Competitive Advantage in the Russo-Ukrainian War:

Ukraine's Technological Potential Against a Kremlin Goliath

Captain Melissa Vargas

ABSTRACT

This study explains the technological context and miscalculations that led to Russia's invasion of Ukraine and explores how public opinion shaped the technological factors that are helping Ukraine gain and maintain a competitive advantage. NATO overestimated Russia in information technology and did not account for collective hybrid efforts outside of Ukraine, emboldening Russia to push physical and ethical boundaries. However, Ukrainian forces and benefactors have been using information technology more efficiently than Russia, among other enablers, to gain a competitive advantage over its seemingly larger and more powerful adversary. Research must be conducted to understand the factors of Russia's shortfalls, properly integrate corporations using a common language, and establish rules of engagement among civilian and military agencies in the cyber domain. History and case study methodologies were used for this research. Russia's historical identity and impunity emboldened the Kremlin to invade Ukraine, underestimating the impact technological benefactors would have on Ukraine as a formidable competitor under Porter's five forces model. This conflict exposes implications for industry integration to cyber defense exercises (CDX). This research is significant because it promotes a common language and framework to integrate private organizations in applying collaborative solutions and boundaries in a domain without borders and limited regulation.

Keywords – cyber defense, cyber domain, CEO, Kremlin, five forces model, hybrid warfare, multi-domain operations, Russia, Ukrainian invasion

CPT Melissa Vargas is an Infantry officer in the U.S. Army currently serving as an Observer Coach/Trainer in Europe at the Joint Multinational Readiness Center. She graduated from the United States Military Academy with a B.S. in Information Technology in 2014 and is earning her M.S. in Information Systems Management from Embry-Riddle Aeronautical University Worldwide. She originally branched into the Field Artillery in 2014 but has been an Infantry officer since 2016.

Professionally, she has held the positions of Assistant Battalion Fire Support Officer, Infantry Fire Support Officer, Fire Direction Officer, Paladin Platoon Leader, Infantry Executive Officer, Regimental Assistant Plans Officer, Squadron Assistant Operations Officer, and Infantry Troop Commander. Across all positions, particularly in the European theater, her primary scope of interest and independent research has been Russian Hybrid Warfare in Fires, Maneuver, and Multi-Domain Operations.

COMPETITIVE ADVANTAGE IN THE RUSSO-UKRAINIAN WAR

Research before 2022 determined that Russia would dominate the cyber domain in a hybrid conflict and questioned civilian tech providers' ability to protect themselves under a cyber-attack.[1] The problem is that NATO and the EU overestimated Russia's information technology advantage and did not account for collective efforts outside of Ukraine. This research examines factors of Russia's shortfalls to integrate businesses properly using a common language. This research study aims to understand which technological factors Ukraine is leveraging against Russia.

Before Russia annexed Crimea in 2014, President Vladimir Putin alluded to Russia's imperialistic ideology that Ukraine is not a country and that its population is of "one people" with Russian roots and cultural identity, undermining the Ukrainian language and heritage.[2] Crimea's annexation developed speculation about Russian capabilities and the ways that it would leverage cyber warfare and information among other technologies that NATO refers to as "hybrid warfare,"[3] perpetuating Russia's misperceived strength, contributing to its traditional impunity, and emboldening Russian aggression against Ukraine prior to its invasion in February 2022.[4]

When countries overestimate Russia, they underestimate their abilities and become reluctant to act for fear of retaliation, emboldening Russia to push physical and ethical boundaries. Additionally, the by-product of civilian technology companies involving themselves blurs lines that differentiate between combatants and non-combatants, potentially endangering employees. Until recent events, research was limited by our inability to observe Russian hybrid tactics and its integration with conventional military tactics. Militarily and commercially, this domain has been contentious in terms of

discussing ethics and regulation. This research is important in understanding the commercial impacts of technology in hybrid warfare, an area that researchers have studied less than the military technological impacts. The research adds to the body of knowledge by evaluating this occurrence of hybrid warfare in the context of commercial business competitive advantage and how worldwide opinion and technological support undermined Russia. The research notes the value of military technology in conventional warfare but focuses on commercial factors for which case studies are limited. Additionally, the research supports recommendations for collaborative information systems training, governance, and legal ethical policy.

