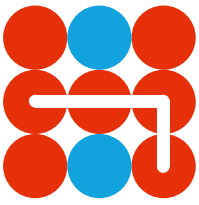
Working Paper 1 • October 2017

Regional Cooperation to Support National Hybrid Defence Efforts

AAPO CEDERBERG, PASI ERONEN AND JUHA MUSTONEN



Hybrid CoE

Working Paper 1/2017

Regional Cooperation to Support National Hybrid Defence Efforts

AAPO CEDERBERG
PASI ERONEN
JUHA MUSTONEN

Summary

Hybrid threats are at their very core interlinked, operating domain-spanning activities that the threat actors, nation states or non-state actors, conduct in order to advance their agenda and attain their goals.

Technological advancements and diffusion combined with wide digitalisation of Western societies, critical infrastructure included, means that a wider range of threat actors can have both a wider geographic reach and a larger set of potential targets within their reach.

When assessing hybrid threats, a thorough review of hybrid threat actors, their means, tools, and goals is necessary. This understanding should guide the self-assessment and vulnerability identification process conducted by countries facing hybrid threats and influencing. The self-assessment should lead to a number of concrete actions to improve the national resilience and hybrid defence posture.

Assessing capabilities to counter hybrid threats, comprehensive national approaches and integrated international response are at the core. The latter emphasises both EU–NATO cooperation and a wide regional cooperation spanning from military to other parts of the society.

In the short term, a regional approach to assessing and analysing hybrid threats and the risks they pose is required. In the Baltic Sea region, the assessment and analysis process should be tightly knit to NATO's ongoing Baltic Sea process and EU's work on preparing a hybrid risk survey.

The EU, NATO and their members have shown their readiness to proceed on this path of widening and deepening cooperation on countering hybrid threats by participating in the workshop organised by Hybrid CoE. The key takeaways from the workshop included an identified need to prepare a concept for a shared digital platform to support better situational awareness exchange on hybrid threats, and to organise a systematic exchange of best practices on countering hybrid threats through seminars, thematic workshops, and exercises.

Introduction

Since the 1990's and the first years of the twenty-first century, our security environment has dramatically changed for the worse and the current situation appears to have become "the new normal". The changes in our security environment have been amplified by the rapid changes in the overall operating environment, where societies are quickly digitalising and becoming more interdependent, despite the recent political trends. The future seems to have become more unpredictable.

It is in this environment that we are witnessing hybrid influencing being carried out. Targets of hybrid influencing have been scattered across the whole society, as the hybrid actors are taking advantage of the vulnerabilities and capability gaps existing in our technologically advanced societies.

For several years, NATO has been following closely the development of the security environment in the Baltic Sea region (BSR). Finland and Sweden have been invited to this BSR assessment together with NATO allies. It is clear that hybrid threats and risks have to be part of this regional assessment process.

The EU is planning to conduct a hybrid risk review based on the EU's Joint Framework on countering hybrid threats released back in April 2016. Currently, the EU member states, led by the Estonian Presidency and supported by the Friends of Presidency group, are discussing how to take forward this work on hybrid risk survey and hybrid risk indicators.

Hybrid Threats Pose a Regional Challenge

Hybrid threats are at their very core interlinked, operating domain-spanning activities that the threat actors, nation states or non-state actors conduct in order to advance their agenda and attain their goals. Hybrid influencing can be seen as continuation of politics with hybrid capabilities.

The agenda varies according to the threat actor and the means that it can command. A more powerful threat actor, such as a regional power, can have geostrategic and world order level goals for its activities and a wide geographic reach, while a less powerful actor, such as a smaller state, or an international terrorist organisation, must settle for less ambitious and more localised, even domestic goals.

Means are the necessary power base that enables the hybrid activities. Means include, but are not limited to, blunt military force and other powerful state organs, such as intelligence services; parts of the national economy that are tied to the command and control structures either officially, or unofficially like in the case of personal networks; international organised crime and other front organisations; technological know-how and capabilities that can be harnessed; and international and domestic media. More generally, the threat actors can harness means across the DIMEFIL (Diplomatic, Information, Military, Economy, Financial, Infrastructure, and Legal) elements of national power.

Activities, or in other words the act of hybrid influencing, can take many kinds of forms ranging from offering short-term lucrative business contracts to military pressure, coercion, and limited use of force at the far end of the spectrum. The activities do not need to be identified as being negative from the target's vantage point, at least not in a short timeframe.

