Hybrid Threats Against the Finnish Society: Reported by YLE News

Ilkka Tikanmäki[1] [2], Jarmo Heinonen[1][2] and Harri Ruoslahti[1][3]
[1]Security and Risk Management, Laurea University of Applied Sciences, Espoo, Finland
[2]Department of Warfare, National Defence University, Helsinki, Finland

ilkka.tikanmaki@laurea.fi

Abstract: Hybrid operations aim at malicious political outcomes in targeted states and societies with strategic deception and shaping civic opinion. Some common hybrid threats are cyber-attacks on critical systems and disruptions of critical services, e.g. healthcare or rescue services. This study looks at how hybrid threats are communicated in mainstream Finnish media. The Finnish public broadcasting company YLE was chosen as the data source because it has a legal obligation to communicate issues without prejudice. Also, this makes it possible to conduct a future comparative study by selecting similarly relevant national news feeds from other countries. The sample, 57 news articles from the YLE English language news feed from between 2022 and 2025, discus hybrid threats. These articles in English were chosen for text analysis with Modeller 18.5 software which does not understand Finnish. Results identify "hybrid impact" as the most used term, with 27 articles mentioning it, while 15 articles mention "hybrid threats" and "hybrid warfare". Analysis of co-occurrences reveals substantial links between government actions, security institutions, and Russia as a major geopolitical actor. The findings indicate that hybrid threats are multifaceted challenges that require coordinated national and international responses. The study helps comprehend how media portrays hybrid threats and suggests the need for more research using native language analysis and broader media sources. The study identifies the frequency and boundaries of key terms related to hybrid threats, in particular hybrid impact, hybrid threats, and hybrid warfare, in YLE news coverage. The analysis of co-occurrence patterns and conceptual connections in the sample texts reveal how hybrid threats are related to actors, institutions, and geopolitical contexts. This scientific contribution of this study is deeper understanding how media contribute to and shape public awareness and understanding of hybrid threats and national responses in Finland; and the practical contribution of the study are its insights into hybrid threats and suggestions on response and future research directions.

Keywords: Hybrid threats, Hybrid impact, Hybrid warfare, Finnish media, Finnish Society

1. Introduction

Hybrid operations are used to achieve desired political outcomes in affected states and societies (Giannopoulos et al., 2021). Hybrid threats may range from cyber-attacks on critical systems to disruptions of critical services, such as energy, banking, and security or rescue services (European Union, 2018; Giannopoulos et al., 2021). Increased use of hybrid influence methods may lead to asymmetric warfare, which is the continuous use of special forces, precision bombs, missiles, electronic and guerrilla warfare, terrorist attacks, and biological or chemical weapons before and during actual war (Arreguín-Toft, 2001; Mack, 1975). Asymmetries are combinations of deception, surprise, and abuse (Cederberg & Eronen, 2015).

Objectives and research questions

This study explores how Finland's national broadcast company YLE reports on how hybrid threats target the Finnish society. The research used Modeller 18.5 text analysis software to examine 57 news articles in English published between 2022 and 2025. The findings reveal that *hybrid influence* is the most frequently used term, indicating a broad and evolving understanding of hybrid operations in public discourse. Co-occurrence analysis highlights strong associations with governmental responses, security institutions, and geopolitical actors, particularly Russia. The study underscores the importance of strategic communication, cross-sectoral cooperation, and resilience in countering hybrid threats, while also identifying limitations related to language translation and sample scope. These insights contribute to a deeper understanding of how hybrid threats are framed in Finnish media and offer directions for future research.

The research question of this study is: How does YLE national news report hybrid threats against Finnish society?

[1]https://orcid.org/0000- 0001-8950-5221

[2]https://orcid.org/0000-0001-7904-4812

[3]https://orcid.org/0000-0001-9726-7956

Structure of the report

The study is structured as follows: after this introduction section, the theoretical background, definitions and conceptualisations of hybrid threats are presented. The method describes the data collection and analysis tool, while the results present findings, including term frequencies and concept maps. In the conclusions, the results and implications are interpreted, limitations and challenges discussed, and suggestions and recommendations for future research are made.

