Hybrid Threat and Information Influence in Connection with Security of Supply

Tehi Palletvuori and Jyri Rajamäki
Laurea University of Applied Sciences, Espoo, Finland

tehi.palletvuori@student.laurea.fi
jyri.rajamaki@laurea.fi

Abstract: Hybrid threat is a multidimensional and hard-to-detect activity. It includes a wide range of actions, from influencing information to the military means by which the hybrid actor achieves its goals. These goals can include weakening or even destroying the target. Security of supply means preparedness and continuity management actions, which aim to safeguard economic activities and related systems that are necessary for the population's livelihood, the country's economic life, and national defense in the event of exceptional conditions and comparable serious disruptions. Both hybrid threat and information influencing can disrupt the realization of the goals of security of supply. This work-in-progress paper proposes a framework, which consists of hybrid threat and its sub-classification, and information influencing as one of the means to implement hybrid threat. The framework also describes the security of supply and elements that are used to combat information influence and maintain the security of supply. In addition, the framework paper discusses what kind of elements measuring the maturity level of an organization's prevention of information influence could consist of.

Keywords: security of supply, hybrid threat, countering information influence, maturity level of information influence prevention, information resilience.

1. Introduction

The ongoing international change in power structures offers a fertile growth environment for hybrid threats. The growing conflict of values between the West and authoritarian states is eroding international norms and institutions and exposing open Western societies to hybrid threats. (Hybrid CoE, 2023) This work-in-progress paper fills the gap that has not been described in the connection between the realization of security of supply goals and hybrid threat and information influencing. The finding of this paper is the proposed framework, which consists of hybrid threat and its sub-classification and information influencing as one of the means to implement hybrid threat. The framework also describes the security of supply and elements that are used to combat information influence and maintain the security of supply. The framework has been created by examining and combining theoretical data. In addition, the framework paper discusses what kind of elements measuring the maturity level of an organization's prevention of information influence could consist of.

2. Framework for hybrid threat and security of supply interaction

According to Iso-Markku (2022) Security of supply is often only seen as guaranteeing the provision of specific materials or goods, such as military equipment or energy supplies. Finnish view on the security of supply is broader. Finnish Security of Supply Act (1992) defines (Figure 1) security of supply as the safeguarding of economic activities and related systems that are necessary for the population's livelihood, the country's economic life and national defense in the event of exceptional conditions and comparable serious disruptions.

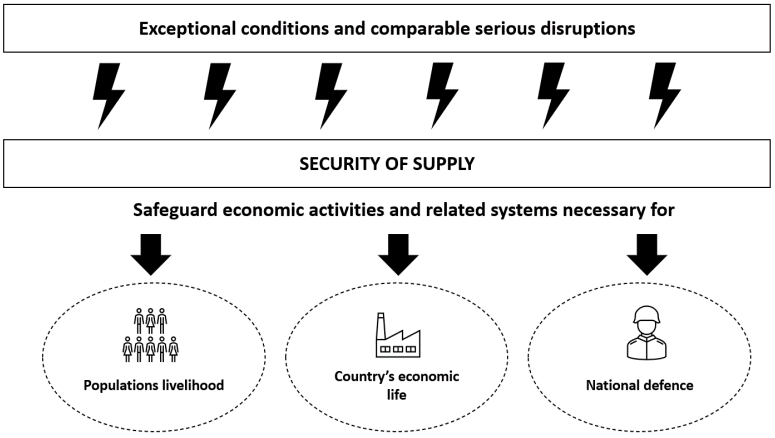

Figure 1: Security of supply (adapted from Finnish Security of Supply Act 1992)

The proposed framework (Figure 2) is divided into five levels. The bottom of the figure is the security of supply, which is the function needed to maintain a functional society during exceptional circumstances and serious disturbances. According to the Finnish Government's decision on the security of supply goals (2018), both hybrid and information influencing can disrupt the realization of the goals of security of supply. By nature, hybrid threats, as well as the threats of the cyber environment, cross borders.

