SAIS
JOHNS HOPKINS
SCHOOL of ADVANCED
INTERNATIONAL STUDIES

CENTER FOR TRANSATLANTIC RELATIONS

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

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

Piret Pernik & Tomas Jermalavičius[1]

Introduction

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

What is Resilience?

The term 'resilience' is used in many contexts. It originates from the field of ecology, where it was initially understood as "the measure of the ability of an ecosystem to absorb changes and still persist."[2] The concept appeared attractive to other fields, especially those involving the management of complex interlinked systems, and therefore it spread beyond its original uses in ecology. It is now employed at different levels (individual, community, state) and in different fields such as psychology, physical infrastructure management, economy, organisational management, community studies, etc. So far, its most popular use in the field of security has pertained to disaster preparedness and anti-terrorism, with cybersecurity and critical infrastructure protection being late adopters.[3] In the light of Russia's 'hybrid' approach to conflict, resilience is now becoming a popular concept within NATO and the EU as a way to frame a holistic strategic response to the threat, combining the 'whole-of-government', 'whole-of-society' and 'whole-of-alliance' perspectives as well as multiple security domains.

[1] Piret Pernik is a research fellow at the International Centre for Defence and Security (ICDS) in Tallinn (Estonia), where she focuses on cyber defence and comprehensive security; Tomas Jermalavičius is a research fellow and a head of studies at the ICDS, working on the issues of resilience, security and defence governance and defence innovation.

[2] Joseph S. Mayunga, "Understanding and applying the concept of community disaster resilience: A capital-based approach." *Summer Academy for Social Vulnerability and Resilience Building* (Munich, Germany) (2007): 2, http://www.ihdp.unu.edu/file/get/3761.pdf

[3] See Jon Coaffee, "From counterterrorism to resilience", *The European Legacy,* Vol. 11, No. 4 (2006): 389–403. Jon Coaffee and Peter Rogers, "Rebordering the city for new security challenges: From counter-terrorism to community resilience", *Space and Polity,* Vol. 12, No. 1 (2008): 101–118. Noor Aisha Abdul Rahman, "The dominant perspective on terrorism and its implication for social cohesion: The case of Singapore", *The Copenhagen Journal of Asian Studies,* 27 (2) (2009): 109–128. Seymour Spilerman and Guy Stecklov, "Societal Responses to Terrorist Attacks", *The Annual Review of Sociology,* 35 (2009): 167–189. Arjen Boin and Allan McConnell, "Preparing for critical infrastructure breakdowns: The limits of crisis management and the need for resilience", *Journal of Contingencies and Crisis Management,* Vol. 15, No. 1 (2007): 50–59. Frank Furedi, "The changing meaning of disaster", *Area,* 39.4 (2007): 482–489.

In generic terms, resilience has been defined as a "process linking a set of adaptive capacities to a positive trajectory of functioning and adaptation after a disturbance."[4] This definition implies that resilience is a process, although it can also be seen as a strategy or as the "capability of a system to maintain its functions and structure in the face of internal and external change and to degrade gracefully when it must."[5] It draws on certain resources of the system and on "dynamic attributes of those resources (robustness, redundancy, rapidity)."[6] This perspective allows a proactive approach to building resilience by means of accumulating necessary resources in a system and ensuring that those resources possess the dynamic attributes required at a time when disruptions occur. System managers can thereby devise policies (e.g. principles, norms and standards, priorities of investments) which are conducive to resilience. This is particularly applicable to enhancing cybersecurity, which we cover later in this chapter.

The EU's Global Strategy defines resilience abroad as "the ability of states and societies to reform thus withstanding and recovering from internal and external crises,"[7] which aligns well with the generic definitions of resilience described above. It reflects the EU understanding that resilience is about capacities for change, adaptation and recovery. The emphasis on reforms flows from one of the key strengths of the EU – projection of its 'soft,' normative, power to stabilize, reform and transform countries seeking its membership or association status. However, when it comes to resilience at home, it speaks of critical infrastructure, networks and services more than of the values, norms, institutions or reforms, taking them as a given rather than something which needs to be protected against the attempts to hollow out and erode member states from within.

NATO also sets its emphasis on infrastructure, civil preparedness, continuity of services, accumulation of reserves and ensuring access to them as well as on various procedures facilitating rapid crisis response. Its major concern is that the Alliance has come to rely heavily on the private sector when moving, deploying and sustaining its forces; therefore it devotes much attention to civilian capabilities and civil-military interaction. This is understandable given its role as a "military responder" and "force multiplier" in military conflicts. Just as the EU, it should not, however, neglect its role in helping countries – both allies and partners – maintain their ability to reform themselves in the face of adversity. After all, as the Warsaw Summit statement states, "The foundation of our resilience lies in our shared commitment to the principles of individual liberty, democracy, human rights, and the rule of law."[8] Should this commitment fall apart, the Alliance's cohesion, solidarity and very existence will be endangered.

