ACIG
APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

Russia's Invasion of Ukraine and National Cyber Security Strategies: Quantitative Comparison

Olesya Vinhas de Souza | Research Division, NATO Defense College-Rome, Italy | ORCID: 0000-0003-2234-8465

Abstract

Shared understanding of the operational environment in the cyber domain is the key enabler of NATO's cyber posture. However, there have been no attempts to evaluate empirically the impact of the war in Ukraine on intra-Alliance coherence. This study applies a novel methodology based on computation text analysis to evaluate the trends within the recently adopted national cyber strategies with regards to the description of threats, risks, and actors involved in carrying out these threats – in particular, Italy, Latvia, the United Kingdom, and the United States. The analysis shows that before the large-scale invasion, the congruence was low between the two continental European states vis-a-vis the UK and the US on threat and risk assessment. After the invasion, these differences became smaller and the language of the updated National Cyber Security Strategies became more homogeneous as measured by the cosine similarity scores. There are still differences in the discussion of relevant actors in cyberspace. The methodology applied here can be extended to measure the cohesiveness of the Alliance's cyber posture along other dimensions.

Keywords

cybersecurity, NATO, war in Ukraine, computational text analysis, national cyber strategies

Received: 13.11.2023

Accepted: 20.05.2024

Published: 18.07.2024

Cite this article as:
O. Vinhas de Souza "Russia's invasion of Ukraine and national cyber security strategies: Quantitative comparison," ACIG, vol. 3, no. 1, 2024, DOI: 10.60097/ACIG/190346

Corresponding author:
Olesya Vinhas de Souza, Research Division, NATO Defense College-Rome, Italy. E-mail: o.vinhasdesouza@ndc.nato.int;
0000-0003-2234-8465

1. Introduction

The ongoing war in Ukraine invigorated scholarly and policy debates about the role of cyber in modern warfare at the strategic and tactical levels because the escalation dynamic did not follow the expected pattern, from cyber to a conventional escalation ladder. Although the intensity of cyber attacks on Ukrainian infrastructure peaked in the early phase of the invasion, to everybody's surprise it was not followed by a cyber Pearl Harbor. In Washington, this subsequently led to the reconceptualisation of cyber from a standalone tool of modern warfare to a critical amplifier of effects across domains. In this process an integrated approach to cyber emerged, particularly in the United States, and most notably was adopted in a recent U.S. Department of Defense 'Cyber Strategy' [1]. At the tactical level, the conflict has been devoid of major changes either in terms of the actors involved or the degree of inter-domain coordination. There seems to be a consensus among cybersecurity experts that the major novelty has been an unprecedented volume of attacks against European NATO members, with a higher share of these attacks accruing on Eastern European and Baltic countries.

This study contributes to the current debate about the effects of the war in Ukraine on the cyber domain by examining whether the Allies moved closer to the shared threat perception in cyberspace since the beginning of the war – the question fundamental for NATO's cyber posture. This study is based on a computational text approach to comparing national cyber strategies for the four Allies that have updated their cyber posture since the beginning of the invasion: Latvia, Italy, the United Kingdom, and the United States. It shows that the saliency of the risk management paradigm vis-a-vis the threat prevention paradigm has increased in some of the European capitals since the invasion and this has subsequently contributed to a greater convergence of threat and risk perceptions within the Alliance. The novel methodology developed in this article can be easily extended to a larger sample to track the internal cohesion within NATO on cyber threat perception as more Allies update their strategies in 2024 and 2025.

The article begins a literature review, and then presents a computational text approach known as cosine similarity. It is based on an analogy with the distance between vectors in Euclidian space and the similarity of the content of the sections of cyber security strategies that focus on the discussion of threats, risks, and actors in cyberspace. The larger the overlap in the vocabulary used in the corresponding sections in the cyber strategies, the greater the

convergence within the Alliance on threat perceptions in cyber. The empirical section utilises the fact that cyber strategies are usually enacted for the period of four to five years and thus when countries enact or update their strategies they face a similar threat environments, which may or may not translate into the same cyber posture. So, this study provides a novel empirical approach to evaluating whether the large-scale aggression against Ukraine increased or diminished the consensus within the Alliance. The key finding is that the transatlantic consensus on the key characteristics of the operational environment has increased as a result of new cyber strategies.

