Atlantic – Black Sea Security Forum

Young Strategic Leaders Security Conference

June 4 2018

Conference Report

Doru Costea, Rapporteur

The **Aspen Institute Romania** in partnership with **NATO's Public Diplomacy Division** and the **Bucharest office of the German Marshall Fund of the United States** organized **the Atlantic-Black Sea Security Forum, June 4-5, 2018,** an international event, part of the **Aspen National Security & Defense program.** The **Young Strategic Leaders Security Conference**, held on **June 4**, represents an essential element of the forum, addressing the community of promising young professionals of the AIR and GMF networks of Fellows and Alumni.

Organized by
Aspen Institute Romania

In Partnership with
Bucharest office of the German Marshall Fund of the United States, NATO's Public Diplomacy Division

Institutional Partners
Ministry of Foreign Affairs, Ministry of National Defence, the Romanian Intelligence Service

Knowledge partners
PwC Romania

Media Partner
AGERPRES, RFI România, Caleaeuropeana.ro

Contributors
Bruno Lete, Daria Catalui, Mihai Todor, Ana Catauta, Sabina Horga, Alin Luchian, Irina Tkeshelashvili

ASPEN INSTITUTE ROMANIA

G | M | F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

Young Strategic Leaders Security Conference
Report

The conference debate focused on the topical issues of cyber security, NATO-EU partnership and the role of the Eastern Flank. The collaboration with the European Union was placed at the core of NATO's long term strategies. Consolidating the Eastern Flank is a key example of crucial regional efforts and planning, however as European affairs and challenges are changing, the Eastern Flank is continuously more questioned: How will you envision a collaboration between the EU (via PESCO) and NATO in regards to the Eastern Flank? and How will the European member states approach its future development? Moreover, the digital age has now consistently marked all layers of life, society, politics, science, and the need for designing Cyber Security tools is no recent discovery. The cyber vulnerabilities that nations, organizations and institutions are currently confronting prove there it is still a long unbeaten track to unfold towards finding viable solutions for the disorderly cyber-attacks. The Cyber Defence Pledge that NATO Allies signed in July 2016 made a clear international statement on the importance of protecting the cyber space and settled a new vision for international education highlighting the role of cyber instruction and cyber defense training. Adding the modern cyber defense to the traditional military defense would call for approaching the biggest challenges in cyber security today and whether there is a role for a common shared responsibility.

As part of the same region, Romania and its neighbors are directly concerned by the future advancement in the area, while facing both impressive challenges and benefitting by equally important opportunities.

The participants were young professionals of the Aspen and GMF Fellows and Alumni communities and their working experience and intellectual assets provided a lively discussion that highlighted both problems and possible ways of solving them in an increasingly challenging (sub)regional and wider security environment.

Some developments in Europe and elsewhere have turned into reasons of serious concern for the future of security and stability, indeed of liberal democracies; the more so as some of present-day realities would have been hardly conceivable a couple of decades ago – to wit, prospects of trade war among allies; centrifugal trends in (relatively) new EU Member States; re-nationalization of foreign policies; uncertainties looming over the trans-Atlantic cohesion, including in the defense field. Moreover, security-related challenges emerge from the steady, unstoppable and ever-widening advance of

technology and point to prospects of 'hybrid-wars' alongside with cyber-attacks and join 'traditional' factors, like militarization in areas bordering EU and NATO and armed conflicts raging in the Middle East – all of which add to the complexity of the on-going drive of the two organizations to adapt to, and cope with, new realities. The Black Sea Area is a most representative 'sample' of said increasingly worrying developments that ultimately boil down to the struggle for leadership.

Cybersecurity has been a component in EU's strategy since 2013 and finds its place in the Permanent Structured Cooperation (PESCO) – inter alia, with the Cyber Rapid Response Teams and Mutual Assistance in Cyber Security. In 2016 EU and NATO signed a technical agreement on cyber defense and cooperation has greatly increased particularly in fields like training, sharing information, research and exercise. Meanwhile, various EU institutions put forward specific rules and regulations and sizeable investments have been made, including in various industries and businesses with a view to enhance related resilience and capabilities. NATO-related institutions were set up, like the Cooperative Cyber Defence Centre of Excellence (CCD CoE) in Tallinn; the Trust Fund on Cyber Defence, which is dedicated to help Ukraine's defensive capabilities to counter cyber threats and is led by Romania; the first phase was completed and Ukraine is expected to step up to challenges.

As of now, PESCO seems to be defined rather by what it is not: it does not mean an EU army, as it faces challenges stemming from the technical variety in the weaponry of the 28 MS. However, it may bode well for the European competitiveness, for increased burden-sharing – including cost-wise – with NATO, for diminished reliance on the US and for a stronger civilian dimension of the military. The issue of military mobility across Europe must be addressed as well, perhaps in a Schengen-like arrangement. At the same time, a question remains as to how this would help the European integration if Europeans go on buying American assets.

