UI brief
No.6
2017
PUBLISHED BY THE SWEDISH INSTITUTE
OF INTERNATIONAL AFFAIRS. WWW.UI.SE

Resilience: Shared, and Forward

Daniel S. Hamilton

The notion of 'resilience' is gaining currency in European and Euro-Atlantic security policy discussions. The European Union, NATO and their respective member states are each building the capacity to anticipate, pre-empt and resolve disruptive challenges to vital societal functions. New energy is apparent in efforts to advance more effective NATO-EU cooperation in the field of resilience. But Brexit and the election of Donald Trump as U.S. President raise questions whether current patterns of cooperation will prevail or be changed in some way.

At the 2016 NATO Warsaw Summit, allies agreed to a set of seven 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 can and must be developed further, and work is continuing to do just that. But there are questions whether and how such cooperation may change due to Brexit and the advent of the Trump administration.

Brexit has raised questions on whether the UK will continue resilience cooperation within EU channels, even though its NATO credentials will still remain valid. The spate of terrorist attacks in the UK in spring 2017 has reinforced the determination of UK authorities to address terrorist threats, including through continued strong cooperation with EU partners. The UK is likely to remain a key actor when it comes to advancing resilience -- at home and among societies abroad. When it comes to situational awareness and intelligence cooperation, however, the UK is more likely to turn to NATO channels than EU mechanisms. When it comes to multilateral intelligence cooperation, the UK is likely to invest with priority in NATO's Warsaw Summit decisions related to intelligence cooperation, including through creation of an Assistant Secretary General for Intelligence, rather than EU channels, which will remain uncertain throughout the Brexit negotiations, which are likely to be fraught and contentious.

The same goes for the United States. Despite uncertainties related to the Trump administration's approach to Europe, the current U.S. government has been clear about its commitment to the NATO Warsaw agenda, including its resilience component. President Trump has insisted that NATO do more in the fight against terrorism – greater NATO focus on resilience can be one important answer. The U.S. Department of Homeland Security, and in particular the Federal Emergency Management Agency (FEMA), continue to be particularly active within NATO channels, working with allies and partners on good practice related to the baseline requirements, and helping to formulate an allied agenda with regard to resilience. To the extent that allies and partners can demonstrate that they are investing resources and attention to this aspect of the Warsaw agenda, they also underscore that they are addressing terrorist threats and carrying an important share of the common defense burden -- both important issues to the Trump administration.

Allies continue to be worried, however, whether President Trump is personally committed to Article 5 of the North Atlantic Treaty. When he attended the May 2017 NATO summit, he chose not to reiterate this long-standing commitment of the United States. In this regard, the current trajectory of NATO's resilience agenda could also be worrisome, because the Warsaw commitment to the seven baseline requirements has been justified under Article 3, rather than Article 5, of the North Atlantic Treaty. Article 3, the so-called "self-help" provision of the Treaty, underscores that each ally's foremost duty is to ensure it can defend itself. This is of course a *sine qua non* of effective mutual defense. But by linking resilience primarily to Article 3, and creating an agenda in which the seven baseline requirements -- and resilience itself -- is treated on a country-by-country basis, rather than as a shared endeavor, the Alliance may have created an "Article 3 trap" for itself at a time when the U.S. commitment to the mutual defense premise of the Alliance is under question.

For this reason alone allies should consider how to emphasize the shared nature of resilience. But substantive reasons related to the resilience challenge itself should further underscore the need to move along these lines.

Current efforts among allies and partners to build a resilience agenda 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 a deeply interconnected world. Resilience must be shared, and it must be projected forward.

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

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

NATO and EU members also share a keen interest in projecting resilience *forward*, since robust efforts by one country may mean little if its neighbors' 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 not only on prevention, but also on 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 consider timely response as a crucial component 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. A Resilience 2.0 agenda that not only

incorporates but also goes beyond current state-by-state efforts to encompass both shared and forward resilience is likely to be welcomed by the Trump Administration as well as the British Government. It would also go far to enhance Euro-Atlantic security, and would offer new avenues of allied-partner and NATO-EU cooperation. Such an agenda might give consideration to the following elements:

Develop and expand the Intelligence-Sharing Agenda set at Warsaw. Slow decision-making based on incomplete or differing intelligence assessments is beginning to be addressed by the Alliance. Improved Joint Information Surveillance and Reconnaissance (JISR) capabilities decided at Warsaw are focusing in the first instance on the most ready forces, such as the NRF. NATO is creating a new Assistant Secretary General for Intelligence and Security who will run a new Division in the International Staff. But problems related to situational awareness and rapid decision making are deep. Brexit will tilt British preferences to NATO channels over those of the EU when it comes to intelligence-sharing. Improved NATO-EU mechanisms in this regard might be the next best channel to ensure continued strong UK participation in intelligence-sharing arrangements beyond NATO. And the next step for NATO would be to create an Intelligence Committee somewhat similar to the Military Committee, consisting of national intelligence officers from each mission.[1]

- 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 officers 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.