2. Literature Review

The rapidly growing open source literature on the cyber dimension of the war in Ukraine can be grouped into (1) tactical studies that have focused on threat environment, types of actors, volume of attacks, geographic distribution of targets, and the types of capabilities used by state and non-state actors and (2) strategic ones that provide a high-level overview of the strategic implications of the cyber capabilities in the future conflicts. The tactical level analysis conducted primarily by think tanks and the IT industry reached the same conclusion that Russia's deployment of cyber capabilities has been haphazard and lacked cross-domain integration as well as cross-actor coordination. It resembled more the activities that were planned and carried out by unconnected networks of non-state actors who did not synchronise their activities with commanders in the theatre. The intensity of these activities picked and ebbed around high-level multilateral events outside Ukraine and the selection of targets outside Ukraine targeted those NATO and EU countries that provided stronger support to Ukraine. Although the geographic scope of the targets surpassed those of the pre-invention level, cyber capabilities have remained the same: DDoS attacks, phishing, malware, ransomware, whispers, hacking, and social engineering [2–9].

One of the unresolved puzzles of the tactical analysis is how in spite of the seeming lack of top-down organisation and/or planning of cyber offensive, the attackers have exhibited a remarkable restraint in the selection of targets outside of Ukraine territory, in such a way not to trigger multilateral or unilateral retaliation by NATO as a whole or some of its Allies. So far, all the ongoing cyber activity has been under the threshold of Article 5 and fortunately has not inflicted either economic or human costs to justify the 'shooting war' that President Biden warned Putin about. It is difficult to

reconcile how the fragmented and unconnected attackers managed to calibrate the intensity of cyber offense in a way not to exceed the Article 5 threshold. Subsequently, the large-scale conventional military confrontation broke out in spite of ominous exceptions of cyber Pearl Harbor.

This triggered the reconceptualisation of strategic uses of cyber capabilities particularly in the United States. The unclassified summary of the Department of Defense Cyber strategy published in September 2023 re-conceptualises cyber capabilities from being able to generate strategic effects by themselves to the ones that amplify the effects of capabilities in other domains. Thus cyber should be integrated into other domains to achieve the desired effects. Achieving this goal requires further investment in offensive cyber capabilities as well as extending the cyber toolbox.

The United States was not the only country that has updated its cyber posture since February 24, 2022, the day of the large-scale invasion. The United Kingdom, three EU members – Latvia, Italy, have released new National Cyber Security Strategies (NCSS). Although most of these strategies received attention from the scholarly community in the corresponding country [9–12], there have been relatively few cross-country comparisons of these recent developments [13]. The goal of the analysis that follows is to address this void.

3. Methods

The research design leverages a cutting-edge computational text methodology to compare cyber strategies. Although this is not the first study to rely on computation text analysis, it is the first one to measure the convergence or divergence on a specific issue. For example, Shafqat and Masood [14] and Song *et al.* [15] use latent topic modelling to identify clusters of countries that have similar NCSS. The small sample size in this study (n=10) is the major constraint on directly applying topic modelling here. Therefore, this study instead utilises cosine similarity scoring to compare vocabulary surrounding threats, risks, and actors – the three most contested policy issues when it comes to finding a shared position with the Alliance. By comparing the vocabulary used before and after the large-scale invasion as well as across the four countries, it is possible to assess whether the internal coherence within the Alliance declined or increased since Feb 24, 2022. Cosine similarity scoring was introduced to natural language processing to measure the distance between different texts. Building on an analogy with

the distance in Euclidean space, cosine similarity computes a dot product or the angle between two vectors. The values are bounded by 0 meaning that there is no similarity at all between the two texts and 1 means that the two texts are based on identical vocabulary. Words could be arranged in a different order, but two texts consisting of the same vocabulary will get the same scores [16, 17].

