FOREIGN INTERFERENCE IN THE DIGITAL DOMAIN

EUISS Workshop

5 April 2022, 9:30-11:30 CET, Videoconference

KEY TAKEAWAYS

- There is a need to better understand the **links between cybersecurity and information manipulation**, including by bringing together stakeholders from both communities. To date, the two communities have mainly worked in distinct settings, resulting in the creation of different vocabularies and policy approaches. One of the first steps needed is to consider information manipulation and cyber operations as a continuum of activities and incidents that may need to be addressed also through a more joined-up approach. Identifying the linkages between these two types of foreign interference is critical for a coherent and comprehensive policy response.
- Malign intent, societal uncertainties in times of crises, and the lack of trust in mainstream media and authorities were considered among the **main drivers of information manipulation**. Several participants agreed on the importance of enhanced transparency, social media accountability, and pre-bunking activities.
- The **connections** between the policies to counter information manipulation and the cyber policy continue to be **underdeveloped** despite a wide set of policy instruments that have been adopted over the past years (including cyber-specific horizontal restrictive measures). While the two communities can learn a lot from each other (e.g. regarding definitions of incidents, (significant) effect and policy responses, there are also critical differences stemming from the historical evolution of both fields that call for caution (e.g. the use of terms such as information security).
- Key areas to focus on should **align four dimensions: doctrine, incident, effect, and response**. For example, in the area of response, despite efforts within both domains to increase resilience (or, conversely, minimise the effects of the lack thereof), there are clear differences in the trajectory of the policy responses. These include diverse approaches to national regulatory measures, international law and norms of behaviour, role of non-state actors or the ways to address rising challenges such as development of capabilities or dealing with the questions of sovereignty and jurisdiction

POLICY RECOMMENDATIONS

1. Develop **a coherent framework** that addresses foreign interference operations along the whole spectrum, with specific focus on nexuses between information operations and cybersecurity.
2. **Rigorous implementation of cyber hygiene that permits a more preventive approach** and helps the audience develop a critical mindset through the design of a technological toolbox. Development of the **EU Cognitive Hacking system** would further contribute to damage control or to change the existing threat narrative.
3. **Enhancement of the quality of information in the public spheres –** incl. support to authoritative and independent media sources and channels, as well as social media accountability to fight disinformation and its amplification across various platforms. Increased emphasis on the **systemic level** of the information manipulation will serve as a leverage to engage media organisations and platforms in a coordinated manner.
4. **Explore further the role of courts, as non-traditional actors,** in addressing media regulation and labelling process to ensure accountability and serve as a deterrent.

Report author	Dr. Naďa Kovalčíková and Dr. Patryk Pawlak
Report date	27 April 2022