Develop and expand the cyber defense agenda. At Wales, cyber defenses were categorized as collective defense.It was noted that certain cyberattacks could constitute an Article 5 attack. At Warsaw: 1) cyber was classified as a separate "domain" which could have significant long term consequences for NATO's command structure; 2) nations made a "cyber pledge" to better defend their own networks (which has been the most vulnerable element of NATO's network); NATO is primarily responsible for defending its own network and this pledge should expand cyber protection provided by individual nations), and 3) NATO's cyber range will be expanded to give nations practice in defending against cyber threats. For the future, NATO will need to more clearly define how it is prepared to use the offensive cyber capabilities of member stated to enhance cyber deterrence. A Cyber Coordination Center and eventually a NATO Operational Cyber Forces HQ will be needed. Both the UK and the U.S. are likely to support such efforts.

Establish special cyber support teams that can be deployed to partner countries to increase interoperability, improve information-sharing and coordinate responses to cyber crisis. Establish individually-tailored projects and expand existing projects in accordance with interests and capacities of partners to enhance their cyber security and defense.

Prospective cooperation areas in cyber defense include increasing interoperability, sharing strategic and technical information and threat assessments, coordinating responses to cyber crisis, and engaging partners into NATO's education, exercises and training activities.

- To support NATO allies' resilience in the cyber security context, cyber experts should be included within NATO Force Integration Units (NFIU). This would help assess vulnerabilities, increase preparedness and interoperability in regards with crisis response.
- Assess the levels of the existing maturity of cyber security and defense capacity in partner countries. Coordinate and synchronize mutual training and assistance projects with the EU in order to avoid overlapping. The Partnership Review and Planning Process (PARP) should include cyber defense elements as part of broader resilience efforts, and planning should to be aligned with the NATO Defense Planning Process (NDPP).
- Partners would benefit from the development of minimal requirements for the protection of their critical infrastructure and in regards with cyber defense.

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.

- Pool EU and NATO resources for Forward Resilience Advisory Support Teams. 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.
- 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.

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.

Daniel Hamilton is the Austrian Marshall Plan Foundation Professor and Director of the Center for Transatlantic Relations at the Paul H. Nitze School of Advanced International Studies (SAIS), Johns Hopkins University.

[1] Hans Binnendijk, *NATO'S Future - A Tale of Three Summits*. Washington, DC: Center for Transatlantic Relations, 2016, http://transatlanticrelations.org/publication/natos-future-tale-three-summits-hans-binnendijk/.

UIbrief

WOULD YOU LIKE TO KNOW MORE ABOUT UI?

The Swedish Institute of International Affairs (UI) is an independent platform for research and information on foreign affairs and international relations.

The institute's experts include researchers and analysts specialized in the field of international affairs. While maintaining a broad perspective, research at UI focuses on unbiased scientific analysis of foreign and security policy issues of special relevance to Sweden. UI as an organization does not take a stand on policy issues.

UI Briefs are short commentaries on international issues, events or trends related to UI's focus areas. They are written by UI staff, UI visiting researchers, or other experts associated with UI. UI Briefs do not require adherence to strict academic conventions. While the author is responsible for the text, the relevant programme director and one additional researcher have reviewed each manuscript.

For more information visit our website: www.ui.se, where you will find up-to-date information on activities at the Swedish Institute of International Affairs (UI). Here you can book seminar tickets, become a member, buy copies of our magazines, and access research publications. You can get in touch with us through email: **info@ui.se or +46-8-511 768 05**

Also, follow us on Twitter @UISweden or like us on Facebook!

SWEDISH INSTITUTE OF INTERNATIONAL AFFAIRS
Visiting Adress: Drottning Kristinas väg 37, Stockholm
Postal Adress: Box 27 035, 102 51 Stockholm
Phone: +46 8 511 768 05 Fax: + 46 8 511 768 99
Homepage: www.ui.se