As noted by Jamie Shea, NATO's and EU's roles in buttressing resilience of most vulnerable and exposed countries often overlap,[9] particularly in such areas as cyber security, strategic communication, civil preparedness and countering Russia's hybrid warfare. Although Russia's hybrid warfare techniques have been extensively analysed, it is difficult to anticipate when, where and what types of stressors will be created and exploited by Moscow – or any other

[4] Fran H. Norris, Susan P. Stevens, Betty Pfefferbaum, Karen F. Wyche and Rrose L. Pfefferbaum, "Community resilience as a metaphor, theory, set of capacities, and strategy for disaster readiness", *American Journal of Community Psychology, 41* (2008):130.

[5] Brad Allenby and Jonathan Fink, "Toward inherently secure and resilient societies," *Science,* Vol. 309, Issue 5737 (2005): 1034.

[6] Fran H. Norris et al, "Community resilience as a metaphor, theory, set of capacities, and strategy for disaster readiness," 135.

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

[8] North Atlantic Council "Commitment to enhance resilience," July 2016, http://www.nato.int/cps/en/natohq/official_texts_133180.htm

[9] Jamie Shea, "Resilience: a core element of collective defence," *NATO Review,* 2016. http://www.nato.int/docu/Review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/index.htm

adversaries – in order to coerce target countries. Russia's approach typically combines both applying a long-term pressure (e.g. hostile propaganda and economic warfare) and opportunistically administering short-term sudden shocks, making it impossible to identify only a single set of capacities needed to cope with its hybrid strategy. A broad-based resilience of potential targets – allies and partners alike – which addresses a wide range of vulnerabilities to both chronic and acute stressors is of vital importance if NATO, in cooperation with the EU, seeks to deny Moscow the achievement of its political and strategic objectives in relation to the Alliance and its partners.

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

Resilience as part of Deterrence by Denial

In broader strategic terms, resilience can be seen as an ingredient of deterrence by denial, or "persuading the enemy not to attack by convincing him that his attack will be defeated – that is, that he will not be able to achieve his operational objectives."[10] Hybrid warfare strategy – essentially a strategy aiming to cause disruption, confusion, destabilisation and paralysis (i.e. shape the behaviour of a target nation) – can be countered by demonstrating that all those aims are beyond reach due to the target's resilience. For instance:

- A high level of a society's competence in critical thinking and in understanding the nature of such hybrid warfare tools as hostile propaganda, political extremism, social 'protest' campaigns or military intimidation – in conjunction with society's trust in the integrity of the political system, political leadership and government's communication – negate the advantages of those tools.
- A strong sense of belonging to a community, citizen empowerment and economic equity as well as of the available mutual support reduces the potential for dividing and polarizing the society and for turning various society's groups against one another and against the nation's institutions.
- A high level of voluntarism and civic participation in the nation's affairs, when harvested by national security and defence organisations, substantially strengthens those organisations in the face of adversity.
- Measures aimed at severely disrupting economic activities (e.g. sanctions, energy supply disruptions, financial destabilisation etc.) fail to achieve the long-term desired effect when encountering high levels of economic development and diversification.
- The ability of critical infrastructure, including communication and information systems, to absorb the impact of sabotage or attacks, quickly adapt and continue delivering satisfactory level of services renders rather futile the attempts to exert pressure via this avenue.

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

- Sufficient and rapidly accessible reserves of financial capital, basic necessities (such as food, fuel, medical supplies) and technical resources (e.g. spare parts and materials for maintaining and repairing infrastructure) ensure that sudden shocks caused by aggressor do not translate into a negative impact on the nation's will to persevere.

The operational challenge lies in demonstrating convincingly that vulnerabilities are truly absent and that a particular society is indeed very resilient in all respects. This starts with the society being cognisant of its own vulnerabilities in the first place and then working to eliminate them. The problem in this regard is that the process of addressing various vulnerabilities may affect various power relations in the nations and, therefore, we "must always address the question of who are the winners and losers of ongoing processes of building social resilience."[11] Some of those 'losers' are bound to become, consciously or not, natural allies of an aggressor in a hybrid conflict – something which is evident not only in countries such as Ukraine or Georgia but even among the political or economic elites of some NATO allies.

Last, but not least, deterrence – by denial or in any other form – lies in the eye of the beholder, which means that an adversary must be sufficiently convinced that its target society is too resilient to succumb to the hybrid warfare approach. This is difficult to achieve, given that each adversary is driven by own logic, rationality and calculations and may assess target's resilience very differently. This, in turn, means that Russia may never stop trying to identify vulnerabilities and then constantly testing and probing a targeted nation. The Alliance, therefore, must develop and continuously maintain deep and sophisticated understanding about the individual Allies and partners in terms of their vulnerabilities, resources, capacities and potential political 'losers' of resilience, as well as about the thinking and calculations of Moscow with regard to those vulnerabilities.

