Gulf Research Center
Knowledge for All
مركز الخليج للأبحاث
المعرفة للجميع

Design for Hybrid Threats – Be Purposeful and Fast

By Walter L. Christman and Ralph Thiele

Imagine that your country has an opponent or even a friend who does not fully agree with the established policies of your government. He is technologically well-positioned and has little scruples in using modern technologies to achieve his own political and economic goals. Since he shuns open, public debate, he seeks covert ways below the threshold of war to achieve his goals. For this purpose, he develops models of perceived targets to plan his attacks. You need to design a response.

Information needed is openly available on the internet. This includes information on communication networks and critical infrastructures, corporate data, personal information about governmental officials, police and military professionals and their families from social media accounts. In planning and preparing the hybrid campaign, AI-supported cyber-campaigns get the attack team anywhere it wants to be. Further information can be obtained via sophisticated microtargeting. Long before the start of a hybrid offense the malicious actor will also seek to provide – commercially or by other means - hardware and software into the target state's business, industry and government agencies as this is the best way to place malware. With the help of Quantum Computing, capable malicious actors may even secretly take over critical infrastructures such as energy and space assets.

Design thinking for defence transformation can help to facilitate innovation and creativity when dealing with complex emergent contexts. Clearly, in a technologically disrupted and more connected world future competition, conflicts and wars will be fought differently. As the pace of change accelerates, new competitors challenge established order. New political, economic, and military power centres are emerging. New technologies are surfacing and adopt faster than ever. This development has facilitated particularly the rise of hybrid threats. Moreover, the panoply of dynamic, and especially digital, technological developments on the horizon indicates that the portfolio of hybrid threats will expand rapidly. The unprecedented scale and pace of technological change supports a ceaseless and pervasive aggression against nation states, businesses and even individuals. The flood of data about human and machine activity puts economic and political power in the hands of malicious governmental and non-governmental actors as these apply pernicious effects on the very legitimacy and thus stability of target states' governmental, economical and societal structures.

Countering the hybrid threat, you need to define the design response in terms of aspiration, and not a problem. Whatever you have as a problem, aspire to not to resolve it, but to dissolve it. Hybrid warfare can be expected to become a long-term strategic challenge. It has evolved into an effective, apparently low-risk instrument of power for governmental and non-governmental malicious actors below the threshold of all-out war, aiming at undermining government institutions and functions, disrupting larger industry and critical infrastructure, global organisations and agencies, targeting critical military capabilities to include C4ISR. Virtual teammates multiply the scope, depth and reach of aggression broadening the envelope for espionage and violence even against individual citizens. We can expect disruptive technologies to provide a variety of malicious actors in the context of hybrid campaigns with additional, powerful options for targeting people and assets virtually and physically, with little risk of attribution or immediate retaliation.

Designing a response is more than a method and technique; it is a way of being in the world. It is working to create possibilities, working with others, and serving them in a manner that has consequences. States and organizations that are best able to anticipate and exploit technological opportunities will likely have a decisive advantage in future competitions, crises and conflicts. Seven technologies that are particularly relevant for the evolution of hybrid challenges and at the same time for meeting respective threats ubiquitous sensors have been identified by the Finland based Hybrid Centre of Excellence[1]:

- **5G** – the upcoming 5th generation mobile radio brings computing power to the edge. 5G nets will be attractive targets of hard- and soft-ware-based cyber threats from malicious actors.
- **Artificial intelligence** – unlocks the full potential of data. It is first choice for strategic fore-sight, improving decision-making and situational awareness, targeting and key enabler of human-machine teaming.
- **Autonomous systems** – have become an indispensable capability in virtual and physical applications. Sooner than later they will bring masses to the battlespace. Some of them will erve as expendables in critical missions.
- **Cyber and electronic warfare (EW)** – are major enablers of hybrid threats. Spectrum warfare combines cyber and EW into a new, crucial capability for mission success.
- **Extended reality** – visualises data and information, and structures interaction between the virtual and analogue worlds through digital technology.
- **Quantum sciences** – will be likely the key source of future disruptive capabilities; Quantum Key Distribution (QKD) has already arrived.
- **Space** – a revolution is underway. Upcoming Low Earth Orbit (LEO) and Medium Earth Orbit (MEO) capabilities are about to multiply outer-space assets, related bandwidth and sensor capabilities.

