International Journal of Education, Vocational and Social Science
https://e-journal.citakonsulindo.or.id/index.php/IJEVSS
E-ISSN : 2963 4954
IJEVSS

Fragmented Convergence: A Bibliometric Analysis of GEOINT for Cyber Warfare in Hybrid Threats

Florentinus Ardhanareswara Swartian
Master of Sensing Technology, Republic of Indonesia Defense University
Aris Poniman
Faculty Of Defense Engineering and Technology, Republic of Indonesia Defense University
Sukendra Martha
Faculty Of Defense Engineering and Technology, Republic of Indonesia Defense University
Asep Adang Supriyadi
Faculty Of Defense Engineering and Technology, Republic of Indonesia Defense University

Corresponding Author: *florentinus.as@gmail.com*

Abstract

The reality of contemporary security threats today is hybrid, where the already integrated physical and digital conflicts demand strategic integration between Geospatial Intelligence (GEOINT) capabilities for Cyber Warfare. Systematic studies have not discussed much about the development and structure of scientific knowledge regarding the convergence between the two domains. This study aims to analyze trends, collaborations, and research gaps in the literature that relate the theme of GEOINT to cyber warfare. This study uses a bibliometric analysis method sourced from data on 149 Scopus indexed articles from 2002 to 2026, with the keywords Geointelligence or cyberwarfare. However, the results of the network analysis reveal conceptual fragmentation. This is shown by the indirect relationship between the keywords used. The conclusion of this study is that although this field of research is growing and recognized in the academic sphere, there is still a large research gap in the operational integration of GEOINT to be utilized in cyber warfare. Therefore, future research needs to be directed towards the development of an integrated framework, supported by inclusive collaboration, to strengthen national resilience in the face of increasingly complex hybrid threats.

Keywords: Geointelligence; GEOINT; cyberwarfare; hybrid threats; Bibliometric Analysis.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

INTRODUCTION

The contemporary world is faced with an increasingly complex and hybrid evolution of security threats, where physical and digital conflicts are no longer separable. This convergence has created a new battlefield where traditional and cyber warfare intersect. In this context, two areas of strategic capability are crucial: Geospatial Intelligence (GEOINT) and Cyber Warfare. A security threat that is hybrid, combining the physical and digital domains. The Hybrid Warfare form of conflict integrates conventional and non-conventional tactics, targeting military and civilian structures. These include cyberattacks, disinformation campaigns, and economic coercion, operating within an ambiguous gray zone between peace and conflict. Cyber threats have become a critical component of hybrid warfare, capable of disrupting communications, impacting physical infrastructure, and creating confusion. These threats exploit vulnerabilities in digital systems, making them a significant challenge to national security. The exploitation of digital vulnerabilities to disrupt critical infrastructure, affecting social stability, demands an integrated and adaptive security approach (Boyte, 2019, 2020; Mikac et al., 2025; Tsetsos, 2025; Wróblewski et al., 2025)

Recognizing the complexity of these hybrid threats, the ability to blend geospatial understanding with cyber operations becomes crucial, this is where the role of Geospatial Intelligence (GEOINT) emerges as a key element that transcends the physical and digital domains to build holistic situational awareness. GEOINT's role in Military Operations has been the backbone of military operations and crisis management. It provides critical insights by integrating geospatial data with other intelligence sources, improving situational awareness and decision-making capabilities. The convergence of the geospatial and cyber domains has created a new battlefield. Cyber operations now leverage geospatial data to improve the accuracy and effectiveness of attacks, further complicating the security landscape. The convergence between geospatial and cyber domains within the framework of hybrid threats is giving rise to a complex new battlefield where geospatial data is a multiplier of strength as well as vulnerability in modern military operations (Mikac et al., 2025; Missiroli, 2025; Wróblewski et al., 2025).

