ÚSTAV
MEZINÁRODNÍCH VZTAHŮ
PRAHA
iir
INSTITUTE
OF INTERNATIONAL RELATIONS
PRAGUE

Resilience Capacity Building – Implications for NATO

Conference Report

June 1–2, 2017

This publication is supported by:

The NATO Science for Peace and Security Programme

Resilience Capacity Building - Implications for NATO

Conference Report

June 1-2, 2017

Table of Contents

Editor's Note
5

Introduction
(*Jiří Šedivý*)
7

Scene Setter: Resilience Training and Education in the Context of NATO
(*Vlasta Zekulić*)
11

Resilience Training and Education: A Perspective from Finland
(*Piritta Asunmaa*)
15

Panel 1:
Understanding Resilience – National and Institutional Approaches
19

Panel 2:
Preparing for Emergencies – Best Practices in Training and Modelling
25

Panel 3:
Resilience Education and Training – Implications for NATO
29

Rapporteur's Observations
(*Jamie Shea*)
35

Key Takeaways & Recommendations
(*Lorenz Meyer-Minnemann*)
41

Annex 1: Programme of the Conference
45

Annex 2: List of Participants
51

Editor's Note

In preparing the report from NATO's Advanced Research Workshop on "Resilience Capacity Building: Best Practices and Opportunities for NATO" every effort was made to accurately capture the essence of the discussions and transcribe the speeches and comments recorded over the course of the conference. The attributed sections are being published with the consent of the authors. The biographies of the speakers and professional affiliations of the conference participants listed in this publication reflect their status as of June 2017. The highlights and italics in the text are editorial. Any errors or inaccuracies in this report are my sole responsibility.

JAN HAVRÁNEK
Editor
Brussels, May 2018

Introduction

AMB. JIŘÍ ŠEDIVÝ
Premanent Representation of the Czech Republic to NATO
Conference Chairman

In the context of rising global instability and the gradual weakening of the liberal international order, preserving the basic functions (and values) of the state and society is essential. The concept of resilience has become one of the central organising principles supporting the stability of a state and the security of its citizens. Resilience, best described as a set of adaptive responses to a rapidly changing, highly interlinked and considerably unpredictable environment, seems to be the recipe for facing sudden systemic crises and strategic shocks.

At the Summit in Warsaw in July 2016, NATO Heads of State and Government pledged to enhance resilience within their nations to underpin the Allies' solidarity and commitment to defend one another.

Resilience is the backbone of the Alliance. It is an essential basis for credible deterrence and effective fulfilment of NATO's core tasks. It is a cross-cutting concept transcending a number of strategic areas for NATO, such as the improvement of civil preparedness, strengthening continuity of government, protection of critical infrastructure, building of cyber defence, investment in military capabilities, and preparedness for CBRN threats.

Resilience also requires engagement with partners and other international bodies, including the European Union. Addressing partners' vulnerabilities and building their capacities can contribute to a broader projection of stability in NATO's neighbourhood. Resilience is also one of the pillars of the European Global Strategy and thus complements the efforts of NATO.

NATO is not starting from scratch in this respect. Elements of resilience are incorporated in NATO's Strategic Concept of 2010. In the Framework for Future Alliance Operations (2015), the Allied Command Transformation has recognised shared resilience as one of the strategic military perspectives. Since the Newport Summit in 2014, as a part of NATO's long-term adaptation, the Allies have focused on enhancing resilience across a number of areas, such as cyber defence, decision-making, logistics, and others.

The Summit in Warsaw has, however, underscored the fact that the resilience of the Alliance relies, first and foremost, on the resilience of its nations and partners. NATO's Civil Emergency Planning Committee (CEPC) has been working in close cooperation with the NATO Military Authorities and selected NATO partners on the implementation of the agreed baseline requirements, including the development, and of tools to support NATO nations. In sum, enhancing resilience requires a comprehensive, cross-government approach by all NATO members. Equally, it requires a structured, holistic approach to training and education in resilience-related areas.

Towards this end, the Czech Republic proposed to organise a workshop that would address the current institutional and selected national approaches to resilience with the aim to identify training priorities, opportunities and gaps, as well as possible mechanisms and platforms.

The effort resulted in the NATO Advanced Research Workshop on *"Resilience Capacity Building: Best Practices and Opportunities for NATO,"* which took place on June 1–2, 2017, in Prague, the Czech Republic.

The workshop was organised by the Prague-based Institute of International Relations (IIR) together with the Finnish Institute of International Affairs (FIIA). The meeting had the goal of broadening the existing network of civilian and military experts on resilience from Allied and partner countries and included experts currently not involved in NATO's core work on resilience.

The report you are reading presents the summaries of the panel discussions (which were held under the Chatham House Rule), and also transcripts of contributions from the keynote speakers and other authors, which complement the discussions.

The first panel looked at the institutional approaches to resilience, and how NATO can benefit from the myriad of national systems. The second panel addressed the best practices and training in resilience and featured case studies from the Czech Republic, Sweden and Israel. The third panel looked at the ways that resilience training and education could be built into the existing structure of NATO.

Dr. Vlasta Zekulić from the NATO Headquarters laid out an important distinction between resilience-related *education* and resilience *training & exercises*. Her briefing paper provided the overall framework for the conference discussions.

Ambassador Piritta Asunmaa, my counterpart at the Finnish Mission to NATO, delivered an outstanding keynote speech during the conference luncheon. In it, she linked resilience to the issue of basic values and human rights.

Jamie Shea of NATO took a complex and futuristic look at resilience. He argued that the future of uncertainty and contingencies had already happened, so it is the highest time for us to prepare for it.

The final section consists of the summary of and recommendations drawn from the three panels and an additional summary by the second rapporteur from NATO, Lorenz Meyer-Minnemann.

Finally, I would like to acknowledge several individuals and institutions that planned and organised this conference.

Jan Havránek, my year-long collaborator and defence counsellor at the time of the event, conceived the idea of a joint civil-military project focused on training and education in the summer of 2016. He was crucial in developing the concept for this event and liaising with a number of stakeholders. He also assembled and edited this report.

We found a natural partner in Finland, whose national resilience system is exemplary. The project benefitted greatly from the expertise and dedication of the Finnish Mission to NATO – Ambassador Pirita Asunmaa, Karoliina Honkanen, and Axel Hagelstgam, who also contributed to this report. We are also grateful for the hospitality of H.E. Helena Tuuri, the Ambassador of Finland to the Czech Republic, and for her hosting of the opening reception in Prague

Michal Kořan and Mikka Wiggel, representing the Institute of International Relations (IIR) in Prague and the Finnish Institute for International Affairs (FIIA), respectively, provided important perspectives and guidance during the preparations of the workshop and also when they served as the moderators of two of the panels.

This event would not be possible without NATO, which kindly provided the funding for it through the Science for Peace Programme, and the support of a number of members of the NATO International Staff. Jamie Shea, the Deputy Assistant Secretary General at the Emerging Security Challenges Division, was essential in reviewing the initial concepts and securing the support for this initiative across the NATO Headquarters. Lorenz Mayer-Minemann was extraordinarily helpful in making sure our focus complemented NATO's ongoing strands of work on resilience. Admiral Pete Gumataotao and his dedicated team at the Allied Command Transformation kindly included us in their series of workshops on resilience. The steadfast conceptual advice from all these experts was invaluable.

Special thanks goes to Kateřina Pleskotová and Lucie Božková (Dobešová), who ensured the smooth organisation of the event – both from Brussels and in Prague.

Finally, we are grateful to all the participants, who made this event meaningful.