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

Enhancing Cyber Defence as part of the Alliance's Resilience

NATO's collective defence principle encompasses hybrid and cyber threats in addition to conventional threats. At the Wales Summit in 2014 the Alliance declared that cyber attacks against one ally may lead to the invocation of article 5 with a possibility to respond by any means, including military force. At the Warsaw Summit in June 2016 NATO recognized that cyberspace constitutes a military domain and the Alliance must deter potential adversaries and defend itself in cyberspace just like it does in land, sea or air. In practice this means that NATO must develop cyber capabilities that would provide credible deterrence and defence against cyber attacks. As a first step, NATO should develop a clear doctrinal framework and

[11] Markus Keck and Patrick Sakdapolrak, "What is social resilience? Lessons learned and way forward," *Erdkunde,* Vol. 67, No. 1 (2013): 12.

procedures, as well as command structure that would allow for the use of cyber capabilities in a standalone role in NATO missions and operations. However, a caveat to keep in mind is that even though cyber defence is part of NATO's core task collective defence, the Alliance's mandate is only defensive and it will not develop offensive cyber capabilities (notwithstanding national offensive capabilities that could be deployed on NATO's operations). Since effective cyber defence is not plausible without employing responsive defence (versus passive measures, that remain into organisation's own networks), it remains to be seen how allies are going to fulfil this task.

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

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

In addition to these measures, NATO reinforced its support to national authorities in protecting their critical civilian infrastructures and energy supplies against hybrid and cyber threats.[12] The Alliance's understanding of resilience includes not only military defence, but also non-military dimensions, including hybrid and cyber threats. NATO's concept of resilience focuses on civil preparedness that includes security of critical infrastructures, continuity of essential services and government, as well as civilian support to military.[13] This approach has common features with a Cold War era concept of total defence that also underlined civil preparedness, and with comprehensive and whole-of-society approaches to security and defence that focus on cooperation with the private sector and civil society. As discussed earlier, NATO links resilience to liberal democratic values as a shared foundation, however, it omits threats related to the cognitive dimension (e.g. information and psychological operations) that in the Eastern view constitute part of a broader informational domain and are used in combination with cyber attacks in peacetime and during conflicts.

Due to interdependencies of communication and information systems, and critical infrastructures, resilience can only be developed through an integrated approach. Disruptions

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

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

of host nation and coalition partner networks and critical infrastructure upon which NATO depends can degrade NATO's ability to conduct operations. Secondly, projecting cyber defence beyond NATO's territory would help to define global cyber security norms and behaviours around liberal democratic values. In recognising this indivisibility of security, the NATO-EU Joint Declaration, signed in Warsaw, stresses the need to "foster the resilience of our partners" through individually tailored projects.[14] Indeed, NATO should project its "soft" side of cyber power in its neighbourhood and globally with an aim to expand secure, open and free cyberspace and advocating democratic liberal values in cyberspace.

NATO has a wide range of cooperation formats with more than 40 partners. These partnerships can be leveraged and further expanded according to cyber defence needs of individual partners.[15] For example, in the existing framework of the Partnership for Peace Planning and Review Process, Georgia, Moldova, Iraq, Jordan have included cyber defence aspects into their capacity-building packages.[16] Non-NATO nations also participate in Smart Defence projects such as Multinational Cyber Defence Capability Development (MNCD2), which focuses on sharing technical information, situational awareness and creating a cyber security assessment team.[17] They have participated at NATO cyber defence and crisis management exercises, and at technical exercises run by the NATO Cooperative Cyber Defence of Excellence. It is possible to include cyber defence issues in their consultations with NATO bodies (28+ meetings) and through staff-to-staff talks. Lastly, NATO educational bodies provide training courses on strategic, operational and technical levels to partners with requisite security clearances.

To further enhance its assistance to partner countries NATO should identify, via cooperation with the research community and recipient countries, individual cyber defence needs in the areas of material and non-material resources, knowledge, expertise, and information sharing. The first area where NATO should consolidate more efforts is increasing interoperability of partners' cyber defence capabilities, communication and information systems and networks, as well as information and threat assessment exchange protocols. Allied Command Transformation maintains that interoperability of communication and information systems upon which NATO's command structure depends is a key element in developing forward presence.[18]