The nature of a hybrid actor and its targets, the resources available to the hybrid threat actor, and geographic considerations among other things impact the types of activities available to the hybrid actor. In order to qualify for hybrid influencing, there need to be two or more activities taking place in an orchestrated manner in support of advancing the hybrid actors' agenda and attaining their goals. From time to time, hybrid influencing that takes place abroad serves the domestic purposes and agenda at home.

Activities can take place in a short or longer time span, and their intensity is calibrated according to the need and target. Hybrid influencing comprises activities, operations, campaigns, and, at the far end of the spectrum, warfare. At times, hybrid activities may appear to have ceased, such as

in the case of so-called frozen conflicts or during perceived peace time, while that particular situation may in reality serve the greater goals of the threat actor, or serve as time used to prepare the ground for future operations.

Targets for the hybrid influencing are typically carefully identified and selected vulnerabilities. Such vulnerabilities range from corrupt individuals in powerful positions to structural problems, such as ethnic divisions. Another way to approach targets is to understand them as societal, military included, capability gaps that the hybrid actor has identified and strives to take advantage of. One way of categorising the targets is the application of PMESII (Political, Military, Economy, Society, Information, Infrastructure) categorisation. Another such categorisation would be MICEPIO (Military, Information, Cultural, Economic, Political, Infrastructure, Other forms), which supports identifying the use of cultural instruments, such as religion or sports, as a tool for hybrid influencing. Successful target selection and operationalisation of the selection demands an in-depth understanding of the target society and availability of necessary means and tools.

Hybrid threats take advance of asymmetries, often employ irregular elements, and utilise various kinds of leverages across domains where hybrid actors have means and tools that fall under their command and control. The activities are typically designed to stay within the grey zone that may be outside of a target's detection capabilities and underneath the target's estimated threshold of major escalation, or justified military response under international law, unless the hybrid threat actor considers such escalation to be beneficial for attaining its goals.

While many defining features of hybrid threats have been present in earlier strategic and military thinking, such as in the political warfare of the Cold War era, the recent technological advancements and their diffusion combined with the wide digitalisation of Western societies, critical infrastructure and means of communications included, sets the current date and hybrid threats apart. Technological developments allow a wide range of threat actors to have both a wider geographic reach and a larger set of potential targets within their reach. Alongside the physical and digital infrastructure, also our critical functions and processes, and cognition can be targeted by the hybrid influencing.

Taking all the above into account together with working definitions of hybrid threats both from NATO and the EU, it is necessary to keep in mind that the art of competitive politics, including warfare, is developing all the time and we often encounter new mutations or rehashes of previously well-known doctrinal approaches. This necessitates the constant research on the potential new threat vectors. Such research enables proactive defensive measures to be taken on top of reac-

tively plugging the existing vulnerabilities based on the lessons learned from the hybrid activities that we have so far witnessed.

The high-end hybrid threats, which have access to and can command a wide array of capabilities, including tools enabling crossing the geographic distance; have integrated hybrid tools into their doctrinal thinking; have demonstrated their intent by applying tools of hybrid influencing to advance their political agenda; and have an outspoken revisionist or even revolutionary political agenda, are the most dangerous and difficult hybrid threats to be deterred and countered.

Such ambitious actors have goals that have at least regional or wider geopolitical significance, where individual countries and hybrid influencing they are experiencing may play just a small part in a larger scheme. Thus, in order to counter such activities effectively, and to understand the grander scheme of things, supranational organisations and multifaceted cross-border cooperation are needed.

National Activities Build a Resilient Society

Response mechanisms to hybrid threats are based in most cases on solid groundwork done on a national level. Nations improving their security posture in relation to hybrid threats must understand the hybrid actors that they are facing; the national vulnerabilities that they have; the national resilience improving actions to address the capability gaps and to mitigate the vulnerabilities; and the areas where international cooperation is necessary in order to make the national counter-hybrid threat efforts more effective and to protect the common regional or international interests.

In order to direct the national resilience build-up efforts to the highest priority targets, it is necessary to have an understanding of the threat that the nation is facing. This analysis should incorporate some estimate over the adversary's strategic goals, the means that it can harness in support of attaining those goals, and the tools available to the hybrid actor, particularly in the affected region. While most of the countries do have the governmental and private sector entities that routinely work on such analysis, international information-sharing provides further details into national analysis.