2. Hybrid Threats

Hybrid threats can be referred to as e.g. disregarding standard rules of warfare with the use of irregular forces in different battlefield domains (Kirk, 2023) or as simultaneous and adaptive uses of political, military, economic, social, media, terrorism, and irregular, disruptive or criminal conflict methods and combinations of these (GAO, 2010).

The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) defines the term hybrid threat as "… an action conducted by state or non-state actors, whose goal is to undermine or harm a target by combining overt and covert military and non-military means" (Hybrid CoE, 2021, p. 1), while Hoffman (2007) sees them as "Threats that incorporate a full range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder, conducted by both states and a variety of non-state actors" (Hoffman, 2007, p. 8).

Mäkelä (2018) describes hybrid action as "a systematic activity in which a state or non-state actor can simultaneously utilise various military means or, for example, economic or technological pressure, as well as information operations and social media" (Mäkelä, 2018, p. 13) and (Puistola, 2018) sees information influence as a strategic deception in which the subject's perception of reality is obscured to achieve the attacker's strategic goals.

Modern social media can be a powerful contributor in shaping civic opinion and for strategic deception, hiding one's final goals and maintaining a facade of legality, and global input of one's narrative through various media (Puistola, 2018). Threats and disruptions to critical vulnerabilities seek to influence public confidence, hamper effective decision-making and create polarisation within the affected society (European Union, 2018; Giannopoulos et al., 2021). Often hybrid influencers aim to keep hybrid effects at a level where escalation into open conflict does not occur by applying effects in ways that are disputable (Mäkelä, 2018). Russia has, for example, intensified hybrid actions that target Western countries with e.g. extensive disinformation campaigns, interference in electoral and democratic processes, political and economic pressure and intimidation, and harmful cyber functions that target to disrupt critical infrastructure, including e.g. knowingly allowing cyber criminals to operate from its territory (NATO, 2021).

Key efforts to combat hybrid threats are awareness, resilience, and response, which combined improve abilities to detect and understand adverse actions at early stages and help improve the sustainability of critical infrastructure, societies, and institutions; close cooperation between European EU Member States, as well as with partner countries and NATO, help combat hybrid threats (European Union, 2018; Giannopoulos et al., 2021). Hybrid influence uses shadow regions where threats are unexpected, and notes that the Finnish model that combines various administrative sectors could be a useful policy for other countries (Finnish Government, 2024).

Hybrid operations focus on identifying weaknesses in the target country (Cederberg & Eronen, 2015) by attacking specific weaknesses with varying tactics and tools and intensity, intending to outperform the strengths of the society under attack (Tikanmäki & Ruoslahti, 2022). Means include political and economic instruments, cyber warfare, threats with military force, cyber operations, and the use of special forces (Cederberg & Eronen, 2015). The use of hybrid tools puts pressure on the destination country, and fighting against their usage requires policy coordination and close cooperation; the EU Strategic Compass and the NATO strategy help the fight against hybrid threats (European Commission, 2020).

(Tikanmäki & Ruoslahti, 2021) note that internal and external security are difficult to separate, as the operational environment is constantly changing in today's globalised world. The Ministry of the Interior of Finland (2016) recommends that actors and authorities exchange staff to better develop operating models towards improved situational awareness and lessening cross-sector barriers that prevent information exchange between administrative sectors (Tiimonen & Nikander, 2016). A situation picture of hybrid influence can be formed by extracting sector-relevant information and drawing real-time conclusions to form a common understanding that

is recently detected or obtained with the latest and confirmed true observations to form a continuity estimate and forecast influencing the decision. (Hyytiäinen, 2021).

3. Method

The Finnish public broadcasting company YLE's Finnish language news feed was chosen as the data source because it is legally obligated to discuss issues without prejudice. Also, this choice will enable future comparative studies possible of public broadcasting company news feeds from other countries, e.g. in the Baltic Sea Region, which are similar targets of hybrid influence.

The first step of the research was to collect data on articles related to hybrid influence that were searched from YLE text news articles in the spring of 2025. Search words hybrid influence, hybrid threats, and hybrid warfare were used, and the search period was from 2022 to 2025. The following table summarises the search words, the number of articles found, and the period from which the findings are from (Table 1).