Scene Setter: Resilience Training and Education in the Context of NATO

LT. COL. (RET) VLASTA ZEKULIĆ
Officer, Strategic Assessment Capacity
Emerging Security Challenges Division, NATO HQ

The perception of safety and security has changed immeasurably in the last decade. Practitioners of hybrid warfare, such as Russia, are often less intent on seizing and holding territory than on destroying or disrupting the ability of governments to function.[1] Experts argue that against hybrid threats alongside illegal immigrants, cyber-attacks, terrorism and other hazards, a military deterrent and a response capability are necessary but not sufficient.

Faced with a variety of different risks, policy-makers have recognised that not all disasters can be averted, and security can never be fully achieved.[2] This explains why resilience has assumed so much importance lately – it aims at making actors sufficiently prepared and exercised to resist, recover from and then adapt to adverse events.[3]

NATO's objectives in this respect – to deter, contain, respond to, and remain resilient to the violent, disruptive, or military efforts of others – have started materialising since the Wales Summit in 2016 as a part of NATO's long-term adaptation. The Allies have focused on enhancing resilience across a number of areas, such as civil preparedness, cyber, decision-making, and logistics, and against hybrid threats. At the Summit in Warsaw, an important step forward was taken by NATO's Heads of State and Government in pledging to enhance resilience within their nations.

---

[1] Franklin Kramer, Hans Binnendijk, and Dan Hamilton, "Defend the Arteries of Society," *US News and World Report*, 9 June 2015.

[2] Corinne Bara and Gabriel Brönnimann, *Resilience. Trends in Policy and Research*, ETH Zürich, Center for Security Studies (CSS), April 2011, p. 6.

[3] National Research Council, *Disaster Resilience: A National Imperative*, Washington, DC: The National Academies Press, 2012, p. 1.

Enhancing resilience is difficult.[4] It requires a comprehensive, cross-government approach to formulate a strategy and follow-on procedures, which are required to assess and maintain resources, and inject resources into systems to keep them functioning in the face of internal or external change. Depending upon the nature of the system – an infrastructure or a society – the resources and the instruments are not always the same.[5]

The way NATO understands resilience focuses less on society itself and more on the core elements required to maintain the overall government capacity so that the government runs smoothly and deploys its forces efficiently, e.g. by avoiding economic and societal disruption through resilient infrastructure and governance – the relevant measures are described in NATO's Seven Baseline Requirements.[6]

Although a state-by-state approach to resilience is important, in this interconnected world a collaborative approach, one that addresses the seams, interfaces and global spaces, is far better fitted to contribute to the Alliance's overall security. By integrating nations and partners' visions of resilience into overarching concepts and policies, NATO can serve as a clearing house and a standardising body that can help corral and focus national efforts, especially in two important areas: education and training.

Education helps increase the understanding of risks and threats against which resilience needs to be built. The Russian hybrid model of warfare leverages every available means to undermine the credibility of an adversary by the use of proxies, terrorist groups, cybercriminals, energy blackmail, sabre-rattling and military manoeuvres; and to expose vulnerabilities and weaknesses in our open and interconnected societies.[7] This way of

---

[4] Academics still debate over the forms of resilience: the simplest way of thinking about resilience considers that resilience refers to the ability to recover from a disturbing event as if it never happened (the "bounce back" scenario). Other approaches value the possibility to not only restore the system after a disturbing experience, but also to learn from this experience to adapt and avoid the likelihood of future attacks ("adaptation"). Myriam Dunn Cavelty, *Resilience in Security Policy: Present and Future*, ETH Zürich, CSS Analysis, n°142, October 2013, p. 2.

[5] Trusted Information Sharing Network for Critical Infrastructure Resilience (TISN). *National Organisational Resilience Framework Workshop: The Outcomes. 5th–7th December 2007*, Mt. Macedon Victoria, Australia, p. 6.

[6] For an overview of NATO's work on resilience, see, e.g., Shea, Jamie, *Resilience: A Core Element of Collective Defence*, Brussels, NATO Review, March 2016 (http://www.nato.int/docu/Review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/index.htm).

[7] See, for instance, Keir Giles, *Handbook of Russian Information Warfare*, Rome, NDC, 2016 (http://www.ndc.nato.int/download/downloads.php?icode=506) or Guillaume Lasconjarias and Jeffrey A. Larsen (eds.), *NATO's Response to Hybrid Threats*, Rome, NDC Forum Paper 24, 2015 (http://www.ndc.nato.int/download/downloads.php?icode=471).

"looking" at our systems can, and should, be taught through an integrated civil-military education programme. Broader learning and education about resilience can also help overcome the problems often encountered by planners and logisticians in differentiating between war-time and peace-time assets and programmes, since the common and joint use of many assets can lower the national costs and build a sufficient redundancy into resilience. This entails an investment of time and human resources into developing a consistent, accepted and accredited approach to learning and education. In time, it can enable nations and the Alliance to develop an ability to simultaneously generate a surge capacity to cope with mass casualties, manage population flows and meet the resource demands of a military force whilst protecting critical infrastructure.

Nevertheless, *know-how* is only the first part of the equation – ***training and exercises*** are the second. Training enhances interoperability among national and partner systems and bodies, the agility of responders and the speed of recovery. Resilience concerns not only physical entities (services or infrastructure) but also the society at large; it underscores the capability of an organisation to continue working under severe conditions and stresses and/or recover as quickly as possible. This domain of readiness should be exercised in real-time conditions and with realistic scenarios, and driven by "brutal" red teaming. Carrying out exercises that simulate strategic and operational catastrophic failures or denial provides another test of material and personal resilience which is rarely practiced, though such exercises are particularly useful for cases in which a single point of failure can cause a cascading effect – for example, a cyber-attack on a critical energy node. This approach to exercises, combined with an enduring education process, particularly towards the trainers themselves, will not only increase people's skill set, but also help build psychological resilience.

Through a more holistic approach to education and training, NATO, its member states and its partners can address the challenge of improving the resilience of its systems, its society and its forces. In achieving this, both the resilience and the deterrence against the full spectrum of security threats of the 21st century will be enhanced.

Resilience Training and Education: A Perspective from Finland

Remarks by
H.E. AMB. PIRITTA ASUNMAA
Mission of Finland to NATO

First of all, let me thank our Czech colleagues for initiating and hosting this conference. Finland has been very happy to contribute to this event. We obviously share a strong interest in resilience capacity building, and it is a topic that is relevant for both the Allies and the partners.

Last night we discussed the challenges of understanding resilience and vulnerabilities in the "modern era." It struck me that maybe we do not realise how great the leaps in science and technology have been during this "modern era." We do not yet fully understand the impact of the technological changes during the last 25 years on our societies. Until we understand these deeper consequences, we will remain ignorant of our vulnerabilities and unable to proactively prevent crises.

It is clear that today's society relies on systems and functions that are highly vulnerable. Few people understand these systems, and even fewer know how to operate them. An important aspect to remember is that the civil infrastructures on which these vital systems and functions rely are designed and built to generate financial profit, not resilience. A large majority of these infrastructures are built with private money and owned by private operators beyond government control.

After the Cold War, we haven't had to face any existential challenges. War has been considered inconceivable in the European theatre, and there have been no truly large-scale natural or other disasters in Europe. Nevertheless, the war in Ukraine and migration movements have unfortunately brought crises much closer to our doorstep, but not on an existential scale. The Ebola outbreak in Western Africa is the closest we have been to an existential threat in recent times, but luckily the virus was not airborne this time.

As a consequence of this, 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. I think it is time to accept that in a severe crisis, not everything can be protected. We must therefore identify functions that are decisive for society's survival, and focus our efforts on them.

Failure to address our vulnerabilities will mean that we will be unprepared in the face of large scale disasters. More importantly, we will be defenceless against an adversary that would look for these vulnerabilities in our societies and possibly exploit them in order to paralyse us. Russia's applications of hybrid warfare in Ukraine and elsewhere are important lessons in this regard. While hybrid threats are predominantly directed towards soft (non-military) targets, the threat of the use of or actual use of military tools (such as little green men, or even heavier weaponry) is inherently part of the hybrid toolkit. From this perspective, resilience is as important for national security as maintaining a credible military defence.