Another issue is the future of the trans-Atlantic cooperation against the background of the trade-related problems, even if the US has not reneged on commitments on the ground – at least not yet. Moreover, America's today trend towards unilateralism may be a 'blip' and it may be appropriate to address it with some patience. To counter the risk of the trans-Atlantic relations entering a diffuse stage it must be kept in mind that, at the end of the day, NATO and EU Members are mostly the same countries. The EU has proved more resilient than probably expected ('we need to remember what good the EU has done') and the different institutionalization of the two organizations may be mitigated

by increased communication between them – which is where PESCO may have an important part to play.

Challenges to the European security as a whole stem from various areas, some of them in terms of geopolitics, while others belong to hybrid threats and warfare. The APT (Advanced Persistent Threat) concept is intensively used in assessing developments in the European security environment as it includes hi-tech tools (in the advanced segment), constant monitoring and collecting data (under the persistent entry) and actors that may pose threats to the status-quo, be they organizations (governments) or individuals.

The militarization of the Black Sea has become the strongest concern and the vulnerability of NATO's Eastern flank is highlighted, particularly since the Black Sea area is where many global interests meet – and clash more often than not. It is widely reckoned that whoever controls the Black Sea may secure influence on the Wider Middle East as well; in this respect, Russia is 'a known quantity', while Turkey's behavior seems to be related to a kind of multiregional approach that may change the balance in the area. Turkey's concerns arguably emerge from the Arab and Kurdish components rather than from a Russia-Iran relationship and, unlike Crimea, Turkey is not an outpost for Russia.

The Black Sea being relatively close to China in terms of geography needs to be addressed under the circumstances of the emergence of US and China as the new poles of the global power; the worst-case scenario would be a Russia-China 'ganging-up' against the rest of (Western) Europe. On the other hand, NATO sees Russia as a threat, whereas all the EU MS do not share this view – a similar situation when about attitudes versus China, which differ among some EU MS, quite widely sometimes.

A conceptual approach, which would promptly trigger concrete decisions, calls for defining whether the NATO-Russia relationship has reached the stage of war and whether the NATO response strategy should be containment or confrontation. A game theory model reveals that containment is the answer – yet, the initiative coming from a NATO strategy should strongly promote predictability, firmness and reasonability, while aiming at persuading Russia of larger dividends brought about by peace than by direct and/or even indirect confrontation. Concrete measures in this direction ought to include acknowledging the strategic import of the Black Sea; coping with the variety of interests and even internal diverse realties in a way that would relentlessly encourage cooperation and dialogue among riparian states; and upgrading and, where needed, creating both military and political tools available to Allies and Eastern Partnership states that would

signal to Russia the high costs of a possible aggression as against the favorable outcomes of, at least, a peaceful cohabitation in the area.

Unity remains key in dealing with, and responding to, hybrid security challenges, from defining the 'enemy' to adopting coherent steps for countering cyber-attacks, as they are more successful when their targets are not united. The re-nationalization of politics in Central and Eastern Europe, as well as elsewhere, favors the spreading of 'polluted' information, just like absence of common understanding of terms hinders efficient joint responses. The definition of the hybrid war is quite broad at the EU level, even as MS look into the matter while bearing in mind sovereignty-related aspects. This leads to difficulties in naming 'the enemy', although the task would be rendered easier by looking for the beneficiaries of various hybrid actions; at the same time, politically-motivated hackers may well be found inside the European States and, in a broader sense, 'computer users' may become 'the enemy' themselves. However, there is a strong specificity in defining 'the enemy' as it may differ in keeping with the level and the domain where adverse actions are discovered.

Effects of said actions are visible already – e.g. in the diminishing pro-EU trends due to Russia's intense use of cyber and hybrid warfare. This reality brings forth the need to increase offensive capabilities for defensive purposes in this field: while it is true that EU and NATO are meant to prevent war, it is less clear what will happen when war actually occurs. Streamlining definitions of terms and strengthening integration, including in the military and the cyber/hybrid fields, should allow for a (counter)offensive of the same kind. Likewise, education is key in fighting 'pollution' of information and is much cheaper than developing hard power; in the same direction, EU has to improve its communication with the public and secure efficient use of funds and programs to improve its own cyber-defense and related capabilities.

Russia's overall economic troubles since the dissolution of the USSR have arguably contributed to inferiority (both actual and perceived) of the Russian military. The lesson Russia has learned is the 'hybrid strategy' that is successfully implemented due to the majority of political leadership hailing from the KGB era. Conditioning, denial and deception, indirect action and leadership intent are the four themes the international intelligence community has identified in Russia's actions that are meant to gain strategic superiority in the Eastern Flank.

There are at least three developments of essential political importance that have been taking place in the strategic communication: the evolution of e-technology, the growth

of information power, and the progress of propaganda as a manipulative instrument to control the public opinion against democracy; there is a close connection between governments' approaches to the strategic communication and their pursue of democracy. If the Black Sea Area is to be considered a strategic link between Europe and Asia, the Eastern Partnership countries need to be factored in NATO strategic communication plans – the more so as Russia is actively promoting an offensive attitude when resorting to this kind of communication. An important element to be considered in preparing and implementing the defensive NATO strategic communication in this direction is the working language, so that information reaches targeted audiences in the Eastern Partnership countries lest they embark on mere day-by-day responses to Russian disinformation and propaganda.