, in which an individual Ally pledges to meet agreed cyber defense standards and NATO itself pledges assistance to those lacking capability to meet those standards, which is then followed with a concrete work plan to achieve certification. NATO at Warsaw took some important steps in this direction.
- ***Enhance NATO's Computer Incident Response Capability (NCIRC)*** by rationalizing and normalizing common funding, strengthening its Rapid Response Teams in order to better assist members under attack who ask for help, and generating greater protection and resilience planning for critical mobile networks, including capabilities development of national cyber cells earmarked for NRF and VJTF.
- ***Task ACT to develop a Cyber Operations Transformation Initiative*** to explore opportunities for multinational training, networking, information sharing and interoperability among the growing number of NATO members fielding operational commands. The model for

this initiative should be the successful special operations transformation initiative of the Riga summit.

- ***Increase support to NATO's Cooperative Cyber Defense Center of Excellence*** in Estonia, which should lead NATO to draft a clear policy on responding to cyber attacks.

Boost NATO-EU and US-EU Cooperation to Enhance Resilience

EU-NATO Cooperation

The NATO partnership with the greatest institutional potential is with the European Union. Given the broad nature of the security challenges we face, and that military means alone will often be insufficient or irrelevant to address them, there is a compelling need for improved cooperation between NATO and the EU. Synchronizing the EU's extensive civilian and small-operations military expertise with NATO's high-end military capacity and transatlantic reach would dramatically improve the tools at the disposal of the transatlantic community.

Without parallel changes in course, NATO and the EU will continue to evolve separately, generating considerable waste of scarce resources, political disharmony, growing areas of overlap, and increased potential for confusion and rivalry.

A new transatlantic security architecture is called for that strengthens both institutions, allowing them to be effective partners. Little progress is likely, however, unless nations can resolve the Cyprus dispute. Differences among Greece, Turkey, and Cyprus have blocked the strategic common good for too long; it impedes a more viable NATO-EU relationship. Overcoming this roadblock to a truly strategic partnership should be the highest priority.

As such efforts proceed, the resilience challenge may offer a way to forge more effective NATO-EU cooperation within existing political constraints. Various initiatives are worth considering:

Important steps have already been taken. In July 2016, both organizations pledged in a Joint Declaration to cooperate to "counter hybrid threats, including by bolstering resilience." Various areas have been identified for enhanced coordination and cooperation, including situational awareness, information sharing, strategic communications, cybersecurity/cyberdefense, crisis prevention and response, and civil-military planning.

A playbook for NATO-EU cooperation, dealing with a range of hybrid-warfare scenarios, has been developed for the areas of cyber defense, strategic communications, situational awareness, and crisis management.

These are all good initiatives. Still, more can be done. In addition, both NATO and EU leaders have acknowledged that they have not yet addressed in any systematic manner how both institutions could help partners become more resilient. Consideration should be given to the following steps.

Develop mechanisms for institutional cooperation, including a NATO-EU Resilience Coordinating Council. Ideally, such a Council would have an inward-looking and an outward-looking dimension.

- **Looking inward**, the NATO International Staff and the EU External Action Service and relevant DGs staff should develop an inter-service mechanism to engage together on a regular basis on exchange of good practice, lessons learned exercises, means to identify and address critical vulnerabilities, shared "sense-making," situational and threat assessments, and early warning and early action procedures.
- **Looking outward**, the Council should engage both private sector actors and non-member governments who are critically involved in global and theatre networks and flows to promote networked resilience. Specifically, the Council would
  - promote public-private partnerships to facilitate wider resilience linked to NATO/EU baseline requirements;
  - engage recipients of resilience measures to ensure effective forward resilience; and
  - engage additional donors to enable the provision of resilience measures.

Pool EU and NATO resources for Forward Resilience Advisory Support Teams that could work to address the highest priority needs in countries where both the EU and NATO are each engaged in projecting resilience beyond their borders, for example in Ukraine and in the western Balkans.

Hold joint crisis management exercises with a focus on forward resilience. The EU and NATO have been conducting such exercises over the past few years; it would be useful to incorporate hybrid or disruptive threats, also with partners, into such exercises.

US-EU Cooperation

Reinforce NATO's pledge with a U.S.-EU Solidarity Pledge, a joint political declaration that each partner shall act in a spirit of solidarity—refusing to remain passive—if either is the object of a terrorist attack or the victim of a natural or man-made disaster, and shall work to prevent terrorist threats to either partner; protect democratic institutions and civilian populations from terrorist attack; and assist the other, in its territory, at the request of its political authorities, in the event of a terrorist attack, natural or man-made disaster.[6] A similar pledge already exists as a part of the EU's Lisbon Treaty,[7] but it is now time to widen the scope to include both sides of the Atlantic.

A Transatlantic Solidarity Pledge would create key preconditions for advancing overall resilience: political impetus, bureaucratic guidance, and operational mechanisms towards that goal. Implementation of a Transatlantic Solidarity Pledge would require U.S. and European actors to work together on a common threat assessment (such as the one required by the EU's Solidarity Clause) and would require EU and U.S. officials to acknowledge, evaluate, and prioritize threats to the shared arteries spanning the Atlantic. Threat assessment could be used as a guide for on-going capacity building in the form of advanced planning and prevention in line with a resilience approach. Yet the Pledge would also require both partners to work through operational response requirements in the event of a major transatlantic breakdown. Issues around Host Nation Support capacities would need to be addressed promptly to transform such a political pledge into an operational reality when it is needed.

Agreement on a Transatlantic Security Pledge would boost political impetus across the spectrum and recalibrate security cooperation towards a clear purpose: building resilience into transatlantic infrastructures. A

---

[6] This would be a political statement and intended to enhance, not replace, Article 5 of the North Atlantic Treaty, by complementing NATO efforts with U.S.-EU solidarity. For details see Daniel S. Hamilton and Mark Rhinard, "All for One, One for All: Towards a Transatlantic Security Pledge," in *The EU-US Security and Justice Agenda in Action*, Chaillot Paper No. 127, December 2011. Paris: European Union Institute for Security Studies. Available at: www.euiss.eu.

[7] The treaty's Solidarity Clause (Art. 222) obliges EU member states to mutual support in the face of a range of new threats; to jointly assess new threats; to coordinate closely in the event of an attack or disaster; and to provide mutual assistance to a stricken state. See Sara Myrdal and Mark Rhinard, "Empty Letter or Effective Tool? Implementing the EU's Solidarity Clause," *UI Occasional Paper*, No. 2 (Stockholm: Swedish Institute of International Affairs, 2010).

high-profile pledge of this nature would help rebuild a sense of common cause across the Atlantic and set priorities to prevent or prepare for any future crisis. This impetus could carry over into diplomatic initiatives in the alphabet soup of transatlantic cooperation frameworks directed at improving coherence through strategic direction.

At the bureaucratic level, a Transatlantic Solidarity Pledge could set the framework for improved technical cooperation among European and U.S. agencies and departments. This level of cooperation, which currently takes place but needs new bearings, should focus on the key transatlantic infrastructures most susceptible to attack and/or disruption.[8] Focus must be placed on the ways these arteries can be made not just more robust—but also more resilient—in the face of disruptions. A focus on these arteries—including how to enhance resilience and manage complicated cross-over disruptions—could guide work related to implementing a Transatlantic Solidarity Pledge.

Toward that end, a renewed focus on coordination could be placed on relations between EU and U.S. operation centers—with the task of providing early warning, situational awareness and crisis coordination support. Such centers could include the DHS National Operations Center (NOC), FEMA's National Response Coordination Center (NRCC), the EU's European Response Coordination Centre (ERCC), and the EU Situation Room in Brussels. These objectives would require regular exercises between EU and U.S. officials to familiarize themselves with procedures and protocols for working together. Other needs include joint investigation teams, including Europol and Eurojust, to cooperate on cases that cross international borders; enhanced cooperation between the U.S. Coast Guard and related agencies with Frontex, the EU border protection agency; collaboration on resilience-related research for instance between the program of Horizon 2020 for European Security Research and similar U.S. efforts; and development of a EU-U.S. Critical Vulnerabilities Security Action

---

[8] See, for instance, Anja Dalgaard-Nielsen and Daniel S. Hamilton, eds., *Transatlantic Homeland Security: Protecting Society in the Age of Catastrophic Terrorism*, London: Routledge, 2005; Antonio Missiroli, ed., "Disasters, Diseases, Disruptions: A New D-Drive for the EU," *Chaillot Paper* No. 83 (Paris: EU Institute for Security Studies, 2005); Robert Whalley, "Improving International Co-ordination and Co-Operation on Homeland Security/Societal Security and Resilience Issues," unpublished paper prepared for Center for Transatlantic Relations/PACER, January 2009; and Jonathan M. Winer, "An Initial International Cooperation Agenda on High Consequence Events for the Obama Administration," unpublished paper prepared for Center for Transatlantic Relations/PACER, January 2009.

Plan to generate mutually supporting strategies to address their own critical foreign vulnerabilities.

One example where U.S.-EU efforts could pioneer shared resilience is with regard to global movement systems, which are integrally linked in today's highly networked and interconnected global economy. The drive to improve efficiency has made these global movement systems more vulnerable not only to attack by terrorists, but to cybercrime and even natural disasters and extreme weather. A EU-U.S. public-private **Global Movement Management Initiative (GMMI)** could offer an innovative governance framework to align security and resilience with commercial imperatives in global movement systems, including shipping, air transport, and even the internet.[9] And if the EU and the United States could achieve agreement, the norms and standards that would emerge could provide a framework for global arrangements.

A EU-U.S. Transatlantic Resilience Council—operating at a similar level as the Transatlantic Energy Council—could be formed to operationalize this initiative, integrating the discussion on societal security, justice and freedom across all sectors and serving as a cross-sector forum for strategic deliberations about threats, vulnerabilities, and response and recovery capacities that cut across sectors and borders. This group would complement existing professional work within established but stove-piped fora. Although new institutions are not the first imperative for building resilience, some degree of structured oversight between both partners is needed to provide strategic perspective on where EU-U.S. cooperation is working and where more attention is needed.

In sum, a Transatlantic Solidarity Pledge, coupled to a concerted package of focused initiatives, would generate the necessary political attention, administrative direction, and operational mechanisms to bind the transatlantic relationship tighter in a time of increasing threat complexity and global flux. It would reaffirm the continued vibrancy of the transatlantic partnership, yet tune it to new times and new challenges.

---

[9] This idea is drawn from a report by IBM Global Business Services, "Global Movement Management: Commerce, Security, and Resilience in Today's Networked World," and a 2005 paper entitled "Global Movement Management: Security the Global Economy," available through www.ibm.com/gbs/government. See also Stephen E. Flynn and Daniel B. Prieto, *Neglected Defense: Mobilizing the Private Sector to Support Homeland Security* (New York: Council on Foreign Relations, 2006).

Project Resilience Forward

NATO members share a keen interest in the societal resilience of other countries beyond the EU and NATO, particularly in wider Europe, since strong efforts in one country may mean little if neighboring countries, with which they share considerable interdependencies, are weak. Russia's hybrid efforts to subvert Ukrainian authority are but the latest examples of this growing security challenge. Allies should be proactive about sharing societal resilience strategies, not only with allies but with selected partners.

Through a strategy of ***"forward resilience,"*** NATO allies and EU member states would identify—very publicly—their resiliency with that of others beyond the EU and NATO, and share societal resilience approaches and operational procedures with partners to improve societal resilience to corruption, psychological, and information warfare, and intentional or natural disruptions to cyber, financial, and energy networks and other critical infrastructures, with a strong focus on prevention but also response. Forward resilience would also enhance joint capacity to defend against threats to interconnected domestic economies and societies and resist Russian efforts to exploit weaknesses of these societies to disrupt and keep them under its influence.

The EU and its member states, and NATO and its allies, should facilitate joint or complementary efforts to project "forward resilience" to EU Eastern Partnership or NATO Partnership countries in areas such as security sector reform, police and gendarmerie training, public health-biosecurity measures, civilian control of the military, or economic reconstruction. In this regard, the EU and its member states, and NATO and its allies, should consider deploying coordinated Forward Resilience Support Teams, at the invitation of EU Eastern Partnership or NATO Partnership countries, to support building resilient capacity in areas ranging from critical infrastructure protection and strategic communications, to disaster prevention, management, and relief, to civil-military cooperation.

Chapter 4

Forward Resilience and Enhanced Cooperation: Bringing Theory to Practice

Mark Rhinard and Bengt Sundelius

The notion of resilience is gaining currency in Euro-Atlantic security policy discussions. The concept suggests the importance of enhancing societies' abilities to resist and withstand severe shocks to the essential arteries that provide societal security. Inside NATO, considerable work has begun on baseline requirements in several areas of importance to fulfill the ambitions of Article 3 of the North Atlantic Treaty, mandating that allies, "by means of continuous and effective self-help and mutual aid, . . . maintain and develop their individual and collective capacity to resist armed attack." A growing chorus of scholars and analysts believe that a resilience focus can help improve compliance with Article 3, with some arguing that resilience must be added as a fourth pillar of NATO strategy, alongside deterrence, crisis management, and cooperative security.[1] Resilience not only builds "bounce back" capacity in allies and partners, it may also have a deterrent effect: strengthened resilience raises thresholds for the effects of attacks and intrusions by antagonists and may contribute to deterrence. The concept was introduced in the July 2016 Warsaw Summit declaration, setting the future direction for strategic priorities.

But is resilience enough? Resilience can be conceived too narrowly, as something done at home without consideration of allies, partners, and neighbors' deeply interconnected capacities for resilience building. The recently introduced notion of "forward resilience" may provide more operational traction.[2] The "forward" element suggests anticipating shocks by building geographical buffer zones in nations that are already closely interlinked with NATO nations through various cross-border flows. The so-called near abroad extends quite far when societies are highly dependent on developments in other jurisdictions. By assisting these neighbors, nations

---

1 Frank D. Kramer, Hans Binnendijk, and Daniel S. Hamilton, *NATO's New Strategy: Stability Generation* (Washington, D.C: Center for Transatlantic Relations/Atlantic Council, 2015).

2 Hans Binnendijk, Daniel S. Hamilton, and Charles Barry, *Alliance Revitalized: NATO For A New Era - Report of the Washington NATO Project* (Washington, D.C: Center for Transatlantic Relations on behalf of the Washington NATO Project, 2016).

also strengthen their own resilience in the face of asymmetric threats such as terrorism or global epidemics like Ebola. The forward dimension also helps planners by focusing on early alert. Forward-looking analyses of potential threats and risks, as well as the capacity to recognize and act upon early indicators of unwanted developments, help to strengthen resilience. Finally, the forward element helps to think about design issues on how to engineer effective bounce back capacities well in advance so as to deter attacks on our societies' weak links.

This chapter addresses a critical precondition for forward resilience as a *shared endeavor*: the capacity to cooperate across boundaries. Seemingly elementary, the capacity to cooperate lies at the heart of all attempts to work out solutions together across sovereign boundaries. Even among allies and partners, effective cooperation can seem in short supply. The Hurricane Katrina international assistance failure,[3] NATO intransigence in Ukraine,[4] and eurozone crisis management[5] offer just a few examples. The capacity to cooperate can be defined as the ability to align interests, adopt shared perspectives, and deploy resources swiftly and with a minimum of transaction costs. These factors are the baseline requirement for building resilience in advance of asymmetrical threats, but also in the face of realized threats: actual attacks, failures, or disasters in the Euro-Atlantic community.

To make this case, we return to the essential scholarly literature on cooperation to extract lessons for enhancing the capacity to cooperate, accepting shared resilience and moving towards building forward resilience. First we examine how cooperation contributes to resilience before turning to factors that enhance one's capacity to cooperate. We then inventory the current state of play in terms of the Euro-Atlantic community's fulfillment of these requirements. We conclude by outlining several key steps necessary to improve the overarching capacity to cooperate.

Cooperation and Resilience

Cooperation seems to be an inherent good, and few observers question its benefits. But what are its benefits in relation to *resilience*? We define

---

[3] Mark Rhinard and Bengt Sundelius, "The Limits of Self-Reliance: International Cooperation as a Source of Resilience," in L. Comfort, A. Boin, & C. Demchak (eds.), *Designing Resilience for Extreme Events* (Pittsburgh: Pittsburgh University Press, 2010).

[4] John Mearsheimer, "Why the Ukraine Crisis Is the West's Fault," *Foreign Affairs*, September/October 2014.

[5] Martin Feldstein, "The Failure of the Euro," *Foreign Affairs*, January/February 2012.

resilience as a capacity of a social system (in this case, a nation-state) to proactively adapt to and recover from disturbances that are perceived within the system to fall outside the range of normal and expected disturbances.[6] *Forward resilience* suggests a collective ability to not just bounce back from a major crisis, but the capacity to react and adapt before a disturbance turns into a crisis. Anticipatory actions in the face of various potential contingencies are part of the forward resilience approach. A high capacity to cooperate can help achieve forward resilience in three ways:

- ***Fewer coordination costs***. Countries with a high capacity to cooperate have lower transaction costs when engaging with others. They are what the literature calls "meta-level" facilitators, because they smooth interactive processes.[7] There is less friction at key points in the incident management timeline: from collectively identifying an emerging threat to taking preventative steps, and from moving resources (see below) to communicating with the public. Much of this involves the presence of simple but formal protocols, which in turn generate informal modalities that smooth coordination. In general, a high degree of cooperation capacity translates into fewer transaction costs that impede both shared sense-making and collective action-taking.
- ***Quicker distribution of assistance***. On the operational side, resiliency requires swift distribution of assistance, material or otherwise, to resolve a potential disturbance before it happens, or to regroup after it strikes. That system may not have the capacities required to recognize an emerging problem, and if a disturbance emerges, it may not have all the resources required to bounce back quickly. Cooperation can potentially improve the movement and distribution of resources to where they are needed, when they are needed.[8] The dis-

---

[6] Comfort, Boin and Demchak, op. cit., p. 9.

[7] P. Milgrom and J. Roberts, "Bargaining Costs, Influence Costs, and the Organization of Economic Activity," in James E. Alt and Kenneth Shepsle, eds., *Perspectives on Positive Political Economy* (Cambridge: Cambridge University Press, 2011).

[8] One way to think about resource distribution is in terms of logistical supply chains. During major crises, the ability to find, move, and distribute critical supplies is placed at a premium. Supply chains, however, are often among the first set of casualties when a disturbance emerges. Indeed, their breakdown can become part of a "cascading crisis" as initial suffering cannot be abated. See U. Rosenthal, R. A. Boin and L.K. Comfort, "The Changing World of Crisis and Crisis Management," in U. Rosenthal, R. A. Boin, and L. K. Comfort, eds, *Managing Crises: Threats, Dilemmas and Opportunities* (Springfield: Charles C. Thomas, 2001), pp. 5–27.

tribution of material supplies is not the only type of activity that effective cooperation can facilitate. Also important is the distribution of intellectual assistance, meaning information and intelligence that can help a social system make sense of an impending development.[9]

- ***Building of social capital.*** On the social side, a powerful effect of cooperation capacity on resilience is generalized reciprocity and social capital creation generated through repeated interactions. Whether we speak of the cybernetic effects of cross-border transactions (Deutsch's "security communities" theory) or Putnam's arguments that cooperation begets cooperation, we know that cooperation facilitates shared expectations, trust-building, and common norm-creation over time.[10] From an academic perspective, the building of social capital reduces defections in cooperation over time. From a practical perspective, forward resilience is enhanced when a general "we" feeling drives actions to enhance preparedness and to reduce risk in sync with the larger community. In the classic choice among exit, voice, or loyalty, cooperation breeds sentiments toward loyalty.

How to Cooperate: Enhancing the Capacity to Cooperate

Research shows effective cooperation is predicated on three elements: shared interests, shared institutions, and shared ideas.

Shared Interests

The simplest propositions found in the international relations literature is that cooperation takes place only when all partners perceive they can achieve gains. The assumption holds that states are the main actors in international affairs, they act on the basis of national interests to maximize their own utility, and the international system is characterized by anarchy. In essence, states jealously guard their own position and cooperate only when they perceive that benefits outweigh costs. The Prisoners' Dilemma shows that cooperation is desirable, but there are myriad disincentives to working together.

---

[9] Rhinard and Sundelius, *op. cit.*

[10] See Jordan Boslego, "Engineering Social Trust: What Can Communities and Institutions Do?" *Harvard International Review*, Spring 2005.

Several implications follow. First, actors are predisposed to cooperation when benefits are clear and calculable.[11] Without clear material incentives, it will be difficult to justify to political superiors or domestic publics why actors should cooperate with their foreign counterparts. An organization that acts strategically to increase its net benefit is thus more likely to display a high capacity to cooperate, however counterintuitive this may appear. Moreover, actors are more likely to cooperate effectively when they see a balanced distribution of gains, e.g., that others will not benefit dramatically more than they will.

Second, actors are more likely to cooperate if they see cooperation as a long-term endeavor. Game theory reminds us that single interaction games, in which players cooperate only once, do not usually result in cooperative outcomes; instead, defection or free riding takes place. By contrast, when those players know that cooperation will be iterative, i.e., ongoing, partners typically cooperate with positive outcomes for all involved.[12] Players can be punished for defecting and rewarded for cooperating over time. Providing assurances that cooperation will continue in the shadow of the future is a key prerequisite to cooperation in the short term.

These rational calculations, while useful to keep in mind in principle, are nonetheless subjectively constructed in reality. Elites frame what is in the national interest and cost-benefit calculations are usually highly politicized. In this regard, several factors stand out in helping to forge the perception of shared interests:

- ***Shared threat perceptions***. Few factors matter more in forging a shared interest than the perception of a common enemy "out there." International security studies are clear on this point, and while some scholars critique the idea of threat construction, it clearly matters in real life.[13] This places emphasis on (a) leveraging political attention following security breaches (terrorist attacks, cyber breakdowns) to focus on a coherent response and future planning, and (b) advancing analysis via universities and think tanks to identify relevant threats, and to understand how they affect a community of nations.

---

[11] R. Axelrod, *The Evolution of Cooperation* (New York: Basic Books, 1984); K.A. Oye, "Explaining Cooperation Under Anarchy: Hypotheses and Strategies," *World Politics* 38(1):1–24, 1985.

[12] Oye, Ibid.

[13] B. Buzan and L. Hansen, *The Evolution of International Security Studies* (Cambridge: Cambridge University Press, 2009).

- ***Clear cost-benefit analysis***. Nations must see, and be persuaded by, clear arguments regarding the importance of common action towards asymmetric threats. Despite the political bias that accompanies such analyses, efforts should be made to provide dispassionate data and hard facts regarding the extent to which nations win by investing in advance planning and capability building.[14]
- ***Leading from the front.*** Elite-level diplomatic declarations set a conducive framework for cooperation.[15] Political declarations (communiqués) can be criticized as symbolic texts promising greater cooperation with little substance attached. Yet they signal to lower level officials that *some* degree of appreciation at high levels of the prospect of cooperation. The same statements suggest that cooperation will be a long-term effort and thus serve to encourage repeated cooperation games. Declarations raise the material incentives to work together—and thus build a more general capacity to cooperate amongst agencies and organization.

The Current Status of Shared Interests in the Euro-Atlantic Community

The end of bipolarity clearly helped to fragment interests within NATO. As has been well-documented, there are doubts regarding how allies interpret their own interests in relation to the Alliance. Namely, there are very different common understandings of the meanings of Articles 3 and 5 in the North Atlantic Treaty. Article 5, for instance, is an essential interest to smaller European allies. The U.S. government, however, seems to be shifting attention away from Article 5 (solidarity in the event of an armed attack) towards Article 3 (self-help) as it relates to burden-sharing and capacity-building in each member of the alliance. Recent events suggest the rise of new threats, including terrorism on European soil, an antagonistic Russia, and mass migration, which may have a cohering effect on interests (and which may serve to counter-balance the U.S. pivot to Asia). Yet here too a single, transcendental threat remains absent. Different allies prioritize different threats, and this can generate tension. However, of equal importance are divisions among European allies—not only about threat prioritization but also about committing limited defense resources.

---

[14] For an example, see R. Bossong and M. Rhinard, "European Internal Security as a Public Good," *European Security*, 2012, pp. 1–19.

[15] K.J. Holsti and T. A. Levy, "Bilateral Institutions and Transgovernmental Relations Between Canada and the United States," *International Organization*, *28*, Autumn 1974, pp. 875–901; M.A. Pollack, *The Engines of European Integration: Delegation, Agency, and Agenda Setting in the EU* (Oxford: Oxford University Press, 2003).

As attention to Article 3 grows in Euro-Atlantic policy circles, can it sustain focus and staying power? Much depends on how the Article is defined, interpreted and, as we argue below, embedded as a shared idea. Article 3 is most relevant to considerations of national resilience as a means toward preparing for aggression as well as the basis for building deterrence against attacks.

Shared Institutions

Cooperation involves actors pursuing their own interests through collaborative means. But cooperation takes place within some form of institutions: sets of rules, procedures, and principles that structure behavior and shape interests.[16] Those institutions leave their own imprint on cooperation efforts and can facilitate or impair the capacity of actors to work together. The literature reminds us that institutions matter in four main ways.

First, institutions can be designed in ways that facilitate cooperation through the functions they perform. For realists, institutions mitigate the effects of international anarchy and make cooperation possible: they can ensure information about the motivations of other and thus build confidence in agreements and lesson the likelihood of defection. Institutions, described as international regimes in this approach,[17] reduce transaction costs that may prevent actors, organizations, and states from cooperating in the first instance. Liberals, of course, see institutions more expansively by serving as neutral third parties (i.e., secretariats) which provide policy-relevant information (such as implementation considerations) that may not be available to the various partners and which help with agenda momentum.

Second, institutions create expectations. Even when actors' interests diverge, regularized interaction leads to a sense of collegiality amongst participants. Collegiality is not just a feel-good trait; it may "permit the development of flexible bargaining behavior in which concessions need not be requited issue by issue during each period."[18] This trait can be particularly helpful during times in which organizations have to respond quickly (and to overcome cooperation obstacles from their own central governments) to work with international partners. Familiar patterns of

---

[16] S. J. Bulmer, "New Institutionalism and the Governance of the Single European Market," *Journal of European Public Policy*, 5(3):365–386, 1998; D.C. North, *Institutions, Institutional Change and Economic Performance* (Cambridge: Cambridge University Press, 1990).

[17] R. O. Keohane, "The Demand for International Regimes," *International Organization*, 36(2):325–355, 1982.

[18] Robert O. Keohane and Joseph S. Nye, "Transgovernmental Relations and International Institutions," *World Politics*, 27(1):46, October 1974.

interaction, communication, and bargaining represent the types of institutions that should facilitate cooperation under duress.

Third, institutions nurture elite networks and advocacy coalitions, thus facilitating more than generic cooperation. "One of the important but seldom-noted roles of international organizations in world politics is to provide the arena for sub-units of government to turn potential or tacit coalitions into explicit coalitions characterized by direct communication amongst partners."[19]

Finally, institutions enforce decisions. High-level political agreements offer broad frameworks for working together (see above), those declarations must be put into operation. International organizations provide the framework for working together, and contain both informal (naming and shaming) and formal (compliance proceedings) mechanisms for enhancing follow-through.[20] Whether technical incompatibilities between national systems—cyber security, for instance—can be ironed out has an important bearing on whether cooperation takes place under times of stress.