The First Impressions Report from the ACT Conference "Interdependency in Resilience," held in Norfolk in May 2017, states that "education is a fundamental building block in achieving resilience; this develops our shared awareness and helps us understand risks and accept the subsequent actions." I could not agree more.

In Finland, there are three main tools for increasing resilience through education: the basic education curriculum, the general conscription system, and national defence courses. Pupils in secondary school receive practical basic information on how to prepare for and react in a crisis situation. For the male population, the general conscription provides not only military training but also a certain basic understanding of national security and everyone's role therein. Finally, the defence forces together with municipal and regional authorities arrange national defence courses for business leaders, politicians and important public servants, in which a comprehensive concept of security is taught and the cooperation between all parts of society is underlined.

Vulnerability and resilience will be one of three core topics that the [recently founded] European Centre of Excellence in Countering Hybrid Threats in Helsinki will be dealing with. Training and education will be key tools for the Centre in strengthening the understanding of the hybrid operating environment.

Finally, I have one more point I would like to raise. There are those who seem to advocate that resilience requires ultimate flexibility and adaptability. It is true that resilience implies a readiness to adapt to changing circumstances, but I do not think resilience means that everything must be flexible and adaptable.

Yes, we must design and build our vital systems in a way that makes them capable of withstanding shock and bouncing back quickly. Yes, we must be prepared to temporarily live without Facebook or Twitter, mobile phones, or, in extreme situations, even water and electricity.

But our core values are not flexible or adaptable. Basic human rights, equality, the rule of law, free and open elections (i.e. democracy), etc. are not flexible; they are absolute. They cannot be changed or adapted to suit a new threat environment.

On the contrary, the stronger the pressure on us to make exceptions from these values and principles, the harder we must resist. The resilience of our core values and principles depends on how strongly we believe in them, and how much we are willing to sacrifice to maintain them. And again, education is the basis for an understanding of the difference between what is fundamental, and what is not.

Panel 1: Understanding Resilience – National and Institutional Approaches

Summary of the Discussion

The panel addressed four institutional approaches to resilience capacity building: the approaches at NATO's Allied Command Transformation, within the United States government, on the level of the European Union, and in Finland.

Resilience has many faces, touching the full spectrum of conflict, all layers of society and a myriad of actors. For NATO, resilience means, first and foremost, improving and maintaining the Alliance's capacity to resist an armed attack. Preparedness is at the heart of resilience, which is in line with NATO's "all hazard" approach: a power outage can be induced by both a natural disaster and state or non-state actors. From the resilience point of view, the perpetrating source does not matter, as the result is the same. NATO's approach to resilience is enshrined in NATO's founding document, the Washington Treaty. In Article 3 of this Treaty, the Allies commit themselves to build capacities (individually and collectively) to resist an armed attack. It is no accident that Article 3 (preparedness) comes before Articles 4 and 5: the Allies are supposed to do their homework (Art. 3), and then ask for political consultations (Art. 4) and assistance from the other Allies (Art. 5). NATO's resilience is very much related to one of the core tasks, collective defence. Resilience has a deterrent value in its own right, and is also an important feature of another aspect of collective defence, rapid reinforcement. NATO's military forces and ability to deliver assistance are dependent on the resilience of civilian infrastructure. Resilience is also supporting cooperative security (with NATO's Partners), and crisis management as well. Rather than being a "fourth core task," resilience is a critical enabler of all three of the existing core tasks that are NATO's core business.

NATO has defined seven baseline requirements for national resilience:

1) Assured continuity of government and critical government services.

2) Resilient energy supplies.

3) An ability to deal effectively with the uncontrolled movement of people.

4) Resilient food and water resources.

5) An ability to deal with mass casualties.

6) Resilient communications systems.

7) Resilient transportation systems.

NATO's Resilience Pledge, adopted in Warsaw in 2016, acknowledges the whole of the government approach reflected in these principles and also the need to work with other actors, including the European Union.

In order to progress better in resilience, nations need to commit resources to and invest in infrastructure, education and capabilities. In this regard, NATO's resilience pledge is therefore closely linked to another commitment, the Defence Investment Pledge (adopted at the Wales Summit in 2014). Spending on resilience should aim over and above the traditional figure of 2% of GDP and not be at the expense of general defence spending.

In May 2017, the Allied Command of Transformation (ACT) in partnership with the City of Norfolk, Virginia, organised a conference entitled "Interdependency in Resilience," which was supported by the Allies, the NATO Partners, and representatives of government, including the municipal and private sectors. The event aimed to catalyse the collaboration among these actors and help build resilience across the Alliance in support of the ongoing activities of the NATO Headquarters in the field of resilience.

The conference formulated four key takeaways that can be universally applied to any system of resilience, be it on the local, national or international level:

- Build persistence in resilience, and make it a habit. The experience from natural disasters and national contingencies shows that even the best resilience system can lead to complacency, and therefore to catastrophe. Such was the result when Hurricane Katrina hit New Orleans in 2004: The city had prepared for a storm, but it had not anticipated the "mother of all storms," so to speak.

- Look at resilience as a capacity that includes the full spectrum of tools provided by all relevant stakeholders (both public and private); make this capacity operational and adaptive at the same time. The operational aspect addresses the issue of business continuity. Innovation in and adaptation of our approaches to resilience can improve the connectivity among the relevant actors.

- Integrate resilience into the education system, and the best practices and lessons learned in this area should be taught as well. This will ensure that those who respond to disasters and contingencies will not make the same mistakes as their predecessors and will deal with crises more effectively. For example, despite the lessons learnt from

the above-mentioned Hurricane Katrina, the same resilience-related mistakes were made again during Superstorm Sandy in 2012.

- Expand the experimentation, modelling and simulation in resilience training. The Allied Command for Transformation can provide assistance to NATO and the Allies with regard to the future exercises and requirements. (Note: For more on this subject, please see the summary of Panel 3.)

The next case study focused on the issues of resilience and critical infrastructure, based on the experiences from the United States, where twelve of the fifteen most costly contingency events since 2001 happened. The lessons learnt apply equally to NATO, or any other governmental organisation, of any size and composition, that seeks progress in resilience. The following points were raised in the corresponding discussion:

- The connectedness of today's world creates interdependencies that often lead to tragic situations; such events reveal how fragile our system is.

- It has become very clear that government by itself cannot effectively ensure that our societies can become more resilient and capable of recovering from and adapting to disruptive events. Such events will inevitably continue to occur in increasingly greater number in the years ahead (fuelled by terrorism, climate change, and other trends).

- Disruptive events that bring about a lot of cascading effects (such as outages of power, disruptions of public transportation, etc.) do not discriminate among the state actors: resilience is therefore needed at the state and institutional level, but civilians have a role in stepping up resilience as well.

- It is necessary to find more effective ways to improve civil society. The importance of civilian involvement in crisis response cannot be overlooked.

- A new role for government is to empower, equip and incentivise citizens to play a role in resilience during security crises or disasters. An average citizen should be able to step in if the government is unable, or sometimes unwilling to take action in such a situation.

- A top-down approach, such as that in the establishment of the Department of Homeland Security, needs to be complemented with a bottom-up approach.

- There are a number of examples of civilian action in catastrophes: "Occupy Sandy" was a movement following Superstorm Sandy in which civilian volunteers collected funding and supported the recovery effort with the use of social media, and no government supervision or leadership was involved in the project. They built partnerships across the private sector, set up distribution centres and took care of citizens in need. Similarly, the largest evacuation of people by sea took place during the attacks of 9/11,

as hundreds of private boat owners helped civilians in Lower Manhattan flee the area of the disaster.

