HOW TO DETER HYBRID THREATS?
Conference summary, 5-6 June 2019

Background

The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) held a conference 'How we can deter hybrid threats?' on 5-6 June in Helsinki. Over 100 participants from the European Union and NATO states, as well as partners from Georgia, Singapore and Australia attended. In depth talks covered the value of attribution, private-public partnerships, imposition of cost, and the tools needed to have an effective hybrid deterrence posture. EU commissioner Julian King provided a keynote speech, with pracitioners and academics from Hybrid CoE member states, EU, NATO and partner countries together with private sector representatives providing expert analysis.

The Conference was held as part of the project led by the Community of Interest on Hybrid Influencing at the Hybrid CoE. The 2019 project explores how states can use different tools they possess in an orchestrated, collaborative manner to deter hybrid interference/influence emanating from both state and non-state actors. The end goal is a Deterrence Playbook available for practitioners from Hybrid CoE member states.

Modern deterrence and its application to hybrid threats

The conference opened by discussing the importance of having an effective deterrence posture in the modern world. Malign state and non-state actors have and will continue to seek political and economic advantage over the Euro-Atlantic community. This threatens both the principles we value and the interests we have, necessitating effective deterrence against the threat of hybrid in its ever changing and evolving forms. To be effective against hybrid threats we need to blend resilience and enhanced defences with proactive imposition of cost against hostile actors.

For this to happen we need to consider all possible measures. If something we value is subject to aggression of interference from an adversary, deterrent options should be considered. In the absence of effective deterrence, our threshold of tolerance will continue to be tested. We must therefore consider what behaviours we are comfortable with and what actions we are not prepared to tolerate. Actions which undermine sovereignty or internal affairs are regarded as key triggers that go beyond acceptable behavior and must be deterred with robust measures. Choosing not to act, while sometimes an act in itself, raises the question of whether certain behaviours "really matter?" The challenge now is to develop a more proactive approach to stop or reduce the behaviors that do matter.

A further area of discussion was the starting point to deter hybrid threats: identification of the adversary's interests and vulnerabilities, together with signaling to convey our willingness to harm these in the event of hybrid interference.

Deterrence Options

There are a wide range of measures available to deter malign activity. The most frequently mentioned options during the conference were public/private attribution, legal tools/powers against individuals, sanctions, deployed military capability, visa revocations/expulsions, seizing of assets, and stratcomms messaging to expose the flaws and hypocrisies perpetrated by the adversary. However there was no "one-size fits all" solution. Some states were in favour of a "deterrence by punishment" approach by escalating above an adversary's actions (what will hurt them the most) as way to deter further behaviour. Others were more inclined to act without causing further escalation and emphasize the prevention of the threats ("deterrenece by denial"). This allowed for better political engagement and avoided adversaries feeling increasingly isolated. It became apparent that different hybrid actors would require differing, tailored approaches, obliging the CoE community to consider the varying interests of adversaries and how each of these might be held at risk.

There was a useful discussion on having a suite of options available, exploring how agreement on just one action can have a strong deterrent, as it shows solidarity with others. The recent EU Cyber Sanctions showed what was possible in multilateral circles. Therefore, when talking about collective deterrence posture, we should aim at providing a range of response options, identifying how these tools support the effort and see what cumulative effect it can give – each partner/ally should feel able to contribute what it can/feels it does best.

Escalation remains a challenging topic, but there was a strong feeling one cannot deter hybrid threats if the adversary knows its actions will not be met by adequately strong responses. We should not limit our response options in the same domain of hybrid aggression against us – by responding in different domains we can sometimes avoid vertical escalation but still send a strong message.

Attribution formed an important part of the discussion. It can be challenging to collect (or communicate) rock-solid proof of hybrid interference, but this should not disincentivize us from using this tool. One expedient solution is to look closely at the target of hybrid aggression to determine which adversary may have had an interest in mounting a threat. We should also aim for better public-private partnership (e.g. in tech or financial sectors), given private sector data analysis and assessment capability. In collective effort, those unwilling to attribute politically could at least choose to avoid contradictory messages, as unity in communications is important. Exposing proxy-patron relations is an important way forward to deter non-state actors from their actions.

Finally, to use the tools we possess efficiently, cross-governmental cooperation is crucial – we need to be sure our military, economic, diplomatic, political, informational and other domains are orchestrated in the same direction. Setting up procedures for quick response also supports deterrence posture. However, at the same time, we should be agile and able to re-calibrate responses to deal with the ever-changing nature of hybrid threats.

Conclusions and outcome

We will never be able to stop hybrid threats completely, but can aim to have a significant impact, reducing the frequency, effect, and impunity of hybrid aggression by raising cost and demonstrating resilience. By nature hybrid is cross-sectoral, ever evolving and making use of new technologies. The Hybrid CoE goal is to be at the forefront, increasing our member states capability, exercising for the unexpected and spreading mutual understanding and best practice. This conference usefully encapsulated the views of experts and allies. Hybrid CoE will now work to capture the views of experts and allies in a flexible 'playbook' of deterrence options which can serve as a tool kit for partners to refer to.