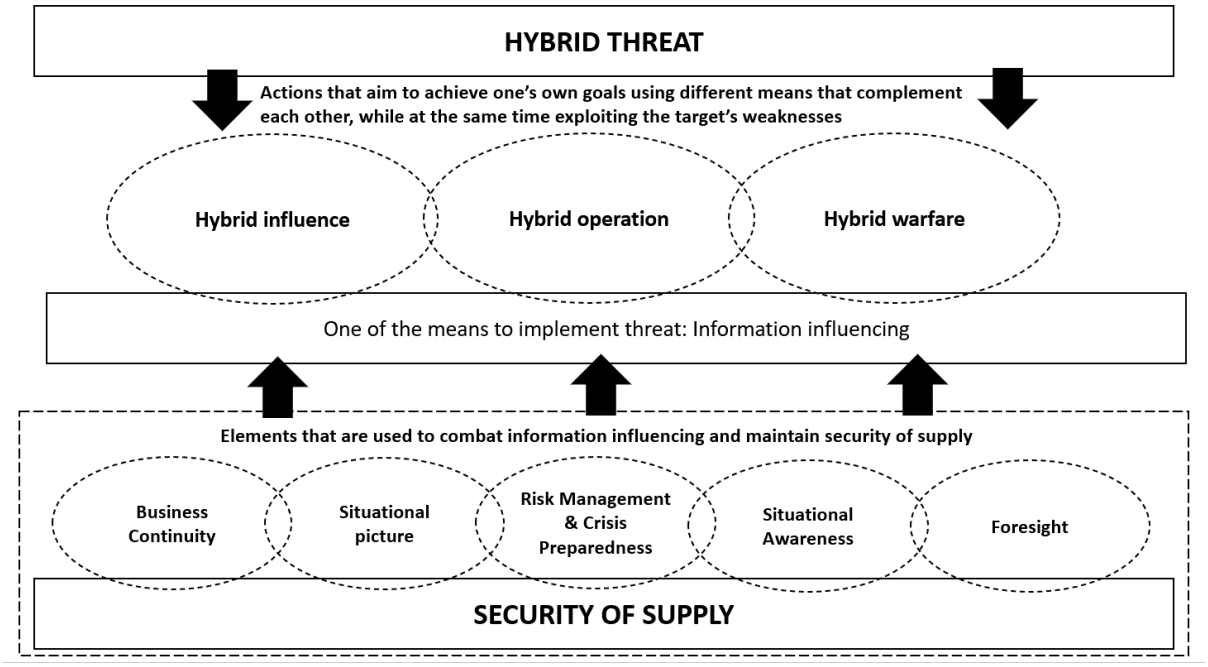

Figure 2: Framework for hybrid threat and security of supply interaction

Information influencing is a systematic activity in which the aim is to implement changes in the target's information and perception environment in accordance with the influencer's own goals through the modification of information (Vocabulary of Comprehensive Security, 2017). This proposed framework focuses on information influencing and elements that are used to combat information influencing and maintaining the security of supply.

2.1 Hybrid threat

On top of the framework (Figure 2) is a hybrid threat and the term relates to conventional or unconventional warfare by which a hostile actor takes advantage of the unclear territory between peace and war (Weissmann, 2021). However, there is no consensus on the definition of the term (Underwood et al., 2022). The problem is also that the terms hybrid threat and/or hybrid warfare are used comprehensively to cover different situations (Weissmann, 2021). Tikanmäki and Ruoslahti (2022) have studied how hybrid terms are discussed in recent scholarly literature. Regardless of the difficulty of defining the term hybrid threat, different actors in society must be able to defend themselves against various hybrid actions. Similar countermeasures may be needed regardless of the name of the term in question. In attribution, it may be more important to specify in theoretical terms what it is about, but in control measures, the functionality and effectiveness of the control measures are essential.