- There are several prerequisites for a government-civilian partnership in resilience building: communication, trust, acceptance of a certain level of risk, and courage.

The notion of the division of labour between the governmental and the nongovernmental can be also applied to the different approaches to resilience on the NATO and the EU level.

Resilience in the European Union is understood as responses to or prevention of crises that could come from both state actors and non-state actors. The events of 2014 – Russia's illegal annexation of Crimea and the migration and refugee crisis – served as a "wake-up call" for the members of the EU. In 2015, the European Commission and the EU High Representative Federica Mogherini were tasked with coming up with options for approaches to resilience that would include both collaboration with NATO and the involvement of the European Union's partners. When it comes to resilience on the national level, the European Union can only help as far as the member states let her. Resilience, as the conference highlighted on a number of occasions, is primarily a national task. The European Union therefore recommended to its members that they assess their vulnerabilities and share their approaches to resilience among each other. Subsequent events, such as the terrorist attacks in Paris or the WannaCry cyber attacks, prompted the EU towards more action in terms of resilience. Since 2017, the EU member states have been defining how far this action can go and to what extent the process can be shared with NATO. In June 2017, the European Union issued a Joint Communication on the "Strategic Approach to Resilience in the EU's External Action." This Communication has built upon the previous approaches to resilience (which were rather related to the EU's humanitarian situation) as well as EU approaches to hybrid threats. The Joint Communication outlined twenty-two areas of resilience where member states have made progress. Most importantly, the Communication acknowledged that a change of mindset is required in order to start building resilience. It also brought forward the role of the European Commission as the key "administrator" of resilience-related projects. It has taken action in several "resilience domains," such as energy security (removal of legal barriers), money laundering (additional measures), or health (promoting a resilience mindset through, e.g., vaccination campaigns).

The EU does not intend to build its own propaganda, but giving correct information, including by countering influence campaigns, is a way to build resilience. Internal strategic communications can prevent radicalisation in society, so the EU currently has two task forces monitoring the Russian and Arabic language press and media so that they would be able to advise the EU leadership in the area of strategic communications.

The Joint NATO-EU Declaration from the Warsaw Summit provided a positive message: NATO and the EU are working together to build resilience both at home and in the partner countries. Moldova has been a good example and a recipient of this coordinated approach to resilience capacity building. Also, both organisations have developed parallel playbooks on how to deal with hybrid threats. Furthermore, when it comes to resilience in military forces, the European Defence Agency (EDA) has stepped up its effort, including in its interaction with NATO.

The panel also discussed the fact cultural differences between nations exists when it comes to resilience. In some countries, citizens do not see themselves as being at the centre of their country's resilience. They may, however, expect the state to deliver on all aspects of resilience on their behalf.

Related to this problem is the issue of national sovereignty. If the state is to delegate some roles in resilience to the private sector (or the citizens), it will have to admit that it cannot cope with every single problem and provide for some elements of security. On the other hand, however, too much control on the side of the private sector may obstruct resilience.

The panel agreed that the role of the government cannot be neglected. The state will always remain the primary responder; it needs to remain the facilitator, the "orchestra leader," who will maximise the synergies from all the actors in resilience. Armed forces, which are a function of a state, are also likely to be the first tool to respond to national contingencies. Our "over-reliance" on the armed forces may not be a big problem, provided that our militaries give adequate capabilities and training to the armed forces to deal with resilience.

The challenge remains to increase the citizens' ownership of resilience. The panel discussed the example of Finland, which combines the citizen-based approach to resilience with a solid institutional infrastructure called the Comprehensive Security Model. The origins of this model date back to the World War 2 survival experience. The tradition of total defence and security of supply were born in the 1940s and 1950s. Within the last decade, the interdependency of the international security environment led to modifications in Finland's approach to resilience. In 2003, the government of Finland approved the first Security Strategy for Society. The strategy focused on the protection of critical infrastructure, which was the first step towards comprehensiveness. Ten years later, however, Finland exchanged its total defence strategy for the Comprehensive Security Model. The difference between these two concepts is stark. The total defence concept was not an acceptable model for many actors, including businesses, some local communities, NGOs, and even some authorities. In contrast, The Comprehensive Security Model addresses both the most obvious hazards and more complex scenarios. This allows all relevant actors in the security system to join up, plan and exercise together. It also

allows for a greater engagement and commitment by civil society. The NGOs are the primary coordinators of the civil society effort and work closely with authorities. In the contemporary security environment, reliable and trustworthy information is crucial, including that from the private sector. This is why the Security Committee of Finland has a permanent private sector representative in addition to the traditional government members (ministers and experts). Overall, the comprehensive approach eventually led to and enabled the establishment of the European Centre of Excellence for Countering Hybrid Threats in 2017. As the security threats keep evolving, the comprehensive security model needs to adapt as well.

Panel 2: Preparing for Emergencies – Best Practices in Training and Modelling

Summary of the Discussion

The panel reflected on the following issues: To what extent are we ready and prepared for "virtual vulnerabilities"? Can sectoral approaches to resilience work? How can we model and prepare for cascading effects? How do we train people in resilience across all operational domains? How do we integrate resilience training and scenario modelling throughout NATO?

In order to train people and create models for contingencies, the panel agreed that involving various stakeholders, horizontally and vertically, in the process is crucial. The discussion featured the example of critical infrastructure networks. In many countries, these networks are in the hands of the private sector, which often results in a lack of understanding of business continuity planning for critical infrastructure on the side of the government. It is therefore essential to bring the private sector into the contingency modelling and risk assessment. But the approach to stakeholders needs to be cross-sectoral. Our system can benefit from impulses from academia and research, which can be from both the national level and international cooperation.

Training and exercising to the point of failure was highlighted throughout the discussion. If an exercise fails, it should be viewed as a positive outcome. If the exercise succeeds, it means that the planners had not considered all the options and variations. As it involves more than learning the best practices, exercising to the point of failure also helps to avoid the worst practices. Cultural perceptions need to be factored in as well. At NATO, with 29 nations present at the table, there is a need to build a leadership culture that accepts that we are exercising to the point of failure. It requires bravery at the leadership level, as the governments like to be portrayed as actors that can handle any crisis. Again, examples can be drawn from the private sector experience. Global corporations carry out exercises regularly, sometimes even a couple of times per months.

Given the changes in the security environment, our scenarios need to change as well. At NATO, for example, we need to move away from the traditional focus on posture management. The scenarios need to be agile, innovative and sophisticated ones that

present realistic challenges of the contemporary environment. They need to highlight the denial of access to systems and critical services beyond the critical infrastructures.

As for training and scenario modelling throughout NATO, NATO needs to keep reaching out to various national stakeholders who can introduce different models, be they civilian or military. The planning of the exercises also needs to be shortened. Understanding what is happening at the strategic level is crucial for the awareness at the tactical level. For instance, NATO's CMX exercise on the level of the North Atlantic Council needs to be synchronised and matched on the level of units and tactical commands.

The case of cyber was used to illustrate the importance of raising leadership awareness. For many leaders, cyber resilience is about information technologies, routers and computers. At the same time, our dependency on cyber has made us very comfortable, but less secure. Every aspect of decision making, governance and control has been moved to cyber space. Today there is no human activity that is not underpinned by processes taking place in cyber. It may be obvious to experts but not to political leaders.

This brings about two inherent risks: the first is that of lack of support, including financial support, for the issue. This risk can be managed, to a certain extent. The second risk is larger: when the real crisis hits, it is likely that the political leaders will be doomed to failure because they lack a basic understanding of the extent of what is required from their end. This perception may be changed only by a real time crisis or by exercising and preparation on the part of the experts. At the same time, bringing the decision-makers to the table is difficult because of their schedules and top-level "distractions." In an ideal world, one should be able to "throw" a scenario at them and surprise them, but this is not always possible.

