DRAFT FOR DISCUSSION

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 jointly 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 a 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 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 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 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.

- ***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.

- ***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 defence. Prospective cooperation areas in cyber defence 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.

- ***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 endeavours, 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 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, 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, could 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 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 EU´s neighbourhood 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 organisations 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.

US-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 bench-marking 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-US 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.