Several specific dimensions of institutional design must be considered if we are to enhance cooperation capacity:

- ***Institutions must be thick.*** There is no institutional shortcut to cooperation. Effective cooperation requires intense, ongoing and rule-bound interaction over long periods of time if interests are to converge and transaction costs (in a crisis) are to be lowered.
- ***Institutions must be fit for purpose.*** A slightly paradoxical element follows from the last: while institutions must be rule-rich, in order to shape interests and interaction effectively, they must be capable of delivering. Many of today's international cooperation platforms are not designed to handle certain kinds of crises, and the preparatory steps they require. The ability to draw in critical information and intelligence, to horizon-scan effectively, to respond in improvised ways when necessary, and to remain legitimate in the eyes of elites and the public is difficult—but necessary.[21]

---

[19] Ibid, p. 51; see also Holsti and Levy, *op. cit.*; P. Haas, "Introduction: Epistemic Communities and International Policy Coordination," *International Organization*, 46(1):1–35, 1992.

[20] J. Tallberg, "Paths to Compliance: Enforcement, Management, and the European Union," *International Organization*, 56(3):609, 2001.

[21] M. Rhinard, "The Legitimacy of Transboundary Crisis Management in the European Union". Conference paper presented to the ECPR SGEU Conference, Trento, Italy, June 2015.

- ***Institutions must facilitate practical implementation***. Nations are famously reluctant to delegate power to outsiders to enforce compliance; only in the EU has this been done with legal, binding effect—and only with some sovereignty safeguards in the Area of Justice, Freedom and Security. Moreover, effective implementation is often lost in the political glow that accompanies high-flying declarations. The relative lack of implementation effort regarding host nation support is worth noting as an obstacle to effective cooperation here. But there are other ways for institutions like NATO and the EU to enhance compliance: through systematic surveillance of implementation progress; by providing resources to assist with implementation; and by naming and shaming.[22]

The Current Status of Shared Institutions in the Euro-Atlantic Community

Europe and the United States do not lack for institutional frameworks; transatlantic cooperation takes place amidst a veritable alphabet soup of mechanisms and institutions. Many observers focus first on NATO, which remains an essential transatlantic security institution and is busier than managing crises in Libya, Afghanistan, and Ukraine—and is now tackling cyber security and (mis)information campaigns as it approaches a strategic rethink. But some areas of cooperation, including law enforcement, domestic intelligence, civil security, and disaster response are well beyond NATO's area of competence, and are better handled in other venues. NATO could—and should—complement such efforts, for instance by helping (as it has already done) with security for mass public events, dealing with the consequences of various natural disasters, or coping with a catastrophic terrorist event, particularly one involving agents of mass destruction.

But we should turn also to the EU, which represents the densest form of institutional cooperation—even across the Atlantic. Not only does cooperation run broad and deep—a critical consideration when designing resilience-enhancing initiatives across the policy spectrum—but the two sides are also enmeshed in security interdependencies. Add to this the fact that the EU is increasingly the institution that European governments use to coordinate their own security policies and action, and it is hard to deny that the EU will be America's essential partner in many of the areas beyond NATO's traditional purview and capacities.

---

[22] C. Knill and D. Lehmkuhl, "How Europe Matters: Different Mechanisms of Europeanization," *European Integration Online Papers*, 3(7), 1999.

The contrast between the highest institutional fora for NATO and for U.S.-EU exchanges is striking. EU-U.S. summits are infrequent and cumbersome. They are not embedded in any organized preparatory machinery, whereby committee work and the resultant policy recommendations are elevated to the political level for final determination. Suggestions to strengthen the processes underpinning this potentially important Euro-Atlantic forum[23] have not yet been met. Compare this to regular NATO summits, which by and large are well prepared and result in guidelines to be implemented by allies and by the secretariat. As many policy areas increasingly overlap between the two multilateral organizations, many have advocated improved cooperation between them. One way to highlight this point would be to merge the NATO summit and the EU-US summit into one set of high level meetings. An initial step toward such a linking of venues was taken in the July 2016 Warsaw Summit.

Shared Ideas

Many factors that condition the capacity to cooperate reflect non-material explanations for political outcomes.[24] Managing severe disturbances depends on perceptions: first, whether actors perceive a crisis as emerging, and second, how they frame a problem and act upon it.[25] Whether partners share mental maps is a key determinant of cooperation capacity.

The first place to look for ideational lubricants to cooperation is in the epistemological bonds between networks. Networks share belief systems that can have a strong effect on cooperation before and after major disturbances. Whereas opposing beliefs may inhibit cooperation, common belief systems have a strong binding effect on those that subscribe to them.[26] Similar findings are found in the epistemic communities approach. Such a community is a "professional group that believes in the same cause-and-effect relationships, truth-tests to accept them, and shares common

---

[23] See D. S. Hamilton and M. Rhinard, "Towards a Transatlantic Solidarity Clause," in P. Pawlak, ed., *The EU-US Security and Justice Agenda in Action* (Paris: EU-ISS Chaillot Papers, 2011).

[24] J. Goldstein and R. O. Keohane, eds., *Ideas and Foreign Policy: Beliefs, Institutions, and Political Change* (Ithaca, NY: Cornell University Press, 1993); P.A. Hall, *The Political Power of Economic Ideas* (Princeton, NJ: Princeton University Press, 1989).

[25] R. A. Boin, P. 't Hart, E.K. Stern and B. Sundelius, *The Politics of Crisis Management: Understanding Public Leadership When it Matters Most* (Cambridge: Cambridge University Press, 2005).

[26] P. Sabatier and H. Jenkins-Smith, eds., *Policy Change and Learning: An Advocacy Coalition Approach* (Boulder, CO: Westview Press, 1993).

values; its members share a common understanding of a problem and its solutions."[27] A community links professionals within particular issue areas, especially issue areas characterized by uncertainty and complexity. Networks, in general, facilitate cooperation through the "creation of collective meaning"[28]—a type of shared sense-making[29] in which members diffuse a way of viewing policy problems and the ways to address them. Since these networks generate consensus on cause and effect relations in the problem being tackled, cooperation tends to be smooth and consensual. When the community imparts its own perspective to decision-makers in different states, that perspective "may, in turn, influence the interests and behavior of other states, thereby increasing the likelihood of convergent state behavior and international policy coordination."[30]

A second set of ideational factors that influence cooperation concerns the presence of trust. This notoriously slippery concept is a central precondition for the presence of security communities in the international relations literature. Adler and Barnett, inspired by the earlier writings of Karl Deutsch, argue that states within a security community are much more likely to cooperate and assist, rather than wage war upon, one another.[31] The determining factor for this state of affairs is the presence of trust generated by increasing transactions; at a certain point, military conflict becomes unthinkable. Management scholars also find trust to be a key antecedent for cooperation. Ring and Van de Ven defined trust as an individual's confidence in the good will of the others in a given group and belief that the others will make efforts consistent with the group's goal. A belief that others will faithfully apply those efforts to achieve group goals may result in *informal* cooperation; a belief that a formal hierarchy is in place to reward cooperative may produce *formal* cooperation.[32]

---

[27] A wide variety of studies have identified epistemic communities at work in the international policy environment. For an overview see Haas, *op. cit.*, p. 55.

[28] E. Adler and P. M. Haas, "Conclusion: Epistemic Communities, World Order, and the Creation of a Reflective Research Program," *International Organization* 46(1):367–390, 1992.

[29] R.A. Boin, et.al, 2005, *op. cit*.

[30] Haas, *op. cit*., p. 4.

[31] E. Adler, E. and M.N. Barnett, eds, *Security Communities* (Cambridge: Cambridge University Press, 1998).

[32] P.S. Ring and A.H. Van de Ven, "Developmental Processes in Cooperative Interorganizational Relationships," *Academy of Management Review* 19:90–118, 1994. See also M. Argyle, *Cooperation: The Basis of Sociability* (London: Routledge, 1991).

But how, precisely, can shared ideas be used to build an enhanced capacity to cooperate? Three points from the above discussion stand out:

- ***Build and promote strategic concepts***. Shared ideas exist at different depths of cognitive adoption with some superficially adopted and others driving deep-seated mindsets.[33] Moving from the former to the latter is an imprecise exercise, but can be facilitated in initial stages by developing internally coherent, operationally useful concepts that appear to fit with nations' interests (see above). Here, forward resilience could prove useful in starting this process.
- ***Embed the concept in policy networks***. The discussion of advocacy coalition frameworks and epistemic communities above highlighted the cohering effect of norms within networks. However, different concepts often co-exist within communities, separated by those that are deep-seated and those that are purely strategic. Achieving the former requires examination, debate, and reflection of new concepts, which over time can become increasingly embedded.
- ***Trust***. The presence of trust is not easily engineered, and can only be gained over time and through positive experience. Here the time frame is counted not in years but in decades. Until 1814, Denmark and Sweden were hereditary enemies and fought numerous wars over territory and clashing interests in the North. After 1905, the notion of solving differences by military force eventually became inconceivable to either party. The evolution of this fundamental trust across nations need to be better understood by scholars and by practitioners with an interest in developing workable approaches for forward resilience based on an acceptance that resilience is shared.

The Current Status Of Shared Ideas among Security Policy Elites of the Euro-Atlantic Community

That community is networked through a wide variety of groupings, not least the think-tank-rich environment in Washington. A proliferation of reports, texts, and institutionalized journals serve as transmission belts for the affirmation of classic ideas and the introduction of new ones. However, several questions remain regarding the presence—or more precisely, the staying power—of shared ideas. One is the extent to which outliers can

[33] J.K. Jacobsen, "Much Ado About Ideas: The Cognitive Factor in Economic Policy," *World Politics*, 47:283–310, 1995.

be brought into the conceptual fold. Not only are some NATO members not committed believers in some prevalent ideas (resilience?), aggressively pedaled counter-narratives are on the rise in the East and South.

There is not yet an established strategic culture or an epistemic community underpinning actions among security professionals in the Euro-Atlantic community. Not only do divisions exist across the Atlantic, perhaps more importantly, they exist among European allies and partners. Moreover, within these nations considerable differences in strategic outlooks and even value preferences have been documented during recent years. As noted years ago by EU scholars, multiple-level dynamics are operating in the security and defense areas that often overtake traditional single-level and inter-governmental deliberations.

Ways Forward To Resilience

This chapter has examined what a high capacity to cooperate looks like, how it contributes to shared resilience and moving toward forward resilience, and how it can be achieved. Specifically, we have looked at the importance of shared interests, shared institutions, and shared ideas—all key building blocks of cooperation as set out in scholarly research. Our analysis confirms that more practical work needs to be done in the pursuit of forward resilience in the Euro-Atlantic Community, namely in each of the three key building blocks.

- ***Shared interests:*** Shared sense-making, with a clear sense of the goals at play, and a convincing narrative regarding the cost-benefit of cooperation, will enhance cooperation capacities. In an enlarged EU and NATO, this is a huge challenge, but think tanks play a major role. More intra-Alliance work is required on forming a shared and enduring threat assessment that can be the basis for strategic direction and settling resource priorities.
- ***Shared institutions:*** While there is no shortage of transatlantic discussion structures relevant to building resilience, many seem tired and unresponsive. A better approach might be to focus on sector-based trans-governmental institutions; specifically, on early warning and alert systems that benefit both sides of the Atlantic and are key for forward resilience. Expert-level working groups are crucial. Agreement on a set of guidelines or a media-grabbing action plan is not the same as ensuring the execution of such a hallowed document.

The most difficult step for NATO ahead lies at the operational level—when busy officials and experts are expected to transform the baseline requirements into actionable improvements at home and in the near abroad. Much follow-through and implementation work will be required after the Warsaw Summit if novel concepts and the baseline requirements are to set roots in the community. Scholars and practitioners working on EU processes have considerable experience and many insights into this part of the work ahead. This is another good reason for strengthening the cooperation among EU experts and those working on security and resilience in a NATO context. Merging NATO and U.S.-EU summits would carry some symbolic weight toward facilitating such mutual learning among sector-based officials and experts engaged in both organizations. In July 2016 in Warsaw, a first step for such a joint meeting was taken.

- ***Shared ideas:*** Forward resilience could play a role in forging a set of shared ideas. This approach involves many practical steps to enhance security inside and around the Alliance. In the aftermath of the July 2016 NATO summit, considerable staff work is now underway to operationalize concrete, baseline requirements for resilience in seven vital areas of concern. Several closed expert workshops are taking place. Yet we must not lose sight of the cohering concepts that offer signposts for the way forward. The necessary mindsets and cognitive frames that guide actions must be developed in collaboration with political, policy, and analyst communities, and defined in a way that makes their benefits crystal-clear to all parties.

The previous point reminds us that shared interests, institutions, and ideas are mutually constitutive and interactive; the presence of one provides a facilitating condition for the others. In this regard, attention should be placed on the two factors that can be most easily influenced: institutions and ideas. Enhanced working group interaction at the operational level (baseline requirements) should be pursued hand-in-hand with the elaboration and embedding of an acceptance of the shared notion and of the necessity of moving toward forward resilience as a guiding frame for action.

Chapter 5

Resilience Inside and Out: A Finnish Viewpoint

Axel Hagelstam[1]

Modern Vulnerabilities in a Hybrid Environment

In the open and interconnected economies of Europe and North America, the critical infrastructures underpinning vital societal functions and services are owned and operated by the private sector. For the last 25 years, societal infrastructures have been designed and built by private enterprises with the aim to sell a commodity and generate a maximum profit-to-investment ratio. Public policies have promoted innovation of new services and technologies to further increase efficiency, profit and convenience, and we have become accustomed to a new set of internet-based services relying on non-stop connectivity. Resilience has not been a relevant factor in this process; at best it has been a by-product of smarter technological solutions. As a consequence, the infrastructures and services upon which society relies for its vital functions are inherently vulnerable to shock and manipulation.

During this same time period, we have not faced any existential threats to our societies, political order or way of life. Until relatively recently, war in the European neighborhood had been considered practically inconceivable, and there have been no large-scale natural or other disasters with real systemic consequences.[2] As a consequence, we have applied a preparedness paradigm that strives to ensure full functionality of all systems and services at all times, regardless of their level of criticality. This preparedness paradigm is now being put into question by the emergence of a new and more challenging security environment.

---

[1] The views and opinions expressed in the following text are those of the author himself, and do not reflect those of the Ministry for Foreign Affairs of Finland.

[2] The 9/11 terrorist attacks were large-scale and did have a significant impact on the political landscape and policies on the United States, with direct consequences for the rest of the world. However, they did not threaten the existence of the U.S. public order, population, or economy. Also, the ongoing large-scale migration into Europe has had significant economic and political impact on several European countries and on the EU, but it does not present an existential threat, although there are those who would prefer us to believe so.

Another element of this debate also deserves some attention. Potentially existential threats to our societies, such as a rapidly spreading pandemic with high mortality rate, a meltdown of the international financial system, or a collapse of our electric grid, are not necessarily new and have not emerged as a direct result of the new security environment. They are threats that have been around for a long time and that have become even more complex because of changes in the structure of our societies and economies. We have consciously paid too little attention to such threats, because mitigating them and preparing for their consequences costs much more than we are willing to pay. One needs only to consider the financial crisis in 2008 or the reaction to the Ebola outbreak in 2014, before it was evident that the virus was not airborne, not to mention the potential consequences of climate change, to realize that the truly existential threats are the ones we are least prepared for, despite the fact that we can see them coming.

What is new is that we are faced with an adversary who has the capability, knowledge, and will to use all vulnerabilities to gradually debilitate the political system, society, and economy of its opponents. In his article "The Value of Science in Prediction," Valery Gerasimov, Chief of the General Staff of the Russian Federation, makes the case of promoting non-linear or asymmetric (hybrid) warfare to achieve political and strategic goals:

> The very "rules of war" have changed. The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness. The focus of applied methods of conflict has altered in the direction of the broad use of political, economic, informational, humanitarian, and other nonmilitary measures—applied in coordination with the protest potential of the population. All this is supplemented by military means of a concealed character, including carrying out actions of informational conflict and the actions of special-operations forces. The open use of forces—often under the guise of peacekeeping and crisis regulation—is resorted to only at a certain stage, primarily for the achievement of final success in the conflict.[3]

[3] Gerasimov doctrine, in *Military-Industrial Courier* February 27, 2013 (translation by Rob Colson, RFE/RL, https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/).

As we are now acclimatizing to this new security environment, we must refocus our preparedness efforts on the most pressing vulnerabilities, and accept that we cannot protect all systems and services at all times. A new resilience paradigm must be based on the fundamental notion that *society will survive, but not necessarily remain intact*. In case of a severe crisis, there will be situations where some functions and services will cease to exist, to our collective inconvenience. This must not only be accepted policy, it must also be communicated to the population, both to prevent false expectations that may undermine public confidence, and to increase personal resilience.

Five Steps to Enhanced Resilience

After accepting that we are not as resilient as we would like and that something needs to be done about it, I would argue that there are five fundamental tasks to fulfil to enhance the civil preparedness of our societies.

The first step is to establish a comprehensive and honest list of the most dangerous vulnerabilities in our individual societies. These vulnerabilities will vary from country to country, depending on their size, economy, military, and so forth.

Second, there is a need to identify which functions are truly vital for society to exist, and the infrastructures and systems upon which these functions rely. This step also involves being able to agree that all other functions are not vital, and therefore not prioritized.

Third, cooperative agreements with the owners and operators of these infrastructures and service providers are necessary to guarantee access in times of crisis, as well as an acceptable level of preparedness beyond *force majeure*.

Fourth, where possible, the public sector must invest in hardening the existing structures to enhance their resilience.

Fifth, where hardening isn't possible, the public sector must create backup systems upon which society can rely should the primary systems break.

These tasks require clarity of purpose, ability to cooperate across the entire public spectrum, political will, and resources. Failure to meet these tasks means that we are unprepared in the face of large-scale disasters, even the non-existential ones. Furthermore, we are defenseless against an

adversary who actively seeks to exploit vulnerabilities in our societies in order to paralyze us and coerce us to his will. Seen from this perspective, maintaining a decent level of civil preparedness is as important as maintaining a capability for military defense.

The Case of Finland

Finland applies a whole-of-government and -society approach to civil preparedness, which draws its functionality and strength from the small size of the administration, economy, civil society, and the relatively high patriotic sentiment among the general population, as well as the conscription-based territorial defense system. The approach is known as the comprehensive security model, and is presented in the Government Resolution for the Security Strategy for Society.[4] Senior decision-making is of course up to the government, supported by parliament, but a large number of decisions are delegated to competent authorities. This means that in a crisis situation, the ministry responsible for the function within which the crisis has erupted takes a leading role on the response, while other authorities assist as appropriate. The practical activities related to comprehensive security are coordinated by the Security Committee, consisting of the permanent secretaries of all government ministries, the general directors of the key government agencies, and the military, as well as representatives of the private sector and civil society, as appropriate.

The Security Strategy for Society identifies seven strategic tasks that need to be fulfilled under all circumstances, and allocates the responsibilities for these to all relevant government authorities. The tasks are:

- ***Management of government affairs***, meaning guaranteeing the functioning of the government, maintaining activities in and with the EU, government communications, situation picture, securing rule of law, and the ability to hold elections.
- ***International activity***, meaning maintaining contacts to foreign states and key international actors, protecting and assisting Finnish citizens abroad and at home, securing foreign trade, maintaining the ability to conduct comprehensive crisis management (military and civilian), and disaster response.

[4] Security Strategy for Society, Government Resolution 16.12.2010, http://www.yhteiskunnanturvallisuus.fi/en/materials.

- ***Finland's defense capability***, including military defense and support to and from other authorities.
- ***Internal security***, guaranteeing protection under the law, maintaining public order and security, emergency services and maritime search and rescue, flood risk management and dam safety, emergency response functions, oil and chemical spill response, border management, and immigration control and the ability to manage large-scale influx of asylum seekers.
- ***Functioning of the economy and infrastructure***, acquiring and allocating financial resources, maintaining the financial system and money management, insurance services, securing the fuel supply, electric power supply, information and communications systems, state administration IT functions, service systems and information security, warning and alert systems, continuation of transportation, food supply (primary production, processing and distribution), water supply, critical industries and services, housing, labor force, education and research systems, environmental monitoring, and waste management.
- ***The population's income security and capability to function***, meaning income security, social and healthcare services, availability of medical supplies and equipment, as well as detection, surveillance, and management of health risks.
- ***Psychological resilience to crisis***, including education, cultural identity and heritage, and religious services.

A revised Strategy is due in spring 2017. The revised Strategy will further define the tasks and responsibilities of the different authorities, and also accentuate the roles and importance of the private sector and civil society in crisis situations. As an example, the civil protection system in Finland, maintained by the Ministry of the Interior, involves an extensive system of public shelters that covers the entire population. The construction sector is required by law to include sheltering facilities in all new residential buildings.

Security of supply is another fundamental part of Finnish preparedness.[5] The level of security of supply in Finland is set by a government decree,

[5] The Finnish concept of security of supply covers a broad range of activities, including the ability to secure the continuity of economic activities and the functioning of the technical infrastructure vital for the livelihood of the population, for the economy and for national defense (see http://www.nesa.fi/security-of-supply/).

most recently issued in 2013 and set to be reviewed in 2018, to take into account recent changes in the security environment. The National Emergency Supply Agency, an agency under the Ministry of Employment and the Economy, is primarily responsible for security of supply. For this purpose, it administers a security of supply fund which draws resources from a small levy on all forms of energy consumption in Finland. This fund finances the operations required for maintaining the levels set in the government decree. Systematic investments both in hardening infrastructure, systems redundancies, and strategic stockpiles, made over the last seven decades, add up to a sizable safeguard, adding resilience against sudden shocks. At the same time, structural changes in both the society and economy during the last two decades have added several new challenges which require further action.

The private sector is actively involved in business continuity management through the National Emergency Supply Organization, supported by the agency carrying the same name. This organization maintains a wide network of branch-specific cooperative pools where businesses and authorities share situational awareness and preparedness-related information. Although there are signs of a tendency, particularly for multinational and foreign-based companies with few ties to the host country, to distance themselves from preparedness activities due to the (relatively small) costs they incur, these effects are so far limited.

In sum, the Finnish comprehensive security system strives to meet the five fundamental tasks through a set of tools, including a whole-of-government approach with a shared situational awareness and minimum preparedness standards, a periodic review of the vital functions in the Security Strategy or Society, a public-private partnership council involving key enterprises, and investments in hardened systems and free-standing backup systems through targeted investments.

Can Resilience be Projected?

A resilient society has built-in redundancies. It is robust, resourceful, responsive, and able to recover quickly. Resilience is as much a quality as a construct—it is not just about building it or planning it, it also must be kept alive and nurtured. This requires constant adaptation, improvement, and willingness to learn. Resilience is also an ability to accept that not everything can be protected against every threat, but that there will be functions and services that will not be maintained in crisis. Also, the pres-

ence of corruption in a political system negates any efforts towards increasing resilience, as these can be circumvented by simple cash.

Resilience is based on the characteristics and qualities of its host society, which vary from country to country in a way that makes it nearly impossible to think of a one-size-fits-all model for resilience. Nevertheless, it is essential to think about resilience from a broader perspective, due to cross-border dependencies that link open and interconnected economies. Particularly countries with small economies and low self-sufficiency are bound to engage in dialogue with neighbors and regional partners to protect economic flows and thereby ensure access to vital goods and services. This in turn requires a common understanding of threats and vulnerabilities, and the need to mitigate them. It is safe to say that national measures alone will not suffice to ensure national resilience. International collaboration is required. At the same time it is important to state that international cooperation under no circumstances can replace national resilience measures. Resilience will always, first and foremost, be a national responsibility.

NATO's Civil Emergency Planning Committee has adopted a set of seven baseline requirements for civil preparedness that together constitute an alliance-wide minimum standard of resilience. This standard can be applied by any country, not just Alliance members, and indeed NATO has decided to share the baseline requirements with some of its partners.

NATO's baseline requirements and resilience guidelines are presented in more detail by Lorenz Meyer-Minnemann in his chapter in this book. This work is an excellent example of how resilience can be projected over a large number of very different societies, economies and state structures. It is of course up to individual countries to ensure that this minimum standard is met. For this purpose, I would argue that, for the European theatre, a concerted effort between NATO as the standard-setting body, the European Union as the regulative body with an ability to offer significant financial support, and the nations as implementing bodies, would have the most potential for success in raising the overall level of resilience.

Chapter 6

Opening the Aperture on Resilience

Hans Binnendijk and Daniel S. Hamilton

Progress at the Warsaw Summit

Russia's hybrid attacks on NATO members and partners, plus indigenous terrorist attacks and those emanating from Da'esh, al-Qaeda, and other radical Islamist groupings and individuals have placed the spotlight on the need to enhance national resilience and civil preparedness. In addition, the new Trump Administration in the United States will be looking for signs that European allies are taking steps to protect and defend themselves. Strong European support for efforts to enhance European resilience may help shape the U.S. Administration's attitude towards the NATO alliance.

NATO's 2016 Warsaw Summit initiated a critical start to this effort. It recognized that national resilience not only strengthens defenses, it can also create a more effective deterrent.

Resilience efforts begin with a renewed focus on Article 3 of the Washington Treaty, which calls on members to "maintain and develop their individual and collective capacity to resist armed attack." Resilience Guidelines were agreed upon by Defense Ministers at their June 2016 ministerial meeting. NATO Baseline Requirements for National Resilience were also developed. At Warsaw, Heads of State and Government issued a separate commitment to "continue to enhance our resistance against the full spectrum of threats, including the hybrid threat, from any direction." Resilience against cyber attacks was the subject of a separate Cyber Defense Pledge which focused on securing national cyber systems.

Thus far, this resilience-building activity has focused primarily on NATO members. Through their resilience commitment, allies stated that they will protect their "populations and territory" in four areas: continuity of government, continuity of essential services, security of critical civilian infrastructure, and civilian support for military operations. Other NATO documents have elaborated on this list to include resilient energy supplies,

management of the uncontrolled movement of people, access to food and water supplies, dealing with mass casualties, and communications and transport systems.[1]

The Warsaw Summit recognized that while resilience is primarily a national responsibility, NATO support can be useful to assess and, upon request, to facilitate national progress.[2] Small Advisory Support Teams are being considered to implement the allies' resilience pledge. Cyber resilience efforts are more mature but still need strengthening. While NATO focuses primarily on military networks, mechanisms exist to share cyber security information and to deploy rapid reaction teams if needed.

In addition, a NATO-EU joint declaration issued at Warsaw highlighted the importance of these two institutions working together to counter hybrid threats and to enhance resilience.[3] If NATO is to be effective in enhancing resilience, it is clear that it must engage much more closely with the EU, which has undertaken a range of activities and initiatives aimed at improving its military and civilian capabilities and structures to respond to crises spanning both societal defense and societal security, including cross-border cooperation on consequence management after natural and manmade disasters. Unless the two institutions develop more effective ways to work together, each will continue to evolve separately, generating considerable waste in scarce resources, political dissonance, growing areas of unnecessary duplicative overlap, and increased potential for confusion and rivalry. Fortunately, there seems to be recognition that new efforts to implement stronger NATO-EU cooperation are required, and are under development.

Progress in understanding the importance of resilience has been significant. It is sound that NATO has focused first on its members and that the scope of resilience-building efforts is fairly narrow for now. Implementation needs to follow rapidly. But as the transatlantic community looks to the future, the current aperture needs to be opened in three areas.

- NATO allies and EU member states will need to look beyond their respective national borders and place greater emphasis on providing forward resilience for their partners and neighbors.