Stephen Hawking once said: "Intelligence is the ability to adapt to a change." In this case, the change starts with education. The "train the trainer" concept was discussed at this point (also in connection with Panel 3). We need to have education programmes in place to train those who are supposed to train others in resilience within the system.

The speed of adaptation of public and private organisations is an important factor that contributes to resilience. Corporations have agility in this respect. There is a need to move beyond the military domain and focus on unconventional aspects of resilience. The example of the "all-hazard approach" exercised by the Swedish Civil Contingencies Agency (MSB) was used to illustrate the measures required for an effective civilian, cross-sectoral approach to resilience. This approach relies heavily on the speed of reaction and psychological defence as the prerequisites for resilience. The measures and steps required in it include:

• Understanding the threats.

- Understanding the intentions of the aggressor.
- Understanding one's own vulnerabilities and gaps.
- Setting up institutional mechanisms that can address the internal gaps.
- Activating the actors through communication schemes to coordinate among stakeholders, check-lists for communication, and monitoring the communication flows and lack thereof.
- Raising awareness and building knowledge through educating both professionals and the general public. For example, as a part of the prevention and mitigation of the influence campaigns, MSB reached out to more than 70 professional organisations and approximately 4,000 decision-makers / crisis-management stakeholders.

Panel 3: Resilience Education and Training – Implications for NATO

Summary of the Discussion

The last panel of the conference differed from the previous two: The first panel gave the basic information on what resilience is and what the various institutional approaches to resilience are. The second panel showcased several good examples of what the best practices in resilience training and education are. The third panel set out to answer the proverbial question "So what?"

The following questions were asked to steer the discussion:

- Is there a template for a "resilience training programme" that can draw upon, for instance, the examples of NATO's stability and reconstruction efforts, such as those in Afghanistan, which connect the civilian and military component?
- How can we bring the notion of resilience closer to the population? Is resilience a tool to "empower" the citizens?
- Can NATO bodies that deal with education and training play a role in this process?
- How do we connect the "expert dots" and link them with strategic thinking and policy-making?
- Is there a way to leverage the best practices in scenario training and modelling?

The panel also explored the possibilities in NATO's resilience toolbox, namely:

- The way to incorporate resilience into the existing curricula of NATO's training and education bodies.
- The feasibility of setting up a central resilience course for NATO.
- The idea of including the partners in NATO's resilience training, both as contributors and as recipients of that training.

The first part of the panel dealt with the Allied Command Transformation's (ACT) approach to resilience. To ACT, resilience is part of the headquarters' long-term mission:

to ensure that the Alliance is ready for the existing operations and future challenges and capable of carrying out the related measures. ACT leads the transformation in the development of NATO.

In May 2017, ACT organised a conference which examined the interdependency of various approaches to resilience to gain a greater understanding of what resilience means to various stakeholders. Four major trends emerged at the conference as preconditions for resilience building resilience building: persistence in resilience efforts, treating resilience as a capacity, expanding experimentation and modelling, and an integrated approach to resilience training and education.

Regarding developing an integrated education on resilience, as was stated a number of times throughout the conference, education and learning are really the fundamental building blocks of any resilience system. Developing a shared awareness through resilience education ultimately helps us to understand the related risks and how we can overcome them.

At the strategic level, increasing education and the shared awareness enables a collaborative dialogue. Such a dialogue is truly required to help us achieve a common understanding among different sectors and different actors. At the individual level, we should be helping the "informed and engaged" citizen, as was also discussed in the previous panels. We need citizens that are able to comprehend the complex environment they now find themselves in.

In summary, education and learning is about developing a shared awareness, enhancing the individual and collective knowledge that enables a collaborative dialogue, and inducing a more engaged approach on the part of both citizens and the whole society.

Concerning the experimentation model and training, it is important that such modules (and the recipients of the training) replicate the reality of the complex security environment. The first panel highlighted that the systems should be exercised to the points of failure. Such training should also consider the interdependency of systems, and how the failure of one system leads to a cascading or domino effect on the other systems. In this context, exercising to the point of failure requires a different mindset for training designers, training developments and influences, and those being trained. In other words, a cultural change in approaches to exercising needs to affect all the participants in this process.

Overall, resilience requires a more holistic approach to modelling a simulation that would cover the physical, cognitive, and human factors. The main challenge is finding out how modelling a simulation can help us understand and manage risks more effectively.

So how do we get there?

Firstly, NATO and the EU should consider strengthening their relationship with academia to discuss and promote the topic of interdependency in resilience across the three sectors involved – the military, civil and private sectors.

Secondly, workshops focused on resilience training can build upon and multiply ongoing NATO efforts in this field. Their scope should be as wide as possible to include the above-mentioned three sectors.

And finally, the concept of exercising to the point of failure should be introduced as a training doctrine that will enable us to test our systems to the breaking point, so that we understand the vulnerabilities and how to mitigate them. This is a taskthat ACT should tackle in setting the requirements for both resilience-related education and resilience training.

The second part of the panel examined the relevance of the existing ACT requirements to resilience capacity building, and how they impact two prominent education institutions affiliated with the Alliance: the NATO School in Oberammergau, Germany, and the NATO Defence College in Rome, Italy.

In the case of the NATO School, there are approximately 105 courses in its catalogue (and more are currently being developed) that are part of the Global Programming (i.e. NATO's education and training requirements). The challenge is finding out how resilience can be best integrated into these courses. Analogies could be drawn to the subject of hybrid warfare. Very often, we see a proliferation of events, courses and training activities related to a once highly particular, but currently "trendy" subject. Hybrid conflict, as a subject of study, for example, required a review of civil-military cooperation courses, information operations courses and strategic cooperation courses to ensure the coherence of the teaching on the subject. As for the resilience, the NATO School is already teaching resilience in its courses. It is not, however, adding the resilience label to it, which is a relatively easy "quick fix."

Establishing a new resilience course would require, however, a detailed education and training requirement analysis. Official accreditation is also needed if we are to involve partners in the course.

Finally, the NATO School would need to leverage the available expertise on resilience so that it would feed into the training requirements analysis for a resilience course. Experts can help NATO define the learning objectives, the depth of knowledge sought, and also the links to the political, strategical, operational and tactical levels. At the end of the day, a resilience module can be compiled from existing courses and curricula.

The research at the NATO Defence College views the concept of resilience as a mindset rather than a technical discipline. A general tendency is to focus on infrastructure

and institutions when dealing with resilience. But perhaps there should be more of a focus on people in studies of resilience. NATO recognises five domains of operations – land, air, space, cyber, and sea. Resilience within each of these domains depends on the people involved – how resilient they are themselves and how they translate this "personal resilience" into the domain and system. Basically, by educating people we increase their resilience. By increasing their resilience, we increase that of our institutions.

Resilience education therefore starts with the basic education on the national level. A nation cannot be resilient without elements of resilience in daily situations being part of the general curriculum. These elements include the individual's ability to respond to contingencies as well as being able to differentiate between "real news" and hostile influential campaigns.

In general, there is a shortage of professionals who would take care of other people's resilience, so institutions such as NATO have to prepare for the long-run in terms of interaction and intervention at the community level in places that are vulnerable to conflict.

But how does NATO bridge the gap between the institution and the public? The challenge lies in striking a balance between making a course complete enough to attract enough high-level attendees, and at the same time making it sufficiently generic so that it would be relevant for a lot of different countries with very different risk profiles and very different needs. Perhaps one solution could be a concept such as the 'train the trainer' concept.

Resilience is changing, and it needs to be continuously checked and examined. Also, we have to really look towards community intervention and local leaders and ways to organise communities, because focusing on the individual or state level alone will not be very efficient. Resilience education needs to take into consideration the local specifics of communities. There is a strong need to include civil society members as well. Furthermore, examples of resilience should be regularly sought from outside the field, namely from the municipal and the local community level.