Table 1: Search words, number of articles found, and period of publication

Search words	Number of articles	Article dates
Hybrid influence	27	4.3.2022-6.5.2025
Hybrid threats	15	4.3.2022-3.4.2025
Hybrid warfare	15	4.5.2022-5.3.2025

Table 1 shows that the articles found were published roughly within the last two years. The term *hybrid influence* (n = 27) was mentioned in almost twice as many articles as the terms *hybrid threats* (n = 15) and *hybrid warfare* (n = 15). The second phase was to transfer the sample article (n = 57) texts via Excel into the Modeller 18.5 text analytics software.

Modeller 18.5 software was chosen for the analysis of the sample of journalistic reports of hybrid threats against Finnish society. Because the Modeler software cannot analyse Finnish texts, the final sample consists of 57 original YLE articles that were written in or translated into English by YLE. Finnish is not an Indo-European language; its different structure and specific vocabulary may make exact translations challenging. Though YLE's English versions have received journalistic approval, some connotations in the translations may slightly differ from the original articles. This conversion, however, would not allow for variations to be distinguished and would not have a significant impact on the results.

The third phase was to analyse sample article texts with Categories and Concepts, with Category Bar as the main method of analysis. *Hybrid Threats* (with co-occurrence links) show the joint species distribution model evaluates distributions of several characters simultaneously and decomposes characters into co-occurrence patterns into parts, and describes concerned environmental reactions and remaining patterns of co-occurrence (Pollock et al., 2014). Concept maps can be used to organise and structure knowledge. The Hybrid Concept web model concept map or conceptual diagram focuses on a diagram that describes proposed relationships between concepts (Hager & Corbin, 1997). The confidence metric method is a way to measure behaviour, system or interest. Unknown Hybrid threads confidence metric method verifies the popularity of a subject and shows if it had a positive or negative impact on the exposed thing (Keefer et al., 2013).

4. Results

Results show that the term *hybrid influencing* occurred in the sample articles nearly twice as often as the other two searched terms, *hybrid threats* and *hybrid warfare,* combined. The sample size (n = 57) demonstrates that hybrid threats, warfare, and influence have been a topical issue between 2022 and 2025.

4.1 Co-occurrence Links from Hybrid Threats

The term *Hybrid threats* was classified by Modeller in six categories in the sample of YLE news articles: combat hybrid threats, major hybrid threat, hybrid threat centre chief and counter potential hybrid threats and hybrid threat of the sample texts (Table 2).

Table 2; Categories of Hybrid threats from Modeller text analysis

Category	Connection
Counter potential hybrid threats	Positive to *Hybrid threats*
Hybrid threats	Positive to *Hybrid threats*
Hybrid threat centre chief	Positive to *Hybrid threats*
Major hybrid threat	Positive to *Hybrid threats*
YLE hybrid threats	Positive to *Hybrid threats*
Combat hybrid threats	Positive to *Hybrid threats*

This analysis is based on the sample of 57 YLE news articles in English because the Modeler software does not recognise Finnish. Due to this language conversion, translation variations may occur when processing the material. However, the conversion does not change the results in a way that would allow for any variation to be distinguished.

The Categories and Concepts, with the Category Bar method of analysis in Modeller 18.5 Text analysing software, produced co-occurrence links from the term *hybrid threats*: practice, learned situations, limits, involvement, properties, the interior ministry and reports. Times like Thursday, and last year explain the reports' activity in the press. Russia was mentioned most often in hybrid threats (Figure 1).