Based on the understanding of the potential threat actor, it is necessary to launch a national vulnerability assessment, where a threat actor's goals, means, and tools are compared with the vital functions of one's own society and other potential targets. Self-assessment should give decision-makers a rough idea where the key vulnerabilities and capability gaps in one's own system reside.

These vulnerabilities are typically country and area-specific, which underlines the need to develop a national approach to address the hybrid threats. In addition to regular self-assessments, it is necessary to have mechanisms in place where situational awareness information originating from different parts of the society – private sector included – gets collected, shared, and acted upon.

Understanding the threat, understanding one's own system and its vulnerabilities, directing resources to address the vulnerabilities, and organising a reliable, all-domain situational awareness unlock the distributed domain-specific detection and response mechanisms. Those activities also enable command and control, and make possible system-wide exercises that are used to improve the overall awareness and to develop a common playbook for coordinated and organised response.

Furthermore, scenario-based exercises in combination with repeated vulnerability analyses and up-to-date situational awareness enable the pinpointing of vulnerabilities that may be hiding on organisational borderlines, out-of-date pieces of legislation, insufficient mandates for agencies and authorities, and confusing or completely missing processes for response mechanisms that involve many actors.

Activities such as those listed above, a part of comprehensive or a whole-of-society security approach, support building overall national resilience, improve preparedness, and help to communicate a deterrence by denial strategy to potential hybrid threat actors. Nevertheless, in order to address the threat that a more ambitious threat actor poses, it is necessary for individual countries to engage in networked cooperation.

Networked cooperation allows participants to enjoy a better situational awareness and greater situational understanding; have a better visibility over adversaries' strategic goals and their own nation's place in those; allow detection, identification and countering hybrid operations and campaigns that span a number countries; and help pool resources and protect assets that serve several countries in a region.

