Research Institute Cyber Defence
Bundeswehr University Munich

Annual Conference CODE 2020 - Summary of Workshop 5

Taking the „I“ in CIDS HQ seriously

Moderation and Organization

Major Stefan Langnau from the mandate of *Germany's Cyber and Information Domain Service HQ* (CIDS HQ; ger. KdoCIR) organized and moderated the overall workshop, while Colonel Harald Belz (KdoCIR) opened and closed the workshop with two short welcoming and farewell speeches. The KdoCIR intern at that time, Dr.-Ing. Nico Merten, moderated the discussions.

Speakers and Panelists

The workshop was comprised by five talks:

- *Challenges of Hybrid Threats and Warfare* by Dr. Johann Schmid from the European Centre of Excellence for Countering Hybrid Threats in Helsinki
- *Narrative Threat Scenarios as Autoimmune Reaction: Explaining Virology in the Culture Centric Domain* by Prof. Dr. Natasche Zowislo-Grünewald from the University of the Federal Armed Forces in Munich
- *Bundeswehr Responses to Challenges in the Information Environment* by Dr. Carolin Busch and Benjamin Fuchs from the Industrieanlagen-Betriebsgesellschaft mbH in Ottobrunn
- *In the Information Domain: Covering and Analyzing the Communication in News Applying AI* by Dr. Raphael Pascke from the Schönhofer Sales and Engineering GmbH in Siegburg
- *How to Cover Demand from a Military Perspective* by Major Stefan Langnau from the CIDS HQ, Bonn

Summary of the Presentations

As the workshop's name suggest, the overall theme was to emphasize and to take a closer look on the factor *information* when thinking and talking about hybrid threats and warfare. Although rather new, the information domain is already considered a key factor in the cyber- and information environment. Thus, the main goal of this workshop was to discuss the development of today's and future capabilities to really understand and act in said environment, and what this means for the Bundeswehr.

Overall, the presentations and discussions were fruitful, and thus, for this report, we want to highlight the following key takeaways:

- Orchestrating means for collaboration and communication between national and international, governmental and non-governmental institutions is key to face emerging challenges in the cyber and information domains.
- Developing skills and tools for correct attribution of hybrid threats, e.g. answering questions such as „*who is the author/initiator?*“ and „*where does the threat originate from?*“, will be important from political, strategic and operational point of views alike.
- One general challenge is that the attacker has a slight advantage over the defender. That is why it is so important to try to be *one step ahead* by identifying newly emerging threats preemptively. In other words, prevention and resilience, if implementable, should be favored over detection and healing.
- Working closely with public media broadcasters to unmask hybrid threats and false information, while enhancing trust in one's own narrative and political system, will be very important in the next years.
- Meanwhile, foreign information and news sources, both, modern and conventional alike will be monitored closely to detect emerging narratives and disinformation sources.
- Although the Bundeswehr already has its own means and capabilities to maneuver in the cyber and information environment, maintaining fruitful cooperations with the private and OpenSource sectors will be key to keep the technological edge.