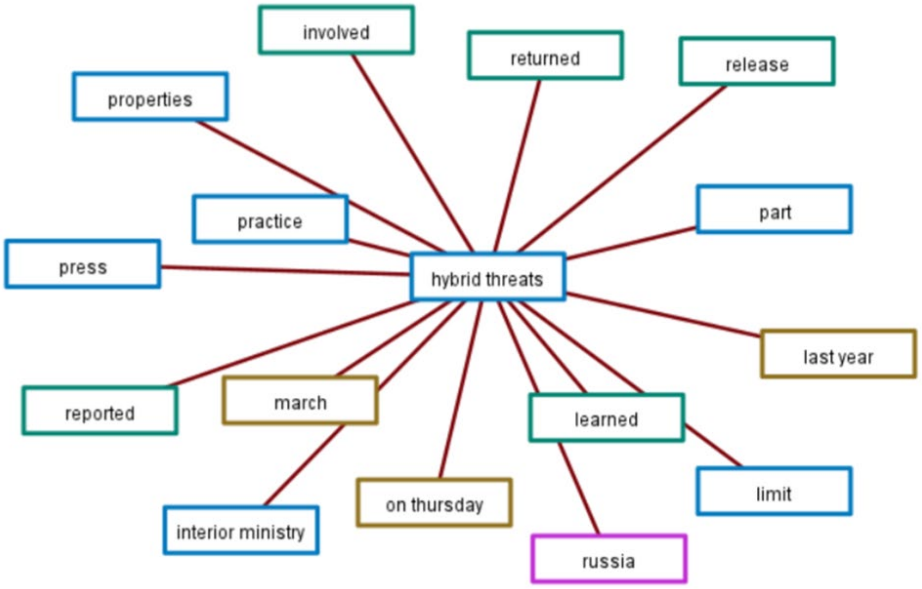

Figure 1: Links to *Hybrid Threats* (with co-occurrence links)

Lines between the boxes indicate connections, and the length of these lines indicates closeness of connection (Figure 1); the colour boxes show action (green), concepts (blue), reference time (brown), and location (purple).

The central term *Hybrid threat* is defined as a concept (blue box), as are practice, part, press, properties, limit, and interior ministry. Of these, practice has the closest link with Hybrid threat. Examples of practice include, e.g. these direct quotes: “Defence Committee backs amendment to expedite calling Border Guard reservists to deal with hybrid threats.” and “Aggression should not be rewarded. Member of Parliament Kiljunen on sick leave following committee chair resignation. Border Guard apprehends Finnish citizen for crossing into Russia.“

The location with a co-occurrence link with the Hybrid threat is Russia. Sample texts include, e.g. these quotes related to the name Russia: “Finnish Security and Intelligence Service SUPO: Russia remains top of Finland's security threat concerns”, “Foreign minister of Finland: Finland to strengthen response against shadow fleets and hybrid influence”, and “Defence minister of Finland: Finland prepared for hybrid influence attempts “.

Three examples about concepts report and involved: “Finnish Security and Intelligence Service SUPO: No increase of cyberattacks in Finland, despite NATO application. Cyber Centre: No increase in cyber-attacks since NATO application. “and “There has been no noticeable increase in the number of cyber-attacks being reported to the National Cyber Security Centre since Finland submitted an application to join the NATO“ and “The war in

Ukraine as well as Finland's application for NATO membership were expected to increase the number of cyberattacks targeting Finland, but so far this has not been the case“ and “The situation may be due to the accelerated speed of Finland's NATO application, which may have taken Russia by surprise, the intelligence service says “

It seems like many news releases and stories are from Thursday, as this is connected and demonstrated in these news examples: “Finnish Members of Parliament on Thursday approved changes to the country's border laws that will enable authorities to shut down borders or limit the number of border crossing points during exceptional circumstances. “

4.2 Hybrid Coe (Concept web Model)

Concept web models (Figure 3) show that hybrid coexistence has strong connections to consequences, full protection, support from other countries and no support from all others. Solid lines between variables indicate a direct connection and dotted lines indicate a loose connection.