Resilience education also continues throughout the higher levels, including the university and subsequent professional training levels. Simply put, you cannot stop educating people about resilience. In that regard, creating specific courses dealing only with resilience may not be a win-win situation, as it provides only a short-term solution.

The academic problem starts with the different approaches to resilience education, and its definition: Resilience was previously seen as a long term means of preparing society to deal with crises as they come. However, we now seem to be using resilience not only as a long term societal preparation, but also as shorter-term crisis management, strategic communication, and other practices which are somewhat more tactical and operational than strategic.

NATO's seven baseline requirements (see Panel 1), though, do provide some basic clarity and guidance; e.g. they provide a basic methodology on how to define vulnerabilities. For many nations, however, revealing vulnerabilities, even among Allies, might also be a cultural problem.

At NATO, any resilience-related training and education should consider the job description and requirements of the NATO Command Structure (NCS). The NCS itself could be considered as NATO's resilience backbone.

At the George C. Marshall Centre, there are a number of residential courses with resilience elements (within, e.g., the counter-terrorism and cyber security programme). Outreach programmes of the George C. Marshall Centre provide opportunities to highlight resilience for similar functionally-themed programmes. One of these programmes is referred to as the "Senior Leadership Seminar." This course may typically involve members of parliament, incoming ministers of defence, state secretaries, etc. Having resilience as one of the themes for this course would be one way of connecting with top level decision makers in regard to this issue.

For any additional extension of courses, especially on the outreach side, a partnership with (a) like-minded institution(s) would be beneficial. Specifically in the case of resilience, a kind of rotation of increasingly ambitious types of cooperation might be pursued:

- First, at the lowest level, more systematic sharing of information about resilience efforts and resilience education should be promoted. It is important to be aware that programmes on resilience exist at other institutions, and that still other institutions are working on such programmes; it would be helpful to exchange agendas with these programmes. It would require additional work but at very little cost.
- Second, the next stage and ambition would be that the institutions could offer more frequent mutual support to each other's resilience-related programmes. If, for example, the NATO Defence College is offering a week-long seminar in resilience, speakers from other entities with special expertise can attend and/or observe it to create or foster a kind of community of experts for dealing with this issue.
- Third, the most ambitious step would be for the institutions to jointly develop and execute a programme. It would require a lot of administrative and substantial preparation, and also a lot of trust. Geographical proximity and existing legal arrangements (such as between the NATO School in Oberammergau and the Marshall Centre) is a plus. In principle, this should apply any public-private, or public-public effort in resilience education.

Regarding the inclusion of the partners in resilience training and education, the panel agreed that it makes sense. But NATO needs to carefully think about some of the more

sensitive aspects of resilience. At the same time, increasing the resilience of (non-competing) partners is a value added for NATO as well. To a certain extent, this is already happening. For example, at the NATO School, about 12% of the resident students are from the Partner countries. (Note: The total student body amounts to approximately 8,300 students.) In addition, some of the aspects of resilience training can be carried out via technology – e.g. advanced distributed learning or e-learning. NATO can do more in this area.

Rapporteur's Observations

Remarks by
DR. JAMIE SHEA
Deputy Assistant Secretary General
Emerging Security Challenges Division, NATO

Before I give my concluding thoughts on the conference, the first thing I want to do is to thank our Czech hosts here. We have worked very well together in taking this conference forward with the collaboration of the Emerging Security Challenges Division, the Operations Division, and our Science for Peace and Security (SPS) Programme. And thank you also to Finland, because the SPS Programme always needs an essential partner, and Finland is always there to be that essential partner. This is really an excellent example of good cooperation, both within the NATO International Staff and between NATO Allied and Partner countries.

A few points of introduction on NATO and resilience: First, **NATO's Resilience Pledge**, which we adopted at Warsaw, may not have gotten as much publicity as other pledges of that summit, such as the Cyber Defence Pledge or, of course, the pledge to spend 2% of our GDP on defence. But I believe that it is one of the most important pledges because **resilience is fundamental to everything we do**. It is fundamental to the way our societies exist, and our possibility to preserve our way of life.

Our resilience is going to be tested in the future as never before. In the 21st century, one could argue that **there are two categories of countries in this world** – those which will develop resilience, albeit through trial and error, and which will therefore survive, and protect their stability, cohesion, prosperity, and freedoms; and those which will not develop resilience, and which will thus increasingly be the targets of attacks and outside interference, and increasingly be beset by crises. It is as simple as that.

Why is this so? We are facing **an unprecedented cluster of different threats** and trends coming at us simultaneously, interacting with each other dynamically and unpredictably, as never before, and making it so that the factors of life which disrupt are now significantly outweighing the factors of life which consolidate and stabilise. And we do not know how long we are going to be in this situation. To paraphrase Richard Clarke, a former advisor to the U.S. President George W. Bush on terrorism, it may "take several generations."

In order to understand what we are up against, we first need to understand what we are defending. **What is of value to our societies?** How do we assess value and assets? Today, for example, data has become, in an economic sense, much more important than oil or material objects. The five biggest companies in the world are data-producing companies. Uber has a market capitalisation of 68 billion dollars, and it does not own anything – except the data from the drivers or the passengers of its cars. Every year, we are producing 180 zettabytes of data. And if you wanted to put that through a basic sort of Internet broadband connection, it would take 450 million years to process that amount of data. Each year we are producing more than the sum total of previous human history. So, in a world where data – something which is invisible and that we cannot really assess – is becoming more important to our survival than physical objects, how do we adapt to that? The second issue is, of course, the notion of complexity, of increasingly integrated and complex systems. The CEO of Google Eric Schmidt once said that "the Internet is the first thing that humanity has built that humanity doesn't understand." We ourselves are often not conscious of our interdependencies and vulnerabilities before things that make us conscious of them happen. Complexity simply means that everything is a target. The function of government now is to try to secure everything – not simply borders, or a certain space, but virtually anything, because anything in a society can be exploited. For example, today, in the United States, election machines redefine national critical infrastructure. There is a rapid pace of change and a compression of activities, which means that the threats we thought were 20 or 30 years away, like climate change, are happening today, and the future has already arrived and is already happening to us.

There is also the issue of uncertainty. Taboos, or extremes, that we thought were outside the scope of our discourse are now part of the new normal. The extremes are now in centre stage. There are no more taboos, so therefore the range of potential possibilities and/or contingencies that we have to factor into our planning, is much greater. Nothing can be excluded. There is, of course, globalisation, which is an incredible thing that both breaks up and fragments societies; and increases divisions and social divides, while also producing this new tissue of connectivity across the world. Everybody can influence everything else, and anybody can attack anything from anywhere at any moment of the day. There are no more physical barriers to the ability to spread instability, and individuals now have the capacity to inflict harm with minimum financial investment, which used to be the domain of the states.

And then, of course, there is the interconnectedness – you can do massive things with very little. Small incidents can lead to massive disruptions across the supply chain. For example, British Airways suffered an outage in a data terminal next to the Heathrow Airport, and then it was paralysed for one week with hundreds of thousands of customers stranded at that airport. And there are other examples like that.

Thus, all these trends are producing two key conclusions. The first one is that we are going to live in societies where security for our politicians is going to be an even more fundamental requirement than aspirations for prosperity. The U.K. elections, where the conservative headline was "Security," were a case in point. We are likely to live in states of emergency for many years, but in comparative normality. For example, the French Parliament will soon be asked to vote for the third time in a year on the state of emergency. Or to give another example, the United States has now lived with the USA Patriot Act for more than fifteen years.