---

1 See NATO Warsaw Summit documents on "Resilience and Article 3."

2 Warsaw Summit, "Commitment to Enhance Resilience," paragraph 4.

3 Warsaw Communiqué, paragraphs 121 and 122.

- The scope of resilience needs to be expanded and the categories of resilience need to be better defined.
- NATO and the EU must create more effective tools to project resilience forward and to deal with the full scope of requirements.

Prioritizing Forward Resilience Partners

NATO allies and EU member states share a keen interest in the resilience of partners and neighbors, particularly those with whom they share considerable interdependencies, since strong efforts in one country may mean little if a neighboring country is susceptible to disruption.

The Warsaw Summit did not neglect the importance of projecting stability to NATO's partners and neighbors, but it was not the primary focus. The Summit noted that "if our neighbors are more stable, we are more secure . . . we are ready to do more to help our partners provide for their own security, defense against terrorism and build resilience against attack."[4] So both allies and partners are to be covered by this NATO initiative.

An important first step in managing the breadth and scope of the resilience enhancement effort will be to organize and prioritize those countries that might need assistance. To begin this process, this chapter offers five categories of countries that appear to need some outside support in strengthening their resilience. We do not include countries (allies or partners) with strong economies and societal structures that might indeed benefit from absorbing best practices. On balance, such countries will be producers rather than recipients of resilience support. Nor do we include Middle Eastern countries currently engaged in significant internal conflict, such as Syria, Libya, or Yemen. These countries in many cases receive direct combat support from the West, but their wars need to be settled before resilience programs such as those envisioned in this chapter would be effective.[5] Afghanistan and Iraq are special cases given the high degree of U.S. and/or NATO involvement over the past decade and a half, and so are also not included in this survey.

---

[4] The Warsaw Declaration on Transatlantic Security, paragraph 7.

[5] Indeed, if peace can come to Syria, Libya, Yemen, and Somalia, major stabilization and reconstruction operations may be needed to keep that peace. But those operations would be of a different scale and nature than the operations to enhance resilience considered here. And there is limited will in the West to take on additional massive stability and reconstruction operations.

For the purposes of this chapter we may distinguish between five categories of priority countries for forward resilience. Two groups encompass NATO allies and EU member states; two groups include countries outside the EU and NATO; and one group includes a mix of NATO/EU members and non-members.

The top priority should be the Baltic states, because they are the most vulnerable members of both the EU and NATO. They have been the target of Russia's destabilization campaign of intense propaganda and efforts at intimidation. Estonia and Latvia have large and potentially unstable Russian minorities. They have traditionally relied heavily on Russia for their energy supply. They are particularly vulnerable to cyber attacks. Their proximity to Russia and relatively weak border security provides Moscow with additional advantages to create mischief.

The second priority encompasses three so-called Eastern Partnership states—Ukraine, Georgia, and Moldova.[6] Russian operations in Ukraine are a model for the Kremlin's hybrid warfare efforts. All three countries have Russian troops on their soil and political parties that tend to be pro-Russian. They are particularly vulnerable to Russian hybrid warfare. Their security is of course not covered by Article 5 of the Washington Treaty, but NATO's Bucharest Summit communiqué indicated that one day Georgia and Ukraine would become members, a position repeated at the Warsaw Summit. Russia's annexation of the eastern Ukrainian region of Crimea and its military intervention, including through proxies, in a second Ukrainian area in the Donbas make it clear that events in this area fundamentally affect European security.

A third priority is the western Balkans. This category includes a mix on NATO members, NATO aspirants, EU members, and other countries such as Serbia that would benefit from a greater Western orientation. Two decades ago, instability in this region led to Europe's largest wars since NATO was created. Many of the issues underlying those conflicts have not been fully resolved. And Russia has sought to destabilize this region as well. Yet the region could be conducive to resilience-building given their general desire to be part of Western institutions.

A fourth priority for projecting resilience is the group of vulnerable nations of North Africa (Tunisia, Algeria, Morocco, and Egypt) plus Jordan. They are particularly important both to contain future flows of migrants

[6] Belarus, Armenia, and Azerbaijan might also be considered in this category, but governments in those countries are not NATO aspirants and are often aligned with Russia.

and terrorists to Europe and also to maintain current peace arrangements between Israel and its neighbors. The defeat of the Islamic State is probably a precondition for successful resilience operations in these states, but it is not sufficient. Current NATO plans to build the defense capacity of these nations is a step in the right direction, but more is needed in the area of civilian preparedness.

Finally, there are several other NATO allies in central Europe that could benefit from enhanced resilience, for example Poland and the other Visegrad states, Romania, Bulgaria, and even Greece. They are less vulnerable to instability created by Russian hybrid warfare than NATO nations in the Baltic states and in the western Balkans, but they could use additional support nonetheless. Many still rely on Russian military equipment and Russian energy supplies.

This set of priorities means that other allies or member states are on balance less vulnerable, not less important. It is worth noting, however, that in some areas of resilience, such as managing terrorist attacks or mass casualty events, all European nations could use help from their neighbors.

The Scope of Resilience

NATO has identified several categories of resilience, but a more comprehensive assessment is needed. This section suggests six broad categories of resilience, each of which is needed to withstand possible future challenges. Together they encompass and expand the scope of NATO's resilience categories. They do not replace the need for countries to spend resources on traditional common defense. Nor do they address economic resilience, which require a separate set of tools.

The first category is ***societal resilience.*** This grouping has to do with political cohesion, agreed values, and questions of identity. It involves reducing the risk of internal conflict and mitigating the impact of misinformation and propaganda. To achieve social resilience, countries will need to maximize minority rights and freedom of the press, develop police and judicial systems deemed to be fair to all, and develop conflict resolution techniques to manage internal crises should they occur. Countries with strong societal resilience will be able to withstand efforts by adversaries to divide their countries with malign influence and infiltration. Countries in the top three priorities above in particular need to strengthen societal resilience.

The second category might be called ***resilient homeland defense.*** This category deals more with protecting a country's territory. It is not necessarily about traditional defenses such as tanks aligned along the border, although that might be included in a country's overall defense package. But resilient homeland defense is a broader concept that might be called making a country "hard for an occupier to to digest." It ranges from effective border security, to maintaining highly trained special forces that can manage an initial crisis without necessarily escalating it, to making it clear that an occupation will be resisted by guerrilla forces. This is particularly important to those frontline states near Russia.

Third, countries need ***resilient critical infrastructures.*** These include cyber security for the country's network; protection of electrical grids and water supplies, including dams; a secure transportation system; access to food supplies; and a sound financial system. Traditional civil defense efforts as well as recent efforts by the EU and NATO have focused on enhancing resilient critical infrastructures. Given the transnational nature of Europe's critical infrastructures, maintaining this category of resilience will need a high degree of international collaboration. Instead of re-inventing the wheel, such efforts could build upon the EU's Critical Infrastructure Warning Information Network (CIWIN), which facilitates the exchange information on shared threats, vulnerabilities and appropriate measures and strategies to mitigate risk in support of critical infrastructure protection.[7]

A fourth category of resilience is ***limiting a society's dependency*** on resources controlled by a potential adversary, or addressing a society's reliance on critical flows abroad so that it can avoid being trapped into vulnerabilities that could endanger lives or vital societal functions. In the case of some NATO/EU members, dependency on Russian gas, oil, and electricity has been reduced but not enough. Russia has a history of using its gas production as a political weapon. The Baltic states in particular are still part of the Russian controlled "power ring." The Baltic states have made some recent progress by developing an offshore LNG terminal in Lithuania, by building a gas pipeline from Poland, and by connecting to the European electrical grid through Poland, Sweden and Finland. Cooperation among the three Baltic countries has not been exemplary, but it has been enhanced by EU investments in trans-European energy infrastructure projects. Finland, Bulgaria, Germany, the Visegrad states, Greece,

---

[7] For more, see http://www.ppbw.pl/fotki/files/files/Aktualno%C5%9Bci/2016-05-23%20prezentacje%20konferencja/Alberto-Pietro%20Contaretti_Komisja%20Europejska.pdf.

and even Italy are also uncomfortably dependent on Russian gas supplies. Another example of dependency relevant to resilience has been central European reliance on Soviet-made military equipment. This dependency is being corrected, but only slowly, given the long life cycles of major defense equipment.

A fifth type of resilience, as highlighted by the Warsaw Summit, is ***continuity of government and essential services.*** The United States, for example, has established elaborate means to ensure the continuity of government, even in case of a major nuclear attack. This requires a combination of a clear chain of command in time of crisis, advanced delegation of authority, evacuation plans and safe havens for leaders, and civil preparedness to maintain services at the grass roots level. Maintaining continuity of government can deter an adversary who may feel that decapitation of a nation's leadership would give them an opportunity to gain control.

In the context of requirements for forward resilience, however, particularly with regard to fragile neighboring states, it may be equally important to consider the degree to which such societies have effective governance, not simply effective government. Government is one important pillar of society, but any individual society's ability to anticipate, prevent and ultimately withstand and bounce back from disruption may depend equally on its governance capacity, i.e., how other sectors of society are engaged, how rules and norms are structured, implemented and enforced, how actors are held accountable, and whether the processes by which these activities are conducted are stable and sustainable. Governance challenges are often at the heart of weak or fragile governments, and can reveal vulnerabilities to disruption. Tackling these broader challenges of governance, rather than just government, is an important consideration for efforts at forward resilience.

The last resilience category is ***management of mass casualty attacks*** or a massive natural disaster. This may be the most developed of the six categories, as it is the classic core of civil defense. Most countries have developed plans to deal with natural disasters, including establishing exit routes, creating shelters, or providing medical care. Now response to massive terrorist incidents must be added to the list. In the defense field, NATO a decade ago developed guidelines for first responders to treat the results of chemical, biological, radiological, and nuclear attack. These NATO Response Guidelines are supplemented by international training and by Advisory Support Teams. While important steps have been taken

to enhance this category of resilience, the sheer magnitude of these potential catastrophes is such that constant attention is needed.

Delivering on Resilience

A review of these six categories of resilience plus the five sets of countries that may need priority assistance in building resilience indicates that NATO allies and EU member states have taken on a major task. To deliver on this promise, priorities need to be set, assistance programs need to be tailored, and support efforts need to carefully organized. Here are a Top Ten set of recommendations that might help the transatlantic community organize for this task.

1. ***Conduct a survey of resilience requirements.*** NATO's newly adopted resilience guidelines provide an opportunity to survey NATO members and partners to identify how countries believe they measure up against these guidelines. The results can be used to guide further support efforts.
2. ***Set priorities.*** NATO analysts might create a matrix using the country priorities and functional requirements suggested in this chapter along with survey results to establish a list of priority activities. For example, the matrix might show that border control in the Baltic states is the top priority. NATO might then use the results of this matrix to identify immediate- and longer-term resilience requirements. This effort could complement the recommended survey.
3. ***Identify those who can strengthen forward resilience.*** NATO's Civil Emergency Planning Committee has compiled a list of civilian experts who could be called upon to support the enhancement of resilience. But given the magnitude of the task, much greater efforts will be needed to identify others who can strengthen and project resilience. No single organization or country has the breadth and capability to deliver on all of these requirements for enhancing resilience. This effort would include identifying those international institutions, nongovernmental organizations, nations, and individuals that have a particular expertise in some element of resilience. For example, NATO's Cyber Center of Excellence and its Computer Incident Response Capability are already helping countries with their network security resilience, while OSCE and institutions such as the U.S. National Endowment for Democracy or the European Endowment for Democracy might be well suited to support societal resilience.

This list of value-added actors should extend beyond NATO members to include countries such as Sweden and Finland. Finnish experience with territorial defense and institutions such as border guards, for example, or Swedish expertise with addressing asymmetrical dependencies on external forces, may mean that these countries could be leaders in cooperative efforts as neighbors seek to enhance their efforts in such areas.

4. ***Develop mechanisms for institutional cooperation.*** Once priorities are set and producers of resilience are identified, an effort needs to be made to link the capabilities of NATO, the EU, OSCE and other relevant institutions. Creation of a NATO-EU Resilience Coordinating Council might prove useful to drive this effort. The NATO International Staff and some combination of the EU's External Action Service and the European Commission's Directorate-General for Migration and Home Affairs should develop an inter-service mechanism to engage regularly on exchange of good practice, identify and address critical vulnerabilities, situational and threat assessments, and early warning and early action procedures. This may be a good way to test the Warsaw Summit pledge to develop closer NATO-EU cooperation.
5. ***Work with host nations to tailor programs.*** Resilience-building efforts will not work without the active cooperation of a host nation. Those who require or desire assistance with their own resilience efforts will need to take a major role in tailoring programs to fit their own needs, based in part on the recommended survey. The NATO-EU Resilience Coordinating Group suggested above might take the lead in working with priority host countries through Individually Tailored Resilience Planning and Review procedures.
6. ***Expand the functions of NATO's Civil Emergency Planning Committee (CEPC).*** NATO's CEPC currently has a mandate to plan for contingencies that involve civilian casualties and to provide civilian expertise in the field of terrorism preparedness, consequence management, disaster response, and protection of critical infrastructure. If the expanded scope of resilience requirements suggested above is accepted, CEPC's responsibilities need to be expanded and more resources will be required. There would be a corresponding shift in its emphasis towards enhancement of national resilience.
7. ***Create Forward Resilience Advisory Support Teams.*** NATO has periodically used Advisory Support Teams for civilian emergency

planning purposes. The resilience commitments made at the Warsaw Summit will require a revitalization and expansion of these Advisory Support Teams. Efforts to build these teams should be accelerated, and consideration should be given to pooling EU and NATO resources for such teams. They might be used to address the highest priority needs, for example in the Baltic states, in Ukraine, and in the western Balkans. Host nations could be encouraged to establish working group-type secretariats to coordinate defense activities with overlapping civil authority and private sector key critical infrastructure functions to enhance national capacity to anticipate, prevent, respond and recover from disruptive scenarios and to provide a key point of contact for Forward Resilience Advisory Support Teams.

8. ***Create a NATO Center or NATO/EU Joint Center of Excellence in Resilience***. Such a Center, dedicated specifically to resilience, could serve as a clearing house for good practices. It would be an inexpensive way to share ideas and could be located in a non-NATO member such as Sweden or Finland to make the point that this is an effort that extends beyond traditional defense.
9. ***Create Partnership Programs for Resilience***. This concept would be modeled on the current U.S. National Guard State Partnership Program, which now operates in 22 European countries and five Middle Eastern countries. In the first instance, these U.S. National Guard programs might be expanded to focus more on resilience issues. But more ambitiously, national partnerships might be created on a framework nation basis to connect NATO members and NATO partners For example, Italy might serve as a framework nation to develop a resilience partnership with a country in North Africa. Sweden might serve as a framework nation to develop a resilience partnership with a country in eastern Europe. This concept could help to decentralize the resilience-building effort and significantly expand its scope.
10. ***Encourage the Establishment of Regional Working Groups.*** Host nations could, in addition to creating national working groups as points of contact for Forward Resilience Advisory Support Teams, establish working groups with like-minded allies and partners in their region to facilitate shared resilience and interoperable efforts. The Nordic and Baltic states, for instance, might consider a regional approach to forward resilience efforts, somewhat similar to such regional mechanisms as Nordic Defense Cooperation (NORDEFCO) or the Southeast European Defense Ministerial.

Chapter 7

The Case for Forward Resilience in the Baltic States

Tomas Ries

Resilience is a high priority for a society if it is unable to meet five security tests:

- Does it perceive the threat, or is there failed or no threat analysis?
- Can it remove or mitigate threats, or are there weak or no pre-emptive strategies?
- Can it deter the threat?
- Can it shield oneself against the threat, or does it lack adequate defensive capabilities?
- Can it dodge the threat, or do geographic or other constraints render that difficult?

Today the answer is No to four of these five security tests. Since January 2014, NATO west of Berlin belatedly, and only partially, recognizes a severe military threat to the three Baltic states. However, it cannot today say Yes to the other four tests, and they are decisive. Over time some of these weaknesses may be addressed, but for the time being they are facts. Thus, forward resilience for the Baltic states is currently highly relevant.

The Baltic Challenge

The challenge to the three small Baltic NATO states of Estonia, Latvia, and Lithuania is a Kremlin that clearly shows hostility to the North Atlantic community, including both the EU and NATO, uses brute force including war to achieve its aims, and is building a military dominance in Europe, and certainly in the Baltic region. At the same time, NATO has concluded that it currently cannot defend the three small Baltic states.

First, Russian military forces facing the Baltic are too big and powerful for the handful of NATO brigades still capable of fighting to match them. In the Zapad 2013 maneuvers held next to the Baltics, for instance, Russia

fielded two Army Headquarters, one Division, and twelve Brigades, along with logistical, air, naval, and tactical nuclear support, for a total force of some 100,000 men. As of the summer 2017, NATO standing forces in the three Baltic states will amount to some 20,000 men, all basically light infantry, and it will take months for the handful of VJTF brigades to even reach the Baltic region. With Russian forces within kilometers of the border and now developing very high readiness levels, NATO currently cannot reinforce the Baltic states in time.

Second, Russia is building up an anti-area/access denial (A2AD) zone around the Baltic which can seal off the three Baltic states from NATO reinforcements. More importantly, their increasingly sophisticated and deeply integrated air defense systems make it make it difficult and costly to engage U.S. air power, which is the only NATO force that can deliver decisive force in time.

Finally, and most crucially of all, Putin has built up a complete nuclear dominance in Europe, allowing him to exert a degree of nuclear coercion that would break NATO. Since the late 1990s Russia has fielded four new theatre nuclear missile systems (the Iskander-M MRBM (700 km range), Iskander-K GLCM (1,500 km), Kalibr SLCM (2,600 km) and Rubezh IRBM (2,000 km) and simulated their use in several military manoeuvers (Zapad 2009, Zapad 2013 and more). It has simulated nuclear bomber strikes against Sweden and has threatened Copenhagen and Norway with nuclear attack. Most important of all, it is clear that the Putin regime has thought long and hard about how to use nuclear force in Europe.

In contrast, liberal Europe is a nuclear void. There are virtually no NATO nuclear forces (less than 200 aging B-61 gravity bombs left over from the Cold War), there is questionable linkage to the U.S. global nuclear deterrent, there are no military and civil preparations for a nuclear crisis or war, and our political leaders are completely unfamiliar with both military power politics and nuclear war. Thus, and this is the most crucial factor, there is no NATO nuclear strategy or political consensus on how to respond to nuclear coercion. In nuclear terms we are headless chickens.

That NATO would crack under nuclear coercion under these circumstances can be forecast with absolute certainty if we compare the current Western nuclear void with the massive efforts on both sides of the Atlantic required and made to ensure credible nuclear deterrence in Europe during the Cold War. Today there is virtually no hope that NATO could reach

consensus in the event of a nuclear crisis with Russia, including the threat of nuclear attack.

The Baltics are thus dangerously exposed. Currently their military security rests on their minute national defense forces and the three symbolic multinational NATO battle groups of around one battalion to be deployed to each state in 2017 and their tenuous political deterrence value. Second, and weightier, is the fact that for Putin an attack on even part of a Baltic state would be a game changer. It would constitute an outright declaration of war against NATO and western Europe. And while the odds are that both NATO and the EU would collapse in such a crisis, such a venture is still fraught with considerable uncertainty and downstream risks for the Kremlin. Moreover, as Putin learned in the Ukrainian Donbas, even the most surgical plans can go very wrong.

The Baltic states are thus living dangerously. If NATO cannot currently defend them we must prepare the dirty default option, which is resilience. For the Baltic states this can be divided into two sorts:

- ***Sovereign and existential resilience***, focusing on the survival of the nation in the most extreme circumstances such as outright invasion.
- ***Functional resilience (Forward Resilience)***, focusing on the ability to absorb shocks and pressure under more normal circumstances, short of massive military invasion.

Sovereign and Existential Resilience

Sovereign resilience is related to protecting the vital core of the nation. It includes protecting the national spirit, independence and territorial integrity. Ideally such resilience rests on retaining at least a part of the national territory and population free from occupation. As noted above, such territorially based resilience is almost impossible for the Baltic states to achieve should Putin launch an all-out military attack. They are too small and too vulnerable to trade space for time, and unlike the Ukraine they cannot keep part of their territory and population independent and sovereign.

Under these circumstances we need to shift from sovereign resilience to existential resilience. This is far more severe. It also focuses on preserving the vital core—the national spirit and identity—but now without retaining part of the territory and population. This is similar to the resilience shown

by France and Norway, for instance, during the Second World War, when their homeland was occupied but a legitimate national identity was retained outside the national borders. This involves:

- ***Survival:*** Ensuring the political core of the nation can survive by evacuating the government and parts of the political elite to retain a legitimate government in exile, as well as other key cultural and symbolic value assets.
- ***Endurance:*** Ensure the continued legitimacy of the vital core in exile, by legal, symbolic, cultural and informational means.
- ***Revival:*** Pressure Russia in various ways to withdraw, from sanctions to outright war, until Baltic sovereignty is restored. Once this is achieved, facilitate the return of legitimate authorities and restore a functioning state.
- ***Peripheral:*** Receive a possible flood of Baltic refugees.

Baltic Functional (Forward) Resilience

Russia is systemically applying pressure against our social, economic and technological foundations. This is pure Sunzi and his notion of *Shi*, or shaping.[1] It is also an evolution of the sophisticated Soviet correlation of forces concept and related active measures campaigns,[2] now considerably upgraded as part of the Russian "New Generation Warfare" or "Multidimensional Warfare."[3] This is also a form of warfare that involves less risk for the Kremlin, and hence is more usable. In fact it is already taking place today.

Forms of Russian functional pressure focus on weakening a targeted state and society to the point where minimal force is needed to impose one's will. This includes enlisting, coercing, confusing, frightening, weak-

---

[1] See Ries, chapter 1 in this volume, and Francois Jullien, *The Propensity of Things. Toward a History of Efficacy in China* (translated by Janet Lloyd). New York: Zone Books,1999, p. 317.

[2] For a useful outline see James H. Hansen, *Correlation of Forces: Four Decades of Soviet Military Development* (New York: Praeger, 1987), pp. vii–xix.

[3] (For a useful outline see Valery Gerasimov, "The Value of Science is in the Foresight. New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations" (translated by Robert Coalson), *Military Review*, January-February 2016: pp. 23–29. Originally published in Russian in *Military-Industrial Kurier*, February 27, 2013; also Charles K. Bartles, "Getting Gerasimov Right," *Military Review*, January-February 2016, pp. 30–38, especially the diagram on p. 35.

ening, damaging and challenging the authority and legitimacy of the target in every way. This can be pursued in various ways:

- ***Multitool:*** all types of cyberoperations, from information warfare to sabotage.
- ***Political and social:*** subversion, information operations and infiltration of individuals, politics and groups.
- ***Events:*** creating or manipulating diplomatic, political/legal, criminal and other events to justify action, destabilize and intimidate.
- ***Infrastructure:*** Using or damaging economic and technological infrastructure.
- ***Economic pressure*** and a host of other functional and social means.

All of these are transnational and many are functionally two-way, which is to say that they extend deeply into other NATO societies through everything from trade to politics.

In an interlinked networked world this social and functional warfare affects everyone's security, not just the direct target. And if it fails, it requires resilience. Until liberal societies, in particular those in NATO, learn how to play this game, we will steadily lose ground to the Putin regime. In fact, we are doing so already, as we watch the erosion of the liberal social and political order. This is admittedly driven by deeper socioeconomic trends of our own making, but Putin can and is exploiting them skillfully.

Chapter 8

Resilience and Alliance Security: The Warsaw Commitment to Enhance Resilience

Lorenz Meyer-Minnemann[1]

Faced with the greatest security challenges in a generation, the NATO Alliance is currently implementing the most significant reinforcement of its collective defense capabilities since the end of the Cold War. While a great deal of public attention has been focused on NATO's military adaptation, concurrent efforts to strengthen the Alliance's ability to resist and recover from attack not just militarily, but also with civilian capacities, have so far been less visible. However, this is changing. At the Alliance's July 2016 Summit meeting in Warsaw, NATO leaders agreed an unprecedented "Commitment to Enhance Resilience." The 28 allies are now working urgently to put this commitment into practice.

The Alliance's renewed emphasis on resilience is based on the recognition of two uncomfortable, but increasingly important trends. First, armed forces today are more reliant than ever on capabilities and infrastructure that are civilian-owned or operated. To have assured access to these capabilities, NATO requires robust civil preparedness in allied nations, across both the public and private sectors. Second, civilian services and infrastructure are potentially vulnerable to outside attack or internal disruption—and such vulnerabilities could be exploited by potential adversaries. Not only could the Alliance's military capabilities be attacked indirectly, but civilian functions could become a primary target. In an age of hybrid threats, strengthening resilience, primarily by improving civil preparedness and cyber defenses, is therefore a critical component of NATO's efforts to deter and defend against the full range of threats.

Modern Resilience for Effective Defense

Resilience is not a new task for the Alliance. Article III of the Washington Treaty stipulates that allies have an obligation to develop and maintain

[1] This chapter reflects the author's personal views and does not represent those of any institution or organization.

the capacity to resist armed attack. Long before the advent of cyber threats and hybrid warfare, this notion of resilience was always understood to go beyond military capabilities. As early as the 1950s, NATO had put in place policies and planning for civil preparedness. By the late 1980s, the Alliance maintained plans for eight NATO civil wartime agencies, which could be stood up in times of crisis or war to coordinate and direct efforts ranging from industrial resource allocation and oil supplies to food production, civil transportation, and the management of refugee flows.

This early NATO collective resilience architecture involved more than 1,400 international civilian experts, as well as corresponding resources in all NATO members' capitals. However, following the momentous changes of the 1990s, it became one of the first peace dividends of the new era. By 2014, when the security environment shifted once again, funding and legal mandates for civil preparedness had all but disappeared in the majority of Allied nations. What remained in terms of residual civil home defense planning responsibility had often shifted to specialized agencies, such as fire and rescue services, which lacked the mandate and resources to undertake robust planning for homeland and Alliance defense.

The near absence, for a generation, of robust national and Alliance resilience planning became apparent when urgent steps were taken to improve NATO's deterrence and defense capabilities with the NATO Readiness Action Plan agreed at the September 2014 Wales Summit. Following an initial assessment by experts within NATO's Civil Emergency Planning Committee, a first report on the state of civil preparedness across the Alliance was presented to NATO Defense Ministers in February 2016. This assessment, together with parallel efforts to improve NATO's and NATO nations' cyber defenses, laid the groundwork for the now ongoing, systematic effort to improve resilience across the Alliance.

Based on an assessment of threats and vulnerabilities, allied defense ministers agreed on a set of minimum standards for national resilience, so-called "baseline requirements," in seven areas that were deemed most critical to NATO's collective defense tasks:

1. ***Continuity of Government***: maintaining at all times the ability to make decisions, communicate them, and enforce them, and to provide essential government services to the population.
2. ***Resilient Energy Supplies***: ensuring that energy supply, including national power grids, are secure and that nations maintain the necessary prioritization arrangements and redundancy.

3. ***Resilient Civil Communications Services***: ensuring that telecommunications and cyber networks remain functional even in demanding conditions and under attacks.
4. ***Resilient Food and Water Supply***: ensuring sufficient supplies are available to both civilians and the military, and safe from disruption of sabotage.
5. ***Ability to Deal with Large Scale Population Movements*** and to be able to de-conflict such movements from potential national or Alliance military deployments and other requirements.
6. ***Ability to Deal with Mass Casualties***: ensuring that health systems can cope even in very demanding situations when there might be simultaneous pressure on civilian and military health care capabilities.
7. ***Resilient Civilian Transportation Systems***: ensuring that NATO forces can move across Alliance territory rapidly and that civilian transportation networks remain functional and effective to support civil and military requirements even when challenged or attacked.