In the face of a new battlefield, the most vulnerable and strategically valuable asset is precisely the critical physical infrastructure of a nation. Hybrid threats pose a significant risk to critical infrastructure, which increasingly relies on interconnected digital systems. These threats can have a ripple effect, impacting a wide range of community functions and essential services. Legal and Policy Framework: Addressing these threats requires a strong legal and policy framework. Comparative studies highlight the need for comprehensive national and international regulations to effectively counter cyber threats. Increasing resilience through international

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

collaboration, public awareness, and integrated civil and government resources is critical. A security culture and proactive defense mechanisms can reduce vulnerabilities and ensure the sustainability of critical services (Beraia & Roszkowski, 2025; Vaseashta, 2022).

Previous studies that tended to address the two domains separately or only reviewed their integration conceptually and causally, this study bridged the two with big data analysis of the scientific literature. It is specifically designed to map knowledge networks, identify conceptual gaps, and analyze the dynamics of global collaboration, thereby generating a comprehensive epistemological map of how academia responds to the challenges of this physical-digital convergence. The use of quantitative bibliometric analysis to objectively and systematically measure and visualize the development and structure of research related to the integration of the two strategic areas of Geospatial Intelligence (GEOINT) and Cyber War in the framework of hybrid threats. This study empirically diagnoses gaps and provides a database and visualization that will be the foundation for the development of future integrated research to more effectively address hybrid security challenges.

METHOD

A bibliometric approach is applied to explore opportunities for the use of geospatial intelligence in the field of cyber warfare. This research focuses on the aspect of scientific mapping, which aims to identify relationships and patterns in the literature through scientific analysis techniques. Techniques such as co-citation analysis, keyword co-occurrence, and research hotspot identification have been used to map scientific trends in cybersecurity and artificial intelligence. Tools like Citespace and VOSviewer enable the visualization of relationships and development patterns in the literature (Li et al., 2020). Various analytical techniques are used in the scientific mapping, including the calculation of publication frequency, the number of citations, the identification of the most referenced publications, as well as grouping by the author's country affiliation analysis unit, journal reputation, and keywords. These techniques allow researchers to quantitatively measure research productivity, impact, and trends. Visualization The overview of the stages is in Figure 1 The research steps are below:

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

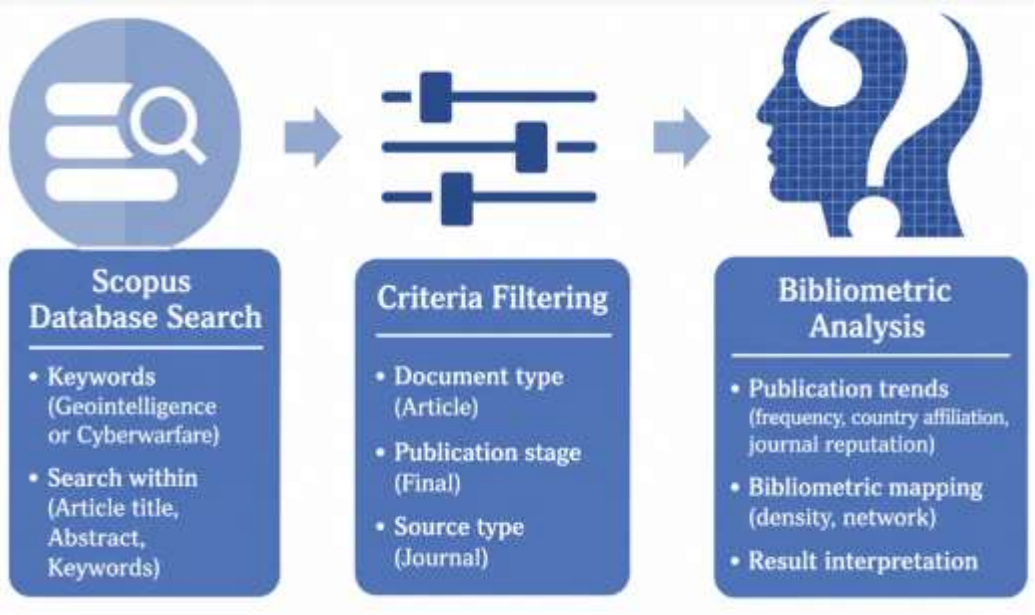


Fig. 1 Research steps
Source: Processed researcher (2026)

