Gulf Research Centre Cambridge
Knowledge for All

15th Gulf Research Meeting

Cambridge, 22-24 July 2025

Workshop No. 12

Enhancing the Gulf States Security against Hybrid Threats: Building Resilience and Regional Cooperation within GCC

1. Directors

Juha Makela
Finnish Defence Research Agency (FDRA), Helsinki, Finland

Antti Sillanpaa
National Emergency Supply Agency, Helsinki, Finland

2. Abstract

This workshop contributes for enhancing a comprehensive security approach for the Gulf Security. What are the hybrid threats (in Arabic التهديدات الهجينة) and hybrid war (الحرب الهجينة) and how are they understood in the Gulf? Gulf region is well-known of its huge investments into high-tech military hardware and many Gulf States rank among the top 15 countries in defence spending as of per centage of their GDP. However, no modern army, strong air force or fleet can constitute effective deterrence against hybrid threats. Hybrid warfare per definition blurs the borders between peace and war by creating a grey zone where society's critical vulnerabilities are intentionally targeted. The aim of hybrid influencing is to operate under the threshold of open conventional war by exploiting interfaces which obscure the tasks and responsibilities between different civilian and military authorities. The workshop aim is to explore and compare best practises with other states and regions in both countering and building resilience against hybrid threats.

3. Context

Both EU and NATO have included hybrid threats into policy documents and strategies. In addition, China and Russia have also adopted the thinking of hybrid influencing. Already in 1999 two Chinese colonels from People's Liberation Army (PLA), Qiao Liang and Wang Xiangsui, published the book "Unrestricted Warfare". The book gives examples of how to wage total war with non-conventional methods. In Russia, similar conceptual amendment in military thinking can be found in Chief of Russia's General Staff, Army General Valery Gerasimov's doctrine. The doctrine

emphasizes on future war in which conventional military means only consist of 20 per cent of warfighting, while non-military i.e., hybrid methods stand for up to 80 per cent. Against this evolving thinking on hybrid the workshop underlines the importance to study hybrid warfare/influencing in the Gulf context. The hybrid toolbox is often described by the acronym DIMEFIL & Cyber (diplomatic, information, military, economic, finance, intelligence, legal) in which every single letter signifies different domains of hybrid influencing.

4. Focus/Objectives

The workshop objectives can be divided into five sub-objectives:

- Defining and unifying the terminology of hybrid threats and hybrid warfare
- Increasing understanding about the hybrid warfare/influencing.
- Exploring and comparing best practices in countering hybrid threats
- Focusing on the necessity of the whole-of-government approach/comprehensive approach
- Understanding legal framework related to countermeasures and resilience building.

Scope of the workshop: hybrid toolbox can be used by state or non-state actors, and in many cases adversaries try to hide out own involvement and maintain deniability by using proxies or even "proxy's proxies". Thus, the workshop maps avenues for joint GCC approach in order to enhance the Gulf regions and its states preparedness against hybrid threats.

5. References

- Aaronson Micheal, Diessen Sverre, De Kermabon Yves, Long Mary Beth, Miklaucic Michael, NATO Countering the Hybrid Threat, National Defense University Fort McNair United States, 2011. [https://apps.dtic.mil/sti/tr/pdf/AD1042838.pdf]

- European Parliament, "Countering hybrid threats: EU-NATO cooperation", European Parliamentary Research ServiceMarch 2017, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599315/EPRS_BRI(2017)599315_EN.pdf].
-
- Charon, Paul & Jeangène Vilmer, Jean-Baptiste, Chinese Influence Operations, The Institute for Strategic Research (IRSEM), 10.2021, [https://drive.google.com/file/d/1AhHevTlIOddtKcRaOl6pkUbZ1oXCOima/view?pli=1]

- Hybrid CoE Working Paper 5, Handbook on Maritime Threats – 10 Scenarios and Legal Scans, November 2019 [https://www.hybridcoe.fi/wp-content/uploads/2020/07/NEW_Handbook-on-maritime-threats_RGB.pdf]