The Warsaw Resilience Commitment

The agreement by allied ministers on the baseline requirements was a key milestone. A few months later, the issue was brought into the political spotlight with the "Commitment to Enhance Resilience" adopted by Alliance Heads of State and Government at the July 2016 Warsaw Summit.

The Warsaw Summit Resilience Commitment makes three critical points. First, it stipulates that resilience is an essential basis for deterrence and effective fulfillment of the Alliance's core tasks. Second, it makes clear that in order to be able to deter and defend against the full range of modern threats, allies need to maintain and protect critical civilian capabilities alongside and in support of military capabilities in an integrated way, and with the involvement of the whole of government and the private sector. Third, it constitutes a political commitment at the highest level by each allied nation to strive to achieve the agreed requirements for national resilience.

Beyond establishing resilience firmly among NATO's priorities, the Warsaw Summit Resilience Commitment is notable for a number of additional fundamental points. Although it takes a deliberately narrow, defense-focused view on resilience, the Warsaw document does note that the

foundation for resilience lies not simply in infrastructure, planning and preparedness—but first and foremost in the NATO nations' shared commitment to common values. Democratic governance, individual liberty, and the rule of law are the first line of defense against hybrid and other threats. The Warsaw Commitment also points out that the NATO requirements, while critical to achieving the Alliance's core tasks, may not be the only lens through which nations view resilience and that there is not necessarily a single path to achieve them. Because resilience is first and foremost a national responsibility, nations must each develop and build systems that suit their own national circumstances and risk profiles, as well as their commitments *vis-a-vis* other bodies such as the European Union. They cannot and will not maintain more than one set of capacities to resist and recover from catastrophic events, be they natural disasters or armed attacks. Finally, the Warsaw Commitment recognizes that NATO's resilience can be enhanced by the work of other organizations, in particular the European Union, and by strengthening the resilience of partner countries in the Alliance's neighborhood.

The Road Ahead—Doing the Homework

NATO members are now working to achieve the Warsaw Commitment, while NATO is putting in place the necessary collective instruments to assist them in doing so. Considerable progress has been achieved in a short period of time, but there are also challenges. Building resilience starts at home. NATO has defined a set of requirements, but allied nations will have to make the necessary arrangements to be able to implement these resilience requirements horizontally across government and the private sector; and vertically from the highest level of national governments down to state, county, and municipal level.

This will need investment. Capabilities and infrastructures such as transportation networks, energy grids, monitoring systems, and telecommunications networks will have to be improved, but the need for investment goes beyond physical infrastructures. An equally important gap exists in human resources and connectivity. National authorities charged with achieving the resilience requirements across the seven sectors will need the appropriate staff, training, and access to information networks to be able do so. For example, a Ministry of Agriculture cannot ensure that food supplies are resilient against hybrid threats if it is not given the manpower to do the necessary planning; the personnel security clearances to interface

with intelligence agencies and with military authorities; and the training to develop modern resilience systems for a modern security environment. The same is true for almost all other areas of government. Planning costs money.

Another area of homework concerns legislation. National governments must have the necessary legal basis to define resilience standards and to enforce them in peacetime and crisis. This begins with adequate provisions for government powers in situations that may remain below the traditional threshold of war defined in emergency legislation; and it may end with the necessary legal authority (and capabilities) to manage, if necessary, population movements in crisis or conflict. In between these are a whole range of other laws and regulations that affect governments' ability to permit movement of allied forces across borders and territory, and provide adequate host nation support even in the most demanding circumstances. Many significant improvements have been made in this regard over the past 24 months, but more work is necessary to ensure that improved legislation translates into more effective arrangements and support at all levels.

Allied nations must also further improve their ability to partner effectively with private sector owners and operators of critical infrastructure and services. Although, in general, private sector owners and operators have a strong commercial interest in being able to minimize disruptions and outages, there are areas in which private sector security or business continuity planning does not go far enough to satisfy national and Alliance security and defense requirements. In these cases, there is a need for Allied governments to incentivize private sector support—be it through intelligence sharing, preferential contracting, or, possibly, funding arrangements. Where such incentives are not feasible or do not prove powerful enough, governments may need to consider enforcing private sector compliance with baseline resilience requirements through appropriate regulation or licensing.

While NATO can set requirements and guidelines, the Alliance itself does not possess legislative or regulatory powers over the private sector, nor is it a funding mechanism for national civil preparedness. This makes transparency and cooperation with the European Union a critical task. Several important steps have already been taken. Boosting resilience against hybrid warfare was highlighted as one of the priority areas for cooperation in the Joint Declaration on NATO-EU Cooperation that was signed on July 7, 2016 by NATO Secretary General Jens Stoltenberg, President of the European Commission Jean-Claude Juncker, and President of the

European Council Donald Tusk. NATO and European Union staffs are actively working to develop further concrete proposals for cooperation and information sharing.

Setting and Assessing Requirements

While the primary responsibility for building a more resilient Alliance rests with national authorities and—where appropriate—the competent European Union bodies, there also remains homework to do for NATO collectively. A critical area is to refine the requirements and to assess progress against them. The Warsaw Summit Commitment sets out very clearly the problem to be solved and the primary ways of solving it, but it does not define in detail what constitutes success, nor does it set a definite timeline for achieving greater resilience. Refining these two aspects is a main priority.

NATO expert working groups are currently defining basic criteria for evaluation of resilience across all of the seven baseline requirements. Along with a set of guidelines that have already been issued to allied nations, these criteria for evaluation will form the basis of a fresh assessment of the state of civil preparedness across the Alliance in the near future. This assessment will be conducted by leveraging the NATO Defense Planning Process, the Alliance's long-standing and proven mechanism to assign capability targets to allies and to assess their performance against them.

This is easier said than done. Unlike military requirements that can be easily quantified, none of the seven NATO baseline requirements are susceptible to a one-size-fits-all solution. For example, how a nation ensures the survivability and continuity of government functions is not only a sovereign prerogative, it is also contingent upon factors that vary widely among allies, including individual constitutional provisions and geography. Likewise, there are many different approaches and political traditions in NATO capitals regarding legislative provisions, cross-government coordination and planning—including on sensitive matters such as use of the military for domestic purposes, intelligence sharing, or law enforcement powers.

Against this background, NATO cannot—and does not strive to—develop a single detailed template for how to achieve resilience across the seven critical sectors. It can, however, be the platform on which Allies can share best practices and successful models in a context of shared purpose

and confidentiality. NATO can also be a platform for engaging private sector interests in frank and open exchanges on respective requirements and expectations. The first series of such exchanges within NATO have been very promising, and they will be continued.

Collective Action

The Alliance must also be in a position to provide concrete practical support to those allies who request it. Many of the necessary tools for helping allies (and third countries) to improve their resilience are already in place. NATO has a cadre of civilian experts from government and industry at its disposal to advise both individual nations and, if necessary, the NATO military authorities, on all aspects regarding the use and protection of civilian resources and infrastructure. This unique expertise is now being reconfigured and trained to be available to member states of the Alliance, but also to third countries, as so-called Resilience Advisory Support Teams.

NATO is also improving training and awareness raising. Such efforts are crucial to ensure that as legislation and arrangements are improved, knowledge of improved procedures actually trickles down to the operational and tactical level. Beyond operational training, there is also a need to rebuild more systematically the links between national and NATO military structures on the one hand and national civilian authorities on the other. Until the 1990s, NATO CIMIC (civil-military cooperation) staff and national civilian resilience planners participated in systematic cross-training. Revitalizing this tradition in NATO military training and education will go a long way to integrating military and civilian aspects of resilience.

Finally, while achieving resilience is above all a national responsibility, NATO must be able to increase civil preparedness collectively, when a crisis situation demands it. The existing NATO Crisis Response System provides both the overarching mechanism and a set of detailed planning tools to achieve this. Civil preparedness must also be exercised, alongside Alliance military exercises. Ensuring that resilience considerations can be effectively integrated into military exercises are therefore a key priority and currently a major line of effort within the competent Alliance bodies.

Conclusion

Long considered a peripheral issue, resilience has once again become core business for the Alliance and for national security planners in allied capitals.

The Warsaw Summit Commitment to Enhance Resilience was an historic reaffirmation that resilience, ensured through systematic civil preparedness and effective civil-military planning, is a central pillar of NATO's collective defense. Requirements have been agreed upon and criteria for success are being defined. The basic process is thus in place, but delivering on the Warsaw Commitment remains a complex undertaking. It will require a holistic view on resilience, both within national governments, across governments and the private sector, between NATO and the European Union, and with partner countries beyond NATO.

Delivering on the Warsaw Commitment will also require continued high-level political attention and investment. NATO Heads of State and Government have provided the high-level political impetus. This must now be followed up at all levels, from national security councils and key government departments all the way down to municipal levels, and across the public and private sectors—to build a more resilient Alliance.

Chapter 9

Resilience as Part of NATO's Strategy: Deterrence by Denial and Cyber Defense

Piret Pernik and Tomas Jermalavičius

Russia's contemporary way of war has been dubbed "hybrid warfare," as it combines a broad range of tools in order to weaken and coerce target countries, with conventional military means being just a small part of an overall mix. Strategic thinkers within NATO, who were concerned about how to respond to this doctrine, latched on to the concept of resilience, which is basically the antonym of vulnerability. We begin by discussing the essence of resilience, proceed to establish how it is related to the concept of deterrence, and then focus on the cyber domain as the sector where the resilience-building efforts are particularly important to the Alliance.

What is Resilience?

The term "resilience" is used in many contexts. It originates from the field of ecology, where it was initially understood as "the measure of the ability of an ecosystem to absorb changes and still persist."[1] The concept appeared attractive to other fields, especially those involving the management of complex interlinked systems, and therefore it spread beyond its original uses in ecology. It is now employed at different levels (individual, community, state) and in different fields such as psychology, physical infrastructure management, economy, organizational management, community studies, etc. So far, its most popular use in the field of security has pertained to disaster preparedness and anti-terrorism, with cybersecurity and critical infrastructure protection being late adopters.[2] In light of Russia's hybrid

---

[1] Joseph S. Mayunga, "Understanding and Applying the Concept of Community Disaster Resilience: A Capital-Based Approach," *Summer Academy for Social Vulnerability and Resilience Building* (Munich, Germany) (2007): 2, http://www.ihdp.unu.edu/file/get/3761.pdf.

[2] See Jon Coaffee, "From Counterterrorism to Resilience," *The European Legacy*, Vol. 11, No. 4 (2006): 389–403; Jon Coaffee and Peter Rogers, "Rebordering the City for New Security Challenges: From Counter-Terrorism to Community Resilience," *Space and Polity*, Vol. 12, No. 1 (2008):101–118; Noor Aisha Abdul Rahman, "The Dominant Perspective on Terrorism and its Implication for Social Cohesion: The Case of Singapore," *The Copen-*

approach to conflict, resilience is now becoming a popular concept within NATO and the EU as a way to frame a holistic strategic response to the threat, combining the "whole-of-government," "whole-of-society," and "whole-of-alliance" perspectives as well as multiple security domains.

In generic terms, resilience has been defined as a "process linking a set of adaptive capacities to a positive trajectory of functioning and adaptation after a disturbance."[3] This definition implies that resilience is a process, although it can also be seen as a strategy or as the "capability of a system to maintain its functions and structure in the face of internal and external change and to degrade gracefully when it must."[4] It draws on certain resources of the system and on "dynamic attributes of those resources (robustness, redundancy, rapidity)."[5] This perspective allows a proactive approach to building resilience by means of accumulating necessary resources in a system and ensuring that those resources possess the dynamic attributes required at a time when disruptions occur. System managers can thereby devise policies (e.g. principles, norms and standards, priorities of investments) which are conducive to resilience. This is particularly applicable to enhancing cybersecurity, which we cover later in this chapter.

The EU's Global Strategy defines resilience abroad as "the ability of states and societies to reform thus withstanding and recovering from internal and external crises,"[6] which aligns well with the generic definitions of resilience described above. It reflects the EU understanding that resilience is about capacities for change, adaptation and recovery. The emphasis on reforms flows from one of the key strengths of the EU—projection of its 'soft,' normative power to stabilize, reform and transform countries seeking

---

hagen Journal of Asian Studies, Vol. 27, No. 2 (2009):109–128; Seymour Spilerman and Guy Stecklov, "Societal Responses to Terrorist Attacks," *The Annual Review of Sociology*, Vol. 35 (2009):167–189; Arjen Boin and Allan McConnell, "Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience," *Journal of Contingencies and Crisis Management*, Vol. 15, No. 1 (2007):50–59; and Frank Furedi, "The Changing Meaning of Disaster," *Area*, Vol. 39, No. 4 (2007):482–489.

[3] Fran H. Norris, Susan P. Stevens, Betty Pfefferbaum, Karen F. Wyche and Rose L. Pfefferbaum, "Community Resilience as a Metaphor, Theory, Set of Capacities, and Strategy for Disaster Readiness," *American Journal of Community Psychology*, Vol. 41 (2008):130.

[4] Brad Allenby and Jonathan Fink, "Toward Inherently Secure and Resilient Societies," *Science*, Vol. 309, Issue 5737 (2005):1034.

[5] Fran H. Norris et al, "Community Resilience as a Metaphor, Theory, Set of Capacities, and Strategy for Disaster Readiness," p. 135.

[6] "Shared Vision, Common Action: A Stronger Europe," *A Global Strategy for the European Union's Foreign and Security Policy*, June 2016, p. 23. http://europa.eu/globalstrategy/sites/globalstrategy/files/about/eugs_review_web.pdf

membership or association status. However, when it comes to resilience at home, it speaks of critical infrastructure, networks and services more than of the values, norms, institutions or reforms, taking them as a given rather than something which needs to be protected against the attempts to hollow out and erode member states from within.

NATO also sets its emphasis on infrastructure, civil preparedness, continuity of services, accumulation of reserves and ensuring access to them as well as on various procedures facilitating rapid crisis response. Its major concern is that the Alliance has come to rely heavily on the private sector when moving, deploying and sustaining its forces; therefore it devotes much attention to civilian capabilities and civil-military interaction. This is understandable given its role as a "military responder" and "force multiplier" in military conflicts. Just as the EU, it should not, however, neglect its role in helping countries—both allies and partners—maintain their ability to reform themselves in the face of adversity. After all, as the Warsaw Summit statement states, "The foundation of our resilience lies in our shared commitment to the principles of individual liberty, democracy, human rights, and the rule of law."[7] Should this commitment fall apart, the Alliance's cohesion, solidarity and very existence will be endangered.

As noted by Jamie Shea, NATO's and EU's roles in buttressing resilience of most vulnerable and exposed countries often overlap,[8] particularly in such areas as cyber security, strategic communication, civil preparedness and countering Russia's hybrid warfare. Although Russia's hybrid warfare techniques have been extensively analysed, it is difficult to anticipate when, where and what types of stressors will be created and exploited by Moscow—or any other adversaries—in order to coerce target countries. Russia's approach typically combines both applying a long-term pressure (e.g., hostile propaganda and economic warfare) and opportunistically administering short-term sudden shocks, making it impossible to identify only a single set of capacities needed to cope with its hybrid strategy. A broad-based resilience of potential targets—allies and partners alike—which addresses a wide range of vulnerabilities to both chronic and acute stressors is of vital importance if NATO, in cooperation with the EU,

---

[7] North Atlantic Council "Commitment to Enhance Resilience," July 2016, http://www.nato.int/cps/en/natohq/official_texts_133180.htm

[8] Jamie Shea, "Resilience: a Core Element of Collective Defence," *NATO Review*, 2016. http://www.nato.int/docu/Review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/index.htm

seeks to deny Moscow the achievement of its political and strategic objectives in relation to the Alliance and its partners.

Equally important is a proper appreciation by the Alliance that Russia will constantly aim to undermine NATO's legitimacy and credibility, so that individual nations feel helpless and having no choice but to acquiesce to Moscow's geopolitical demands. The efforts of the Alliance—through its strategic communication, public diplomacy and outreach—to ensure high levels of trust in and support to its core tasks, policies and strategies among the general public of the allies and partners, as well as constant reassurance that "no one will be left behind" in the face of adversity, are fundamental to countering this. It is as much about the upstream effort of NATO to remain legitimate, relevant, visible, cohesive and credible as about downstream buttressing of the most exposed or vulnerable nations (so-called "forward resilience").

Resilience as Part of Deterrence by Denial

In broader strategic terms, resilience can be seen as an ingredient of deterrence by denial, or "persuading the enemy not to attack by convincing him that his attack will be defeated—that is, that he will not be able to achieve his operational objectives."[9] Hybrid warfare strategy—essentially a strategy aiming to cause disruption, confusion, destabilization and paralysis (i.e., shape the behavior of a target nation)—can be countered by demonstrating that all those aims are beyond reach due to the target's resilience. For instance:

- A high level of a society's competence in critical thinking and in understanding the nature of such hybrid warfare tools as hostile propaganda, political extremism, social protest campaigns or military intimidation—in conjunction with society's trust in the integrity of the political system, political leadership and government's communication—negate the advantages of those tools.
- A strong sense of belonging to a community, citizen empowerment and economic equity as well as of the available mutual support reduces the potential for dividing and polarizing the society and for turning various society's groups against one another and against the nation's institutions.

---

[9] David Yost, "Debating Security Strategies," *NATO Review*, Winter (2003), http://www.nato.int/docu/review/2003/issue4/english/art4.html.

- A high level of voluntarism and civic participation in the nation's affairs, when harvested by national security and defense organizations, substantially strengthens those organizations in the face of adversity.
- Measures aimed at severely disrupting economic activities (e.g., sanctions, energy supply disruptions, financial destabilization, etc.) fail to achieve the long-term desired effect when encountering high levels of economic development and diversification.
- The ability of critical infrastructure, including communication and information systems, to absorb the impact of sabotage or attacks, quickly adapt and continue delivering satisfactory level of services renders rather futile the attempts to exert pressure via this avenue.
- Sufficient and rapidly accessible reserves of financial capital, basic necessities (such as food, fuel, medical supplies) and technical resources (e.g., spare parts and materials for maintaining and repairing infrastructure) ensure that sudden shocks caused by aggressor do not translate into a negative impact on the nation's will to persevere.

The operational challenge lies in demonstrating convincingly that vulnerabilities are truly absent and that a particular society is indeed very resilient in all respects. This starts with the society being cognisant of its own vulnerabilities in the first place and then working to eliminate them. The problem in this regard is that the process of addressing various vulnerabilities may affect various power relations in the nations and, therefore, we "must always address the question of who are the winners and losers of ongoing processes of building social resilience."[10] Some of those losers are bound to become, consciously or not, natural allies of an aggressor in a hybrid conflict—something which is evident not only in countries such as Ukraine or Georgia but even among the political or economic elites of some NATO allies.

Last, but not least, deterrence—by denial or in any other form—lies in the eye of the beholder, which means that an adversary must be sufficiently convinced that its target society is too resilient to succumb to the hybrid warfare approach. This is difficult to achieve, given that each adversary is driven by own logic, rationality and calculations and may assess target's resilience very differently. This, in turn, means that Russia may never stop trying to identify vulnerabilities and then constantly testing and probing

[10] Markus Keck and Patrick Sakdapolrak, "What is Social Resilience? Lessons Learned and the Way Forward," *Erdkunde*, Vol. 67, No. 1 (2013):12.

a targeted nation. The Alliance, therefore, must develop and continuously maintain deep and sophisticated understanding about the individual Allies and partners in terms of their vulnerabilities, resources, capacities and potential political losers of resilience, as well as about the thinking and calculations of Moscow with regard to those vulnerabilities.

The Alliance's emerging strong emphasis on the cyber domain is one of the areas where NATO can leverage its collective power to address critical vulnerabilities of individual allies and partners and to bolster their resilience. Potentially, this is one of the most promising sectors where civil-military synergies, public-private partnerships, EU-NATO cooperation and involvement of NATO's partners can be pursued to achieve the desired effect. It is also the sector where the negative impact (e.g. debilitating and paralysing cyber attacks) would reverberate across multiple sectors of individual nations (financial systems, industrial production and distribution, energy supply, foreign trade, government services, media communications, etc.) and which, therefore, is quite central to maintaining overall national resilience. We turn to examining policies and measures in this domain which NATO is applying, or could apply, to enhance cyber resilience of the Allies and partner nations.

Enhancing Cyber Defense as Part of the Alliance's Resilience

NATO's collective defense principle encompasses hybrid and cyber threats in addition to conventional threats. At the Wales Summit in 2014 the Alliance declared that cyber attacks against one ally may lead to the invocation of article 5 with a possibility to respond by any means, including military force. At the Warsaw Summit in June 2016 NATO recognized that cyberspace constitutes a military domain and the Alliance must deter potential adversaries and defend itself in cyberspace just like it does in land, sea or air. In practice this means that NATO must develop cyber capabilities that would provide credible deterrence and defense against cyber attacks. As a first step, NATO should develop a clear doctrinal framework and procedures, as well as command structure that would allow for the use of cyber capabilities in a standalone role in NATO missions and operations. However, a caveat to keep in mind is that even though cyber defense is part of NATO's core task collective defense, the Alliance's mandate is only defensive and it will not develop offensive cyber capabilities (notwithstanding national offensive capabilities that could be deployed on

NATO's operations). Since effective cyber defense is not plausible without employing responsive defense (versus passive measures, that remain into organization's own networks), it remains to be seen how allies are going to fulfil this task.

So far a key priority for NATO has been the protection of infrastructures, systems and networks owned by NATO's organizations, comprising over 50 sites. Acknowledging that cyber defense is only as strong as a weakest connected node to the Alliance's networks, at the Warsaw Summit nations pledged to increase the protection of national communication and information systems and critical civilian infrastructures. Just as defending their societies against hybrid threats is the responsibility of individual allies, so too is cyber defense. Unfortunately notable gaps in the development of capacities and capabilities across allied nations pose a considerable vulnerability to everyone. Therefore it is in the interest of all that NATO assesses and guides those countries lagging behind. Weak member states could free-ride without investing in cyber defense self-protection and rapid response measures, while advanced nations would be obliged to provide assistance under the mutual defense clause.

Therefore, to ensure a uniform level of cyber defense across the Alliance, nations agreed to augment financial and other resources allocated to the development of national capacity and capabilities, speed up the implementation of cyber defense capability targets in the framework of NATO's defense planning process (NDPP), as well as improve skills and expertise, information and intelligence sharing. The Allies have also agreed to implement baseline security requirements in protecting their critical civilian infrastructures upon which NATO systems depend on, and NATO has the ability to monitor progress in achieving the agreed goals. The Cyber Defense Pledge should hence alleviate concerns related to uneven burden sharing among nations, and if implemented, help to mitigate vulnerabilities related to the inter-connectedness of networks and infrastructures. Its purpose is to ensure that weak member states are able to respond to cyber attacks in a timely and effective manner. Identifying and patching vulnerabilities would also strengthen deterrence against cyber attacks.

In addition to these measures, NATO reinforced its support to national authorities in protecting their critical civilian infrastructures and energy supplies against hybrid and cyber threats.[11] The Alliance's understanding of resilience includes not only military defense, but also non-military dimensions, including hybrid and cyber threats. NATO's concept of resilience

focuses on civil preparedness that includes security of critical infrastructures, continuity of essential services and government, as well as civilian support to the military.[12] This approach has common features with a Cold War era concept of total defense that also underlined civil preparedness, and with comprehensive and whole-of-society approaches to security and defense that focus on cooperation with the private sector and civil society. As discussed earlier, NATO links resilience to liberal democratic values as a shared foundation, however, it omits threats related to the cognitive dimension (e.g., information and psychological operations) that in the Eastern view constitute part of a broader informational domain and are used in combination with cyber attacks in peacetime and during conflicts.

Due to interdependencies of communication and information systems, and critical infrastructures, resilience can only be developed through an integrated approach. Disruptions of host nation and coalition partner networks and critical infrastructure upon which NATO depends can degrade NATO's ability to conduct operations. Secondly, projecting cyber defense beyond NATO's territory would help to define global cyber security norms and behaviors around liberal democratic values. In recognising this indivisibility of security, the NATO-EU Joint Declaration, signed in Warsaw, stresses the need to "foster the resilience of our partners" through individually tailored projects.[13] Indeed, NATO should project its soft side of cyber power in its neighborhood and globally with an aim to expand secure, open and free cyberspace and advocating democratic liberal values in cyberspace.

NATO has a wide range of cooperation formats with more than 40 partners. These partnerships can be leveraged and further expanded according to cyber defense needs of individual partners.[14] For example, in the existing framework of the Partnership for Peace Planning and Review Process, Georgia, Moldova, Iraq, Jordan have included cyber defense aspects into their capacity-building packages.[15] Non-NATO nations also participate in Smart Defense projects such as Multinational

---

[11] Paragraph 135 of Warsaw Summit Communiqué. http://www.nato.int/cps/en/natohq/official_texts_133169.htm.

[12] Paragraph 73 of Warsaw Summit Communiqué. http://www.nato.int/cps/en/natohq/official_texts_133169.htm.

[13] NATO-EU Joint Declaration. http://www.nato.int/cps/en/natohq/official_texts_133163.htm

[14] There are four geographic patrneship cooperation formats: Partnership for Peace (includes 22 states), Istanbul Cooperation Initiative (4 states), Mediterranean Dialogue (7 states), and Partners Across the Globe (8 states).

[15] http://www.nato.int/cps/en/natohq/topics_68277.htm.

Cyber Defense Capability Development (MNCD2), which focuses on sharing technical information, situational awareness and creating a cyber security assessment team.[16] They have participated at NATO cyber defense and crisis management exercises, and at technical exercises run by the NATO Cooperative Cyber Defense of Excellence. It is possible to include cyber defense issues in their consultations with NATO bodies (28+ meetings) and through staff-to-staff talks. Lastly, NATO educational bodies provide training courses on strategic, operational and technical levels to partners with requisite security clearances.

To further enhance its assistance to partner countries NATO should identify, via cooperation with the research community and recipient countries, individual cyber defense needs in the areas of material and non-material resources, knowledge, expertise, and information sharing. The first area where NATO should consolidate more efforts is increasing interoperability of partners' cyber defense capabilities, communication and information systems and networks, as well as information and threat assessment exchange protocols. Allied Command Transformation maintains that interoperability of communication and information systems upon which NATO's command structure depends is a key element in developing forward presence.[17]

In 2014 the Alliance established the Partnership Interoperability Initiative and the Defense and Related Security Capacity Building programs in order to increase interoperability with partners. To attract more partners NATO should cut red tape by simplifying application processes and procedures to these programs, as well as create additional tailored programs based on individual needs of partners. The Alliance has recently developed an Individually Tailored Roadmap Capstone Concept that should simplify existing partnership programs and improve cooperation by increasing shared situational awareness and trust. Pilot projects that include cyber defense aspects have been launched with Finland, Georgia and Jordan.[18]

---

[16] Multinational Cyber Defence Capability Development (MNCD2), http://academia-militar.pt/images/CDSDP2016/Apresentacoes/1.NATO-CD-Smart-Defence-Projects_MNCD2.pdf. Other Smart Defense projects in cyber defense are the Malware Information Sharing Platform (MISP) and the Multinational Cyber Defence Education and Training (MN CD E&T) project.