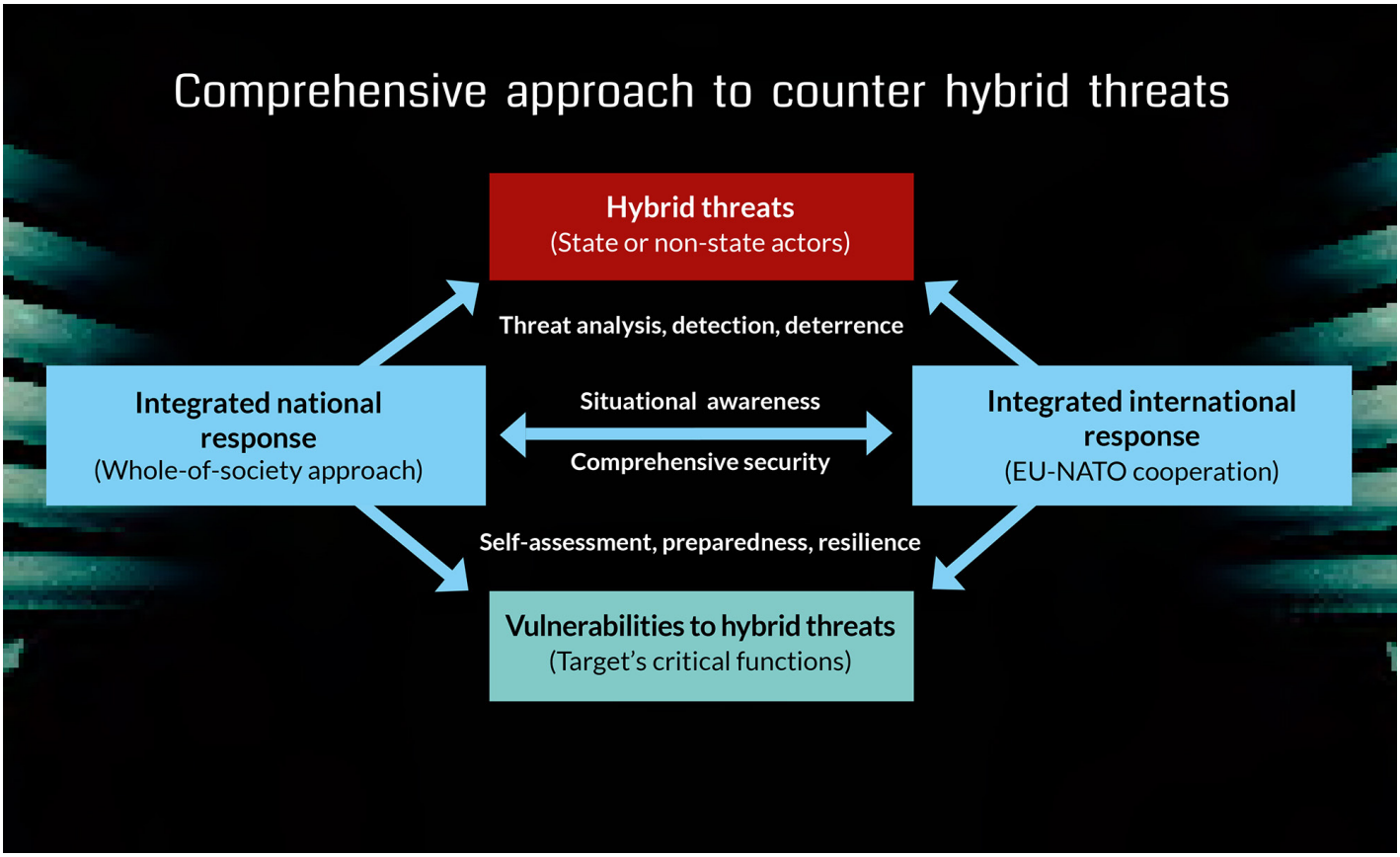


Figure 1. Comprehensive Approach to Counter Hybrid Threats

Regional Cooperation Hardens the National Hybrid Defence

Ambitious regional, or wider geostrategic, goals of an adversary utilising a wide gamut of tools for hybrid influencing forces individual countries to seek for closer cooperation both regionally, but also in a wider geostrategic context. Individual countries acting alone without supranational coordination and shared situational awareness don't have the means for an efficient hybrid defence.

The Baltic Sea region brings together EU member states, NATO allies, and transatlantic partners. To bring together, and to ensure the successful and well-coordinated cooperation, all countries and organisations need to share a set of common regional goals and have a shared venue for coordination. One key venue for such cooperation, particularly in the area of hybrid threats and their strategic analysis, is the recently inaugurated European Centre of Excellence for Countering Hybrid Threats.

The regional cooperation can take various forms, many of which are already on-going, but could be improved, or brought under a common umbrella for better coordination. One good regionally active forum for coordinating cooperation is NORDEFCO, which

could be used as a functioning blueprint for wider cooperation, both domain and geographic area wise.

From a more geostrategic and geographic viewpoint, the Baltic Sea region offers a natural environment, where wide cooperation and collaboration can be seen to be particularly meaningful. The geographic area ranging roughly from the North Sea and the Arctic to the Black Sea forms an area where events and their potential direct outcomes, and second and third order effects, can be seen as strongly interlinked.

Examples of such events vary from the retaining of control over strategically important land masses, such as the Suwalki Gap or the island of Gotland, to responding to uncontrollable regional migrant flows, or ensuring collectively functioning of cross-border critical infrastructure. Thus, close cooperation is needed to create, manage, and improve region-wide response mechanisms.

When countering hybrid threats, key challenges are situational awareness, often shared by civilian and military actors, as well as preparedness and resilience of civilian sectors of the society. Military defence alone is not capable of deterring and defending against the hybrid actors operating below the thresholds of warfare and response, the threshold of attribution, and even below the threshold of detection. Thus, in the case of deterring and countering hybrid threats, the concrete areas of cooperation should include, but not be limited to, the military domain.

As an example, the protection of critical infrastructure, which is mostly under civilian and often also private ownership, should be an integral part of regional cooperation. Functioning communications networks; media; financial systems; electricity grid; natural gas terminals, storage facilities and supply pipelines; airports; harbours; sea, rail and road transport systems; wider logistics networks and their supporting systems; and various sensor and information collection systems, just to name a few examples, all enable the critical functions in individual societies and in a wider region. In most cases, these infrastructures span across the national borderlines, not only physically, but also when looked at from the perspectives of ownership and control over the systems. These interlinkages and interdependences underline the necessity of regional cooperation.