4. Results

Before presenting cosine similarity scores, it is useful to highlight the diversity of cyber strategies of continental European Allies (see Figure 1). This figure was produced by the European Union Agency for Cybersecurity (ENISA) to provide a common yardstick for comparing approaches to cyber security within the European Union. It seeks to group strategies based on stated objectives. Although there has been an upward trend in the number of objectives mentioned in cyber strategies, there has been significant variation in the scope of objectives included in them, which makes systemic comparison across countries difficult because of different priorities reflected in the strategies. The objectives range from establishing a rapid response capability to balancing security and privacy and underscore the challenges for systematic comparisons across countries because these objectives are not consistently presented either over time or across the countries.

Therefore, this study focuses on the sentences containing the keywords that appear persistently across the countries and over time: threat(s), risk(s), and actor(s). The extent of similarity or dissimilarity in the vocabulary used when discussing these terms provides insights into the evolution of intra-Alliance coherence over time, especially after the large-scale innovation. Sinc the large-scale invation, only four countries rolled out cyber strategy updates: Italy, Latvia, the United Kingdom, and the United States. The United States updated both the National Cyber Security Strategy issued by the White House as well as the Cyber Strategy published by the Department of Defense. Both of them were included in the study.

Table 1 compares how the discussion about threats, risks, and actors shifted over time. Both the United Kingdom and the United States White House strategies exhibited a high level of consistency over time in the discussion of these terms. This is surprising because of the changes in the administration from President Donald Trump to President Joe Biden. More changes were observed in the DoD strategies, particularly, with respect to risks and actors

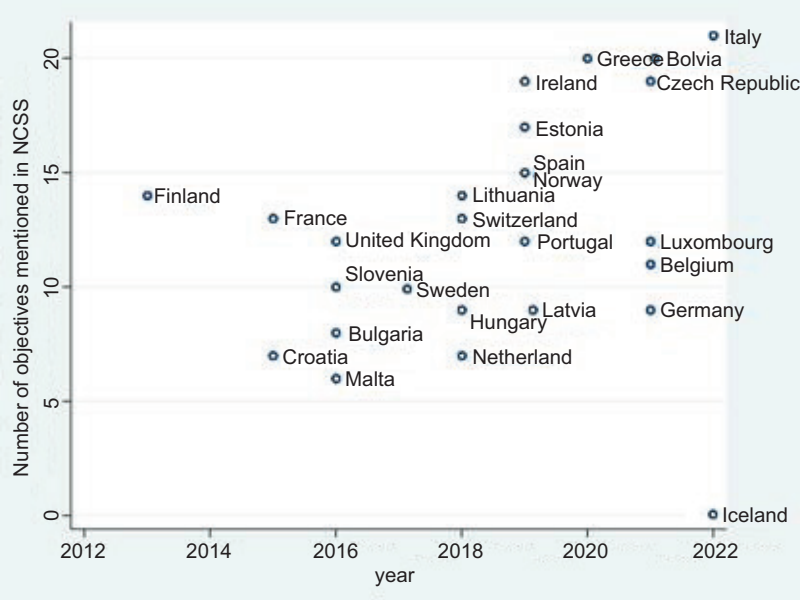

Figure 1. Number of cyber objectives in NCSS increases over time.
Source: Constructed by the Author from ENISA's interactive map available at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map. [Accessed: Dec. 20, 2023].

Table 1. Cosine similarity scores before and after the invasion.

	Italy 2017 & 2022	Latvia 2019 & 2023	United Kingdom 2016 & 2022	United States	
				White House 2018 & 2023	DoD 2018 & 2023
Threat(s)	0.49	0.84	0.97	0.92	0.80
Risk(s)	0.58	0.84	0.93	0.89	0.62
Actor(s)	0.48	0.48	0.93	0.83	0.68

Source: Cosine similarity scores were computed by the author using scikit-learn package for Python after extracting sentences with relevant keywords and merging them into text blocks by year and country.

involved. The carryover from the 2017 to 2022 strategy in Italy was comparatively low across all keywords.

Table 2 provides examples of sentences that were analyzed for each keyword for Italy to underscore the fundamental shifts in the complexity of the discussion surrounding the issues. If the 2017 strategy focuses on the concert measures, e.g. National Security R&D Center to deal with the threats, the 2022 focuses on the activities of the Intelligence Community to deal with cyber threats. Although

Table 2. Examples of excerpts from Italy's Cyber Security Strategies.

