Forward Resilience: Protecting Society in an Interconnected World Working Paper Series

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

Daniel S. Hamilton

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

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

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

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

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

Ensuring the resilience of one's society is foremost a task for national governments. Resilience begins at home. Yet in an age of potentially catastrophic terrorism, networked threats and disruptive hybrid attacks, no nation is home alone.

---

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

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

Emerging challenges will require even greater shared resilience.[3] Moreover, national resilience and collective defense must be understood as mutually reinforcing elements of the same overall effort to enhance deterrence.

NATO's Role

While resilience requires a broad approach with significant civilian political and economic aspects, it also has major military components. NATO military forces, even in small number, can be effective to back up local border forces or special operations forces to detect and neutralize foreign insurgents. National forces should be primary, in keeping with Article 3 of the Washington Treaty. But NATO allies can assist where requested, for example, for protection of key industrial, commercial and transportation nodes (especially those intended for use in reception of reinforcements), counter insurgency operations and para-military police functions, responses to civil emergencies and covert operations, and crisis response management.

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

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

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

NATO should set resilience standards and individual allies should each make a Pledge on National Resilience to meet those standards at the Warsaw Summit pursuant to Article 3 of the North Atlantic Treaty, whereby allies commit to "maintain and develop their individual and collective capacity to resist armed attack." This pledge would encompass protection of civilians and infrastructure; maintaining essential government functions and values; protecting and defending cyberspace; modernizing resilience capacities; and promoting transatlantic resilience across the Alliance.

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

> • ***Develop civil-military Resilience Support Teams,*** small operational units that could offer support to NATO member national authorities in such areas of emergency preparedness including assessments; intelligence sharing, support and analysis; border control; assistance to police and military in incident management including containing riots and other domestic disturbances; helping effectuate cross-border arrangements with other NATO members; providing protection for key critical infrastructures including energy; and, in the cyber arena, support to and enhancement of NATO's Cyber Response Team. These NATO teams could work in parallel with similar EU groups using the same playbook. In certain countries, Resilience Support Teams could be collocated with NATO Force Integration Units, and help national responses with NATO military activities including especially special operations activities.[5]
>
> • ***Create "National Resilience Working Groups."*** Encourage relevant nations to establish working group-type secretariats to coordinate defense activities with overlapping civil authority and private sector key critical

[3] Franklin D. Kramer, Hans Binnendijk and Daniel S. Hamilton, *NATO's New Strategy: Stability Generation*. Washington, DC: Atlantic Council of the United States/Center for Transatlantic Relations, October 2015.
[4] Alexandra de Hoop Scheffer, Martin Quencez, and Martin Michelot, "The Five Most Contentious Issues on the Road to Warsaw," GMF Policy Brief, December 2015.
[5] Kramer, Binnendijk, and Hamilton, op. cit.

infrastructure functions to enhance national capacity to anticipate, prevent, respond and recover from disruptive scenarios and to provide a key point of contact for outside assistance, including NATO Resilience Support Teams in the east, focused on the development of resilience and response to hybrid threats; in the south, focused on resilience and humanitarian requirements; and throughout the Alliance, focused on cyber and particularly its support to the electric grid and finance. Such a group should also have continuous situational awareness of a state's hybrid risk assessment. Coordination, integration, and exercises at the national level will make outside support from NATO and other organizations most useful.

• ***Encourage the establishment of regional working groups.*** In addition to national working groups, concerned nations could establish working groups with overlapping issues— one approach would be to look to the nations in the framework arrangements for the east and for the south--with invitations later for others to join as they deem desirable. This would be somewhat similar to such regional mechanisms as Nordic Defense Cooperation (NORDEFCO) or the Southeast European Defense Ministerial.

• ***Include resilience events in NATO exercises, training, education and operational planning.*** Resilience events should be included especially in NATO Crisis Management Exercises (CMX) and cyber exercises such as the annual cyber coalition exercises.

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

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

Develop a more robust strategic communications strategy to address Russia's information operations, particularly where Moscow seeks to exploit social and political differences in allied states, including those with sizable ethnic Russian or Russian-speaking populations.