The initial stage of the research begins with an article search using relevant keywords. The keyword used in writing this scientific article is KEY (Geointelligence OR cyberwarfare) on what is considered the most frequently used keyword. The document search is carried out until 2026 through the Scopus database. In addition to keyword selection, this study also applies inclusion and exclusion criteria to select articles to be analyzed. The search and screening process was carried out through several systematic steps, which resulted in 149 articles used for the data.

After the article filtering process, the data obtained in RIS format is entered into the Vosviewer application for further visualization and analysis. The application generates a bibliometric map that includes co-occurrence analysis (with a keyword analysis unit). The results of this visualization show collaboration networks, topic density, and theme progression based on time. At the interpretation stage, the researcher elaborates and gives meaning to each article that has been filtered, by reading and interpreting the published research content. Conclusions are drawn from important findings relevant to the context of the relationship between GEOINT to support its primary defense in the field of cyber warfare, while identifying opportunities for further research in areas that are still rarely explored.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

PUBLICATION TRENDS

Publication trends are a method used to collect and analyze data to predict future developments based on past and ongoing patterns. In the context of this study, the purpose of the publication trend analysis is to map the development of research articles that specifically discuss policy innovations in Indonesia, with limited data sources from articles that have been published in the Scopus database. The bibliometric research then forms a map and network that can be visualized through the mapping results, where the data that has been extracted in RIS format is processed with the help of the VOSviewer application. The application is able to visualize a bibliometric network that includes authors, journals, publications, as well as the relationship between citations, bibliography, and writing patterns, thus providing a structural picture of the dynamics of research in the field.



Fig. 2 Trend in the number of research publications related to Geoint and Cyber War
Source: Scopus processed researchers (2026)

Based on data obtained since 2002 which can be seen in Figure 2. The trend in the number of research publications related to GEOINT and Cyber War, found that the distribution of articles related to GEOINT and cyber warfare has increased. When divided over a span of 8 years, there is an average increase in the number of publications. In the period of 2002-2009, there was only 1 publication in each year, whereas in 2004, 2005, and 2008 there was not even a single publication. In the 2010-2017 range, there began to be an increase in the number of publications, where on average every year there were 5 publications. In the 2018-2025 range, it has increased to 13 publications per year. Interestingly, in 2026 1 publication has appeared, this can be a sign of a positive trend of increasing publications in this theme.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

Manuscripts were published in 123 journals, 15 of which had more than one publication as can be seen in the table. Shown in Table 1. Journal Index Ranking and Number of Article Publications that the keywords searched for are in the Journal with a high percentile and cite score. This shows that the results of research are innovative, up-to-date, and significant for their fields. Articles that pass the selection here show that the topics, methodologies, and research findings are considered of high value and contribute significantly to the advancement of the discipline. Publication in a journal with a strong reputation remains a strong indicator that the study meets the strict standards and deserves the attention of the scientific community.

Table 1. Journal Index Ranking and Number of Article Publications

No.	Journal Name	Number of Articles	*Percentile*	*Cite Score*
1	*Journal of Military Ethics*	5	78%	1.3
2	*IEEE Access*	4	90%	9.0
3	*IEEE Security and Privacy*	4	93%	4.8
4	*Comparative Strategy*	3	42%	1.0
5	*Computers and Security*	3	99%	13.3
6	*International Journal of Cyber Warfare and Terrorism*	3	53%	2.5
7	*Journal of Strategic Studies*	3	88%	4.5
8	*Applied Cybersecurity and Internet Governance*	2	N/A	N/A
9	*Defense and Security Analysis*	2	61%	1.8
10	*Herald of the Russian Academy of Sciences*	2	72%	1.0
11	*Insight Turkey*	2	29%	0.7
12	*International Journal of Information Security*	2	81%	6.3
13	*Journal of Cyber Security Technology*	2	83%	5.5
14	*Nonproliferation Review*	2	48%	1.2
15	*Review of International Geographical Education*	2	N/A	N/A
16	Other journals with only one article count	108	-	-