In 2014 the Alliance established the Partnership Interoperability Initiative and the Defence and Related Security Capacity Building programs in order to increase interoperability with partners. To attract more partners NATO should cut red tape by simplifying application processes and procedures to these programs, as well as create additional tailored programs based on individual needs of partners. The Alliance has recently developed an Individually Tailored Roadmap Capstone Concept that should simplify existing partnership programs and improve cooperation by increasing shared situational awareness and trust. Pilot projects that include cyber defence aspects have been launched with Finland, Georgia and Jordan.[19]

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

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

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

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

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

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

Another model of how NATO and coalition partners have worked together to improve interoperability and information sharing in operations, exercises and training events is NATO's Federated Mission Networking (FMN). The framework includes policy, processes, procedures, standards and physical components such as static and deployed networks, services and supporting infrastructures.[20]

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

Alliance's Cyber Threat Assessment Cell integrates technical data from NATO sources with threat assessments provided by Allied countries.[21] Situational awareness on cyber threats merging technical data with a strategic view should be shared with selected partners that have concluded agreements on information sharing with the Alliance. It has been recommended in the past that NATO should expand its current cyber intelligence capacity and build up a capacity to coordinate responses to cyber crisis.[22] Considering that a cyber crisis in the neighborhood can affect NATO's ability to lead operations, coordination of responses to cyber attacks is necessary.

Partners should be engaged also in the areas of early warning, prevention, and analysis of cyber threats. It has been likewise recommended that NATO should establish forward presence teams in the Baltic States to support them to counter hybrid threats.[23] Since NATO partners' values and degrees of interest in cooperation with the Alliance vary, in countries that show desire, NATO could deploy Cyber Vulnerability Assessment Teams with a task to identify vulnerabilities in their networks, increase interoperability and establish coordination relationships for crisis response. In case of emerging cyber crisis that is likely to affect NATO's operations or organisations, the Alliance could deploy Cyber Rapid Reaction Teams as part of broader Resilience Support Teams.[24] These measures would also allow identifying cross-border and cross-sector interdependencies of critical infrastructures upon which NATO depends on.

Agreements with national and military computer emergency teams of partner countries to exchange technical threat information should be concluded with NATO Computer Incident Response Capability (NCIRC). NATO has concluded such agreement with the EU, but information sharing with the EU should be expanded to include nontechnical sensitive information.[25] For example, NATO Cyber Threat Assessment Cell should share best practices

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

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

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

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

[24] Ibid.

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

with EU's Hybrid Fusion Cell, and NATO Cooperative Cyber Defence Centre of Excellence with Hybrid Threats Centre of Excellence when the latter will be established.

Selected partners with high-end cyber capabilities and established trust-based cooperation (like Finland, Austria, Sweden, Switzerland, Ireland, Australia and New Zealand) should be granted more opportunities. They have participated and observed NATO's cyber defence exercise Cyber Coalition. Host Nation support agreements that Finland and Sweden have concluded with NATO for crisis assistance should include the possibility to exchange cyber information, cooperate on threat and vulnerability assessments, and coordinate responses to cyber crisis. Finland and Sweden have joined the NATO Cooperative Cyber Defence Centre of Excellence, and Austria is a contributing nation.[26]

If cooperation may be challenging in highly sensitive areas information and intelligence exchange, cooperation should be encouraged in educational and training activities that help to increase trust, build up knowledge base and skills sets. NATO should further expand partners' engagement in its exercises and trainings, for example, partners could hold national and regional technical exercises at the NATO's cyber range. NATO should also facilitate assistance from advanced Allies to develop partner countries' cyber capacity. Allies have provided cyber-defence-related training and material support to Ukraine under the NATO-Ukraine trust fund.

Cyber threats defy organisational borders, most critical infrastructure is operated by the private sector, and various non-state actors yield significant power, knowledge and expertise in cyberspace. As noted above, bolstering resilience can be achieved only through an integrated approach involving key stakeholders. NATO has engaged industry in its cyber defence activities through the NATO Cyber Industry Partnership.[27] Technical agreements on information sharing and improving situational awareness have been concluded with cyber security companies such as Symantec, Cisco, Fortinet and others, and industry also participate in NATO exercises and trainings, as well as Smart Defence Projects.[28] The Alliance should continue leveraging its partnership with industry and provide grants to research community in order to conduct projects in target countries to help them to ensure cyber defence.

Recommendations

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

[26] Sweden is contributing a national expert and has decided to join the centre.

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

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

- Much more effort has to be dedicated by NATO and the EU to studying and understanding what deters Moscow, how it assesses vulnerabilities of target countries and how it seeks to exploit those vulnerabilities to its strategic ends. This has to be linked with early warning and strategic anticipation efforts.
- NATO should establish individually-tailored projects and expand existing projects in accordance with interests and capacities of partners to enhance their cyber security and 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.
- NATO should consider establishing special cyber support teams that can be deployed to partner countries with the aim to increase interoperability, improve information sharing and coordinate crisis response.