[17] Remarks by Jeffrey Lofgren on 7 June 2016 at NITEC2016, Tallinn. http://www.nitec.nato.int/wp-content/uploads/2016/06/NITEC-16-PROGRAMME.pdf.

[18] Joint press conference by Petr Pavel, Curtis Scaparrotti and Denis Mercier, 18 May 2016, http://www.nato.int/cps/en/natohq/opinions_131048.htm?selectedLocale=en.

Another model of how NATO and coalition partners have worked together to improve interoperability and information sharing in operations, exercises and training events is NATO's Federated Mission Networking (FMN). The framework includes policy, processes, procedures, standards and physical components such as static and deployed networks, services and supporting infrastructures.[19]

Sensitivity related to offensive cyber capabilities and fear of disclosing one's own vulnerabilities have been obstacles in fostering trust that is fundamental for cooperation, and especially information and intelligence sharing. NATO should work closely with partners to expand mutual information and threat assessment sharing, a critical aspect of defending against hybrid and cyber threats. NATO and EU agreed at the Warsaw Summit to share information and—to the extent possible—intelligence between staffs, cooperate on strategic communication, and expand existing cooperation on cyber security and defense, including operations, exercises and training. The EU has a wide toolbox of strategies, policies, procedures and technical measures to support non-military aspects of cyber security in member states and partner countries.

The alliance's Cyber Threat Assessment Cell integrates technical data from NATO sources with threat assessments provided by Allied countries.[20] Situational awareness on cyber threats merging technical data with a strategic view should be shared with selected partners that have concluded agreements on information sharing with the Alliance. It has been recommended in the past that NATO should expand its current cyber intelligence capacity and build up a capacity to coordinate responses to cyber crisis.[21] Considering that a cyber crisis in the neighborhood can affect NATO's ability to lead operations, coordination of responses to cyber attacks is necessary.

Partners should be engaged also in the areas of early warning, prevention, and analysis of cyber threats. It has been likewise recommended that NATO should establish forward presence teams in the Baltic states to sup-

---

[19] Federated Mission Networking http://www.act.nato.int/fmn.

[20] Remarks by Sorin Ducaru, Assistant Secretary General for Emerging Security Challenges, NATO on 7 June 2016 at NITEC2016, Tallinn.

[21] Jason Healy and Leendert van Bochover, "Strategic Cyber Early Warning: A Phased Adaptive Approach for NATO", Atlantic Council issue brief, 2012; and Jason Healy and Klara Jordan Tothova, "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow," Atlantic Council issue brief, September 2014.

port them to counter hybrid threats.[22] Since NATO partners' values and degrees of interest in cooperation with the Alliance vary, in countries that show desire, NATO could deploy Cyber Vulnerability Assessment Teams with a task to identify vulnerabilities in their networks, increase interoperability and establish coordination relationships for crisis response. In case of emerging cyber crisis that is likely to affect NATO's operations or organizations, the Alliance could deploy Cyber Rapid Reaction Teams as part of broader Resilience Support Teams.[23] These measures would also allow identifying cross-border and cross-sector interdependencies of critical infrastructures upon which NATO depends on.

Agreements with national and military computer emergency teams of partner countries to exchange technical threat information should be concluded with NATO Computer Incident Response Capability (NCIRC). NATO has concluded such agreement with the EU, but information sharing with the EU should be expanded to include nontechnical sensitive information.[24] For example, NATO Cyber Threat Assessment Cell should share best practices with EU's Hybrid Fusion Cell, and NATO Cooperative Cyber Defense Center of Excellence with the Hybrid Threats Center of Excellence when the latter will be established in Finland.

Selected partners with high-end cyber capabilities and established trust-based cooperation (like Finland, Austria, Sweden, Switzerland, Ireland, Australia and New Zealand) should be granted more opportunities. They have participated and observed NATO's cyber defense exercise Cyber Coalition. Host Nation support agreements that Finland and Sweden have concluded with NATO for crisis assistance should include the possibility to exchange cyber information, cooperate on threat and vulnerability assessments, and coordinate responses to cyber crisis. Finland and Sweden have joined the NATO Cooperative Cyber Defense Center of Excellence, and Austria is a contributing nation.[25]

If cooperation may be challenging in highly sensitive areas information and intelligence exchange, cooperation should be encouraged in educational and training activities that help to increase trust, build up knowledge

---

[22] F. Kramer and B. Craddock, "How NATO Can Defend the Baltics from Conventional and Hybrid Attacks," 16 May 2016, Atlantic Council, http://www.atlanticcouncil.org/blogs/natosource/yes-nato-can-succeed-in-defending-the-baltics.

[23] Ibid.

[24] http://www.nato.int/cps/en/natolive/news_127836.htm?selectedLocale=en.

[25] Sweden is contributing a national expert and has decided to join the Center.

base and skills sets. NATO should further expand partners' engagement in its exercises and training, for example, partners could hold national and regional technical exercises at the NATO's cyber range. NATO should also facilitate assistance from advanced Allies to develop partner countries' cyber capacity. Allies have provided cyber-defense-related training and material support to Ukraine under the NATO-Ukraine trust fund.

Cyber threats defy organizational borders, most critical infrastructure is operated by the private sector, and various non-state actors yield significant power, knowledge and expertise in cyberspace. As noted above, bolstering resilience can be achieved only through an integrated approach involving key stakeholders. NATO has engaged industry in its cyber defense activities through the NATO Cyber Industry Partnership.[26] Technical agreements on information sharing and improving situational awareness have been concluded with cyber security companies such as Symantec, Cisco, Fortinet and others, and industry also participate in NATO exercises and trainings, as well as Smart Defense Projects.[27] The Alliance should continue leveraging its partnership with industry and provide grants to research community in order to conduct projects in target countries to help them to ensure cyber defense.

Recommendations

- The Alliance should develop and continuously maintain a comprehensive picture of the vulnerabilities of allies and partners to 'hybrid warfare' scenarios and tailor its resilience-building assistance measures to the needs of particular nations. However, it should remain cognisant that national resilience is the responsibility of the national governments.
- The Alliance should establish a comprehensive system of national resilience indicators (Resilience Monitor/Index), covering all relevant domains, to monitor and assess the overall state of resilience in individual nations. This would provide a basis for more focused and specific measures—at the national and NATO levels—to address the short, medium and long-term needs.
- Although NATO is paying most attention to infrastructure, networks and civil preparedness, it should also include societal resilience into

[26] http://www.nicp.nato.int/.

[27] NATO's Cyber Defence, 27 Juy 2016. http://www.nato.int/cps/en/natohq/topics_78170.htm.

its monitoring, assessment and support measures. This is particularly important from the perspective of maintaining the Alliance's credibility, cohesion, unity and public support to its mission.

- Much more effort has to be dedicated by NATO and the EU to studying and understanding what deters Moscow, how it assesses vulnerabilities of target countries and how it seeks to exploit those vulnerabilities to its strategic ends. This has to be linked with early warning and strategic anticipation efforts.
- NATO should establish individually-tailored projects and expand existing projects in accordance with interests and capacities of partners to enhance their cyber security and defense. Prospective cooperation areas in cyber defense include increasing interoperability, sharing strategic and technical information and threat assessments, coordinating responses to cyber crisis, and engaging partners into NATO's education, exercises and training activities.
- NATO should consider establishing special cyber support teams that can be deployed to partner countries with the aim to increase interoperability, improve information sharing and coordinate crisis response.
- To support NATO Allies' resilience in the cyber security context cyber experts should be included into NATO Force Integration Units (NFIU). This would help assess vulnerabilities, increase preparedness and interoperability in regards with crisis response.
- To support projecting resilience in NATO partner nations NATO and the EU should first assess the levels of the existing maturity of cyber security and defense capacity in the target countries. They should coordinate and synchronize mutual training and assistance projects in order to avoid overlapping. Partnership Review and Planning Process (PARP) should include as part of broader resilience also cyber defense elements, and planning should to be aligned with the NATO Defense Planning Process (NDPP).
- Partners would benefit from the development of minimal requirements for the protection of their critical infrastructure and in regards with cyber defense.
- NATO allies should develop a clear political guidance concerning which activities will be open for different partners, taking into consideration willingness of an individual partner to cooperate with the Alliance, as well as their maturity level. Some partners should be

engaged into partnerships with industry and into various NATO's education and training efforts (cyber defense courses, cyber ranges, cyber hygiene platforms, etc.). Some parters should be engaged in planning phases of crisis management and cyber defense exercises. Engagement in these activities and in the Federated Mission Networking should be widened beyond the current range of seven partners.

- While common funding of partnership activities and the establishment of trust remains challenging along with management difficulties of common endeavors, NATO could facilitate a lead/framework nation approach that would contribute to the setting up of specific trust funds and tailored training projects. A lead nation could promote specific projects, task and working groups where other nations could plug in.
- In addition to providing technical cyber defense training, consulting partner nations on how to develop their national cyber security and defense programmes, policies and strategies would contribute to the development of common terminology and increase partners' understanding of cyber threats, as well as promote adherence to fundamental democratic values in cyberspace activities.

Chapter 10

Forward Resilience in the Age of Hybrid Threats: The Role of European Intelligence

Björn Fägersten

Discussions on hybrid warfare and hybrid threats have dominated the European security debate in recent years.[1] Hybrid threats usually refer to a coordinated mixture of military and non-military and covert and overt means in order to reach specified objectives. As such, hybrid tactics are about increasing uncertainty in a conflict situation, blurring the line between war and peace and between aggressor and victim. Intelligence work is one important tool that can be used to reduce the uncertainty that characterizes security policy in general and hybrid threats in particular. How can national and international means be employed to counter hybrid threats? What are the main vulnerabilities of European states and the resilience needed to withstand hybrid threats and tactics?

Hybrid Threats and Intelligence

The European Union (EU) increasingly functions as a security provider. While Article 4(2) of the Treaty on the European Union makes it clear that national security is the prerogative of member states, other measures and policies in the realm of security have been added incrementally to the Union's remit. With activities in the field of safety, internal security, external crisis management, and civil protection, the Union is effectively closing in on the vague concept of national security.

When national governments, and increasingly the European Union, make decisions relating to security they do so under conditions of uncertainty—who is the enemy, what course of action is most suitable, and what long-term effects can be envisioned. In an age of hybrid war and threats, this uncertainty is bound to increase. One key element in countering hybrid threats is reducing the level of uncertainty. This can be facilitated by independent media, strong academia, civil society, and so forth. But

[1] I would like to thank Costan Barzanje and Denise Peters for excellent research assistance in preparation of this chapter.

governments can employ intelligence[2] agencies to reduce uncertainty in areas where other knowledge producing functions are insufficient.

This chapter discusses how intelligence efforts—national as well as international—can be employed to build resilience in the face of hybrid threats. To grasp the role of intelligence as a tool, I will first look at the vulnerabilities of European states and the resilience needed to withstand hybrid threats and tactics.

Vulnerability and Forward Resilience

Modern Western states have specific societal vulnerabilities in the face of hybrid threats.[3] Indeed, one can argue that within this larger group, the northern states with open societies, trade-dependent economies, and a relative lack of domestic strategic resources stand out among Western societies.[4]

A first area of vulnerability is the political cohesion within vital cooperation forums. For most European countries this would constitute a mix between the European Union, NATO and the OSCE. Political cohesion within these bodies, and especially the EU and NATO, is a precondition for the management of common political and security problems. The risk of decreased decision-making capacity within these bodies due to hybrid tactics—by, for example, supporting fringe parties, co-opting weak national leaders or dividing countries by modes of negotiation—constitutes a considerable vulnerability.[5]

A second area would be control of territory and critical infrastructure. Ukraine, and the annexation of the Ukrainian region of Crimea, illustrates

---

[2] Intelligence agencies can be distinguished from these other functions in regards to *security* and *secrecy*. The first implies that intelligence agencies are foremost interested in questions that pertain to security—be it human, national or international. The second—secrecy—has a dual meaning as it applies to the often concealed and protected nature of the sought information as well as the stealthy manner in which intelligence organizations tries to acquire this information.

[3] For an overview, see Claudia Major and Christian Mölling, *A Hybrid Security Policy for Europe*. SWP Comments, 2015/C (22), 2015.

[4] See for example Mika Aaltola, "Forward Resilience and Networked Capabilities: Finland's Softer Power Tools in the Wake of Ukraine," in Daniel S. Hamilton, Andras Simonyi, Debra L. Cagan, eds., *Advancing U.S.-Nordic-Baltic Security Cooperation*. Washington, DC: Center for Transatlantic Relations, 2014, available at: http://transatlanticrelations.org/ [Accessed November 23, 2016].

[5] Major and Mölling, *op. cit*.

the territorial threat of hybrid tactics. The abduction and detention of an Estonian security official on Estonian territory proves that even EU members encounter threats on, and ultimately to, their territory. Cyberattacks on critical infrastructure such as Sweden's air control systems or Germany's parliament proves that vulnerabilities regarding state control are not limited to physical territory.

Third, Western societies are vulnerable in the area of societal cohesion. Religious and ideological radicalization, ethnic conflict and minority conflicts can be instigated by external actors in a hybrid conflict situation either through support of specific groups or by efforts to fuel conflicts among groups. Last, and as indicated initially, Western societies are hugely dependent on a variety of global flows. Ever more interdependent, European states—and those in the north in particular—need to manage flows of energy, data and capital and secure the access points to these flows.[6]

The ability of states to resist and recover from disturbances regarding the vulnerabilities outlined above is referred to as resilience in this chapter. As such, resilience is a perishable shock-absorbing capacity at the national level. However, growing interdependencies means that resilience is not merely a national affair, and neither is it confined to current interdependencies—others may emerge over time. The term *forward resilience* has been suggested to cover these spatial and temporal extensions of the concept.[7] The spatial dimension relates to the fact that just as with sovereignty, resilience is today shared over borders. All of the vulnerabilities suggested above have clear transboundary logics. For European political cohesion and flow security it is rather obvious, as they are transnational by nature. But territorial control is also shared in Europe today, as the migration crisis has illustrated. Critical infrastructures are interwoven where, for example, the resilience of one state's air control capacity is a security concern for all. And societal cohesion is linked as well, as many of radical elements cooperate and operate across borders. The temporal dimension relates to the fact that the threats pinpointing the above vulnerabilities can be addressed along a wide continuum ranging from forecasting and trend analysis via current operations to post-event analysis and adaptation.

---

[6] Aaltola, *op. cit*.

[7] See Daniel S. Hamilton's chapter in this volume for further discussion of the concept of forward resilience.

Hybrid Threats and Forward Resilience in EU Strategy

The transboundary nature of the hybrid threats outlined above has increasingly been addressed in the European Union by propositioning conjoint measures to foster resilience. To this end, the European Commission and the High Representative adopted a Joint Framework on countering hybrid threats in April 2016.[8] The Framework lists four areas along with an action plan of 22 measures where development at both EU and member state level should be made in order counter hybrid threats. The four main areas in the framework are 1) raising awareness, 2) building resilience, 3) preventing, responding, and recovering from crisis 4) stepping up cooperation with NATO and other organizations. Many of the suggested actions are to be included in projects already in force or undergoing implementation. The actions also call for member state cooperation and action since the Framework applies in context of the Common Foreign and Security Policy (CFSP), and thus rely on competence that lies within the national sphere. Some of the measures that have already been taken in a response to the Framework include the introduction of a Hybrid Fusion Cell, the launch of a contractual Public-Private Partnership (cPPP) for cybersecurity, the signing of a code of conduct with Facebook, Twitter, YouTube and Microsoft to prevent radicalization, and the signing of a joint declaration between the EU and NATO calling for further cooperation on countering hybrid threats.[9]

In June 2016 the EU also launched its new Global Strategy for the European Union's Foreign and Security policy (EUGS).[10] In the EUGS, the EU elaborates an integrated approach linking internal resilience with EU's external actions, noting that "security at home depends on peace beyond our borders," and accordingly places geographical priority from Central Asia to Central Africa. Given the current turbulence in the region, ranging from the prevailing Russian threat to terrorism to refugee flows, the Strategy emphasizes that one of the key strategic priorities of the EU

---

[8] European Commission, *Joint Framework on Countering Hybrid Threats*. Brussels: European Union, April 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018 [Accessed November 23, 2016].

[9] The Council of the European Union, *CFSP Report—Our Priorities in 2016* (Document: 13026/16) General Secretariat of the Council: Brussels, 2016, available at http://data.consilium.europa.eu/doc/document/ST-13026-2016-INIT/en/pdf [Accessed November 23, 2016].

[10] European Union, *A Global Strategy for the European Union's Foreign and Security Policy*. Brussels: European Union, 2016, https://eeas.europa.eu/top_stories/pdf/eugs_review_web.pdf [Accessed November 23, 2016].

is to invest in state and societal resilience by strengthening the capacity of the EU and its neighbors to withstand internal and external crisis. The EUGS Implementation Plan,[11] released on November 14, 2016, presents implementation proposals to the EUGS in the area of security and defense. Both the EUGS and its Implementation Plan describe a Europe that needs to adapt and update its take on security. In this endeavor, the countering of hybrid threats play an important role, and much effort is being put into increasing expertise and assistance to partners through strategic communication and better cyber security along with the protection of networks, critical infrastructure, and energy security. The Plan proposes resilience as a method to counter hybrid threats and stresses the need for common analysis of crisis and coherent and comprehensive joined-up action.

Concerning resilience, the EU is developing an equal amount of strategies in terms of strengthening the ability of its member states and partners to handle crises, and to efforts to prevent such crises from happening. For that reason the concept of resilience was included in the Joint Framework previously mentioned. It was also addressed in the EUGS and the ensuing Implementation Plan. The means of implementation for enhancing resilience are proposed as strategic operational actions aimed at increasing cooperation in security by establishing mechanisms for exchange of information and by coordinating actions to deliver strategic communication, address strategic vulnerabilities in strategic and critical sectors such as cybersecurity and critical infrastructures, and by preparing for coordinated responses by defining effective procedures to follow.

These strategic actions are prevalent, for instance, in EU ambitions to further develop its strategic partnerships. Here NATO, the UN, OSCE and the African Union are of great importance. For example, efforts to implement the jointly agreed priority areas for strengthening the UN-EU Strategic Partnership on Peacekeeping and Crisis Management will be made. The EU and the OSCE will also enhance their common work on operational capabilities, promotion of stability, inviolability of borders, adherence to human rights and fundamental freedoms, rule of law, media freedom, and fair democratic elections. In addition, the next EU-Africa Summit will offer a potential opportunity to reconsider the Peace and Security Partnership between the two sister organizations in light of the renewed approach to capacity building in the field of security. Furthermore,

[11] European Commission, *Implementation Plan on Security and Defence.* Brussels: European Union, 2016, https://eeas.europa.eu/sites/eeas/files/eugs_implementation_plan_st14392.en16_0.pdf. Accessed November 23, 2016.

special consideration is to be given to the Common Security and Defense Policy's (CSDP) partnerships with partner countries that share EU values and are able and willing to contribute to CSDP missions and operations to promote resilience in the EU's surrounding regions. The importance of security in the Review of the European Neighborhood Policy (ENP)[12] and the forthcoming initiative on resilience-building as part of the broader implementation of the EUGS should also be taken into account. Moreover, the EU looks into enabling a more rapid response in the event of a crisis. Accordingly, it seeks to improve the usability and deployability of the EU's rapid response toolbox where synergies with other high readiness initiatives, notably within NATO, will be made along with large-scale and regular live civil and military exercises and the development of a rapidly available common pool of strategic lift assets for the deployment of EU Battlegroups.

In relation to the resilience approach, above all, two questions have been heralded: 1) what does resilience and resilience-building actually mean; and 2) what are the implications of the rise and application of the resilience approach in EU policies.[13] However unclear what the concept of resilience entails and how it is to be applied, what is clear is that it has come to pose a challenge as a concept in its own right. Wolfgang Wagner and Rosanne Anholt concede that the dispersion of resilience in a range of fields has led to the confusion of what it supposed to mean. They do however acknowledge that the reason for its omnipresence in the EUGS is that it relates to a broad range of fields and referent objects, for example, externally it relates to the enhancement of resilience of states and societies in the EU's broad neighborhood, and internally by strengthening critical infrastructure, networks and services.[14]

Ana Juncos acknowledges the introduction of resilience in the EUGS's "principled pragmatism" approach as a move towards a more pragmatic foreign policy that allows for the EU to take into account both the need for cooperation and at the same time face competition on the part of other

---

[12] European Commission, *Joint Communication; Review of the European Neighbourhood Policy.* Brussels: European Union, 2015, https://eeas.europa.eu/enp/documents/2015/151118_joint-communication_review-of-the-enp_en.pdf. Accessed November 23, 2016.

[13] Ana Juncos, "Resilience As the New EU Foreign Policy Paradigm: A Pragmatist Turn?" *European Security*, online, 2016. Wolfgang Wagner and Rosanne Anholt, "Resilience As the EU Global Strategy's New Leitmotif: Pragmatic, Problematic or Promising?" *Contemporary Security Policy*, 37(3), 2016, pp.414-430. F. de Weijer, *Resilience: A Trojan Horse for a New Way of Thinking?* ECDPM Discussion Paper(139), (2013).

[14] Wagner and Anholt, *op. cit.*, p. 415.

international powers.[15] However, she finds the adding of "principled" to the pragmatic turn as problematic in its continued adherence to liberal logic and achievement of universal values."[16] As such, the EU is caught between two different logics—the old neo-liberal stance that considers threats, defense geopolitics and liberal intervention, and the new logic of risk, resilience, complexity and capacity-building. The principled pragmatism approach, she argues, will not only expose the EU to charges of arbitrariness and inconsistency in its external actions, it also risks undermining the principles it stands for by not corresponding to its normative standards.[17] In contrast, Wagner and Anholt appreciate resilience as a practical middle ground between an "over-ambitious liberal peace-building and under-ambitious objective of stability." Whereas the practicality of liberal peace poses an impractical endeavour, the adoption of stability as a new paradigm would stand in dire contrast to the idea of Europe as a normative power with the aim of promoting democracy, rule of law and human rights. Wagner and Anholt argue, however, that resilience, with its positive objective of focusing on solutions rather than on problems along with its disposition for practicality, has posed as the perfect middle ground.[18] Furthermore, they argue that resilience is far more cautious than liberal optimism and allows for an understanding of crisis as inevitable, if not imminent, and as such offers a means to balance expectations of what the EU can accomplish.[19]

However the concept of resilience may develop and be used in the EU context, the strategic ambition—as put forth in official documents—sseems to recognize the need to prioritize a mutual approach and combined effort to enhance resilience by anticipating crisis through risk assessment, focus on prevention and preparedness, and enhanced swift response and recovery from crisis.

Mapping the Roles of Intelligence

Having first discussed the hybrid threat and the vulnerability states face, and second the EUs strategic ambitions in the resilience field, what is the role of intelligence in building forward resilience? In this section I

---

[15] Juncos, *op. cit*., pp. 8, 11.

[16] Ibid., p. 11.

[17] Ibid., p. 13.

[18] Wagner and Anholt, *op. cit*., pp. 413, 417, 418.

[19] Ibid., p. 424.

will suggest four generic functions that intelligence services can perform in the face of hybrid threats.

Identify Vulnerabilities at Home and Abroad

In line with the overarching function of intelligence—to reduce uncertainty—intelligence agencies and security services have a key role in identifying the vulnerabilities within the societies and organizations they are tasked to protect. This could imply analysis of decision-making capacity within international security organizations, identify what parts of a country's critical infrastructure is most vulnerable and most likely to be targeted, follow the work and organization of radical political elements, and make assessments of flow dependency and security.

These tasks could be performed with a short time horizon in the form of a stress test of core societal functions or by long-term scenario analysis, i.e., spanning the temporal dimension of forward resilience. Likewise, analysis of other countries' vulnerabilities is common within intelligence work, either as collaborative effort or without cooperation from the target country.

Address Such Vulnerabilities at Home and Abroad

In many cases, intelligence agencies also have a role in the subsequent phase of addressing identified vulnerabilities. Tasks could be to shore up decision-making procedures, staging civil and military crisis exercises, secure access points that connect countries to global flows etc. This can be done well in advance (long-term training) or with a focus on immediate capacity improvement. Vulnerabilities can also be addressed abroad, for example through benchmarking and security sector reform. A good example is the way Western intelligence and security services helped reform their equivalents in eastern Europe prior to NATO and EU accession. This work was carried out bilaterally as well as multilaterally in forums such as Club de Bern and the Counter-Terrorism Group. By addressing vulnerabilities within the new members' security sector, security was improved both home and abroad and conditions for future security cooperation was met.

Warn Against and Monitor Hybrid Threats

Warning and monitoring is a fundamental task of intelligence and security services and relates to all of the vulnerabilities above. As in the tasks

above, warning and monitoring of threats can be done nationally, in cooperation with partners or even on behalf of unknowing partners. It could also be performed with a long time horizon as horizon scanning or early warning or as more immediate situational awareness. Collaborative warning and monitoring requires a shared understanding of vulnerabilities as well as perceptions of threats.

Counter Hybrid Tactics

Finally, intelligence and security services have a role in countering hybrid tactics as they take place. This could imply security services averting sabotage or intrusion of "little green men" or it could be intelligence agencies with offensive cyber capabilities that thwart ongoing attacks. While this is task that is played out in real time, it can be practiced and prepared, also in cooperation with partners.

Challenges of European Intelligence Cooperation

The section above outlined the roles of intelligence in building forward resilience to hybrid threats. Both the temporal and spatial dimensions of forward resilience demands functioning international cooperation in the intelligence field. In Europe, such cooperation has developed considerably over the last 15 years and now covers law-enforcement intelligence, security service cooperation on terrorism and internal security, as well as civil/military intelligence cooperation in support of foreign and security policy.[20] While cooperation has developed extensively—see the fact box—challenges prevail. Four challenges stand out when considering cooperation against hybrid threats.

Diverging Member State Interests

Countries share intelligence, or establish joint intelligence functions, if they believe this furthers their interests.[21] Economics of scale and the need to support common policy objectives often offer a rationale for cooperation. But other interests balance these benefits, such as the risk of expos-

---

[20] For a recent overview see Björn Fägersten, *Intelligence and decision-making within the Common Foreign and Security Policy*. Sieps, [online] 2015(22epa), 2015, available at http://www.sieps.se/sites/default/files/2015_22epa_eng.pdf, accessed November 23, 2016.

[21] Björn Fägersten, *For EU eyes only? Intelligence and European security*. EUISS, [online] (8), 2015, available at: http://www.iss.europa.eu/publications/detail/article/for-eu-eyes-only-intelligence-and-european-security/, accessed November 23, 2016.

Fact Box—EU Intelligence Structures

INTCEN—EU intelligence and situation centre: The main hub for intelligence analysis within the EU. Situated within the External Action Service, INTCEN produces reports and briefings based on contributions from the member states' intelligence services, material from other EU bodies and opens sources. INTCEN mainly provides intelligence support to the CFSP but also covers issues of an internal character such as counterterrorism.

INTDIR—Intelligence division of the EU military staff: Works closely with INTCEN but is solemnly devoted to military affairs. It reports to various bodies within the European External Action Service (EEAS) but particularly to the Military Committee. INTDIR often produces joint reports with INTCEN under a work format called Single Intelligence Analysis Capacity (SIAC).

EUROPOL—European Police Office: A hub for exchange and analysis of criminal intelligence. Information originates from member states, open sources and third parties such as international organizations and countries beyond the EU.