Secondly, all the domains will continue to be contested. When I first joined NATO, the Mediterranean was the *mare nostrum*, "our sea," defining the borders of NATO's operations. That is now gone. In whatever space there is today, there is contestation, rivalry, and conflict. Military commanders no longer have the comfortable choice of being able to decide where they are going to fight the battle on their terms. We have to be able to fight in terms of contesting, on our side, all of those spaces as well. And then the spectrum of conflict is larger; it is not just the kinetic aspects anymore. We now have cyberspace as well. This is why the concept of resilience is important: there is the notion of how we design these spaces, the notion of protecting and defending them, and the notion of recovering from attacks and incidents. And we have to be able to handle all three.

The threats are becoming increasingly discriminate. Who would have thought that young girls at a pop concert in Manchester or migrants in certain camps would become a sort of pseudo-military target? **Also, weapons are becoming increasingly customised**, like Stuxnet, which can attack a particular system in a particular operating plant at a particular time.

So what are the consequences for NATO? A lot has been said today about civil-military cooperation. I agree with the points that were made. We need to understand the civilian culture much more, and how civilian structuresoperate. **A clear division of labour** is essential, and we need to analyse where NATO's capabilities can help. For example, we could use NATO's units in the Baltic States and Poland while they are forming their relationship with the police, the border guards, or the emergency services, so that they could handle a wider variety of different tasks **than just classic military tasks**. We need to understand legal authority, because when civilians and militaries act together, there is often a very sensitive issue present: that of **who has the legal authority**. The command and control arrangements for bringing civilians and the military together are complicated, and we need to look at them. Who ultimately is in charge?

The education and training piece has been brought out very well earlier, but I would like to mention three issues that have not been featured so prominently in the discussion so far. The first is **awareness**. We talk a lot about awareness, but what exactly do we mean by that term? In the Watergate crisis, the American Senator Howard Baker said, "What

did the President know and when did he know it?" And to paraphrase that question, I would say that strategic awareness is what exactly we need to know and when we need to know it. For example, if an aircraft is on a potentially dangerous course, do we need to know, so that we can act, when it is 100 miles away from us, when it is 50 miles away from us, or when it is ten or five miles away? How far away does it have to be for us to still have a situational awareness which is actionable and can be acted upon?

In NATO, we make the mistake of seeing situational awareness in geographical terms too much, but we also have to be able to deal with the nominative threats, such as terrorism, artificial intelligence, cyber-security, etc. We need to improve the handling of the cross-cutting issues, which today is different than in the Cold War.

The second issue is the **crisis management aspects and the decision-making aspects**. We cannot regard hybrid warfare simply as confirming that a war is about to take place. If we say that we are only interested in Article 5 and beyond, we are in danger of being paralysed. We need to keep addressing the issues below the Article 5 threshold and phase our decision-making and deterrence adequately. And we need to gear our exercises more to that end.

The third point is that we need to ramp up our **cooperation with the other key actors**. Industry is increasingly a part of the whole resilience effort. In the cyber area, the relationship with industry is fundamental in terms of intelligence sharing, situational awareness, and the backup that it can provide in a crisis situation. We are now in an age in which the responsibility for security is being spread among an ever-larger number of actors. Cyber is a good example of this. Today, in this area, the military no longer have the monopoly role that they have when they deal with conventional threats.

Of course, in the resilience area, we have the issue of **responsibility of an individual**, i.e. how much, in the future, does the individual need to do himself or herself? Take the foiled Thalys train attack in 2015, for example, in which the perpetrator was subdued by the passengers. This is a clear illustration that the last line of resilience is going to be the citizen, who, in a dangerous situation, cannot sit back and wait for the government to provide the solution but has to act himself or herself. The more resilience is decentralised and anchored in the population, the stronger it will be.

So how do we train civilians to be ready? **Strategic communications** are going to be important in terms of making our citizens aware of the threats that they need to face and educate themselves about. For example, cities are now becoming more important as the basis of resilience than countries as such. City organisation, practicing emergency ambulance services, back-up hospitals, and a good police force are all services that determine how quickly a city can get back on its feet after a terrorist attack or a major incident.

Overall, we need to broaden the debate in the Alliance among the key actors and partners, including the European Union. We need to have a real good sense that if a crisis comes, we are ready for it. And that is my concluding remark: Are we ready? And if we feel we are ready, what makes us certain that we are really ready when that crisis comes along?

Key Takeaways & Recommendations

Based on the summary by
LORENZ MEYER-MINNEMAN
Head, Civil Preparedness
Operations Division, NATO HQ

General Points on Resilience

- All participants agreed that resilience is a critical capability.
- The question is not WHETHER but WHEN a disruptive activity may be directed against us.
- Resilience is a critical enabler for NATO's collective defence and also for NATO's deterrence.
- Resilience does not reside solely with governments, international institutions, NATO or the European Union, which may be an uncomfortable truth.
- Resilience starts with the citizens and communities, and then it spreads to regions, the national level, the private sector, NATO, and the EU.
- Building resilience from the top down is not necessarily the best approach. Often grassroots solutions to building resilience are more effective. Citizens need to be empowered to drive resilience.
- Synchronising and guiding various resilience efforts at different levels is critical, but the coordination is not easy. There are many individual and institutional tools available for this (the NATO Defence Planning Process was featured as one such tool).
- There is only one kind of resilience; not a single private sector resilience, national resilience, NATO resilience, or EU resilience.
- Various aspects of resilience are interdependent, and it requires a "whole community" and "all hazard" approach to tackle all aspects of resilience.

Improving Resilience

- The workshop showcased the models of Finland, Sweden and also Israel as examples of resilience models that focus on the citizen. All these models are predicated on a national context and local specificities. No single national model exists that would be applicable to other nations.

- Lessons learnt are key; the foundation for resilience lies in education – education of the citizens, education of the private sector, and education of elites, the political and economic leaders, who can be involved in resilience-related exercises.

- Resilience exercises are at their best if they are conducted to the point of failure, as was brought up a number of times at the workshop.

- Building elements of resilience into NATO exercises has proven difficult; the traditional military planner's approach is to build only a few, if any, obstacles into scenarios – and the result is that the troops always arrive magically at the required location without any hindrance in the scenarios. The reality of NATO's European deployments over the past few years points to the contrary, however.

- NATO needs to be honest about its resilience exercises in the sense of allowing for failure even in large-scale exercises.

- Resilience is not just a question of planning; the participants pointed to changes in mind-sets, changes of culture, and improvement of the connections between various exercise activities as changes that could improve resilience.

Translating Resilience into Training and Education

- Most of the work in resilience training and education must be carried out on the national level. It has to focus on leadership, trainers ("train the trainer") and the general public. Civilian, professional and non-governmental organisations can provide a platform for such an effort.

- NATO and the EU can make important contributions to it, but resilience training and education is ultimately the responsibility of the individual nations.

- Panel 3 suggested a systematic inclusion of resilience in NATO's training and education and also, to some extent, in NATO's research activities. That systematic inclusion needs to happen at all levels – at the NATO Defence College and the NATO School in Oberammergau, but also in the Centres of Excellence.

- NATO should review the existing courses in its academic bodies and select a handful that would merit a resilience module. Courses at national entities (and within the wider NFS) could be leveraged as well.
- Improved information sharing and exchange among these institutions is the key prerequisite for enhanced networking and mutual support.
- Resilience training ideas and concepts should be adequately reflected within the NATO Command Structure. It is worth examining individual post descriptions to identify the beneficiaries of resilience training.
- Systematic resilience training and education can help to change mindsets and cultures, as suggested above. Resilience needs to be trained and exercised persistently.
- NATO's resilience context is somewhat narrow and focused on defence and lends itself to the inclusion of selected NATO partners in it. But NATO needs to first clarify the purpose of its resilience training before it becomes part of NATO's defence capacity building measures. The scope of information sharing is just one obstacle. The meaning of resilience to NATO is not the same as its meaning to everyone else.