Design thinking to counter hybrid threats is accompanied by the need to establish multiple Action Learning platforms that can enhance civil-military collaboration in response to complex challenges with the aim of fostering greater organizational and social coherence. Clearly, technology driven hybrid threats affect the Gulf states as these have built their

[1] This is a key finding of the Hybrid COE, Helsinki, project *Hybrid Warfare: Future & Technologies*. Roughly 200 representatives from governments, industry and research centres have come to this conclusion. R. Thiele/J. Schmid. Hybrid Warfare: Future & Technologies (HYFUTEC) Mind the gaps. https://www.hybridcoe.fi/wp-content/uploads/2020/09/20200915_HYFUTEC_info.pdf

respective visions of the future on instrumentalizing the benefits of technological innovation for expanding prosperity and security. Many have looked for new ways of defence and security cooperation with countries such as China, India and Russia, with Egypt and Turkey. By diversifying partnerships, Gulf leaders have strived for a degree of strategic autonomy, while at the same time opening doors for outside powers to engage in the region.

Immense investments aim to reduce the states' dependence on oil by facilitating the emergence of a robust private sector. The coronavirus pandemic and dramatic shock to oil prices have hit their economies hard. As it remains important for the economic transformation to succeed, defence and homeland security have a critical role. The massive drone and missile attack on the Abqaiq oil processing plant and the Khurais oil field on September 14, 2019, points at imminent threats posed by hybrid actors. There is a clear risk of further attacks on Gulf states' critical infrastructure.

Traditional defence and deterrence, conventional and nuclear arsenals are of little use against malicious hybrid actors. Until today, the requirements of meeting the explosive mix of internal and external hybrid threats have neither found sufficient focus in their respective conceptual consideration nor in defense and homeland security spending. While the Gulf states have the adequate affinity towards innovation and front-end technologies, they clearly have growth potential towards orchestrating available resources and technology to adequately do the job.

Two core elements of a future strategy need to be orchestrated — resilience and superior action. Societal resilience, i.e. withstanding shock and stress of opponent´s hybrid campaigns needs to be coupled with government abilities to respond to hybrid attacks in agile and proportionate ways, outmanoeuvring malicious actors in a multidomain battlespace. To this end a *design thinking* approach would help to develop creative, flexible, and successful strategies for better dealing with upcoming hybrid challenges. It would enable to

- Anticipate malicious actor approaches warfare and identifying various trends, emerging issues, and exploring how they might interact.
- Assess how different actors may evolve their approaches to hybrid warfare.
- Explore how malicious actors in sustained hybrid conflict may coevolve.[2]

It would facilitate knowledge and experience-sharing in pursuit of what U.S. Army General Stanley McChrystal in his book, *Team of Teams*,[3] has called "*shared consciousness leading to empowered execution*". Time is running. Be Purposeful and Fast.

[2] Richard Kaipo Lum. Sensing the Future of Warfare. Vision Foresight Strategy. 2020. https://www.visionforesightstrategy.com/post/sensing-the-future-of-warfare

[3] Stanley McChrystal, *Team of Teams: New Rules of Engagement for a Complex World*. New York 2015.

About the Authors:

Dr. Walter L. Christman is a pioneer in the global adoption of new cooperative ventures in education and research to enable enhanced regional and global security. A retired U.S. Department of Defense career civilian, he is the principal architect of seven U.S. Secretary of Defense initiatives, three of which were endorsed by a President of the United States. He is President of Global Strategic Analysis, LLC and Founding Chairman of the Global Challenges Forum Foundation.

Colonel (ret.) Ralph Thiele is President of EuroDefense (Germany), Chairman of the Politico-Military Society and Managing Director of StratByrd Consulting. He is the host of SpaceWatch.Global's online format: Space Café "Black Ops by Ralph Thiele", discussing with guests military space, defence and hybrid warfare.