CTG—Counter Terrorism Group: Consists of EU member states together with Norway and Switzerland and is positioned outside of EU structures, even though it provides analysis to various EU decision-making bodies.

FRONTEX—The European border management agency: Functions as both a consumer and a producer of intelligence. Produces risk assessments on data received from national border authorities and other sources.

SATCEN—The EU Satellite Centre: Produces geospatial and imagery intelligence products on behalf of the High Representative of the Union for Foreign Affairs and Security Policy (HRVP). The primary sources of satellite data are commercial providers but SatCen has some access to national resources as well.

ing one's sources and methods, the risk of being deceived through cooperation or a concern for national autonomy. In sum, even in relation to hybrid threats and shared resilience, it has to be acknowledged that regardless of the sound economy of sharing and cooperating as well as an overall interest in furthering a specific joint policy or instrument, cooperating states will in some instances deem it counter to their interests to take part in common intelligence work.

Bureaucratic Resistance

Not only member states have interests, so do their intelligence professionals, and at times they differ considerably.[22] The reasons may vary. Cooperation may be impeded by different organizational cultures in the concerned countries. Equally important, professional cultures differ among police forces, security services and intelligence agencies, which is challenging in areas when these forces need to join up, such as in the counter-terrorism field. Bureaucratic self-interest plays a part as well, for example when new cooperative arrangements threaten investments in long-time personal networks. The sum of these bureaucratic factors implies that governments' ambitions do not always translate into reality. The short history of multilateral intelligence cooperation in Europe provides plenty of examples. The ambition to put Europol at the center of the fight against terrorism, repeated after most terrorist attacks on European soil, has for example been severely obstructed by the fact that national security and intelligence agencies have not been willing to strengthen their cooperation with a police body.

Lack of Cross-Sectoral Cooperation

One challenge of a more specific nature is the cross-sectoral demand that hybrid threats put on intelligence work. The fact that hybrid tactics spans several domains (civil society, cyber, the military realm, etc.) means that intelligence-sharing to counter these tactics must cover a broad range of actors and organizations. This is usually difficult enough to accomplish at the national level, and even more so on an international level.

Temporal Mismatch

An adjacent challenge is that of differing temporal perspectives in relation to hybrid threats. Looking at the information flows in support of EU foreign policy, there is, or at least there has been, a mismatch between the temporal dimensions of support and demand. Until now, intelligence support has been strongest in the short- to medium-term perspective, looking at issues three months to two years ahead. Current intelligence has been of a non-clandestine nature, essentially coverage of news reports and other open sources in real time. This is in contrast to the policy cycle of the EU's foreign policy, where most effort goes into either long-term structural

[22] Ibid.

reform programs or the deployment of civil and military missions where open source intelligence is not enough.[23]

Conclusions and Policy Recommendations

This chapter has discussed the hybrid threats that befall European countries and the increased levels of uncertainty they entail. One of the ways to respond to these threats is to build resilience at home and in partner countries and the strategic ambitions of the European Union in this field have thus been analyzed. Finally, the roles of national and international intelligence in supporting resilience have been outlined, as have the challenges that beset international intelligence cooperation. Based on this analysis, what could then be done in order to allow for improved intelligence support to resilience building at home and abroad?

First, one important contribution would be to establish genuine multilateral intelligence training. Many of the challenges to international intelligence cooperation and information sharing have roots in insufficient levels of trust and lack of knowledge of the bureaucratic and cultural procedures in partner countries and agencies. These often deep-rooted barriers to cooperation are difficult to circumvent by intuitional novelties or executive orders. They can, however, be mitigated by training, whereby individual officials learn the habit of multilateral intelligence. The EU IntCen, which now hosts the new hybrid fusion cell, already runs training modules for newly seconded analysts. This could rather easily be scaled up and offered to all new national recruits, not only those manning EU intelligence positions, but also to non-intelligence officers within the EU bureaucracy (such as analysts working in the external EU delegations), to NATO officials in order to familiarize officials with each other's systems and, to some extent, to analysts from security agencies in partner countries. Considering that intelligence support to resilience building needs to be done in coordination with other countries as well as other forms of agencies, joint training schemes would be an effective way to establish a solid base for such cooperation.

Second, more interaction between policymakers and intelligence analysts would allow for better appreciation of the roles and needs of each category. Much of the intelligence output from the EU system is today communicated in high-level briefings, by senior managers or analysts to

[23] Fägersten, supra note 15.

senior decision makers. Considering the time frame of these decision-makers, briefings are often focused on the most pressing issues of the moment. More interaction and perhaps new forms of interactions further down in the respective hierarchies would lay the ground for intelligence support in different temporal phases, allowing for example the intelligence branch to contribute also to long-term preventive work. Such low-level but continuous interaction would bridge the gaps between the different time horizons with which different parts of the EU bureaucracy work.

Third, more intelligence output within the EU system should be produced as open source, allowing for a more efficient response against hybrid tactics. As discussed above, the aim of hybrid tactics is to increase uncertainty in any given situation. The referent object of such uncertainty could be an official decision-maker but could also just as likely be the general public or more targeted individuals. Therefore, the value of correct information and threat analysis that is fast, open and easily verified is substantial. Considering that multilateral intelligence products rarely are based on the most sensitive information, the step towards making more of the output as open source should be manageable.

Last, also considering that intelligence support might be directed towards partner countries, and that the concept of resilience is rather vaguely defined in EU parlance as discussed above, it is vital that such support live up to the demands set by liberal democratic principles. Intelligence activities are in many political systems tied to oppression and stability of non-democratic regimes. While the Arab spring did not deliver the democratic transitions many hoped for, it did deliver a strong lesson for Western powers aiming to invest in stability in troubled countries of the region. To the extent that European intelligence resources are engaged in the projection of forward resilience, caution will have to guide mission design.

Chapter 11

Temporal Projection of Societal Resilience in the EU: A Dynamic Organization Approach

Tim Prior[1]

Systemic Societal Resilience, Connectivity, and Vulnerability in the EU

Modern Western societies are characterized by global connectedness. Connectedness generally strengthens social systems, yet it can also increase the exposure and sensitivity of social systems to disturbances (natural, technical, and social), because the increasing connectedness of social systems requires increasingly complex system-critical services like transport, communications, energy, finance, or regional security.[2]

The progressive increase in complexity of social-technical systems through time has mirrored a realization that perfect security is theoretical at best. Despite the evolution and sophistication of risk prevention practices (in both the private and public sectors), threats and hazards cannot be completely avoided, but measures to cope with disturbance can be established. In this context of imperfect societal security, advocating resilience has become a standard cross-scale approach, in many cases tagged on to traditional security policies, rather than being applied as a stand-alone approach.[3]

This brief chapter borrows a theoretical understanding of the nature of vulnerability (considering especially the interplay between sensitivity and exposure to risks and threats) in order to examine the notion of "for-

[1] With valuable contributions and suggestions from Aglaya Snetkov, Florian Roth, Andreas Wenger, Christian Nünlist, Oliver Thränert, Linda Maduz, all from the Center for Security Studies at ETH Zurich.

[2] L. K. Comfort, "Risk, Security, and Disaster Management," *Annual Review of Political Science* 8:335–356 (2005); Susan L. Cutter, "The Landscape of Disaster Resilience Indicators in the USA," *Natural Hazards* (2005), pp. 1–18. doi: 10.1007/s11069-015-1993-2.

[3] F. Roth and T. Prior, "The Boundaries of Building Societal Resilience: Responsibilization and Swiss Civil Defense in the Cold War," *Behemoth. A Journal on Civilisation* 7(2):91–111 (2014).

ward resilience" in the context of future security challenges in Europe. While Europe's security institutions are built around solidarity, member states are characterized by a set of specific socio-economic, cultural, technical, and political attributes. These attributes influence the countries' abilities to cope with different risks or threats, stressors and disturbances.[4] In this context an understanding of how these attributes translate into important systemic, Union-relevant vulnerabilities is fundamentally important for the resilience of the European Union (EU). As an open system of connected nations, systemically addressing and adapting to vulnerabilities, presents an atypical, but constructive, paradigm for addressing contemporary and future security challenges.

"Forward resilience" is here taken to reflect an approach to project resilience temporally from points of strength, where resources to support resilience exist, to points of vulnerability, in order to increase overall systemic resilience. We draw on several examples of security risks to explore attributions of vulnerability in the European Union. For the purposes of this chapter, we view the EU as systems of connections, where mobility and communication (two key elements influencing locations of exposure and sensitivity in the context of the security risk examined here) connectivity determine center and periphery from a vulnerability perspective, and which are not primarily geographical. In such systems, we suggest that systemic societal resilience, organized by the EU through ad-hoc and distributed foresight, is fundamental in building cross-Union solidarity to security risks, in addressing perceptions of Union vulnerability, and building capacity where necessary.

Vulnerability and Resilience

Very simply, vulnerability is interpreted in a negative sense as the "susceptibility to be harmed."[5] While in most contexts many factors influence whether someone or something will be harmed, vulnerability is often conceptually composed of three interrelated elements. To be vulnerable something must first be exposed to a risk or threat, and exposure is possibly the most obvious component of vulnerability. Second, to be vulnerable an entity must also be sensitive to the consequences of that risk or threat.

---

[4] N. Brooks, "Vulnerability, Risk and Adaptation: A Conceptual Framework," *Tyndall Centre for Climate Change Research Working Paper*, 38, pp. 1–16 (2003).

[5] W. N. Adger, "Vulnerability," *Global Environmental Change* 16(3):268–281 (2003). doi: 10.1016/j.gloenvcha.2006.02.006.

Third, vulnerability can be reduced by an entity's capacity (intrinsic or extrinsic) to adapt to the risk or threat to which it is exposed and sensitive, and is therefore also considered an influential element of vulnerability. Given the component nature of vulnerability, the magnitude of each component's influence on vulnerability changes with different risks or threats, and in the context of the entity exists.

By contrast, resilience is interpreted in a very positive sense as the ability of a system, person, or entity to withstand, bounce back and cope, and/or adapt to external (or internal) stress or disturbance. This positivity has propelled the popularity of resilience to the forefront of modern transformations in many aspects of security and safety politics (including disaster management, cyber security, critical infrastructure protection, social disturbance, etc.).[6] The drive to build resilience, to address systemic vulnerability, incapacity, or weakness, is at the heart of these transformations.

Above all, resilience is anticipatory and systemic. Where a traditional security management approach assumes that known risks or threats are manageable through preventive actions, mainly organized and executed through strong centralized structures, adopting a resilience approach acknowledges the existence and persistence of existing risks and the necessity to understand systemic vulnerability in order to prepare for potential future shocks and disturbances. This systemic perspective also requires contributions and responsibility across a broader set of institutions, actors, and civil society, highlighting the necessity of distributed action and reaction responsibilities. From a social systems perspective the notion of resilience draws heavily on the principle of self-organization, which is seen to play a central role as a fundamental precondition for the adaptation of complex, but vulnerable or disturbed systems.

Vulnerability and resilience are closely connected ideas. Indeed, resilient systems can be less vulnerable. However, vulnerability and resilience are also generally considered to be specific to particular risks or threats. This means that something may be vulnerable to one risk, and not to another, likewise one system may be resilient in the context of one risk, but not another. This specificity of both system characters implies a lack of symmetry between them—as one character rises, the other does not necessarily fall.[7]

---

[6] T. Prior, F. Roth, and M. Herzog, "Transformations in European Natural Hazard Management: There and Back Again," in R. Bossong and H. Hegeman, eds., *European Civil Security Governance: Diversity and Cooperation in Crisis and Disaster Management* (London: Palgrave MacMillan, 2003).

[7] G. C. Gallopín, "Linkages between Vulnerability, Resilience, and Adaptive Capacity," *Global Environmental Change* 16(3):293–303 (2006).

A perception of vulnerability can be construed as weakness from a security perspective, but from a resilience perspective, understanding the elements of vulnerability is key to coping with potential disturbances and shocks. The desire to build resilience into systems, especially based on an understanding of the components of vulnerability (risk/hazard, exposure, sensitivity, and adaptive capacity), is closely connected to establishing organizational capacity to quickly respond to risk or threat triggers, and react appropriately.

A Systems View of Center and Periphery

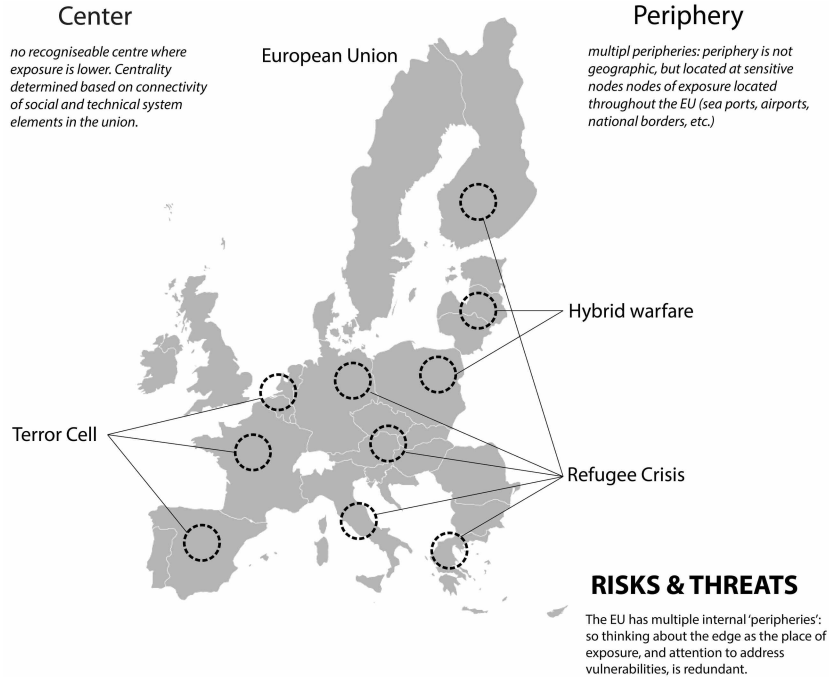
Traditional notions of internal and external security are complicated by the cross-border interdependence of the critical service systems supporting modern societies,[8] especially in the EU and surrounding countries. When countries seek to secure the critical services their populations require, transboundary systems create particular challenges, including in particular sharing management and maintenance responsibilities.

In international politico-economic unions like the EU, dealing with transboundary systemic disruptions should be simplified by existing organizational frameworks. More often though, these unions expose exactly the vulnerability in countries' relationships (witnessed by declining within-union solidarity) that highlight the difficulty of transboundary system management and security. Three risks (or threats, depending on the point of reference) highlight the importance of these issues in the European Union: the current refugee migration crisis, terrorism, and Russia's hybrid warfare. In each of these cases, Union fragility is typically expressed as vulnerability, but not necessarily at the traditional geographic periphery. EU boundary nations such as Greece, Italy, and Austria are inundated by refugees as transit countries, while Germany, Sweden, and France face the challenge of settling many of these refuges. Cultural differences expose western European cities to violent extremism and terror attacks in the geographic center of the union. Baltic and Scandinavian country members of the EU are sensitive to hybrid warfare, an approach used by Russia in the Ukrainian crisis in 2014, but Germany's reliance on Ukrainian gas for heating also makes it sensitive to similar threats.

---

[8] R. Mugavero, V. Sabato, and C. Stallo, "Territorial Security: Architectures, Methodologies and Integrated Systems for the Information Management in Multi-Risk Scenarios," *2012 IEEE First AESS European Conference on Satellite Telecommunications (ESTEL)*, 2–5 Oct. 2012.

Figure 1: Multiple peripheries, with no geographic center in context of risks & threats.



These risks challenge the traditional notion of the center and the periphery, especially because they are driven by population mobility and cross-Union cultural variability. In the context of these risks or threats it is not clear what is center and what is peripheral. While geographically peripheral Baltic countries might be exposed and sensitive to the threat of hybrid warfare, geographically central countries like France and Germany are exposed and sensitive to risks and threats associated with terrorism and refugee migration. Therefore, projecting vulnerability geographically from a central secure position onto a peripheral insecure position is no longer valid, especially in highly complex, mobile societies like that existing in the EU. Likewise, projecting resilience forward geographically from the center to the periphery also makes little sense given the nature of the modern threat/risk environment. Rather, resilience should be projected forward from positions where threat-specific capacities exist, and where vulnerabilities are lowest.

Supporting Societal Resilience Projection with Ad-Hoc Resilience Foresight (Temporal)

While geography has traditionally been a key factor in international politics, increasing connectivity between people, societies, technology, and nations has seen the importance of geography change in international relations. Connectivity and interdependence across domains (social, environmental, economic, political, cultural, technical) implies the need to think of systems rather than of geographies, where systemic connections and linkages across nodes of influence determine the center and periphery of systems. A systemic perspective highlights that the density of nodes of connection reflects influence or importance, where stability develops or dissipates, where resources for resilience exist or don't, where vulnerabilities are reduced or increase. Examining national unions or alliances from a systemic perspective can support cross-Union vulnerability analysis, and the pseudo-temporal projection of resilience using threat foresight and risk scenarios.

Rather than expending resources on strengthening the geographic periphery as a buffer for the center, dedicating the resources to Europe-wide (including external to the Union) foresighting for preparedness will yield a better investment towards regional resilience though a coordinated focus on threats/risks that builds international cohesion and solidarity, close to and beyond a point of focus. There can be no development of societal resilience without establishing a medium to long-term view of vulnerabilities and resilience. In situations of unpredictability or uncertainty, proactive approaches that help decision makers plan for future potential disturbances, and to understand vulnerabilities, can best be used to identify areas of priority for different partners/members, and whether or not a set of common concerns can be discerned. The anticipatory nature of resilience lends itself well to addressing real and perceived cross-Union vulnerabilities. Within the existing organizational structures of the EU, for example, cross-Union resilience requires an investment in foresight practice to anticipate systemically potential risks and threats, which identifies vulnerabilities, and can be drawn on to develop cross-Union adaptive capacities.

Research by Weber, Sailer, and Katzy[9] highlights the way foresight can be used in a fluid and case-specific manner to build resilience, especially

[9] Christina Weber, Klaus Sailer, and Bernhard Katzy, "Real-Time Foresight — Preparedness for Dynamic Networks," *Technological Forecasting and Social Change* 101:299–313 (2015). doi: http://dx.doi.org/10.1016/j.techfore.2015.05.016.

within dynamic and unpredictable network circumstances, such those presented by the current unpredictability in threat and risk in the context of the EU. Ad-hoc rather than strategic management-based foresight processes can encourage self-organized decision environments characterized by flexibility and dynamism. In the context of the EU, an ad-hoc foresight approach should then draw on a distributed collaboration among all members and neighbors in a relational manner. While the EU seeks to assure within-Union security through actions of integration and solidarity, establishing a clear picture of the future threat landscape requires the inclusion and cooperation of EU-external neighbor countries. Engaging neighbors in ad-hoc vulnerability foresight would be driven by the results of completed vulnerability foresight practices, which would cue the involvement of additional partners as necessary. The ad-hoc nature of the process is characterized by the ability to engage or disengage partners in response to the changing threat landscape.

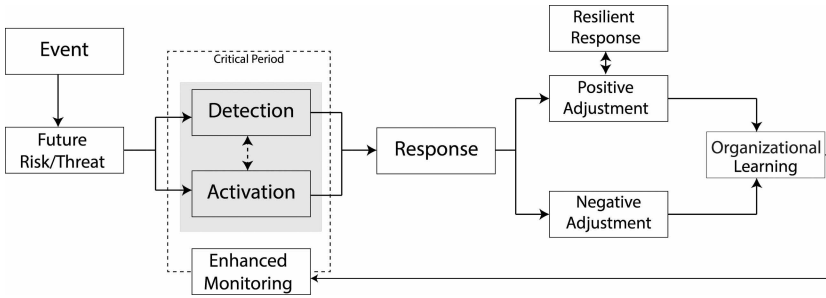
Importantly, switching from a centralized approach to strategic foresight to a more self-organized and relational one will require within-Union agreement to engage in an ongoing process to identify, and initially focus on a narrower set of core security priorities. Figure 2 illustrates a prospective conceptualization of societal resilience based on organizational principles. Effective ad-hoc foresighting to address cross-Union vulnerability and build societal resilience would most effectively be undertaken during the "critical period" as identified by Martin and Sunley,[10] with "detection" and "activation" highlighted especially as points at which a distributed ad-hoc foresight and planning process should be undertaken.

A decentralized and ad-hoc approach to foresight for preparedness and resilience also addresses traditional issue myopia (for instance, peripheral vulnerability versus central strength), by devolved and inclusive issue identification and communication. Inclusive processes toward societal resilience through foresight can help to prevent similar issues from recurring. For instance, when security organization is centralized, without appropriate mechanisms for distributed input in planning, gaining new perspectives on how existing or past issues can be solved is limited. Collaborative and distributed ad-hoc foresight could be the basis of an inclusive concept to bring groups/states together across different spaces (systemic and geographic) rather than creating or widening dividing lines, or fomenting competition.

---

[10] Ron Martin and Peter Sunley, "On the Notion of Regional Economic Resilience: Conceptualization and Explanation," *Journal of Economic Geography* 15(1):1–42 (2015). doi: 10.1093/jeg/lbu015.

Figure 2: A conception of organizational resilience.[11]



In the EU context, just as collaborative and distributed approaches to vulnerability through foresight for resilience building can increase Union solidarity, so too can solidarity within the EU build resilience. Providing opportunities for, and leveraging the value of local and regional connections beyond the EU, though, is hugely important for building self-organized resilience, and for promoting integrated approaches to addressing vulnerability, encouraging cohesion around key issues among EU members, and assuring EU security in the medium to long-term. The capacity of local actors, institutions and organizations to collect context-specific threat and vulnerability information can increase trust in local services and build system solidarity. For instance, Baltic countries are sensitive to hybrid warfare, and it is in the national responsibility to ensure security against such threat. Yet, the EU as an integrated collective that wants to ensure critical services to the EU society can support these countries by adopting supportive mechanisms or regulations (like, for instance, the Civil Protection Mechanism). The EU must facilitate and coordinate the systemic cohesion of member states around issues of common interest (including risks and threats), rather than permitting regional disintegration. This entails member states recognizing and acknowledging that threats across the EU differ, and each country's ability to address a particular threat also differs—there are nationally specific social, cultural, political or economic reasons that create a specific country context influencing their actions relating to threats. If members are interested only in addressing issues nationally, then the value of the Union in countering the risks these threats bring is diminished. Additionally, because threats can also originate from outside the Union, with impacts on the union, EU members

[11] Adapted from Martin and Sunley.

must also recognize and acknowledge that incorporating non-members of the EU in threat identification and assessment is also necessary. Non-members are no longer peripheral, but then become central players in identification, assessment and management.

Keys Points, Directions and Recommendations

a) ***Resilience is anticipatory.*** The value of the resilience paradigm is its anticipatory nature: uncertainty is accepted, and acceptance is the first step in addressing uncertainty. In this context, forward resilience requires functional anticipation. Foresight is a practical tool for early detection. Forward resilience should be driven temporally through self-organized foresight exercises focused on threat identification, threat-specific vulnerability assessments, and threat-specific capability assessments. In the same way the EU Civil Protection Mechanism standardizes and identifies disaster response resources across the Union, results of threat-specific capability assessments should be shared in order to identify resources for addressing threats or mitigating risk, and resource gaps where resources should be directed. Functional anticipation through foresight should precede and determine subsequent physical actions of support or intervention in and outside of the union.

b) ***Ad-hoc organization.*** Functional anticipation in an uncertain threat landscape requires flexible and adaptive participation by multiple actors. Participation in early detection activities should be organized in an ad-hoc manner as required based on threat appearance, not necessarily led by the politically strong or the geographically central. The need for flexibility means avoiding institutionalisation of the anticipatory activities, rather relying on existing, or fostering new operational networks within and between relevant agencies. Even so, these ad-hoc processes must be recognized nationally, and this might effectively be done through institutionally facilitated joint activities (like threat response and risk mitigation exercises) conducted between EU members and near neighbors. Self-organization differs from facilitated organization, but aligns with systems resilience thinking.

c) ***Organizational information sharing and access for proactive planning.*** Non-institutionalized inter-agency anticipation (foresight) activities must be supported by the creation of a threat/capability

information repository to support organizational learning. A multinational information center where participants can communicate experiences and identify key lessons can help EU members and neighbors to better understand the type and impact of actual and potential threats. Better ways of sharing information, supported by structures like Europol's Secure Information Exchange Network Application (SIENA), should be the basis for early detection, early warning, and information on capabilities. Europol's European Counter Terrorism Center also provides an interesting model on which a broader threat information center might be based, providing operational and strategic support in assessing and responding to threats. Non-EU members must be encouraged to contribute knowledge to this resource.

d) ***Systemic cohesion for unity.*** Stability and cohesion in uncertain threat contexts requires unity. In processes of threat anticipation and risk mitigation, unity means finding inclusive mechanisms rather than exclusive ones. This has two implications: first, EU members must acknowledge that threats are perceived and felt differently among the members of the Union; second, non-EU countries, whose borders, infrastructures, or other services are shared, also have an important role in threat and risk mitigation. Therefore, information-sharing structures, non-institutional self-organized networks, and anticipatory activities must necessarily involve all actors and should inform a regional threat prioritization process, which should direct threat mitigation (and ultimately, response) resources to those issues of greatest regional (not national) priority.

Chapter 12

How NATO and the EU Can Cooperate to Increase Partner Resilience

Anna Wieslander

At the Wales summit in 2014, the Enhanced Opportunities Program (EOP) was introduced for a disparate group of Partner nations, which had received a Gold Level of interoperability and collaboration with the Alliance: Sweden, Finland, Jordan, Georgia, and Australia. The initiative has enabled Sweden to efficiently work together with NATO and Finland on Baltic Sea region security in a 28+2 format. At the Warsaw summit in July 2016, the need to increase EU-NATO cooperation to counter hybrid threats and build resilience among members and beyond was highlighted.

The fact that both Sweden and Finland are EU members is an asset that should be explored in the 28+2 format to strengthen resilience. This can be developed in the context of the Baltic Sea region to prepare for hybrid threats, but also in joint efforts by NATO, Sweden and Finland to address fragility in the Eastern and Southern neighborhood.

The Growing Focus on Resilience

Until recently, resilience was mainly used in reference to developing states to assist them in state-building capacity. Both the EU and NATO have worked with resilience projects in candidate and partner states to the East and to the South. These projects aim at strengthening institutions in society dealing, for instance, with elections, anti-corruption, the juridical system, mass media, education and training, democratic control of the armed forces, civil-military planning, gender equality, etc.

Due to a perceived ambition of Russia and ISIS/Da'esh to undermine the unity and the value base of the West, there is an increased focus on resilience also in mature, well-functioning democracies, such as NATO allies and EU member states. Resilience in this regard is viewed as important in order to resist propaganda and information campaigns, attempts to influence business, societies and economic flows, and attacks on information technology (IT) and cyber-related infrastructure. Resilience, in

other words, is a way to respond to the hybrid threats that were highlighted as a result of Russian warfare in Ukraine in 2014. Ultimately, it is about safeguarding the value-based foundation upon which the EU and NATO rest. Consequently, strengthening resilience can be viewed as a preventive action aimed at solidifying societies and avoiding escalation of crises both within and outside of the EU and NATO.