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

Totals	149

Source: Scopus processed researchers (2026)

Next Figure 3. The distribution map of the author's home country of affiliation shows 49 home country affiliates of the authors who have collaborated on the publication of the article. From the image, it can be read that the darker the hue of a country, the more articles published by the author from the country of the article author's affiliation. It appears that the United States is the country with the most article contributors, which is 54 articles. The United States has demonstrated dominance in the research and application of GEOINT and cyber warfare through the development of advanced technologies, geopolitical strategies, and the integration of cyber capabilities in military operations. Other countries that contributed the largest articles were South Korea with 11 articles, India and the United Kingdom with 9 articles each, Russia and Italy with 8 articles each, Brazil, Portugal and Spain with 5 articles each. Another 16 countries contributed between 2-4 articles and the remaining 24 countries contributed 1 article each (Singh et al., 2025; Smirnov, 2018).



Fig. 3 Affiliate distribution map of the author's home country
Source: Scopus processed researchers (2026)

BIBLIOMETRIC MAPPING

Advanced bibliometric analysis uses VOSviewer to visualize the connections between keywords, including network visualization, and density visualization. In this case, the occurrence keyword is limited to a minimum of 5, so that out of 160 keywords, only 20 keywords are

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

interrelated. As shown in Table 2. Keyword Clusters below:

Table 2. Keyword Clusters

Cluster	Number of Keywords	Keywords
1	8	*China, cyberspace, **cyberwar**, internet, national security, strategic approach, United States, war*
2	7	*Computer crime, cyber-attacks, cyber-crimes, cybercrime, **cyberwarfare**, denial-of-service attack, network security*
3	3	*Artificial intelligence, cyber security, cybersecurity*
4	2	***Geointelligence**, security*

Source: Scopus processed researchers (2026)

The results of the depiction can also be seen in Figure 4. Density visualization. The yellow color indicates high-density areas, which are topics that have been extensively discussed in the study. On the other hand, blue to purple marks areas with low density, which indicates research gaps or topics that are still rarely explored. The results of this visualization provide a clear guide to identifying areas that are mature and areas that still have potential for further development. It appears that cyber warfare keywords are much more discussed than Geointelligence keywords.

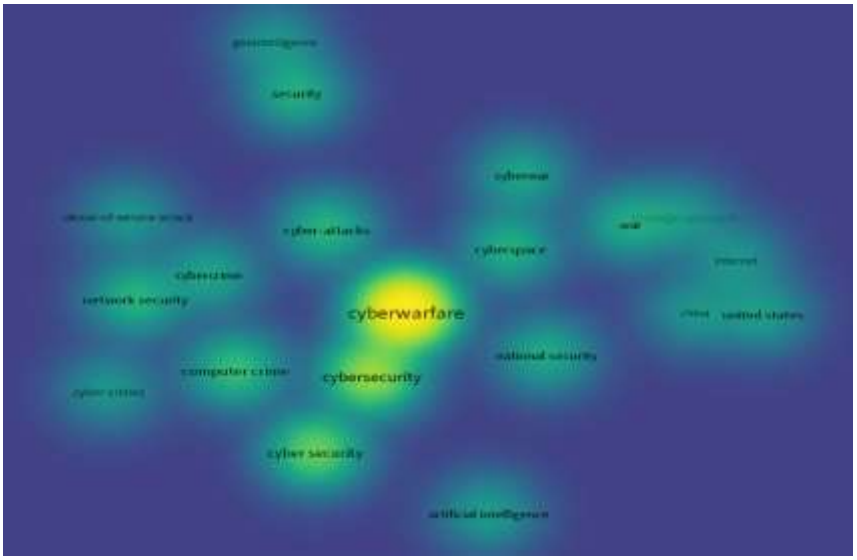


Fig. 4 Density visualization

Source: Scopus processed researchers (2026)