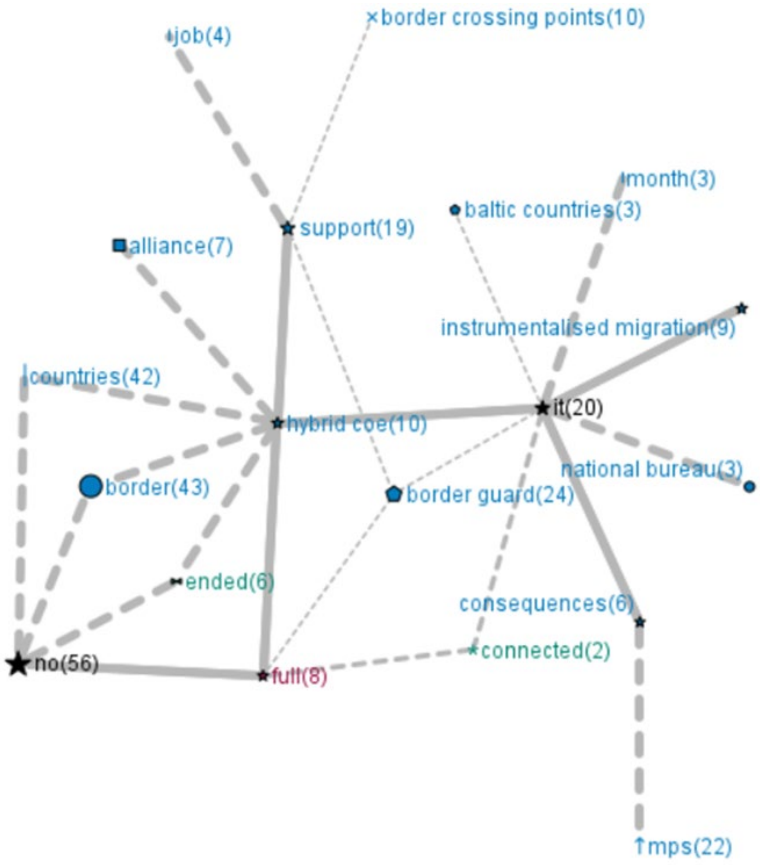

Figure 2: Hybrid Coe (Concept web model)

There are connections to instrumentalised migrations, national bureau, border, other countries, alliances, jobs to do, and Russians were ending. Thinner connections are border guard, connections to hostile countries, border crossing points and Baltic countries.

Examples from news on instrumentalised migration and border include: “Finland's land border crossings with Russia have been closed for about a year, due to Russia funnelling asylum seekers from third countries to the border. The practice is called instrumentalised migration, a form of hybrid warfare. “

Examples that write about Members of Parliament: “Finnish MPs on Thursday approved changes to the country's border laws that will enable authorities to shut down borders or limit the number of border crossing points during exceptional circumstances. “

5. Conclusions

The growing significance of hybrid threats in the Finnish national debate is highlighted in this study, which can be seen in YLE news coverage in 2022–2025. Analysis of the sample data indicates that the term *hybrid influence*

appears more often than *hybrid threats* or *hybrid warfare*, indicating a wider range of concepts in media stories. Strong links between co-occurrence analysis and government actions, security institutions, and geopolitical actors, particularly Russia, indicate that hybrid threats are seen as both internal and external challenges.

The findings show the importance of strategic communication, situational awareness, and multidisciplinary cooperation in addressing hybrid threats. The Finnish model, which integrates various administrative sectors, seems to be a promising strategy for addressing crises and responding effectively, and can serve as a model for other nations.

Limitations of the study

The study was based on English versions of originally Finnish articles. Even though these translations have journalistic approval, the subtleties and connotations may differ from the original Finnish texts, which may affect the precision of the semantic comparison. The use of texts in English is necessary as Modeller 18.5 does not process Finnish. Native language analysis tools could have captured more linguistic and cultural context, but this limitation prevents them from being captured completely. It is possible that the articles do not accurately depict longer-term trends or changes in hybrid threat narratives over time since they focus on the years 2022–2025.

Suggestions for future research

Future research should examine how hybrid threats are presented in various contexts. This could be achieved by expanding the research to other media channels and international news coverage, e.g. on the Eastern flank of the Baltic Sea Region. Examining the role of social media platforms in shaping public perceptions and spreading the hybrid effect could improve traditional media analysis. Future research could examine how media reporting on hybrid threats can affect public policy, government responses, and international cooperation strategies.

Acknowledgements

Acknowledgements are paid to the “Improving rescue services preparedness for hybrid threats” project, funded by the Fire Protection Fund and conducted in collaboration with the Finnish Association of Fire Officers. The views expressed are those of the authors, and the granting authority cannot be held responsible for them.

Ethics declaration: Ethical clearance was not required for the research.

AI declaration: The paper's spelling was verified using the artificial intelligence tool.