The Cyber Dimension

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

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

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

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

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

• ***Establish the means to allow SACEUR to plan for, integrate and employ the contributions of members' cyber forces for defensive, offensive and exploitative cyber operations.*** While NATO is unlikely to agree to establishing offensive cyber capabilities for the Alliance itself, individual Allies do possess these capabilities and those capabilities may need to be coordinated in time of crisis or conflict.

• ***Consider Mutual Cyber Standards Pledges.*** National networks that connect to the NATO network can be weak, creating potential vulnerabilities for the entire system. The Alliance might address this problem via a "mutual cyber pledge," grounded in an Alliance-wide certification system, in which an individual Ally pledges to meet agreed cyber defense standards and NATO itself pledges assistance to those lacking capability to meet those standards, which is then followed with a concrete work plan to achieve certification.

• ***Enhance NATO's Computer Incident Response Capability (NCIRC)*** by rationalizing and normalizing common funding, strengthening its Rapid Response Teams in order to better assist members under attack who ask for help, and generating greater protection and resilience planning for critical mobile networks, including capabilities development of national cyber cells earmarked for NRF and VJTF.

• ***Task ACT to develop a Cyber Operations Transformation Initiative*** to explore opportunities for multinational training, networking, information sharing and interoperability among the growing number of NATO members fielding operational commands. The model for this initiative should be the successful special operations transformation initiative of the Riga summit.

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

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

a. EU-NATO Cooperation

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

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

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

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

EU and NATO leaders should each affirm their commitment to enhance the overall resilience of their members, including through EU-NATO cooperation. This could happen at the June 2016 European Council and the July 2016 Warsaw Summit. The NATO Secretary General and the EU High Representative and Vice President of the European Commission should issue a joint statement that underscores this joint initiative and sets forth practical means to advance it.

The EU and its member states, and NATO and its allies, should develop coordinated strategic communication mechanisms to counter disinformation, expose and condemn hybrid actions.

The NATO International Staff and the EU External Action Service 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, situational and threat assessments, and early warning and early action procedures.

The EU Intelligence Fusion Cell and the NATO Intelligence Center, allies and member states should try to commit to making intelligence releasable to EU and NATO simultaneously wherever possible, and making sure that each is aware information has been shared by marking it appropriately.

Hold a joint crisis management exercise in 2017. The EU and NATO have been conducting such exercises over the past few years; in 2017 it would be useful to focus on hybrid or disruptive threats.

The EU should engage with NATO centers of excellence in order to benefit from insights generated in such fields as cyber defense, strategic communications, civil-military cooperation and crisis response in relation to hybrid threats.

b. US-EU Cooperation

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

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

Agreement on a Transatlantic Security Pledge would boost political impetus across the spectrum and recalibrate security cooperation towards a clear purpose: building resilience into transatlantic infrastructures. A high-profile pledge of this nature would help rebuild a sense of common cause across the Atlantic and set priorities to prevent or prepare for any future crisis. This impetus could carry over into diplomatic initiatives in the alphabet soup of transatlantic cooperation frameworks directed at improving coherence through strategic direction.

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

---

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

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

[8] See, for instance, Dalgaard-Nielsen and Hamilton, op. cit.; Brimmer, op.cit; Antonio Missiroli, ed., "Disasters, Diseases, Disruptions: a new D-drive for the EU," *Chaillot Paper* No. 83 (Paris: EU Institute for Security Studies, 2005); Robert Whalley, "Improving International Co-ordination and Co-Operation on Homeland Security/Societal Security and Resilience Issues," unpublished paper prepared for Center for Transatlantic Relations/PACER, January 2009; Jonathan M. Winer, "An Initial International Cooperation Agenda on High Consequence Events for the Obama Administration," unpublished paper prepared for Center for Transatlantic Relations/PACER, January 2009.

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

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

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

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

Project Resilience Forward

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

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

• ***The EU and its member states, and NATO and its allies, should facilitate joint or complementary efforts to project "forward resilience" to EU Eastern Partnership or NATO Partnership countries*** in areas such as security sector reform, police and gendarmerie training, public health-biosecurity measures, civilian control of the military, or economic reconstruction.

• ***The EU and its member states, and NATO and its allies, should consider deploying coordinated Resilience Support Teams,*** at the invitation of EU Eastern Partnership or NATO Partnership countries, to support building resilient capacity

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

in areas ranging from critical infrastructure protection and strategic communications to disaster prevention, management and relief, and civil-military cooperation.