Countering Hybrid Threats: Policy Options for Building Resilience to the Kremlin Playbook in Europe: *Hybrid threats after Russia's invasion of Ukraine*

Velizar Shalamanov, Institute of Information and Communication Technologies, Bulgarian Academy of Sciences; former Minister of Defence

1. **Recognize Russian hybrid threat as a main challenge for National security and development of Bulgaria in NATO and EU – "defeat the network approach"**

- Corruption is an instrument of Russian influence and they use the positions in special services, communist party businessmen and organized crime
- We need to recognize the root causes for our problems.
- We have to bready to defeat the network behind the main threat

2. **Main problem – Governance – inter-sector cooperation, NATO/EU cooperation with focus on Intelligence and Prosecution / Administrative measures**

- Clear role of the Parliament, Government and critical executive instruments. From policy, strategy to execution with resources and democratic control.
- Professional analysis and design of the processes and organizations
- Proper implementation of the technology
- Train and develop people

3. **Key instrument of change Security council of the Government (Director of National Intelligence) and MoD in the NATO FW / BGR-USA strategic cooperation (incl. cyber resilience and countering hybrid threats / Cognitive Information Operations)**

The Alliance faces a range of challenges in emerging domains of conflict. These domains can arise from the introduction of new and disruptive technologies. The domains of space and cyber, for example, came out of developments in rocket, satellite, computing, telecommunications, and internetworking technologies. The increasingly widespread use of social media, social networking, social messaging, and mobile device technologies is now enabling a new domain: cognitive warfare. In cognitive warfare[1], the human mind becomes the battlefield. The aim is to change not only what people think, but how they think and act. Waged successfully, it shapes and influences individual and group beliefs and behaviours to favour an aggressor's tactical or strategic objectives. In its extreme form, it has the potential to fracture and fragment an entire society, so that it no longer has the collective will to resist an adversary's intentions. An opponent could conceivably subdue a society without resorting to outright force or coercion.

- Director of National Intelligence proposed since 2017.
- MoD has a NATO instruments – CMDR CoE and NFIU, new battle group and potentially Maritime Security Center, NIAMDS, …
- BGR-USA Strategic partnership with dimension on cyber resilience – could encompass hybrid threats resilience
- EU arrangements – dissertation of Maria

[1] https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html