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

Figure 5. The network visualization below shows a map of the relationships between keywords that appeared in 149 research articles. Each circle represents a single keyword, with the larger size of the circle indicating that the keyword is appearing more and more frequently in the article set. The different colors of the circles indicate that the keywords belong to a similar group or cluster of topics, where keywords in the same color tend to be thematically interrelated. The connecting lines between the circles illustrate the co-occurrence between these keywords in the same article. The thicker the line, the stronger the relationship between the two keywords. This visualization helps identify the most dominant core topics (large circles), research networks that have been formed, as well as potential research gaps based on groups of keywords that are still separate or less connected. The keyword Geointelligence does not seem to be directly connected to cyberwarfare or cyberwar, but through the keyword security.

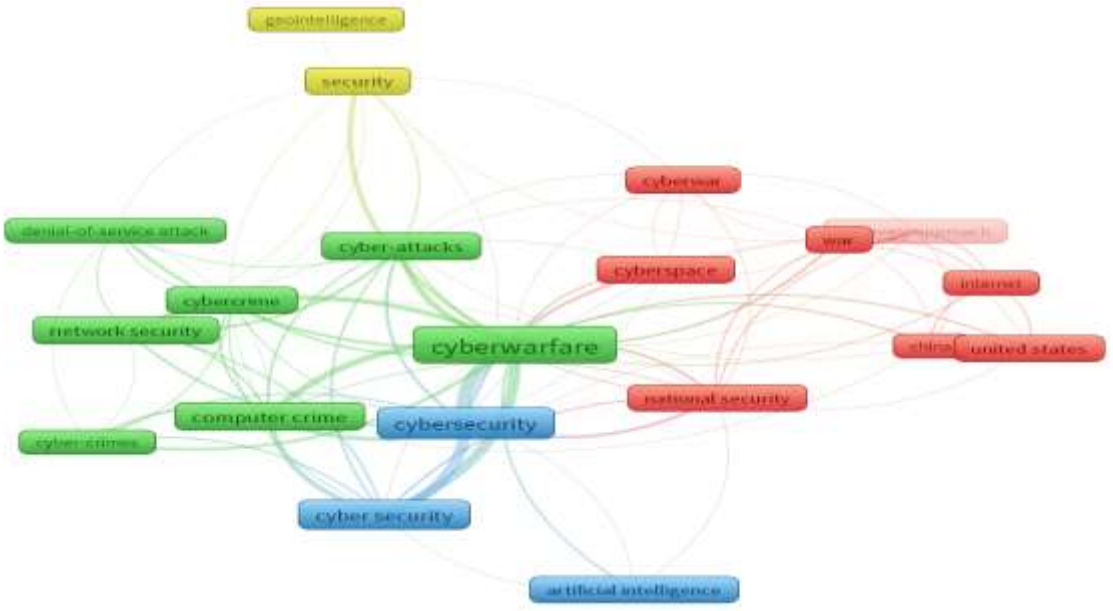


Fig. 5 Network visualization

Source: Scopus processed researchers (2026)

DISCUSSION

Based on the analysis of temporal trends, research integrating GEOINT (Geospatial Intelligence) with cyber warfare shows significant developments in the last two decades. The early period (2002-2009) was characterized by very low productivity, where academic awareness and operational urgency regarding the relationship between geospatial intelligence and the cyber domain were immature. Entering the second decade (2010-2017), there was a noticeable

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

increase. This surge can be attributed to the escalation of global cyber threats and the geospatial data revolution, which has sparked the interest of researchers and policymakers to explore the potential confluence between the two domains. The peak of productivity occurred in the 2018-2025 period, reflecting the consolidation of this field as a dynamic and relevant research area, driven by the acceleration of digitalization and geopolitical conflicts that increasingly involve cyber aspects.