	2017	2022
Threat	• 'Create a National Cybersecurity R&D Center responsible — among other things — for developing malware analysis, security governance, Critical Infrastructures' protection, threat analysis, etc' • 'National cyber protection and ICT security require an in-depth knowledge of both technological and human vulnerabilities as well as of the threat that exploit them'	• 'The intelligence collection and analysis, aimed at protecting Italy's political, military, economic, scientific and industrial interests, is entrusted to the Intelligence Community, which for these purposes also provides, even though the conduct of cyber operations, for the activities aimed at the detection and systematic monitoring, prevention and contrasting of the most insidious cyber threats perpetrated in or through the digital environment'
Risk	• 'Implementing national cyber risk management' • 'Analysis of costs related to cyber events is a useful baseline for financial planning and allocation of resources, since risk relevance is proportional to event probability and impact'	• 'The risks implied by such complexity – and the potential many economic, social and political implications – range from technological dependence and loss of strategic autonomy of the State to anthropogenic threats, in which human error is added to the initiatives of hostile actors, characterized by different degrees of sophistication and driven by different, but equally harmful, intentions'
Actor	• 'Improving cyber actors' technological, operational, and analytic capabilities' • 'Enlarge and better define the number of actors operating in security relevant sectors' • 'That is why interoperability among actors should be fortified at national and international level'	• 'Beyond the competent institutional actors – which do not end with those mentioned above[1] – this strategy is inspired by a "whole-of-society" approach, which also involves private operators, the academic and research world, as well as civil society as a whole and citizenship' • 'For each measure, associated with the most characterizing goal, the actors responsible for the implementation and all the other subjects involved are indicated, excluding the direct beneficiaries of the measures'

Source: Extracted from Italy's NCSS for 2017–2021 and 2022–2026.

both sentences propose a solution, the language is district. Thus, the computed cosine similarity scores capture well this shift in the context in which these key issues are discussed.

Another peculiar difference between the 2017 and 2022 excerpts is the degree to which risks, threats, and actors are mentioned jointly in 2022 and in completely non-overlapping sentences in 2017. This can be used as an indicator of whether risks and threats are perceived as interchanging or not. Threat mitigation and risk management constitute two fundamentally different approaches to cybersecurity. Threat either exists or not, risk is always there but to a different degree. Threats comprise malign activities of state actors motivated by geopolitical considerations and cyber criminals driven by economic gains. Their activities threaten the interests of the general public and a diverse range of internet users. Resilience to cyber threats emerges as the result of the implementation of

comprehensive measures that promote trust and societal awareness. Risk management entails coordinating and integrating across sectors the same approach to risk management, one that takes into account not only the presence of malign actors but also the growing importance of autonomous systems (e.g. AI) that impact both resilience and threat environment in new ways. Risk management requires coordination among different levels of government and sectors. [18, pp. 13–15].

Do the new strategies reflect a greater degree of congruence across the countries on threat and risk perceptions? In the aftermath of the large-scale invasion, both the EU and NATO have enhanced their cyber toolkit to provide assistance to the member states facing cyber attacks, while at the same time homogenising the level of cyber resilience across the Alliance. Table 3 reports cosine similarity scores for each of the countries. The diagonal scores are always 1 because they correspond to the correlation of the country with itself. Therefore, we focus below on off-diagonal terms. Panel A corresponds to the old strategies and Panel B to the updated ones. One of the striking features is that we see greater similarity across all indicators in the new strategies, with only one exception: the differences in the perception of actors between Latvia on the one hand and the UK and US White House strategy increased in the updated versions. Threats are the issue that has the highest level of similarity across the countries whereas actors have the lowest level of similarity. The results also point to the division between the military and civilian approaches to cyber security. The US White House strategy is more similar to the one of the UK rather than to the U.S. DoD's strategy. Overall, Table 3 suggests that although strategies are becoming longer and more comprehensive in terms of their objectives trans-Atlantic discussions of threats, risks, and actors are becoming more homogeneous. And this is a great news for the Alliance.