Kalniete and Pildegovičs (2021) interpret the hybrid threat as an umbrella term covering a range of destabilizing and synchronized civil and military actions. These activities may include disinformation and cyber-attacks, causing political or financial corruption, infiltrating agents of influence, pressuring independent media, and purchasing critical infrastructure (Kalniete and Pildegovičs, 2021). Wigell, Mikkola and Juntunen (2021) have proposed hybrid threat classification to be divided into hybrid interference, hybrid operations and hybrid warfare. In this proposed framework hybrid threat is divided accordingly into three parts, which are hybrid influence, hybrid operation and hybrid warfare. Due to the fact, there is no agreement on the definition of terms this proposed framework uses close to self-explanatory terms to divide hybrid threat actions from soft to hard. Influence actions are softer actions than war actions, and operations are in between those two. Term influence

is also used to distinguish this classification from Wigell et al. (2021) classification of which content has not been examined in detail.

2.2 Combat elements

The proposed framework (Figure 2) includes five elements, which are used to combat information influencing. Those elements are business continuity, situational picture, risk management and crisis preparedness, situational awareness, and foresight as the fifth element. Business continuity refers to those measures that enable the organization to manage various disruptions that threaten its operations with pre-planned and implemented arrangements and management tools (Hopkin, 2018). Business continuity management is a strategic and operational preparedness process approved by the top management of the organization that improves the security of supply (Klemm, 2019). According to Hopkin (2018), business continuity planning is a comprehensive management process that identifies potential threats to the organization and the effects on the business that these threats may cause if they materialize. In this model, business continuity management ensures that relevant entities can fulfill their duties.

The vocabulary of Comprehensive Security (2017) defines the situational picture as a compiled description of the prevailing conditions and the events that created the situation at the time it occurred. A situational picture ensures that the position and role of relevant entities are known and thus can be managed accordingly. Situational awareness means an understanding of what is happening or happened, and the circumstances that influence it, as well as the goals of the different parties and possible development options, and it can be based on a situational picture (Vocabulary of Comprehensive Security, 2017). According to Jantunen (2015), disinformation and information encryption, and censorship can be used to influence the situational picture, but influencing situational awareness requires influencing the interpreter of the situational picture. Foresight means the process of developing knowledge and understanding about the future of a specific unit of analysis or actor system (Piirainen and Gonzalez, 2015). In this model situational awareness brings an understanding of the dynamics of the situational picture. Foresight provides the capability to predict and analyze the potential development of the situation.

Risk means the impact of uncertainty on goals (Finnish Standards Association, 2018). Risk management is a systematic activity and includes, in addition to risk analysis, the planning, implementation and monitoring of the necessary measures, as well as corrective measures (Vocabulary of Comprehensive Security, 2017). Measures to strengthen crisis resilience are preparedness for threats related to the well-being and safety of society. These threats include, for example, hybrid threats, the effects of climate change, disasters caused by humans and nature, and the aftereffects of epidemics and pandemics. The joint preparation, planning, training and implementation of various actors in society is carried out in broad cooperation. One important part of crisis resilience is securing the security of supply in all conditions. (Finnish Government, 2020) The four abovementioned combat elements are used for risk management and crisis preparedness, which are the core functions to combat information influencing to maintain the security of supply.

3. Discussion

An individual, authority, private sector actor or non-governmental organization that is subject to hybrid threat is not necessarily the actual target, but rather a tool to achieve the hybrid actor's goal. The proposed framework has focused on information influencing actions on an organizational level, not on an individual citizen level. An organization's prevention of information influence maturity level can be measured. By measuring the maturity level organization can enhance its combat capability against information influencing.

Information influencing maturity level measure elements could be related to defining the roles and responsibilities and information resilience training and countermeasure process. Also, risk management, business continuity management, preparedness, crisis management and situational picture and awareness-related elements could be added to the maturity level self-assessment tool.

The framework will be used to create the structure and different parts of the maturity level assessment tool. The structure and sub-areas of the maturity level of countermeasures against information influence create a basis for further work, where a battery of questions can be created for the measure, which authorities and companies can use when examining the maturity level of their own organization's countermeasure against information influence.

Regarding countermeasures, it is necessary to understand our role as part of the EU and the fact that hybrid threats and their various means know no boundaries, just like cybercrime. The measures to combat hybrid threats are implemented locally in cooperation with authorities and the private sector, as well as non-governmental organizations and citizens. Organizations in both the public and private sectors and non-governmental organizations are preparing for information influence and countermeasures.

