COLLABORATIVE DOCTORAL PARTNERSHIPS – CALL 2020

THEMATIC FIELD 7: Graphical Causal Modelling for addressing Hybrid Threats

JRC RESEARCH AREA DESCRIPTION

Hybrid Threats are by nature a complex issue which requires a multidisciplinary approach. They deploy a combination of means and attack vectors, ranging from cyber-attacks, physical attacks and economic influencing to media campaigns. In addition, the links between the various activities aim to remain rather unclear while the adversary seeks to remain "below the radar". This complexity and the stealth mode of hybrid threats are identified as the main challenges in this area. In addition, security experts tend to work in very specific topics (e.g. cyber security), thus they may lose perspective of the overall security landscape and complexity of Hybrid Threats.

In order to address Hybrid Threats, it is paramount to obtain a better understanding of vulnerabilities and their respective root causes which can be leveraged by adversaries in order to conduct a successful hybrid activity. Currently there is a strong tendency in various scientific disciplines (not only in security) to correlate observations (association) in an effort to gain a better insight on the topic of interest and if possible embark in forecasting activities. However, this is not always enough because it fails to provide an explanation of the root causes of certain phenomena. To this end Graphical Causal Modelling is proposed as a powerful tool which can help analysts and policy makers to obtain a better understanding of the underlying phenomena that can enable hybrid activities with the objective to support forecasting as well. This research activity will aim at enabling the transition from association to causation.

The JRC has worked during the last years in this domain and it has developed a conceptual framework for Hybrid Threats. This framework will be the starting point for the proposed research activity. At the end of this project the following major breakthroughs are expected:

1) Develop a causal modelling framework taking stock of the findings of the conceptual framework of hybrid threats
2) Identify the necessary datasets that have to be monitored by security agencies in order to feed-in the causal modelling framework
3) Develop what-if scenarios using the causal modelling framework in order to identify how specific policies might affect the level of vulnerability of societies to hybrid threats.

The candidate should have familiarity with the security domain ideally a security analyst. Any experience in cybersecurity, physical security, critical infrastructure protection, geopolitics would be considered as an asset.

MAIN POLICY FIELDS

The work will mainly contribute to the Hybrid Threats policy as this is described in the two Joint Communications of 2016 and 2018. In addition, it will contribute to the objectives of the security and defence union.

LINKS / URL WEBSITES

- https://ec.europa.eu/jrc/en/research-topic/critical-infrastructure-protection

LINKS / REFERENCES TO PUBLICATIONS

- Communication from the Commission to the European Parliament, The European Council and The Council, Twentieth Progress Report towards an effective and genuine Security Union, COM(2019) 552 final
- Joint Communication To The European Parliament and The Council, Joint Framework on countering hybrid threats a European Union response, JOIN(2016) 18 final
- Feng, Nan et al. “A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis.” Inf. Sci. 256 (2014): 57-73.