In addition to having a common vision for regional cooperation to counter hybrid threats; understanding the key players that should be included; establishing or revamping the existing venues that support the coordination work; and identifying concrete areas for cooperation, the information sharing must take place in all levels and all processes.

As was reflected by the Prime Minister of Finland at the inauguration of Hybrid CoE, a culture of sharing information is important. Sharing information on situational awareness, as well as open source intelligence, is needed to promote a shared view on our common security environment and events unfolding in it. Without well-functioning information

flows and processing on all levels ranging from tactical to strategic, the coordinated and well-targeted response cannot take place.

An effective coordination of regional activities demands a shared situational awareness and understanding in all levels, and a shared playbook that has been supported by education, training, and exercises. Coming full circle back to the national capabilities, mature and well-functioning cooperation on an international level rests on the work done well on the national level.

Key Takeaways from the EU–NATO Workshop on Hybrid Risk Assessment

On 16 October 2017 in Helsinki, Hybrid CoE convened the EU–NATO workshop on hybrid risk assessment in the Baltic Sea region, inspired by the initiative of the Finnish and Swedish Foreign Ministers on 6 September. With staff-level participation in this workshop, EU (EEAS) and NATO (International Staff, Centres of Excellence for Cyber Defence, Strategic Communication and Energy Security) demonstrated their readiness to proceed on the path of widening and deepening cooperation on countering hybrid threats.

As a scene-setting framework for the workshop discussions, the concepts and ideas of this Working Paper were introduced at the workshop as food for thought. During the day, some 30 participants had interactive discussions on hybrid threats and situational awareness, on sectoral vulnerabilities to hybrid threats and bridging capability gaps as well as on exchange of best practices between states on developing their comprehensive security models.

Operationally, the key takeaways were the following:

1. The workshop discussions will feed into NATO's work on assessing the regional security environment and the EU's work on hybrid risk survey and hybrid risk indicators. As seen appropriate by EU Member States, Hybrid CoE could serve in analysing responses to hybrid risk survey and in developing hybrid risk indicators.

2. A shared situational awareness on hybrid threats would benefit from a digital platform, on which relevant civilian sector stakeholders and hybrid analysis producing entities from participating states would be able to share information and research on hybrid activities. This kind of platform should be available also

for use by the EU (Hybrid Fusion Cell) and NATO (Hybrid Analysis Branch). Hybrid CoE will continue developing the concept further and will study possibilities to establish such a digital platform on situational awareness.

3. Development of integrated national responses to hybrid threats would be served by a more systematic exchange of best practices of the comprehensive security models and their realisations in different states. Table-top and scenario-based exercises, efforts to enhance resilience in critical civilian sectors and identification of legislative vulnerabilities were mentioned as possible themes of such an exchange. In the Baltic Sea region, a more systematic exchange of best practices should be triggered and supported by a regularly organised regional seminar convening experts from countries of the High North and the Baltic Sea region. Hybrid CoE will continue the planning of such a regional seminar on countering hybrid threats to be organised in February 2018, and will invite BSR countries to share their best practices.

Authors:

Aapo Cederberg is an Associate Fellow of the Global Fellowship Initiative at the Geneva Centre of Security Policy (GCSP). Mr. Cederberg served as a Secretary General for the Security Committee of Finland for six years. Prior to that he worked as the head of strategic planning and foresight at the Ministry of Defence. He has a decorated career in the Finnish Defence Forces, where he retired as Colonel (G.S.).

Pasi Eronen is the lead researcher for the DC-based think tank Foundation for Defense of Democracies in their Russia Project. Outside of the research context, his professional career includes working for the Finnish Ministry of Defence, and in crisis management missions both with the EU and NATO. Pasi earned a master's degree in Security Studies from Georgetown University, USA.

Juha Mustonen is Director of International Relations of the European Centre of Excellence for Countering Hybrid Threats. He is a Finnish diplomat, having worked with EU CFSP, NATO crisis management, Nordic cooperation, transatlantic relations and UN affairs. He is Master of Political Science (IR) and has attended LISC at Geneve Centre for Security Policy.

The European Centre of Excellence for Countering Hybrid Threats
tel. +358 400 253800
www.hybridcoe.fi

The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) serves as a hub of expertise to enhance civil-military capabilities, resilience, and preparedness to counter hybrid threats with a special focus on European security and on EU–NATO cooperation.