EU-NATO Cooperation Historically Marked by Difficulties

For three main reasons, EU-NATO cooperation has historically been marked by difficulties to agree at the political level. First, Turkey being an allied but a non-EU member poses certain requirements; second, up until 2008 France was not a member of the Integrated Military Command in NATO, and third, the accession of Cyprus into the Union in 2004 was pursued even though the Greek-Turkish divergence on the status of the island remained—and continues to remain—unsolved.[1]

For many years, the focus of institutional cooperation has been on crisis management and the so-called Berlin-Plus arrangements from March 2003, which allow for the EU to use NATO planning and capabilities in crisis management operations. Though Berlin-Plus yielded an immediate success for operations in Macedonia (2003) and Bosnia and Herzegovina (2004), it has not been used since.[2] Collaboration in crisis management has overall been limited. Currently, NATO-EU partnership covers some concrete cooperation in the western Balkans, in Afghanistan, and off the coast of Somalia.[3]

In the aftermath of the illegal Russian annexation of Crimea and war in eastern Ukraine, a new sense of urgency emerged regarding the need to develop cooperation between the EU and NATO in order to successfully counter hybrid threats. As a NATO diplomat put it: "EU-NATO cooperation has moved from 'nice' to 'need.'"

---

[1] See for instance A. Missiroli, "EU-NATO Cooperation in Crisis Management: No Turkish Delight for ESDP," *Security Dialogue* 33:9; S. Duke, "The Future of EU–NATO Relations: a Case of Mutual Irrelevance Through Competition?" *European Integration*, 30(1):27–43, March 2008.

[2] R. Wessel and S. Blockmans, eds., *Between Autonomy and Dependence: the EU Legal Order Under the Influence of International Organizations*, (The Hague: Asser Press, 2013), p. 259.

[3] Press statements by the NATO Secretary General Jens Stoltenberg and the EU High Representative for Foreign Affairs and Security Policy, Federica Mogherini, Meeting of NATO Ministers of Foreign Affiars, Dec 1–2 2015, online at http://www.nato.int/cps/en natohq/opinions_125361.htm.

The United States has been a driving force behind the reset. The underlying motive has been the need to strengthen the European contribution to the transatlantic relationship. The complementarity, rather than rivalry, that has developed between the organizations in past years has been reassuring from an American perspective. The UK has played a central role in balancing European and transatlantic forces, but due to Brexit, uncertainty has re-emerged on how the pendulum will swing, and once again increased the risk that overlapping systems could be created that do not deliver capabilities but costs.

Hybrid Strategies and Resilience

Since 2014, both staff to staff level contacts, and contacts at the political level, have increased substantially. NATO Secretary General Jens Stoltenberg has met several times with High Representative Federica Mogherini as well as the President of the European Council, Donald Tusk, and they have attended each other´s ministerial meetings on a frequent basis.

Initially, there was an ambition to work side by side to develop strategies on how to deal with hybrid threats, and to some extent this was possible at staff level. However, in the end, NATO moved faster than the EU and approved a strategy on December 1, 2015 and an implementation plan on February 11, 2016, while the EU framework on countering hybrid threats did not land at the table of the Defense Ministerial Meeting until April 19, 2016.

In the summer of 2016 at the NATO summit in Warsaw, NATO and the EU, the latter represented by both the President of the EU Commission Jean-Claude Junker and Donald Tusk, issued a joint declaration as a landmark for establishing even closer cooperation. In the declaration, the organisations committed to:

> Boost our ability to counter hybrid threats, including by bolstering resilience, working together on analysis, prevention, and early detection, through timely information sharing and, to the extent possible, intelligence sharing between staffs; and cooperating on strategic communication and response. The development of coordinated procedures through our respective playbooks will substantially contribute to implementing our efforts.[4]

[4] Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization, July 8, 2016.

In addition, parallel and coordinated exercises on hybrid are to be planned for 2017 and 2018, and resilience of partners in the east and south are to be addressed "in a complementary way through specific projects in a variety of areas for individual recipient countries, including by strengthening maritime capacity."

NATO Strategy on Hybrid Threats

How do the hybrid strategies of NATO and the EU compare? The NATO strategy on countering hybrid threats is structured along the lines to *prepare—deter—defend*. Enhanced intelligence and surveillance is a key part of NATO's response to hybrid threats, while it also constitutes a challenge when it comes to indications for early warning, since these are likely to be found in civil society rather than on the military side when it comes to hybrid threats. Cooperation with the EU, which looks at civil society much more closely than NATO, could therefore increase the ability to capture early signs substantially.

The implementation plan focuses on "prepare," for instance, how to organize NATO Headquarters and coordinate with member states and the EU in order to improve the ability to identify, recognize and attribute hybrid actions and to respond quickly.[5] In the strategy it is recognized that in order to be more effective in countering hybrid threats, NATO is committed to working even more closely with the EU.[6]

One important finding, and challenge, in the process of addressing hybrid threats within NATO has been that a lot of actions do not fall within the responsibility of the Alliance, but on the member states themselves.[7] This in turn has led to the question of resilience, which has become an integrated part of the hybrid strategy.

NATO has set seven *baseline requirements* to be assessed:

1) assured continuity of government and critical government services;

---

[5] Press conference by NATO Secretary General Jens Stoltenberg following the meeting of the North Atlantic Council at the level of Defence Ministers, 11 Feb 2016 online at http://www.nato.int/cps/en/natohq/opinions_127972.htm?selectedLocale=en

[6] Press conference by NATO Secretary General Jens Stoltenberg following the meeting of the North Atlantic Council at the level of Defence Ministers, 11 Feb 2016 online at http://www.nato.int/cps/en/natohq/opinions_127972.htm?selectedLocale=en

[7] Interviews with NATO officials in Brussels Dec 2015 and Stockholm January 2016.

2) resilient energy supplies;
3) ability to deal effectively with the uncontrolled movement of people;
4) resilient food and water resources;
5) ability to deal with mass casualties;
6) resilient communications systems; and finally
7) resilient transportation systems.[8]

In order to assist allies in meeting those requirements, NATO has agreed to create *resilience advisory support teams*, as recommended by Hans Binnendijk, Daniel Hamilton and Frank Kramer, to offer expertise, a form of internal consulting, on areas such as cyber attack response, civil-military planning and coordination, protection of critical infrastructure, and so forth.[9]

A *NATO hybrid cell* is expected to cooperate with the EU Hybrid Fusion Cell through direct liaison, as well as regular sharing of analyses and lessons identified.[10] Closely linked to countering hybrid threats are NATO's *Centers of Excellence* (COEs) on a range of topics, for instance Energy Security in Vilnius, Strategic Communication in Riga, and Cyber Defence in Tallinn. The COEs assist in doctrine development, identify lessons learned, improve interoperability and capabilities, and test and validate concepts through experimentation.[11]

---

[8] "Resilience: A Core Element of Collective Defence," *NATO Review*, http://www.nato.int/docu/Review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/index.htm; Press conference by NATO Secretary General Jens Stoltenberg following the meeting of the North Atlantic Council at the level of Defence Ministers, 11 Feb 2016 online at http://www.nato.int/cps/en/natohq/opinions_127972.htm?selectedLocale=en

[9] Interviews with NATO officials in Washington, October 2016, Brussels Dec 2015 and Stockholm January 2016. See Franklin D. Kramer, Hans Binnendijk, and Daniel Hamilton, *NATO's New Strategy: Stability Generation* (Washington, DC: Center for Transatlantic Relations/Atlantic Council, 2015), https://issuu.com/atlanticcouncil/docs/natos_new_strategy_web.

[10] Joint Framework on countering hybrid threats, p. 17.

[11] According to the NATO website, "Centres of Excellence (COEs) are international military organisations that train and educate leaders and specialists from NATO member and partner countries. They assist in doctrine development, identify lessons learned, improve interoperability and capabilities, and test and validate concepts through experimentation. They offer recognised expertise and experience that is of benefit to the Alliance, and support the transformation of NATO, while avoiding the duplication of assets, resources and capabilities already present within the Alliance."

EU Framework on Hybrid Threats

The EU framework on countering hybrid threats is similar to that of NATO with regard to recognizing the primary responsibility of member states, and the need for further coordination and cooperation with NATO. The framework suggests actions that member states can conduct, such as *hybrid risk surveys* to identify key vulnerabilities, and develop capacities for proactive strategic communication. It also identifies areas for the Commission to intensify work in:

- critical infrastructure protection, including energy networks and safety, transport and supply chain security, and space.
- public health protection and food security
- cybersecurity
- targeting hybrid threat financing
- building resilience against radicalisation and violent extremism
- increasing cooperation with third countries.

While the EEAS is tasked to set up a *EU Hybrid Fusion Cell* to "receive, analyse and share" information related to hybrid threats, the suggestion to establish a *Center of Excellence* for countering hybrid threats will be established in Finland. Resilience is highlighted as an integrated component in countering hybrid threats, both when it comes to members and partners.[12]

EU-NATO Coordination and Cooperation on Hybrid Threats

A range of areas have officially been identified for enhanced coordination and cooperation between NATO and the EU, including:

- situational awareness
- information sharing
- strategic communications
- cybersecurity/cyber defense

[12] European Commission and the High Representative for Foreign Affairs and Security Policy (2016). Joint Communication to the European Parliament and the Council. Joint Framework on Countering Hybrid Threats, a European Union Response. Brussels 6.4.2016 JOIN82016) 18 final.

- crisis prevention and response
- civil-military planning[13]

A *playbook* for NATO-EU cooperation, dealing with a range of hybrid-warfare scenarios, has been developed for the areas of cyber defense, strategic communications, situational awareness and crisis management. The aim is to speed up decision-making and to answer in advance questions about who does what.[14]

Partners Not Yet Targeted for Deepened Cooperation

While both Jens Stoltenberg and Federica Mogherini have acknowledged that there is greater potential for more cooperation in helping partners to become more capable of securing themselves in Europe, the Middle East and North Africa, this has not yet been addressed in a systematic manner.[15]

However, in order to truly build resilience, enhanced NATO-EU cooperation should not be limited to member states. NATO and EU could combine resources and complement each other to deal with fragile and failed states. A major challenge ahead would then be to efficiently coordinate defense building capacity support with development aid and economic support. This should be developed to include partner cooperation, to the east and the south. Both Finland and Sweden are active contributors to support development in these regions through a broad range of policy areas, from development to the military. Sweden, together with Poland, took the initiative to start the Eastern Partnership (EP) within the EU in 2009.

The EU remains a much bigger player in terms of resources, both in terms of funding and personnel, for partner cooperation. Nevertheless, the assessment of the EU Neighborhood policy conducted during 2015 sets the ground for a rapprochement between the institutions in two major

---

[13] EU Framework p. 17; J. Shea, "Resilience: A Core Element of Collective Defence," *NATO Review Magazine*, online at http://www.nato.int/docu/review/2016/Also-in-2016/ nato-defence-cyber-resilience/EN/index.htm.

[14] Interview with NATO official in Brussels, May 9 2016, "New Threats are Forcing NATO and the EU to Work Together," *The Economist*, May 7, 2016.

[15] Press statements by the NATO Secretary General Jens Stoltenberg and the EU High Representative for Foreign Affairs and Security Policy, Federica Mogherini, Meeting of NATO Ministers of Foreign Affairs, Dec 1-2 2015, online at http://www.nato.int/cps/en/natohq/opinions_125361.htm.

ways. First, the EU is shifting its regional approach towards a more individualized efforts towards countries, which is more in line with how NATO works. Secondly, the EU for the first time includes security as an area of cooperation, thereby coming closer to the NATO agenda. In the latter, there is also a challenge when it comes to duplication, but a rough division of labour should work, based on NATO dealing mainly with the military aspects and the EU with the civilian.

Areas of NATO focus include military training, democratic control of the armed forces, civil-military planning, counter-terrorism, and countering improvised explosive devises. These programs are in place for Jordan and Iraq, and could possibly be introduced also in Tunisia, Libya, and Morocco.[16]

The EU highlights civilian security sector reform, civil protection and disaster management, tackling terrorism and preventing radicalization, disrupting organized crime, fighting cybercrime, and chemical, biological, radiological and nuclear risk mitigation.[17]

Consequently, the risk of overlaps mainly exists in the areas of security and defense dialogues, in counter-terrorism and cybersecurity, but in all, to a large extent, the support is complementary. The greater problem has to do with lack of coordination, information sharing, and exchange of assessments that would enable efficient resource pooling and a comprehensive approach to tackle fragility and vulnerabilities in a partner country.

Hybrid Threats in the Baltic Sea Region

The hybrid threat is central when it comes to cooperation in the Baltic Sea region, something that also has been reflected in the political and military assessments pursued by NATO regarding the area, with Sweden and Finland invited to join in the process. The need to deepen cooperation on situational awareness, intelligence sharing, cyber security and strategic communication, has been acknowledged by all parts.

---

[16] "NATO Training for Iraqi Officers Starts in Jordan," April 2, 2016, *NATO News*, Deputy Secretary General Alexander Vershbow at the Lennart Meri Conference, May 14, 2016.

[17] "Review of the European Neighbourhood Policy," Joint Communication to the European Parliament, The Council, the European Economic and Social Committee and the Committee of the Regions, SWD(2015)500 final, Brussels Nov 18, 2015; Joint Declaration of the Eastern Partnership Summit (Riga, 21–22 May 2015).

Due to the high degree of security interdependence in the region, a crisis in the region would affect all countries regardless of EU or NATO membership. That makes the call for concrete improvements in resilience and crisis management capabilities realistic and recognized by most actors.

During spring 2016, this has been highlighted through a range of exercises. NATO has conducted a crisis management exercise focused on hybrid threats in the Baltic Sea region. Sweden and Finland were invited to participate, which gave useful insights to current systems and procedures in and between NATO and partners, their strengths and weaknesses.

The European Defence Agency (EDA) has conducted a hybrid threats table-top exercise that involved some 80 experts from EU member states, EU institutions and NATO, with similar lessons learned on the importance of situational awareness and information sharing, civil-military cooperation and fast decision-making processes.[18]

In addition, the American think-tank CNAS (Center for a New American Security) organized a table-top exercise in Washington DC, featuring nearly 50 high-level participants from Europe and the United States, to test possible challenges to Baltic security, including hybrid warfare elements. The tabletop exercise has resulted in an open report, "Assured Resolve: Testing Possible Challenges to Baltic Security," which includes conclusions of interest for deepened EU-NATO cooperation, such as:

- The lack of integration of intelligence due to "significant institutional stovepipes" between the EU and NATO.
- The EU can prove useful in serving as a "convening authority" for non-NATO nations such as Finland and Sweden, and critical assistance could be provided through the EU´s Solidarity Clause and Mutual Assistance Clause.
- The lack of an adequate mechanism for all the crucial players to confront hybrid threats hampered the West in creating a unified response.
- Confronted with an aggressive Russian disinformation campaign, neither institutions such as NATO and the EU nor national govern-

[18] "EDA Presents Hybrid Threat Exercise Findings to Defence Ministers," Luxembourg 19 April, 2016 online at https://www.eda.europa.eu/info-hub/press-centre/latest-news/2016/04/19/eda-presents-hybrid-threat-exercise-findings-to-defence-ministers.

ments could successfully deal with it. There was significant confusion both vertically and horizontally.

Developing the EOP to Strengthen Resilience

The fact that both Sweden and Finland are EU members, and as such could help promote further EU-NATO cooperation, has been highlighted but not yet fully explored in the EOP. Sweden and Finland provide strong voices in the EU as net contributors to crisis management and have a long tradition of involvement in neighbourhood issues, not least to the East. Thus, they can with credibility and competence assume leading roles in pursuing questions and issues of common interest. The EOP could be used to address the need to strengthen resilience in NATO and EU member states, as well as to the east and in the south.

While there are good reasons to continue to keep a strong focus on Baltic Sea region security in the format of NATO, Sweden and Finland, there are also arguments for broadening the agenda on resilience and make full use of the EU membership of the two partners.

Another important aspect of opening up the EOP agenda is to avoid a perception of competition between sub-regions, such as the Baltic Sea and the Black Sea regions, for instance, by bridging understanding of challenges and measures that need to be taken to strengthen the security for the whole security community. Strengthened stability to the east and in the south promotes security for all, also in the north. NATO, the EU and partners could undertake additional actions to strengthen resilience within and beyond their borders:

EU-NATO Cooperation

- As suggested in the review of the EU's neighborhood policy, member states could take the role of lead partner for certain initiatives or to accompany certain reform efforts. The role of lead partner could be used to promote NATO-EU cooperation in specific projects for countries that are devoted to bridging the two organizations closer together. Sweden and Finland should put those words to action.
- By forming task groups open for other members, Sweden and Finland can assume the role as lead partners to strengthen EU-NATO coop-

eration on Baltic Sea security and resilience to the East and in the South.

- The task groups could more specifically address the following issues:

Baltic Sea region security

1. For the Baltic Sea region, a comprehensive maritime framework can be created. It would endorse the full spectrum of hybrid threats and how to address them, e.g. civil and military measures and responsibilities to secure trade and energy flows, as well as borders and state institutions. Such a framework could build on existing EU-related frameworks such as the EU strategy for the Baltic Sea region, and the 28+2 work in NATO on Baltic Sea region security.
2. The StratCom Centre of Excellence in Riga could be used to plan how the EU, NATO and partners could connect in order to ensure efficient strategic communication to counter hybrid threats. This would include suggestions for both vertical and horizontal organization and points of contact in individual countries, as well as NATO and the EU. Furthermore, the whole spectrum from proactive to crisis management should be covered.
3. A roadmap for creating combined NATO-EU resilience teams, to be used in early phases of suspected hybrid crisis, could be developed. Meanwhile, Sweden and Finland should be able to provide expertise to NATO resilience teams, and to draw upon the expertise of the teams if needed.

Strengthening resilience to the East and in the South

1. In countries where both NATO and the EU are active in strengthening resilience, such as Ukraine, Moldova, Georgia, Iraq and Jordan, the organizations should develop closely coordinated country-based, comprehensive frameworks to tackle state fragility and vulnerabilities. Within each framework, the roles, projects, goals and resources for each organization would be declared.
2. In each program country, regular meetings at staff level between NATO and the EU should be conducted in order to ensure information sharing and coordination as the projects proceed.
3. In areas where there is a risk for overlaps, such as security and defense dialogues, counter-terrorism and cybersecurity, NATO and the EU should strive to develop closely coordinated, generic

frameworks in order to ensure a common view on the challenges and how to deal with them, as well as roles and responsibilities.

4. Procedures for the exchange of assessments of projects on resilience, including lessons learned sessions, should be established.

Chapter 13

The Arguments for a Center of Excellence for Countering Hybrid Threats

Charlotta Collén[1]

Changes in the European Security Environment, Hybrid Threats, and the Need for Enhanced Resilience

The European security environment has been greatly influenced by two events in which the hybrid nature of non-linear warfare has come to the fore, mainly the Russian intervention in Ukraine and the rise of the Islamic State of Iraq and the Levant (ISIL). Russian action in Ukraine has destabilized the security of the eastern neighborhood of Europe, sending ripple effects all through the Continent. ISIL has equally given rise to instability in the southern areas of Europe, increasing radicalization and terrorism outside and within the borders of Europe. Security has thus become intrinsically both an internal and external issue for states and must be met with a new sense of resilience and societal preparedness. The link between hybrid threats and terrorism is acknowledged but is, as of yet, in need of closer inspection and analysis.

The sense of threat has changed in international relations and so has the notion of actors creating and countering them. The EU strongly recognized these changes in its guiding document *A Global Strategy for the European Union's Foreign and Security Policy*, in which it is stated that "The EU will pursue a multifaceted approach to resilience in its surrounding regions," pursuing "tailor-made policies to support inclusive and accountable governance, critical for the fight against terrorism, corruption and organized crime, and for the protection of human rights."[2]

Hybrid or non-linear threats refer to actions whereby military and non-military means are combined to achieve specific objectives, with the aim of exploiting vital vulnerabilities of the target (state) and giving rise to

[1] The opinions expressed in this chapter only reflect those of the author, not the Ministry of Defense of Finland.

[2] https://europa.eu/globalstrategy/sites/globalstrategy/files/eugs_review_web.pdf.

uncertainty and ambiguity. The aim of the actions is to undermine the ability of the state to perform crucial decision-making processes within its society or neighboring countries. Due to their complicated nature, hybrid threats and actions are best countered through a network-based approach involving nation-states supported by international actors such as the EU and NATO with specific means and instruments. Hybrid threats should be countered with a comprehensive, conceptual, balanced and multidimensional approach strengthening the overall resilience of the state. Nationally, Finland applies the concept of societal security—a whole-of-government approach. Preparedness requires networking with civil society and the business community. Societal preparedness is part of a holistic approach to deterrence.

Whole-of-Government Preparedness[3]

Countering hybrid threats and building resilience requires comprehensive actions by all stakeholders in security both on the national and international level. The EU has the ability to deal with security threats in a comprehensive manner making use of its different instruments in sequence or simultaneously. The Finnish model of societal security and whole of government preparedness could be an appropriate model to transfer to the EU and NATO level. Hybrid threats require governments to adapt to security issues in a dynamic way transcending inter-agency boundaries. A comprehensive or holistic way of dealing with hybrid threats can help direct scarce resources and strategic capabilities to where they are most needed. As a consequence, new expertise will emerge that is better equipped to deal with systemic, transboundary threats. The EU and NATO can help develop and disseminate good practices in this regard, but in order for these practices to emerge, a great deal of analysis and research followed by training and education is needed. This is where a Center of Excellence is called for.

Resilience

Resilience is defined here as the state's ability to withstand pressure directed at its vital functions and decision-making ability in times of dis-

[3] Please refer to the chapter in this book by Axel Hagelstam for further discussion on the whole-of-government approach to resilience in Finland.

ruption, crisis and conflict. Strong resilience requires good governance, which the multitude of instruments and expertise within the EU and NATO should be able to uphold and strengthen. Resilience requires a sufficient level of situational awareness, strategic communication and decision-making ability. Growing interdependencies between states make threats to neighboring countries or indeed their fragility pose transboundary threats to all societies. Natural disasters, whether man-made or non-man-made, and aggressions by state and non-state actors pose threats to increasingly large areas of states, groups of states and populations. This will entail closer cooperation between and within states to prevent and counter hybrid, conventional and non-conventional threats. A common threat assessment benefits both NATO and the EU and their respective member states. The research agenda of the Center for Excellence for Countering Hybrid Threats could focus on drafting strategies in countering hybrid threats, improving societal preparedness and resilience to that end. Capability-based planning should build on strong evidence and research.

The ability to confront hybrid threats and enhance resilience is thus enhanced through four principles:

- ***Social preparedness:*** We must understand where institutional vulnerabilities lie. Besides that, we should also define the critical functions of society that need to be sustained and secured under all circumstances.
- ***Enhanced early recognition and situational awareness:*** The ability to identify threats starts with shared perceptions of what kind of threats we face and may face in the future. Situational awareness is a crucial precondition for successful threat analysis.
- ***Developed procedures and policies:*** Sometimes there is no need for new capabilities, just more effective procedures. Clear analysis and decision-making processes are an important part of the response.
- ***Coordination:*** We should coordinate all instruments that may be needed to counter hybrid threats. The EU has a particular role in promoting coordination as it is able to connect many policy areas that should be engaged simultaneously when countering hybrid threats.

European Union

A Joint Communication on Countering Hybrid Threats[4] by the Commission and the High Representative for Foreign Policy was issued on April 6, 2016. The Communication addresses five issues areas of concern: 1) situational awareness; 2) enhancing resilience; 3) counter-measures; 4) strategic communication and 5) cooperation with partners, NATO in particular. On April 19,[5] the Foreign Affairs Council and the Defense Ministers called for implementation of the Communication.

Along with the recommendations outlined in the Communication, an EU Hybrid Fusion Cell is established alongside the EU Intelligence Center (IntCen). The main task of the Fusion Cell is to enable the exchange of classified and non-classified information amongst member states, EU institutions and third parties. The Fusion Cell is to produce analysis and reports on hybrid activities focusing in particular on third countries. The analysis will be based on information provided by member states, EU delegations and the Commission. The Joint Communication expresses interest in establishing a separate Center for Excellence as the Fusion Cell is not envisaged to provide any policy recommendations or to conduct any long-term capacity-building in countering hybrid threats. The Fusion Cell is furthermore not tasked to provide strategic level research, exercise or training in countering hybrid threats, as this is envisioned in the Communication to be the main objective of the future Center of Excellence. The exchange of information between the Fusion Cell and the Center of Excellence will require a Security Agreement and protected lines of communication.

EU and NATO in Resilience and Societal Preparedness

Comprehensive preparedness and resilience is of great importance to NATO.[6] NATO's responses to hybrid threats are based on three key actions: to prepare, deter and defend. In order for these actions to succeed NATO will have to develop the ability to support partner countries in

4 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=FI, accessed 12.7.2016.

5 http://data.consilium.europa.eu/doc/document/ST-8022-2016-INIT/en/pdf, accessed 12.7.2016.

6 NATO Warsaw Summit Communiqué, Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Warsaw 8–9 July 2016, http://www.nato.int/cps/en/natohq/official_texts_133169.htm.

developing good governance and reliable institutions in order to strengthen their resilience and ability to respond to hybrid threats. The Center of Excellence can be of great help to NATO in this regard. Seating a liaison officer from NATO to the Center may provide for even closer cooperation and should therefore be considered an option. Non-EU members of NATO should also be kept updated on the developments of the Center of Excellence as they are equally entitled to the services it is envisaged to provide.

Hybrid threats are significant to NATO, EU and European countries at large. A closer cooperation in this matter between EU and NATO is important as these threats are best met with the resources of both organizations inevitably bringing them two closer together. Countering hybrid threats entails many actions outside the remit of traditional force projection. The EU completes NATO capabilities in countering hybrid threats especially regarding situational awareness, strategic communication, cyber defense and civilian-military cooperation. NATO subsequently recommends closer ties with the EU on a staff-to-staff basis, strengthening coordination and mutual assistance to the country experiencing hybrid threats or attacks. NATO and EU have developed separate but complementary play books on countering hybrid threats. In order to best support this cooperation the Center for Excellence would benefit from being independent of EU structures. Any duplication with the existing NATO Centers of Excellence can be mitigated with pertinent planning.

The Tasks and Objectives of the Center of Excellence for Countering Hybrid Threats

Objectives and tasks

The hybrid Center of Excellence for Countering Hybrid Threats, focusing on strategic level analysis, research and training, is envisaged to support NATO, EU and member states, NGOs and private sector actors in countering hybrid threats and strengthening societal resilience. In the interest of creating a flexible and open source of expertise for the international community, the Center of Excellence is thought to function outside formal EU and NATO structures as a multi-national, cross-disciplinary network. The Center of Excellence has at the moment of its inception attracted the interest of twelve countries,[7] the EU's External Action Service and NATO.

[7] Spain, the UK, Italy, Latvia, Lithuania, Poland, France, Sweden, Germany, Finland, Estonia, and the United States.

Complementarity with existing institutions and instruments, including the newly established EU Hybrid Fusion Cell, is seen as essential. The tasks of the center are envisaged to include strategic level dialogue on protecting societal vulnerabilities from hybrid threats, academic analysis of hybrid threats and inherent vulnerabilities, collecting best practices and lessons learned, and educating, training and exercising, all with the aim of strengthening capabilities to counter hybrid threats.

The aim could be to tackle hybrid threats though a comprehensive approach focusing on three baskets: 1) hybrid influence, 2) hybrid terrorism and 3) responding to hybrid threats and strengthening resilience. Hybrid influence is manifold, making use of military, political, information, economic, and cultural resources, and it can be connected with critical infrastructure, cyber security and migration flows. Hybrid terrorism is thought to include actions of multiple kinds in order to enhance a particular goal, by for instance combining cyber-attacks with ideological rhetoric. Strengthening the ability of a society in countering hybrid threats emanates from strong efforts to strengthen societal resilience through early warning, situational awareness, codes of conduct and developing of procedures and processes.

