Hybrid threats and the EU

State of play and future progress

Conference Report

On 2 October 2017, the Estonian Presidency of the Council of the EU and the EU Institute for Security Studies (EUISS) organised a high-level conference in Brussels to reflect on the nature of hybrid threats and the EU's present and future responses to them. The conference brought together high-level policymakers and think-tankers to critically analyse the progress made and to chart a way forward. The conference was structured around three panel sessions and keynote speeches were delivered by Federica Mogherini, the High Representative for the Union's Foreign and Security Policy and Vice-President of the European Commission, Jyrki Katainen, Vice-President of the European Commission for Jobs, Growth, Investment and Competitiveness, and Jüri Luik, the Estonian Minister of Defence. Estonia's Ambassador to the Political and Security Committee, Lembit Uibo, and the EUISS Director, Antonio Missiroli, introduced and concluded the conference. This report summarises the main lines of thought and debate during the conference.

Session I – The EU and hybrid threats: where do we stand?

The panel was in agreement that hybrid threats pose a clear and present danger to the EU. The WannaCry attack in May spread to over 150 countries and it is believed that Russia has interfered in numerous elections over the past few years. In particular, it is thought that hybrid tactics are being used by Russia to offset the challenges it is facing in developing its military. In this regard, panellists identified money as its main hybrid tool, as Russia uses its financial resources to obtain political influence. Groups such as Daesh also thrive on financial flows to fund their terrorist activities. Vulnerabilities in and around Europe are being exploited, especially in the eastern and southern neighbourhoods where weak governance institutions exist.

The EU has responded in a number of ways. Not only has it established a Hybrid Fusion Cell in the European External Action Service to detect, deter and respond to hybrid threats, but it is actively working to ensure closer cooperation between various EU institutions. The audience also learned how the recently established European Defence Fund could be used to fund hybrid-relevant programmes related to, for example, cyber defence. There is clearly a need for greater awareness raising and resilience building. The EU needs to devote more attention to ensuring the protection of critical infrastructure, energy security and diversification, cyber security, health and pandemics, financial service security, etc. There is, however, a need to carefully consider how the Union responds to hybrid threats because any steps to close our societies (through trade restrictions and/or tighter regulations) may undermine the very factors that ensure the EU's prosperity.

Hybrid threats have also led to much closer cooperation between the EU and NATO, resulting in a common understanding of hybrid threats and the identification of 42 specific action points. A tangible example of this cooperation is the recent joint EU-NATO crisis management exercise conducted in a hybrid environment. However, it was acknowledged that the EU and NATO still have to improve their decision-making processes to ensure that the two organisations can rapidly and effectively respond to hybrid threats. This is vital because hybrid threats manifest themselves

differently in any given context – EU and NATO responses will have to be tailored because there is no one size fits all approach to hybrid threats. Here, it is vital to ensure that the recently established Hybrid Centre of Excellence in Helsinki is properly resourced.

Finally, the EU has altered the way it approaches strategic communications. From a time when the EU was unable to effectively communicate what it does in the world, now it identifies and debunks harmful narratives and myths with its own stories and narratives. The EU does not, however, use strategic communications as a weapon in the way that some actors do. There is still, however, a need to more effectively tie together the EU's communications to the outside world and within the Union itself. There is also recognition that developing EU-wide awareness raising campaigns is challenging because awareness and interest in hybrid threats differ across the EU.

Session II: Cyber resilience: lessons and good practices

Panellists agreed that the frequency and severity of cyber-attacks will not only ensure continued political buy-in but they will also challenge the EU to continuously develop its resilience strategies. Cyber-attacks could disrupt the functioning of societies, democratic processes, the individual security of citizens, financial markets, etc. There is also a danger from the possible proliferation of cyber tools. For these reasons, the panel agreed that there is a clear need to maintain political attention on cyber security long beyond the Estonian Presidency of the Council of the EU.

Panellists suggested that even if international and national bodies need to cooperate the first line of defence and cyber resilience rests with governments. Accordingly, national cyber capacities should be developed both in terms of how governments enforce international law and how they recruit, train and retain cyber experts. However, it was equally acknowledged that no member state is able to deal with cyber threats alone. Collaboration is a must.

The EU has responded in a number of ways. The European Commission is following a three-pronged approach under its digital single market initiative: first, promoting cooperation between member states; second, nurturing technological innovation on cyber by supporting cutting-edge research and industrial collaboration; and third, the European certification of digital products and services to ensure safe use. Furthermore, the Commission has proposed a 'blueprint' for how the EU and member states can respond quickly and jointly to large-scale cyber-attacks. The Commission has also decided to build on the existing European Agency for Network and Information Security with a fully-fledged EU Cybersecurity Agency. This Agency will organise yearly exercises, share knowledge and help implement the Directive on the Security of Network and Information Systems.

Furthermore, the EU is developing a Cyber Diplomacy Toolbox designed to respond to attacks through sanctions, international cooperation, dialogue, capacity building, joint investigations, etc. For example, the European External Action Service is already nurturing cyber dialogues with the US, China, India, Japan, South Korea, and soon, Brazil. Recently in Tallinn, the European Defence Agency hosted the EU's first table-top exercise on cyber defence for EU defence ministers. The nature of cyber threats today also means that EU-NATO synergies are required and this can come in the form of regular joint exercises and training.

Session III: Strategic communications: progress and future work

Focusing on the southern neighbourhood, the audience learned how media warfare is as important to jihadist fighters as conventional weapons. Daesh, for instance, pays its media operatives seven times more than its fighters. The panel agreed that strategic communications play a central role in countering radicalisation, but many stressed that underlying conditions and structural issues need to

be addressed. Propaganda amplifies grievances and ideology. Terrorists are not simply radicalised on the basis of propaganda and so a greater understanding of grievances and ideology is required.

Many of the speakers also referred to the need to ensure cooperation between diverse actors such as academia, industry, government and civil society. In particular, the panel argued that these partnerships are vital if the different elements of hybrid threats including energy dependency, the funding of political parties, corruption, defence planning, etc. are to be understood.

In terms of the EU's response, it was acknowledged that greater efforts have been made to call out fake news and to identify suspect sources (for example, by analysing media ownership). Even though the EU's capacities for strategic communications are still in their infancy, efforts have been made to interconnect all relevant bodies in the EU system and to pool existing communications budgets so as to ensure optimum impact.

The EU is also placing greater emphasis on communications with a youth audience and it is trying to improve media literacy overall. Much energy is going into creating a positive narrative of the EU. Yet, strategic communications need to be tailored to different audiences and contexts. An example of the EU's increased efforts on strategic communication is the work of the East StratCom Task Force, which counters pro-Kremlin media dissemination in Europe. Even though the Task Force is seen as a robust and credible service, it will clearly take time to improve the EU's strategic communications and to ensure coordination between the member states.

Note: the views of the panellists and participants do not necessarily reflect the views of the Estonian Presidency of the Council of the EU or the EU Institute for Security Studies.