- Mazzucchi Nicolas, "Hybrid CoE Paper 14: AI-based technologies in hybrid conflict: The future of influence operations", June 2022 [https://www.hybridcoe.fi/wp-content/uploads/2022/06/20220623-Hybrid-CoE-Paper-14-AI-based-technologies-WEB.pdf]

- S. M. Azharul Islam, The Valery Gerasimov Doctrine, Bangladesh Institute of Peace and Security Studies,[https://bipss.org.bd/pdf/The%20Valery%20Gerasimov%20Doctrine.pdf]

- Marcellino William, The Rise of Generative AI and the Coming Era of Social Media Manipulation 3.0 Next-Generation Chinese Astroturfing and Coping with Ubiquitous AI, RAND Perspectives 2023, [https://www.rand.org/pubs/perspectives/PEA2679-1.html]

- Presl Jan Daniel Dominik, NATO StratCom COE, Russian Civilian Outreach and Information Operations in Syria, 2022, [https://stratcomcoe.org/publications/russian-civilian-outreach-and-information-operations-in-syria/222]
- Qiao Liang and Wang Xiangsui, "Unrestricted Warfare", (Beijing: PLA Literature and Arts Publishing House, February 1999 [in pdf-format https://www.c4i.org/unrestricted.pdf]

6. Papers Focus/Topics

Workshop directors encourage multidisciplinary experts, scholars and practitioners from a wide range of expertise (DIMEFIL & Cyber) to contribute with their academic papers. We divide the workshop into two parts. The first part deals with the hybrid threats and the second on countering these threats. We especially welcome papers that deal with both hybrid threats and their countermeasures of one state of GCC as a whole. Special focus is put on exploring cooperation potential within GCC-member states.

Potential topics might include:

Part I - Threats

- Use of hybrid methods (DIMEFIL & Cyber) as a weapon against the Gulf states/GCC
- Hybrid Threats and methods
- Disinformation and inauthentic campaigns as hybrid tools
- Information and cyber – two sides of the same coin
- Different roles of mis-/dis-/mal-information in hybrid threats
- AI and expansion of inauthentic behaviour in social media

Part II – Policy measures and defence against hybrid threats

- How to detect and response against hybrid threats
- Threat analysis and emergency response, national/GCC-level emergency centres/HQs
- Whole-of-government approach in countering hybrid threats
- GCC-international (e.g. NATO-EU) cooperation in countering hybrid threats
- Citizens and private sector's role in countering hybrid threats

7. Paper Structure, Referencing, and Format

Authors should refer to the GRM Paper Guidelines.

8. Publication Plans

We intend to publish all selected workshop papers that fulfil publication criteria in one edited volume (GRM joint publication or joint GRM Security Workshops publication) during Q4/2024 or latest Q1/2025.

As a second alternative we prepare to publish all papers in special issues of academic journals in cooperation or by the advice of the Gulf Research Centre and under the supervision of the workshop directors.

9. Directors' Bio Notes

LtCol (G.S), Dr. Juha Mäkelä is Chief of Information Technology Division at the Finnish Defence Research Agency. In addition he also works as Finnish Defence Forces (FDF) Middle East expert. His previous assignments include Visiting Researcher's post at al-Ahram Centre for Political and Strategic Studies in Cairo, Egypt. Between 2019 and 2022 he worked as Finland's Defence Attaché for Türkiye, Lebanon and Georgia.

Dr. Antti Sillanpää is Chief Preparedness Expert at the National Emergency Supply Agency of Finland, where he is focusing on information influence. He is leading a team of experts at Knowledge Centre on Information Resilience.Dr. Sillanpää worked for the Secretariat of Security Committee of Finland 2011-2021. His tasks were related to hybrid threats, especially cyber, election interference and information influence as well as preparedness of society. Between 2015-2018 he was assigned to NATO Strategic Communications Centre of Excellence in Riga, Latvia. His post was Chief of the Technical and Scientific Development Branch.
He holds a Doctor of Science in Technology degree from the Helsinki University of Technology, a Master of Social Science degree from the Helsinki University and a Master of Economics degree from the Helsinki School of Economics. His doctoral thesis focused on networks, competition and strategies.