5. Conclusions

NATO's cyber posture has been evolving rapidly since the large invasion along the threat prevention trajectory. The Vilnius summit became a major milestone in this regard. It established an incident response facility to which 11 Allies have already contributed. To avoid the moral hazard problem mentioned above, it also introduced a verification mechanism to ensure that the Allies continue investing in their own cyber capabilities and established ways to enhance private R&D in cyber security by creating the Defense Innovation Accelerator for the North Atlantic (DIANA) funding

Table 3. Cross-country comparison of threat, risk, and actor description.

	Panel A 2016–2021					Panel B 2022–2023				
Threat	**Italy**	**Latvia**	**UK**	**US WH**	**US DoD**	**Italy**	**Latvia**	**UK**	**US WH**	**US DoD**
Italy	1.00					1.00				
Latvia	0.55	1.00				0.89	1.00			
UK	0.50	0.77	1.00			0.89	0.91	1.00		
US WH	0.50	0.77	0.91	1.00		0.86	0.89	0.92	1.00	
US DoD	0.41	0.66	0.82	0.80	1	0.82	0.84	0.87	0.86	1.00
Risk	**Italy**	**Latvia**	**UK**	**US WH**	**US DoD**	**Italy**	**Latvia**	**UK**	**US WH**	**US DoD**
Italy	1.00					1.00				
Latvia	0.61	1.00				0.89	1.00			
UK	0.57	0.73	1.00			0.87	0.85	1.00		
US WH	0.59	0.75	0.88	1.00		0.85	0.84	0.89	1.00	
US DoD	0.48	0.53	0.75	0.76	1	0.77	0.74	0.76	0.74	1.00
Actor	**Italy**	**Latvia**	**UK**	**US WH**	**US DoD**	**Italy**	**Latvia**	**UK**	**US WH**	**US DoD**
Italy	1.00					1.00				
Latvia	0.54	1.00				0.66	1.00			
UK	0.60	0.70	1.00			0.79	0.65	1.00		
US WH	0.57	0.67	0.83	1.00		0.71	0.62	0.88	1.00	
US DoD	0.39	0.42	0.56	0.50	1	0.70	0.59	0.86	0.83	1.00

Source: Cosine similarity results were computed by the author using the scikit-learn package for Python, after extracting sentences containing relevant keywords and grouping them into text blocks based on year and country, See Table 1.

mechanism [19]. This is also happening at the same time that the EU level cyber security mechanisms are evolving. The EU's Strategic Compass adopted in March 2022 seeks to enhance 'through capacity building, capability development, training, exercises, enhanced resilience and by responding firmly to cyberattacks against the Union, its Institutions and its Member States using all available EU tools.' It aspires to strengthen the EU strategic autonomy in cyberspace 'to protect, detect, defend and deter against cyber attacks' [20].

This is happening at a time when the consensus within the Alliance on the threats, risks, and actors is growing. Although we cannot attribute any causality between these two important trends, we have to be mindful of the importance of common threat perceptions and the assessment of the operational environment in the cyber domain.

This study applied a novel methodology to quantify the trends within the Alliance in the discussion of threats, risks, and actors involved and found that recently adopted cyber strategies point to greater consensus on cyber issues than before the full-scale invasion.

Disclaimer

The views expressed are the author's alone and do not necesseraly reperesent those of NATO or the NATO Defense College.

References

[1] U.S. Department of Defense. (Sep. 12, 2023). *Summary: 2023 Cyber strategy*. [Online]. Available: https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF. [Accessed: Feb. 01, 2024].

[2] Cyber Peace Institute. (Dec. 21, 2023). *Cyber dimensions of the armed conflict in Ukraine-Q3,* 2023. [Online]. Available: https://cyberpeaceinstitute.org/publications/cyber-dimensions-of-the-armed-conflict-in-ukraine-q3-2023/. [Accessed: Dec. 24, 2023].

[3] Digwatch Online Platform. *Ukraine conflict: Digital and cyber aspects.* [Online]. Available: https://dig.watch/trends/ukraine-conflict-digital-and-cyber-aspects. [Accessed: May 01, 2023].