In terms of quality and knowledge dissemination, many manuscripts are published in reputable journals that have impressive percentile and cite scores. Publications in these well-known journals are an indicator that innovative research in the field of GEOINT and cyber integration is considered to be of high value, has gone through a rigorous review process, and is recognized as making an important contribution to the advancement of security and strategic science. However, network visualization reveals an interesting dynamic. The keyword Geointelligence is not directly connected to cyberwarfare or cyberwar, but is only indirectly connected through intermediary nodes such as security. This pattern reveals that in the body of existing literature, the two fields are still often discussed separately. This weak and indirect relationship suggests that operational conceptualizations that explicitly integrate geospatial capabilities with cyber operations are still rare, marking fragmentation in academic discourse.

Density Visualization reinforces this gap by showing a striking disparity in research intensity. The area of cyber warfare appears with a high level of research maturity. It reflects an established academic consensus around threats, doctrines, and strategies in the cyber domain. In contrast, the Geointelligence area appears faint, which confirms that despite its importance, in-depth exploration of its role in the cyberwarfare ecosystem is still very minimal.

The dominance of the United States as the largest single contributor (54 articles) in the global collaboration map confirms the country's leadership and research investment capacity in the field of defense and cyber-integrated security. Nonetheless, the participation of 48 other countries shows that interest in this topic is global. Countries such as South Korea, India, the United Kingdom, Russia, and Italy have made significant contributions, though not as much as the US. This dominance reflects how national strategic priorities, technological superiority, and advanced defense-industrial complexes can shape the global knowledge landscape. The existing literature to date is strongly colored by the perspectives and research agendas based in the US. The large disparity between the volume of U.S. contributions and those of other countries also reveals gaps in research capacity, access to resources, and perhaps strategic priorities.

GEOINT's integration research and cyber warfare have shown rapid growth and legitimacy

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

in reputable journals, but still face challenges such as conceptual fragmentation, research focus disparities, and geographic dominance in knowledge production. These fragmentation findings actually highlight a strategic research gap, where indirect connectivity through the concept of security opens up great opportunities for future research specifically designed to bridge the two domains, for example through the development of integrated frameworks such as the use of real-time geospatial analysis for cyberattacks, location-based mapping of critical infrastructure, or the integration of GEOINT in cyber operations planning. Going forward, the greatest opportunity lies in groundbreaking research supported by inclusive international collaboration, which not only fills academic gaps but also provides a resilient framework for policymakers and practitioners in the face of increasingly complex hybrid threats in the digital era.

CONCLUSION

The use of Geospatial Intelligence (GEOINT) for Cyber Warfare is strategic to deal with hybrid threats, although in reality current global research still shows significant gaps. Although the volume of publications has increased rapidly since 2010 and is published in reputable journals, there is still conceptual fragmentation in which academic discourse is still running in parallel and very poorly integrated substantially, only weakly connected through general concepts such as security. The global map points to the unbalanced dominance of the United States, reflecting the inequality of research capacity, while the participation of other countries is still scattered and limited.

The results of this study show a quantitative empirical and visual knowledge map, so that it can function as an objective foundation for developing a holistic research agenda, scientific policy, and national defense strategy. Practically, it can be clearly identified as a research gap which is an opportunity to develop an operational framework that directly bridges geospatial analysis with cyber operations. Tee is involved in the development of GEOINT's integrated models and frameworks in the cyber warfare cycle, for example for geolocation of threats, spatial impact analysis of attacks, and location-based critical infrastructure protection, to reduce capacity gaps and build collective resilience to hybrid security threats in the digital era.