Composition and Working Methods

Initially the Center could provide all interested parties with relevant networks of experts, both governmental and non-governmental. The working method of the Center could be network-based so as to align interested parties into communities of interest, focusing on certain forms of hybrid threats and analyzing ways (in terms of governance structures and methodologies) to counter this particular hybrid threat or form of hybrid action. The Secretariat, to be established in Helsinki, would coordinate the flows of information between the communities of interest, in addition to keeping close ties with identified points of contacts in the member states. These points of contact would in turn coordinate networks of experts in their respective countries, giving the member states engaging in the work of the Center of Excellence freedom of initiative with regards to participation and agenda setting. The headquarters would in its own right lead work on research, training and exercises, in addition to preparing the steering board meetings and coordinating work with partner organizations such as the EU and NATO.

Research and Strategic Analysis

The aim of the research activities of the Center of Excellence could include analysis of the phenomenon of hybrid threats and the interdependencies it creates between societal functions including the underlying strategies and logics of disruption. The research could make use of open source data and a network-based cooperation between experts and organizations. The research framework should be firmly anchored in evidence-based decision-making producing analysis, doctrines, scenarios, and training methods in helping to identify and counter hybrid threats.

Training and Exercising

The training activities of the Center should be based on information gathered through research and strategic assessments. In addition, the Center should produce training modules and material for different forms of exercises, which would then be utilized in internet-based course portals helping participants to understand the basics of hybrid actions. In addition, one important task would be to enhance the ability of political decision-makers to take appropriate actions to counter threats by providing table-top exercises of various kinds.

Developing Preparedness and Resilience

State resilience is founded on societal preparedness in all spheres of life, with a special focus on protecting critical infrastructure against hybrid threats through inter-agency coordination. The model of upholding and strengthening societal preparedness is based on the Finnish view of a whole-of-government approach to societal security. In order for societal preparedness to work efficiently in a complex environment, responses and skills need to be developed so as to accommodate prudent action against any form of hybrid threats. The Center should therefore along with its partners evaluate different working-methods and tools with which to best counter these threats. The aim is to establish a Center of Excellence which brings together the best possible knowledge Europe has to offer in the pursuit of countering hybrid threats.

Chapter 14

Forward Resilience: Five Warnings

Alyson JK Bailes

Forward resilience is an instantly attractive concept to any security buff, and should not be hard to explain to the public either. It echoes the traditional concept of forward defense applied by NATO in Cold War times, but goes much further than that.

Forward defense used to mean concentrating military capacity, and thus deterrent effect, in the Alliance's border areas closest to the potential foe. The proposed focus of forward resilience lies beyond, and often well beyond, the borders of our own nations and alliances. It applies not narrowly to traditional defense, but to the myriad other dimensions of modern security in which borders have lost most of their meaning.

Our economic security depends on far-reaching chains of supply, of services and labor as well as energy sources and other essential goods. Our modern infrastructures now typically involve region-wide links and even global co-dependencies in areas like transport, communications and IT security. Our human security is exposed to challenges ranging from non-traditional violence and crime, through pandemics, to short-term and chronic environmental hazards: all capable of spreading rapidly across huge distances, and even if not, of threatening us with secondary effects from failures in the weakest links. Pursuing security 'upstream' to improve resistance, resilience and recovery in those territories and systems—both physical and intangible—on which we depend so critically should be an eminently worthwhile use of resources.

To be sure, before operationalizing such a concept it needs to be carefully defined and delimited. The military vulnerabilities of important partners abroad are commonly covered, at least in principle, by extended deterrence (including nuclear balances) and regional alliances. Conflict risks that are damaging both for their locales and for ourselves are dealt with under the headings of conflict prevention, intervention, and peace building. Many human security problems in less fortunate areas are best addressed through the familiar range of means associated with aid for development.

Especially when the latter extend to supporting good security governance, however, they overlap with the proposed new concept and could fruitfully be challenged by it. When helping a poor country or one recovering from conflict to build efficient, democratic armies, why not also consider how trained military personnel (and their assets) could and should be used in civil disasters? When building law and justice systems, why not look at emergency response capacities in parallel? They also have the responsibility to protect, and may raise similar issues of human dignity and equal rights. When looking at economic and financial hindrances to sustainable growth, why not include the issue of disaster funds and insurance? (Good ideas on micro-insurance might be almost as productive as the experiments made so far in micro-finance.) In the crucial field of climate policy, meanwhile, we have already grasped that adaptation—to improve the odds on surviving unavoidable climate shifts and disasters—demands no less attention than mitigation.

Generally, it seems right to develop the forward resilience concept within the bounds of what we would call the homeland security or societal security agenda in our own jurisdictions. That leaves an extremely wide sphere for action, especially if interpreted with sensitivity to local conditions. The top ten challenges for policies aiming at resilience in Sweden, Spain, or Canada will hardly be the same in Ukraine, Nepal, Mozambique, or Peru. Further, in Western nations (and institutions) the competence of agencies specializing in this field can be shaped by quite arbitrary factors, including variations in the civil-military dividing line and the ability of other specialized departments to defend their territory. When extending our vision potentially to the whole world's resilience, it would be wrong to separate off *prima facie* any given field of civil security policy, whether it be public health or climate change or the handling of civil disorder. An open mind should also be kept on the vexed issue of migration. Its upstream causes and ultimate effects may lie well beyond the reach of resilience policy; but as a physical process it puts strains—both material and psychological—on the issuing, transit, and receiving territories that share many features with other civil emergencies and raise parallel issues of management.

A second demarcation issue arises when planning the policy's active content. We have reason to be concerned about every phase of comprehensive security management in neighboring regions and others that we depend on. But how much should a programme of forward resilience, as such, attempt to cover? Should it try to absorb existing activities upstream in the security cycle, such as threat and risk assessment, and efforts for

mitigation by such means as conflict prevention, international regulation, development assistance and humanitarian aid? It may be more practical, at least at first, to focus on phases nearer the end of the cycle such as short-term forecasting of attacks and disasters; management of actual emergencies with or without international participation; recovery, reconstruction and lesson-learning. However, depending on the context, an essential stage in working with others—both nations and non-European regional organizations—may be to introduce and debate the whole over-arching concept of resilience with them. It should certainly be possible to cover aspects of preparedness such as hardening, diversification, and redundancy, as well as exercises and training. And if focusing on resilience in new frames of partnership throws up new understandings and insights about how other specialized areas of security governance might contribute, by all means let those ideas be shared with those responsible. The new concept should not become another stove-pipe.

All this said, like many things in public policy, forward resilience may prove easier to sell than to deliver. In the rest of this chapter, five pieces of unsolicited advice will be offered about possible mistakes or omission and commission that should be avoided when developing the concept. The author's only motive is to create the best possible conditions for its success.

Forward in Every Sense

One of the most clichéd mistakes in security policy is the Maginot mentality. Because resilience literally implies bouncing back to a normal condition, it is tempting in our own as well as other countries to define the goal as perpetuation of a status quo. This is clearly not satisfactory for nations whose security and/or governance is still substandard; but it also carries the risk of missing upcoming shifts in the threat and risk pattern. We should not be speaking to outside partners on the basis of our past experience so much as of their future needs. The ongoing trend in our *relationship* with neighbors and partners seems fated to be one of increasing connection and dependency: but the local trend in their civil security *environment*—and hence the demands on and potential of their resilience—could either converge further with or diverge from our own under the influence of climate, economic development, and geo-strategic factors among others.

As just one example, we have recently become accustomed to pandemics that move from poorer locations to richer ones, generally having originated in human-animal contact. Our ideal towards the affected partners would be to help them stop the threat at source. But the spread of chronic rich men's diseases already goes in the other direction, and who can say that a future plague might not start from a rich country because of antibiotic resistance? For such reasons, longer-term forecasting and speculative foresight efforts should be part of the larger conception of a forward resilience policy, and wherever possible should be integrated into the resulting exchanges with others.

Recognize Responsibilities

The separation between upstream and downstream in today's security connections is in fact increasingly artificial. Not only do human movements like tourism and migrant labor bring growing numbers of people into contact with previously remote risk environments, but the very question of where responsibility and ownership lie for a given security space can be called in doubt by economic and technological processes. For instance, who is responsible for human and environmental resilience in the context of Arctic shipping? The ships, their cargoes and crews do not belong to, and were not even invited in by, the people of the Arctic's own sparse settlements. It makes sense to speak to the latter about how they might be helped bear the local impact of a disaster like an oil spill, but not about how to extend forward protection for the ships, or the possible new oil and gas rigs, themselves. The responsibility as well as capacity for that clearly lies with the owners and operators from the West and Russia, who introduced this new activity to a remote and fragile area. It has in fact been recognized recently by the International Maritime Organization's adoption of a Polar Shipping Code, in which responsibilities and costs lie firmly with the shipowners, even if flagged at the other end of the earth.

To take another case, the spate of outsourcing of services as well as manufacturing processes to remote developing countries over the last two decades has been driven by economic forces with scant regard to security. Insofar as it may force local people to work in inhuman and dangerous conditions, as exposed by scandalous cases like factory fires, it amounts to a morally reprehensible outsourcing of risk. But it also makes little sense in terms of security of supply, or the continuity of service which is key to companies' own reputation, to root your whole operation in a locale that

has both a far worse risk profile (given natural conditions, disease, civil disorder etc) and weaker capacities for resilience.

Where entities in the prosperous countries themselves own and initiate activity in exposed locations, economic logic as well as morality should guide them to extend their own standards of health, safety, security awareness, protection and insurance to the communities concerned. Their own resilience and business continuation planning needs to stretch right down the supply chain, and might then best be defined as extended resilience, rather than forward resilience, which implies an external partner. Of course, it is easier and cheaper for a multinational company to follow the alternate track of resilience planning that involves diversification and redundancy: simply to shrug off a location where something goes wrong, and invest again—with the same lack of security foresight—in another. Here, if the drive for forward resilience is serious, it may ultimately need to resort to regulation: developing a concept of extraterritorial security liability in parallel with the provisions already existing for sexual and terrorist offences abroad.

Respect Local Ownership

Despite the point just made, the great majority of what needs to be done for improved resilience beyond our own borders should be and will be done by the local authorities, business sectors, and communities themselves. When launching a new program of dialogue and cooperation with them under the flag of forward resilience, much trouble could be saved by reflecting on the lessons long and painfully learned in the field of conflict management about local ownership. There are several aspects here, including the care that must be taken to avoid over-reliance on aid, and the dangers of a talking down approach that results in double standards. Especially when we are trying to protect shared networks and lines of dependency, or to tackle hazards of universal incidence like pandemics, the logic of building common standards, operating procedures, and so forth should be far clearer than in some other realms of security. Our partners, however, can only become co-owners of these systems if they have the economic and other practical means to carry their share. The financing of forward resilience may seem a sordid and unwelcome issue to raise at this stage, but it needs to be debated well up front—and it needs to be sustainable.

It is not, however, only shortage of means that may make local partners hesitant to join in common efforts for resilience or at least, to keep them going for long. Resilience has crucially important psychological and cultural components that can combine with material factors—and differences along the temporal scale—to demand very different solutions for different environments. The story of violent conflict offers plenty of cautionary tales against simply imposing an outside model, but also against the superficially more reasonable approach of trying to find a local argument and/or constituency for the solution we prefer. Successful and lasting settlements are those that not only give active roles to all local players who need to be included, but build on deep-seated local strengths and traditions. If these are different from the factors that underpin resilience in our own systems, so be it; in learning about them we can only improve and expand our own understanding of what the concept means.

Be(a)ware of Politics

A further, less-rational complicating factor in the civil security field is that of political differences both within and between states. No one having watched Europe's efforts to handle abnormal southern migration flows in 2015–16 could fail to see that EU nations—closely integrated as they are—have very different political attitudes and sensibilities about migrants, by no means simply proportionate to the material interests at stake. Germany has shown an example of internal differences, where the political establishment have taken one attitude and large parts of the general public have begged to differ. Naturally this undermines the chances of successful nation-to-nation cooperation, and has even raised the specter of backsliding in some established European common endeavors such as the Schengen zone.

Not all areas of public policy important for resilience, of course, have the same politically explosive quality as migration and multi-culturality. Yet what is non-sensitive for one country (or regional grouping) may be a political hot potato for another. Even among the five Nordic states, who have made special efforts since 2009 to upgrade their joint efforts for resilience through the Haga process, fundamental issues have been posed by diverging attitudes towards the role of the military and towards sharing leadership with the private business sector. Approaches to emergency handling may also run into issues of central/local power-sharing and legal/judicial processes where even heavily integrated nations feel strongly about pre-

serving their own models. The only general advice that can be offered here for a forward resilience initiative is to research the ground carefully and try, if possible, to avoid the pitfalls of political sensitivity and division that risk sabotaging rational cooperation from the outset. Who offers the partnership and how it is offered could easily become the first stumbling point.

Be Sure You Have the Answers

There are two issues here, both related to competence. First, decisions on which international organizations to work with and through for a forward resilience programme should be based on their capability and general appropriateness, not on institutional politics or wishful thinking about boosting the institutions themselves. For the Euro-Atlantic community, both NATO and the European Union (EU) may seem natural tools for outreach in resilience policy, not least as they have large and well established frameworks of external partnership. But when the two sides of the Atlantic wish to cooperate themselves in non-military security and emergency handling, they do so to an overwhelmingly greater degree through the EU than through NATO. The EU has the sectoral competence, the funds, and the ability to regulate that the Alliance lacks. Through the hold it exerts over its several applicant countries, it has a unique chance of getting them to join common systems and standards even while they await full entry. NATO is indispensable, rather, in any context that requires the application of hard military expertise and assets, which may be relevant at many stages starting with data acquisition and analysis. It goes without saying that the best results will be reached by using both institutions in combination on a basis of comparative advantage.

However, there are many specific fields of resilience promotion in which different institutional frameworks might be the first choice. For globally interconnected systems, action at the UN level or in the various specialized agencies makes most sense. At the other extreme, for certain kinds of physically limited emergency shaped by the local environment, neighborhood institutions like those existing in Europe's Far North, the Baltic Sea region and the Black Sea region can prove surprisingly effective, for reasons that include their low political salience and ability to mobilize non-state constituencies. In other parts of the world, the possibility of structuring partnership in a top-down way through existing regional security organizations should at least be looked at, since it might have potential

to strengthen those institutions as well as guaranteeing transnational approaches.

The remaining point is that we—in this context meaning basically the Euro-Atlantic community—cannot build a forward resilience program on the assumption that we know all the answers, even for our own cases. Time and again, in contexts ranging from the UK's winter floods of 2015–16 to the region-wide migrant crisis, Western societies and governments have been caught out by essentially known hazards and have suffered more damage and slower recoveries—including political fallout—than the public might reasonably have expected. The reasons may include any and all of the difficulties discussed above, but perhaps also broader factors like the debilitating effect of the still-not-surmounted global economic crisis. Against such a background, it is commendable that the developed West should contemplate new efforts for exporting security in a new conceptual framework that has potential to advance local partners' interests even more than our own. It seems best, however, to develop any initiative for forward resilience in a sober spirit that recognizes how much we have to learn as well as teach.

About the Authors

Daniel S. Hamilton is the Austrian Marshall Plan Foundation Professor and Executive Director of the Center for Transatlantic Relations at Johns Hopkins University's School of Advanced International Studies. From 2001–2015 he also served as Executive Director of the American Consortium for EU Studies. He has led the international policy work of Johns Hopkins University's PACER consortium, designated as a U.S. Center of Excellence in Homeland Security Affairs, was co-director of the ministerial level bioterrorism exercise *Atlantic Storm*, and has published widely on resilience issues. He has served as U.S. Deputy Assistant Secretary of State responsible for NATO, OSCE, Nordic-Baltic and transatlantic security affairs; U.S. Special Coordinator for Southeast European Stabilization; Associate Director of the Policy Planning Staff for two U.S. Secretaries of State; and Director for Policy in the Bureau of European Affairs. In 2008 he served as the first Robert Bosch Foundation Senior Diplomatic Fellow in the German Foreign Office. Recent publications include *Alliance Revitalized: NATO for a New Era* (2016, by the Washington NATO Project); *The Eastern Question: Russia, the West and Europe's Grey Zone* (2016, with Stefan Meister); *Rule-Makers or Rule-Takers* (2016, edited with Jacques Pelkmans); *Advancing U.S.-Nordic-Baltic Security Cooperation* (2014, edited with Andras Simonyi and Debra L. Cagan).

Robert Bach works with a variety of academic research and consulting groups on projects related to community resilience, countering violent extremism, affordable housing and inequality, and U.S. relations with Cuba and the Caribbean. He also consults with the U.S. Department of Homeland Security. From 1993 to 2000, he served in the U.S. Department of Justice as the senior policy and planning official for the Immigration and Naturalization Service. He received his Ph.D from Duke University and has been a professor at several universities for much of the past 30 years.

Alyson JK Bailes was a British diplomat and scholar. After postings in Budapest, at NATO, and in Bonn, she served from 1984–1987 as Deputy Head of the Policy Planning Staff at the Foreign and Commonwealth Office in London; as Deputy Head of Mission, Consul-General, and a member of the Sino-British Joint Liaison Group on the Future of Hong Kong at the British Embassy in Beijing from August 1987 to November 1989; as a guest scholar in 1990 at Chatham House; and as Deputy Head

of Mission and Consul General at the British Embassy in Oslo from 1990-1993. In 1994 she became Head of the Security Policy Department at the Foreign and Commonwealth Office in London. She served as Vice President for the European Security Program at the Institute for EastWest Studies (now EastWest Institute) in New York from April 1996 to August 1997. She served as Political Director of the Western European Union in Brussels from September 1997 to July 2000. She served as British Ambassador to Finland from November 2000 to June 2002, and was Director of the Stockholm International Peace Research Institute (SIPRI) from 2002-2007. From 2007-15 she was an assistant professor at the University of Iceland and visiting professor at the College of Europe from 2010-2015. She authored many articles in international journals, and some book chapters, on subjects principally related to European defense, regional security cooperation, and arms control. This chapter was her last published contribution before her death in April 2016.

Hans Binnendijk is a Senior Fellow at the Center for Transatlantic Relations at Johns Hopkins University's School of Advanced International Studies. Until July 4, 2012, he was the Vice President for Research and Applied Learning at the National Defense University and Theodore Roosevelt Chair in National Security Policy. He previously served twice on the National Security Council staff. He has also served as Principal Deputy Director of the State Department's Policy Planning Staff and as Legislative Director of the Senate Foreign Relations Committee. He has received three Distinguished Public Service Awards and a Superior Service Award. In academia, he was Director of the Institute for the Study of Diplomacy at Georgetown University and Deputy Director and Director of Studies at London's International Institute for Strategic Studies. He is author or co-author of more than 100 articles, editorials and reports. His most recent book is *Friends, Foes, and Future Directions*, published by RAND (2016). He serves as Vice Chairman of the Board of the Fletcher School of Law and Diplomacy and was Chairman of the Board of Humanity in Action.

Charlotta Collén is a Special Advisor for Research at Ministry of Defense of Finland. She has previously worked as Special Advisor for Policy Planning and Research at the Ministry of Foreign Affairs of Finland. She holds a Master's degree in Social Sciences from the Åbo Akademi University in Turku, Finland where she is in the process of defending her thesis on European Foreign Policy and the Case of European Security and Defence policy (CSDP). In academia she has been teaching and publishing in EU affairs, while pursuing a career in the Foreign and Defense Services of Finland.

Björn Fägersten is the Director of the Europe Program and a Senior Research Fellow at the Swedish Institute of International Affairs. His research interests cover intelligence, European integration, political risk, security policy and international institutions. He has a Ph.D in political science from Lund University, Sweden, and has held research fellowships at Harvard's Kennedy School of Government and at the European University Institute.

Axel Hagelstam is currently Counselor for Civil Emergency Planning at the Finnish Mission to NATO and Vice-chair of NATO's Civil Protection Group. Previously he has worked as Political Adviser at the European Parliament, Special Adviser at the Finnish Ministry of Defense and as Researcher at the National Emergency Supply Agency. He holds a Master of Political Science from Åbo Akademi University.

Tomas Jermalavičius is Research Fellow and Head of Studies at the International Centre for Defense and Security in Tallinn, Estonia, where he focuses on issues pertaining to science, technology and innovation, defense industry, security and defense governance and management (especially civil-military relations, whole-of-government approach and organizational culture), foresight and resilience. Prior to joining ICDS, Tomas worked at the Baltic Defense College, first as deputy director of the College's Institute of Defense Studies from 2001–2004, and later as dean of the college from 2005–2008. In the latter capacity, he was also the editor of the journal *Baltic Security and Defence Review*. He was also involved in the Prometheus Program of Transition Studies at the Euro-College of the University of Tartu, the post-graduate military diplomacy program at the Lithuanian Military Academy as well as in various projects of the Estonian Academy of Young Scientists (ENTA). In 1998-2001 and in 2005, he worked at the Defense Policy and Planning Department of the Lithuanian Ministry of National Defense. At the end of 1998–beginning of 1999, he was a research fellow at the Swedish National Defense Establishment (FOA, now FOI). He holds a BA in political science from the University of Vilnius, an MA in war studies from King's College London and an MBA degree from the University of Liverpool.

David J. Kaufman is the Vice President and Director for Safety and Security at CNA, a nonprofit organization that provides in-depth research and applied analysis to government leaders. From 2009 to 2015 he served as the Associate Administrator for Policy, Program Analysis, and International Affairs at the U.S. Federal Emergency Management Agency. He is a member of the National Academies of Science's Resilient America Roundtable;

former faculty at the Naval Postgraduate School's Center for Homeland Defense and Security; and has previously served in several senior positions in the U.S. Department of Homeland Security.

Lorenz Meyer-Minnemann is the Head of Civil Preparedness in the NATO International Staff. In this capacity, he is responsible for supporting NATO nations in ensuring resilience for crises and conflict, including hybrid warfare, and for ensuring effective civil support to Alliance planning and operations. He was appointed to the position in February 2015. He began his NATO career in 2001 and he has held numerous positions, including as policy planning advisor in the office of NATO Secretary General Anders Fogh Rasmussen, as political affairs officer responsible for NATO Summit meetings and relations with the United Nations, and as desk officer for the Caucasus and Central Asia in NATO's Political Affairs and Security Policy Division.

Piret Pernik is a Research Fellow at the International Centre for Defense and Security in Tallinn, Estonia. Her research focuses on cyber security strategy and policy, cyber security threats and risks, and other related issues. In addition she has been involved in research and training projects on strategic decision-making in cyber security and defense. Her research areas include cyber security and defense strategies and policies in Estonia, the European Union, OSCE and NATO. She also analyses and recommends ways to foster public-private cooperation on national and international levels. In her research activities she actively cooperates with international and domestic stakeholders from government entities, private sector, and with academic and research communities. Before joining ICDS, she worked in the Estonian Ministry of Defense. She has served as an adviser to the National Defense Committee of the Riigikogu (Estonian Parliament).

Tim Prior is head of the Risk and Resilience Research Team at the Center for Security Studies (CSS) of ETH Zurich. He has completed a Doctorate in Social and Environmental Psychology from the University of Tasmania (Australia), a Master's degree in Environmental Science from James Cook University (Australia), and completed his undergraduate studies in quantitative ecology. Before joining the CSS, he was a research principal at the Institute for Sustainable Futures at the University of Technology, Sydney. His research has focused on risk and decision-making under uncertainty, particularly in relation to individual, community and organizational preparation and response to environmental risk. His most recent work has included foresighting research on natural resource security in Australia,

as well as exploring new mechanisms for risk communication with respect to natural hazards like wildfire.

Mark Rhinard is Professor of International Relations at Stockholm University and Senior Research Fellow at the Swedish Institute of International Affairs. His research examines international cooperation on complex threats, with a special interest in the European Union. His recent works include *Theorising Internal Security Cooperation in the European Union* (with Raphael Bossong; 2016, Oxford) and *The European Commission* (with Neill Nugent; 2015, Palgrave).

Tomas Ries is Senior Lecturer in Security and Strategy at the National Defense College in Stockholm, Sweden. He has worked with security studies since 1979, and his three main interests are the globalizing security environment and future trends; the epistemological and practical challenges of the new security environment; and the essence of strategy and security. He served as Director of the Swedish Institute of International Affairs from 2005 to 2010, Senior Researcher at Finland's National Defense College from 1997 to 2004, as Deputy Director of the Geneva Center for Security Policy in 1996–1997, as Senior Researcher at the Institute for Defense Studies (IFS) in Oslo from 1988 to 1992, as a Researcher at the Norwegian Institute of International Affairs (NUPI) from 1986 to 1988, and as Nordic Correspondent for the International Defense Review in Geneva from 1981 to 1991. He holds a Ph.D. from the Graduate Institute of International Studies at Geneva University. He has written two books and over one hundred articles and research studies.

Bengt Sundelius is Professor of Government of Uppsala University and the Swedish Defense University. He serves as strategic advisor to the Director General of the Swedish Civil Contingencies Agency and has published widely on national and societal security, crisis management and Nordic relations.

Anna Wieslander is Director for Northern Europe at the Atlantic Council and Secretary General of the Swedish Defense Association. She was previously Deputy Director at the Swedish Institute of International Affairs. She has held positions as Head of the Speaker's Office in the Swedish Parliament, Secretary of the Swedish Defense Commission and Deputy Director of the Swedish Defense Ministry. Her expertise is in security and defense policy, NATO and Partnership for Peace, the transatlantic link, and issues affecting the defense industry.

Forward Resilience

Protecting Society in an Interconnected World

Daniel S. Hamilton, Editor

The capacity of a society to anticipate, pre-empt and resolve disruptive challenges to its vital functions has become a high priority for many countries across the Atlantic and around the world. But is resilience enough to deal with disruptive threats in a deeply interconnected world? In this volume eminent authors argue that state-by-state approaches to resilience are insufficient. Not only must resilience be shared, it must be projected forward, and traditional notions of territorial security must be supplemented with actions to address flow security - protecting critical links that bind societies to one another. Authors include

Robert Bach
Alyson JK Bailes
Hans Binnendijk
Charlotta Collén
Björn Fägersten
Axel Hagelstam
Daniel S. Hamilton
Tomas Jermalavičius
David J. Kaufman
Lorenz Meyer-Minnemann
Piret Pernik
Tim Prior
Mark Rhinard
Tomas Ries
Bengt Sundelius
Anna Wieslander

This project was conducted by the Center for Transatlantic Relations at Johns Hopkins University's School of Advanced International Studies, together with the Swedish Civil Contingencies Agency, the Swedish Atlantic Council, the Finnish Ministry of Defense and the Finnish Ministry of Foreign Affairs.

SAIS JOHNS HOPKINS
SCHOOL of ADVANCED
INTERNATIONAL STUDIES

Center for Transatlantic Relations
The Paul H. Nitze School of Advanced International Studies
The Johns Hopkins University
1717 Massachusetts Avenue, NW, 8th Floor
Washington, DC 20036
Tel: (202) 663-5880
Fax: (202) 663-5879
Email: transatlantic@jhu.edu
Website: http://transatlanticrelations.org

$35.00
ISBN 978-0-9907721-5-6
53500>
9 780990 772156