[4] S. Duguin, P. Pavlova. (2023). *The role of cyber in the Russian war against Ukraine: It's impact and the consequences for the future armed conflict.* [Online]. Available: https://www.europarl.europa.eu/thinktank/en/document/EXPO_BRI(2023)702594. [Accessed: Oct. 17, 2023].

[5] H. Lin, "Russian cyber operations in the invasion of Ukraine," *The Cyber Defense Review,* vol. 7, no. 4, pp. 31–46, 2022.

[6] G.B. Mueller, B. Jensen, B. Valeriano, R.C. Maness, J.M. Macias. (2022). *Cyber operations during the Russo-Ukrainian war: From strange patterns to alternative futures*. [Online]. Available: https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war. [Accessed: Oct. 02, 2023].

[7] T. Starks. (Feb. 16, 2023). "What we've learned from a year of Russian cyber-attacks in Ukraine," *The Washington Post* [Online]. Available: https://www.washingtonpost.com/politics/2023/02/16/what-we-learned-year-russian-cyberattacks-ukraine/. [Accessed: Feb. 19, 2023].

[8] M. Willet, "The cyber dimension of the Russia–Ukraine war," *Survival*, vol. 64, no. 5, pp. 7–26, 2022, doi: 10.1080/00396338.2022.2126193.

[9] A. Paulus. (Dec. 09, 2021). *German cybersecurity policy*. [Online] Available: https://directionsblog.eu/. [Accessed: Jan. 05, 2024].

[10] F. Oorsprong, P. Ducheine, P. Pijpers, "Cyber-attacks and the right of self-defense: A case study of the Netherlands," *Policy Design and Practice*, vol. 1, no. 23, 2023, doi: 10.1080/25741292.2023.2179955.

[11] A. Jacuch, "Comparative analysis of cybersecurity strategies. European Union strategy and policies. Polish and selected countries strategies," *Modeling the new Europe,* vol. 37, pp. 102–120, 2021, doi: 10.24193/OJMNE.2021.37.06.

[12] J. Neville, "Posturing US cyber forces to defend the homeland," *The Cyber Defense Review,* vol. 8, no. 2, pp. 105–128, 2023.

[13] A. Mishra, Y.I Alzoubi, M.J. Anwar, A.Q. Gill, "Attributes impacting cybersecurity policy development: An evidence from seven nations," *Computers & Security*, vol. 120, 2022, doi: 10.1016/j.cose.2022.102820.

[14] N. Shafqat, A. Masood, "Comparative analysis of various national cyber security strategies," *(IJCSIS) International Journal of Computer Science and Information Security,* vol. 14, no. 1, pp. 129–136, 2016.

[15] M. Song, D.H. Kim, S. Bae, S.J. Kim, "Comparative analysis of national cyber security strategies using topic modelling," (*IJACSA) International Journal of Advanced Computer Science and Applications*, vol. 12, no. 12, 2021, doi: 10.14569/IJACSA.2021.0121209.

[16] A.R. Lahitani, A.E. Permanasari, N.A. Setiawan, "Cosine similarity to determine similarity measure: Study case in online essay assessment." 4th International Conference on Cyber and IT Service Management, Bandung, Indonesia, 2016, pp. 1–6, doi: 10.1109/CITSM.2016.7577578.

[17] D. Gunawan, C.A. Sembiring, M.A. Budiman, "The implementation of cosine similarity to calculate text relevance between two documents." 2nd International Conference on Computing and Applied Informatics 2017 28–30 November 2017, Medan, Indonesia, 2018, pp. 1–6, doi: 10.1088/1742-6596/978/1/012120.

[18] T. Kosub, "Components and challenges of integrated cyber risk management," *ZVersWiss*, vol. 104, pp. 615–634, 2015, doi: 10.1007/s12297-015-0316-8.

[19] NATO. (Jul. 11, 2023). *Vilnius Summit Communiqué* [Online]. Available: https://www.nato.int/cps/en/natohq/official_texts_217320.htm. [Accessed: Nov. 14, 2023].

[20] European Commission. (2022). *The Strategic Compass of the European Union*. [Online]. Available: https://www.strategic-compass-european-union.com. [Accessed: Jan. 23, 2023].