FUTURE DIRECTIONS

The main limitations of this research are conceptual fragmentation (no direct link between GEOINT keywords and cyberwarfare) and the dominance of a US perspective, which limits generalizability to a global context. Weaknesses of this method include: (1) the database is Scopus-

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

only, thus ignoring articles from other sources; (2) the keywords are too narrow without synonyms such as geospatial intelligence or cyber operations; (3) the minimum occurrence threshold of 5 results in many minor topics being left unmapped; and (4) the lack of qualitative analysis to explain the causes of fragmentation in depth. Validation can be achieved through triangulation with multiple databases (Scopus + Web of Science), keyword expansion, and sensitivity analysis to thresholds. Future research should: (a) develop an operational framework that explicitly links GEOINT to the cyberwar cycle; (b) expand collaboration across countries and disciplines; (c) combine bibliometrics with qualitative systematic literature reviews; (d) utilize AI/deep learning to monitor long-term post-attack infrastructure recovery; and (e) conduct comparative studies across regions. In this direction, future research will not only improve the method's weaknesses but also produce more tangible policy impacts.

REFERENCES

Beraia, E., & Roszkowski, R. M. (2025). THE HYBRID WARFARE UNDER THE EURASIAN GEOPOLITICS – GEORGIAN CASE | WOJNA HYBRYDOWA W RAMACH GEOPOLITYKI EUROAZJATYCKIEJ. GRUZJA – STUDIUM PRZYPADKU. Przeglad Strategiczny, (18), 38–47. https://doi.org/10.14746/ps.2025.1.3

Boyte, K. J. (2019). A Comparative Analysis of the Cyberattacks Against Estonia, the United States, and Ukraine: Exemplifying the Evolution of Internet-Supported Warfare. In National Security Breakthroughs in Research and Practices. https://doi.org/10.4018/978-1-5225-7912-0.ch007

Boyte, K. J. (2020). A Comparative Analysis of the Cyberattacks Against Estonia, the United States, and Ukraine: Exemplifying the Evolution of Internet-Supported Warfare. In Cyber Warfare and Terrorism Concepts Methodologies Tools and Applications. https://doi.org/10.4018/978-1-7998-2466-4.ch071

Li, Z., Xian, M., Liu, J., & Wang, H. (2020). The Development Trend of Artificial Intelligence in Cyberspace Security: A Brief Survey. Journal of Physics Conference Series, 1486(2). https://doi.org/10.1088/1742-6596/1486/2/022047

Mikac, R., Cesarec, I., & Sazonov, V. (2025). Hybrid threats as challenges for the protection of critical information infrastructure in cyberspace: A comparative analysis of Croatia and Estonia. In Digital Environment and Small States in Europe Challenges Threats and Opportunities. https://doi.org/10.4324/9781003594796-12

Missiroli, A. (2025). 'Hybrid' threats. In Handbook of European Union Governance.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

https://doi.org/10.4337/9781803925189.00042

Singh, N. K., Jash, A., & Nanjappa, Y. (2025). Navigating the nexus: geopolitical, international relations and technical dimensions of US-China cyber strategic competition. Cogent Social Sciences, 11(1). https://doi.org/10.1080/23311886.2025.2499171

Smirnov, A. (2018). Revision of the U.S. Cyberstrategy under Donald Trump: Preamble for aggression? | НОВЕЙШИЕ КИБЕРСТРАТЕГИИ США – ПРЕАМБУЛА ВОЙНЫ? Mezhdunarodnye Protsessy, 16(4), 181–192. https://doi.org/10.17994/IT.2018.16.4.55.11

Tsetsos, K. (2025). Preparing Civilian Infrastructure for Potential Cyber and Hybrid Attacks. In Co Evolution of Technology and Warfare Reshaping the Battlefield. https://doi.org/10.4324/9781003520160-9

Vaseashta, A. (2022). Applying resilience to hybrid threats in infrastructure, digital, and social domains using multisectoral, multidisciplinary, and whole-of-government approach. In Building Cyber Resilience Against Hybrid Threats. https://doi.org/10.3233/NICSP220017

Wróblewski, W., Wiśniewski, M., & Bieniasz, J. (2025). Civil Protection and Domestic Security in Contemporary Hybrid Warfare. In Civil Protection and Domestic Security in Contemporary Hybrid Warfare. https://doi.org/10.4324/9781003503859

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License