For further academic research, an interesting topic would be to further clarify combat elements when countering hybrid threats and information influence that threaten the security of supply. There is no previous scientific research on this subject, and this might be because the security of supply is seen material related functionality.

References

Finnish Government (2020) Government Report on Finnish Foreign and Security Policy, [online], Publications on the Finnish Government 2020:30, https://julkaisut.valtioneuvosto.fi/handle/10024/162513.

Finnish Government decision on security of supply goals (2018) Valtioneuvoston päätös huoltovarmuuden tavoitteista 5.12.2018, [online], Finnish Ministry of Justice, Edita Publishing Ltd., https://www.finlex.fi/fi/laki/alkup/2018/20181048.

Finnish Standards Association (2018) SFS-ISO 31000:2018 Risk Management – Guidelines, [online], 2nd edition, SFS Online, https://online.sfs.fi/.

Hopkin, P. (2018) Fundamentals of risk management: Understanding, evaluating and implementing effective risk management, Fifth edition, Kogan Page Ltd, London.

Hybrid CoE (2023) Hybrid threats as a concept, [online], The European Centre of Excellence for Countering Hybrid Threats, https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/.

Iso-Markku T. (2022) The EU and Finland's Security of Supply: A "turn" in EU thinking provides new opportunities, but significant differences remain, [online], Finnish Institute of International Affairs, FIIA Briefing Paper 330, https://www.fiia.fi/julkaisu/the-eu-and-finlands-security-of-supply.

Jantunen S. (2015) Infosota: "iskut kohdistuvat kansalaisten tajuntaan", 2nd edition, Kustannusosakeyhtiö Otava, Helsinki.

Kalniete, S. and Pildegovičs, T. (2021) Strengthening the EU's resilience to hybrid threats, European view, 20(1), 23-33. doi:10.1177/17816858211004648.

Klemm, K. (2019) Huoltovarmuus: Varautumisella Selviytymiskykyä, Tietosanoma, Helsinki.

Piirainen, K.A. and Gonzalez, R.A. (2015) Theory of and within foresight — "What does a theory of foresight even mean?", Technological forecasting & social change, 96, pp. 191-201, doi:10.1016/j.techfore.2015.03.003.

Security of Supply Act (1992) Laki huoltovarmuuden turvaamisesta 18.12.1992/1390, [online], Finnish Ministry of Justice, Edita Publishing Ltd., https://www.finlex.fi/fi/laki/ajantasa/1992/19921390.

Security Strategy for Society (2017) Yhteiskunnan turvallisuusstrategia, Government resolution / 2.11.2017, [online], The Security Committee https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf.

Tikanmäki, I. and Ruoslahti, H. (2022) How are Hybrid Terms Discussed in the Recent Scholarly Literature?, Proceedings of the 21st European Conference on Cyber Warfare and Security, Thaddeus, E., Nabeel, K. and Cyril, O. (Eds.), doi: 10.34190/eccws.21.1.457.

Underwood, A., Emery, A., Haynsworth, P. and Barnes, J. (2022) All Quiet on the Eastern Front: NATO Civil-Military Deterrence of Russian Hybrid Warfare. Joint Force Quarterly : JFQ, 105, pp. 75-85.

Vocabulary of Comprehensive Security (2017) Kokonaisturvallisuuden sanasto TSK 50, [online], Sanastokeskus TSK, The Security Committee https://turvallisuuskomitea.fi/viestinta/kokonaisturvallisuuden-sanasto/.

Wigell, M., Mikkola, H. and Juntunen, T. (2021) Best Practices in the whole-of-society approach in countering hybrid threats, [online], European Parliament, Directorate-General for External Policies of the Union Brussels https://data.europa.eu/doi/10.2861/379.

Weissmann, M. (2021) Conceptualizing and countering hybrid threats and hybrid warfare: The role of the miliary in the grey zone, Hybrid Warfare: Security and Asymmetric Conflict in International Relations, Weissmann M., Nilsson, N., Palmertz, B. and Thunholm, P. (Eds.), doi:10.5040/9781788317795.