References

Cederberg, A., & Eronen, P. (2015). *How can Societies be Defended against Hybrid Threats?* (Strategic Security Analysis No. 9; p. 11). Geneva Centre for Security Policy - GCSP.

European Commission. (2020). *The EU Security Union Strategy: First Progress Report* (p. 4) [Progress Report]. European Union. https://ec.europa.eu/info/sites/default/files/securityunion_factsheet.pdf

European Union. (2018). *A Europe that Protects: Countering Hybrid Threats | EEAS*. https://www.eeas.europa.eu/node/46393_en

Finnish Government. (2024). *Government report on Finnish foreign and security policy* (Government Report No. 2024:35; p. 55). Ministry for Foreign Affairs of Finland. https://urn.fi/URN:ISBN:978-952-383-929-8

GAO. (2010). *GAO-10-1036R Hybrid Warfare* (p. 28).

Giannopoulos, G., Smith, H., & Theocharidou, M. (2021). *The landscape of hybrid threats: A conceptual model: public version.* (Policy Report No. EUR 30585 EN; p. 58). Publications Office of the European Union. https://data.europa.eu/doi/10.2760/44985

Hager, P. J., & Corbin, N. C. (with Internet Archive). (1997). *Designing & delivering scientific, technical, and managerial presentations*. New York: Wiley. http://archive.org/details/designingdeliver0000hage

Hoffman, F. G. (2007). *Conflict in the 21st Century: The rise of hybrid wars.* Potomac Institute for Policy Studies.

Hybrid CoE. (2021). Hybrid Threats. *Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats*. https://www.hybridcoe.fi/hybrid-threats/

Hyytiäinen, M. (2021, May 20). *Data integrity and situation picture of management* [Invited presentation]. Scientific Advisory Board for National Defense (MATINE) Research Seminar 2021, Webinar.

Keefer, C. E., Kauffman, G. W., & Gupta, R. R. (2013). Interpretable, Probability-Based Confidence Metric for Continuous Quantitative Structure–Activity Relationship Models. *Journal of Chemical Information and Modeling*, *53*(2), 368–383. https://doi.org/10.1021/ci300554t

Kirk, J. A. (2023). Irregular and Hybrid Warfare. *NCO Journal*, *July 2023*, 1–4.

Mäkelä, J. (2018, May 23). *Maritime hybrid threats* [Oral presentation]. Sotatieteenpäivät, National Defence University.

NATO. (2021, June 14). *Brussels Summit Communiqué issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 14 June 2021* [Press Release (2021) 086]. NATO. https://www.nato.int/cps/en/natohq/news_185000.htm

Pollock, L. J., Tingley, R., Morris, W. K., Golding, N., O'Hara, R. B., Parris, K. M., Vesk, P. A., & McCarthy, M. A. (2014). Understanding co-occurrence by modelling species simultaneously with a Joint Species Distribution Model (JSDM). *Methods in Ecology and Evolution*, *5*(5), 397–406. https://doi.org/10.1111/2041-210X.12180

Puistola, J.-A. (2018, May 23). *Comprehensive security and hybrid influence* [Oral presentation]. Sotatieteenpäivät, National Defence University.

Tiimonen, H., & Nikander, M. (2016). *Interdependence of Internal and External Security: Will the operational culture change with the operational environment?* (Governmental Report No. 37/2016; p. 88). Ministry of the Interior. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79230/37_2017_Interdependence%20of_nettiin.pdf?sequence=1&isAllowed=y

Tikanmäki, I., & Ruoslahti, H. (2021). Interdependence of Internal and External Security. In T. Eze, L. Speakman, & C. Onwubiko (Eds.), *Proceedings of the 20th European Conference on Cyber Warfare and Security* (pp. 425–432). Academic Conferences Inter Ltd.

Tikanmäki, I., & Ruoslahti, H. (2022). How are Hybrid Terms Discussed in the Recent Scholarly Literature? In E. Thaddeus, K. Nabeel, & O. Cyril (Eds.), *Proceedings of the 21st European Conference on Cyber Warfare and Security* (Vol. 10, pp. 296–304). Academic Conferences and Publishing Limited.