Annex 1: Programme of the Conference

Day 1 (June 1, 2017)

Venue: Residence of the Ambassador of Finland to the Czech Republic, Sibeliova 6, Prague 6, Czech Republic

19:00 – 21:00

Opening Reception

Opening Remarks:

H.E. HELENA TUURI
Ambassador of Finland to the Czech Republic

Welcoming Remarks:

H.E. JIŘÍ ŠEDIVÝ
Permanent Representative of the Czech Republic to NATO

Scene-Setter:

"Redesigning Resilience for the Modern Era – Understanding Vulnerabilities and Interdependencies"

PETE GUMATAOTAO
Deputy Chief of Staff, Strategic Plans & Policy, ACT

Day 2 (June 2, 2017)

Venue: Ministry of Foreign Affairs, Czernin Palace, Mirror Hall, Loretánské náměstí 1, Prague, Czech Republic

08:30 – 09:00

Registration of Participants

09:00 – 10:30

Panel 1: Understanding Resilience – National and Institutional Approaches

How can NATO better progress in resilience? Is resilience an informal fourth core task of NATO? Can there be a division of labour between NATO and the EU? Is there a clear distinction between multinational and domestic efforts in resilience?

Moderator:

MICHAL KOŘAN
External Researcher
Institute of International Relations, Czech Republic

Panelists:

PHIL ANDERSON
Associate Director for Research and Development
Global Resilience Institute, Northeastern University, USA

SANDRO CALARESU
Deputy Director
Crisis Management and Planning Directorate, EEAS

BURCU SAN
Director for Preparedness
Operation Division, NATO

VESA VALTONEN
Secretariat of the Security Committee
Finland

10:30 – 11:00

Coffee Break

11:00 – 12:30

Panel 2: Preparing for Emergencies – Best Practices in Training and Modelling

Are we ready and prepared for "virtual vulnerabilities"? Can sectoral approaches to resilience work? How can we model and prepare for cascading effects? How do we train resilience across all operational domains? How do we integrate resilience training and scenario modelling across NATO?

Moderator:

MIKAEL WIGELL
Senior Research Fellow
The Finnish Institute of International Affairs, Finland

Panelists:

DANIEL BAGGE
Head of the Cyber Security Policies Department
National Cyber Security Center, Czech Republic

JAMES CASSIDY
Director
OAKAS, UK

MARIA NILSSON and **DOMINIK SWIECICKI**
Senior Research Fellows
Swedish Civil Contingencies Agency, Sweden

URI BEN YAAKOV
Professor
International Institute for Counter-Terrorism, Israel

12:30 – 13:30

Working Lunch & Remarks

H.E. PIRITTA ASUNMAA
Head of Mission
Mission of Finland to NATO

13:30 – 15:30

Panel 3: Resilience Training and Education – Implications for NATO

How can NATO further explore and promote best practices? Is there a blueprint model for resilience training? How can one structure resilience training to address the different needs of Allies and partners?

Moderator:

JAN HAVRÁNEK
Defence Counsellor
Permanent Delegation of the Czech Republic to NATO

Panelists:

CHRIS BENNETT
Staff Officer
Strategic Plans & Policy Branch, ACT

TIMOTHY E. DREIFKE
Commandant
NATO School, Oberammergau

MATTHEW RHODES
Professor
George C. Marshall European Center for Security Studies

15:30 – 16:00

Final Summary

JAMIE SHEA
Deputy Assistant Secretary General
Emerging Security Challenges, NATO

LORENZ MEYER-MINNEMANN
Head of the Civil Preparedness
Operations Division, NATO

16:00 – 16:15

Closing Remarks

H.E. JIŘÍ ŠEDIVÝ
Permanent Representative of the Czech Republic to NATO

Annex 2: List of Participants

PHIL ANDERSON
Northeastern University Global Resilience Institute

H.E. PIRITTA ASUNMAA
Mission of Finland to NATO

DANIEL BAGGE
National Cyber Security Centre, Czech Republic

URI BEN YAAKOV
International Institute for Counter-Terrorism, Israel

CHRIS BENNETT
Allied Command Transformation

SANDRO CALARESU
EU, European External Action Service

JAMES CASSIDY
OAKAS, Ltd., UK

JIŘÍ CHALUPA
Permanent Delegation of the Czech Republic to NATO

DAVID CHOVANEC
Ministry of Interior, Czech Republic

JOHN CLARKE
GCM European Center for Security Studies, Germany

TIMOTHY E. DREIFKE
NATO School, Oberammergau, Germany

LUCIA FIGULI
University of Žilina, Slovakia

CHRISTIANE FJÄDER
The Finnish Institute of International Affairs

CHRIS GODWIN
OAKAS, Ltd., UK

PETE GUMATAOTAO
Allied Command Transformation

AXEL HAGELSTAM
Mission of Finland to NATO

JAN HAVRÁNEK
Permanent Delegation of the Czech Republic to NATO

KAROLIINA HONKANEN
Mission of Finland to NATO

TAŤÁNA JANČÁRKOVÁ
National Cyber Security Centre, Czech Republic

DOMINIK JANKOWSKI
Ministry of Foreign Affairs of the Republic of Poland

JAN JIREŠ
Ministry of Defence, Czech Republic

SHAUL KIMHI
Tel-Hai College, Israel

DAVID KLAIN
Dynamis, Inc., USA

MICHAL KOŘAN
Institute of International Relations, Czech Republic

JURAJ KRUPA
Slovak Security Policy Institute, Slovakia

JUKKA KUPILA
Radiation and Nuclear Safety Authority (STUK), Finland

KATRI LIEKKILÄ
National Emergency Supply Agency, Finland

GUSTAV LINDSTRÖM
Geneva Center for Security Policy

CLAUDIA MAJOR
Stiftung Wissenschaft und Politik, Germany

DANU MARIN
Information and Documentation Center on NATO, Moldova

LORENZ MEYER-MINNEMANN
NATO, Operations Division

FRANTIŠEK MIČÁNEK
NATO Defence College, Italy

ALESSANDRO NIGLIA
Atlantic Treaty Association, Belgium

MARIA NILSSON
Swedish Civil Contingencies Agency

ZBYNĚK PAVLAČÍK
Jagello 2000, Czech Republic

KARIM PELTONEN
The Finnish National Rescue Association (SPEK)

TIMOTHY PRIOR
Center for Security Studies Zurich, Switzerland

PASI RANTAKARI
Ministry of Defence, Finland

MATTHEW RHODES
GCM European Center for Security Studies, Germany

ANNA ROININEN
Embassy of Finland to the Czech Republic

JOHANNA SALOVAARA-DEAN
Embassy of Finland to the Czech Republic

BURCU SAN
NATO, Operations Division

JIŘÍ SCHNEIDER
Aspen Institute, Czech Republic

JAMIE SHEA
NATO, Emerging Security Challenges Division

VOLODYMYR SOLOVIAN
Center for Army, Conv. and Disarmaments, Ukraine

DOMINIK SWIECICKI
Civil Contingencies Agency Sweden

H.E. JIŘÍ ŠEDIVÝ
Permanent Delegation of the Czech Republic to NATO

BENJAMIN TALLIS
Institute of International Relations, Czech Republic

H.E. HELENA TUURI
Embassy of Finland to the Czech Republic

MIKKO VÄHÄ-SIPILÄ
National Emergency Supply Agency, Finland

VESA VALTONEN
Security Committee, Finland

BENEDIKT VANGELI
Ministry of Interior, Czech Republic

MIKAEL WIGELL
The Finnish Institute of International Affairs

JAMES WITHER
GCM European Center for Security Studies, Germany

VLASTA ZEKULIĆ
NATO, Emerging Security Challenges Division