KREMLIN IDEOLOGY

To fully appreciate how the public came to misperceive Russia's power, a review based on chronology articulated a contextual understanding of the research that further perpetuated its image. Recognizing the annexation of Crimea in 2014, the post-Ukrainian Russian invasion in 2022, and the period between them drew common threads and themes that spanned over 200 years. An assessment of the degree to which each theme has been examined then promoted continued exploration of pervasive knowledge gaps.

Well before Russia annexed Crimea, the Kremlin held beliefs about Russia's place in the world as an empire. Most literature concerning Russian identity and history points to evidence that it is imperialistic by nature and has made efforts to undermine Baltic and Slavic states since the 1900s.[5] Most sources neglected to address Russian imperialist patterns dating as far back as the 1700s. Research often minimized its historic pattern of expansion despite being a relatively weak global power. From the 1700s to the 1940s Peter the Great, Alexander I, and Stalin achieved victories that resulted in expansive land acquisitions but did not result in dramatically increased purchasing power or quality of life. At the height of three expansions, Russia proved to be brittle yet resilient in three embarrassing losses against Crimea in 1856, Japan in 1905, and the Cold War. It was large on land but relatively weak on paper and inaccurately presented itself as more powerful than it really was. Its imperialist behavior was expected.

The literature after Russia's annexation of Crimea was the most extensive, in which research and speculation of hybrid warfare further elevated perceptions of Russia as a military power. Its concept of subversion was already widely established before 2014 as a strategy to undermine Western political powers internally.[6] Though subversion and hybrid warfare are used almost interchangeably and have very similar characteristics, the key difference is that subversion includes actions that may be integrated with covert cyber and military assets but intends to keep Russia away from open conflict. When Russia is involved in a direct, open conflict, more aggressive hybrid warfare measures are synchronized, such as using cyber-attacks on infrastructure shortly before moving military assets prior to an invasion. Case studies of Crimea's annexation perpetuated Russia's powerful image and deterred impunity.

Since Russia invaded Ukraine in February 2022, academic and open-source discussions have focused on Russia's targeting of Ukrainian private and public information systems in hybrid warfare, but there is limited research on the civilian and commercial assets that are aiding Ukrainians. Research cites military and commercial agencies that aid Ukraine in collective efforts and allude to the ethical implications among government agencies, and very little concerning its civilian benefactors.[7] Due to the evolving nature of the conflict, research on public opinion impacts, the commercial business factors that helped Ukraine gain a competitive advantage, and the resulting ethical implications are limited.

HYBRID METHODOLOGY: A HISTORICAL AND CASE STUDY APPROACH

The research questions, which required a comparative analysis across history and its application to current events, determined a hybrid historical and case study methodology. The purpose of the research was twofold – to better understand the historical context and patterns leading up to the Russo-Ukrainian war and to gain a deeper understanding of the recent events that contradicted researchers' predictions about Russia's skill in a hybrid war. "A history-informed agenda…allows us to develop more informed causal theories about achievement (or failure to achieve) of organizational outcomes such as growth, survival, or a sustainable competitive advantage."[8] The historical method established patterns that resulted in the widely accepted prediction that Russia would dominate in the cyber domain. Historical research methods and qualitative data are useful when studying changes in strategy as they unfold over time.[9] Case studies are most effective in investigating humans and interactions with technology, as well as determining and proposing ethical borders in a discipline.[10] A hybrid approach was the best method to address themes across history, recent events, and ethics. Both methods are innately descriptive and often absent experimental data.[11]

Sampling Design

Source sampling consisted of three chronological areas which later resulted in three key themes. The chronological areas were the periods before the annexation of Crimea, the dwell period between this annexation and the Russian invasion of Ukraine, and the period immediately after the invasion up to the present. Sampling from these periods was important because it established that deeply rooted Russian imperialism drove the inevitability of the invasion, that NATO and the EU perceived Russia as much stronger than it was, and that Russia proved to be not so formidable, contrary to historical predictions.[12] The themes that arose from sampling these distinct time frames and comparing them were that researchers misperceived Russia in terms of its hybrid prowess and that technological support from outside Ukraine played a significant role in its recent performance.[13] The sampling design was primarily chronological for a comparative measure but also ensured analysis of sources from opposite perspectives across the themes.

Materials

Qualitative data were gathered for this research, with limitations. First, the possibility of direct interviews with Ukrainian combat forces was considered. However, this method would have required lengthy legal reviews and unlikely bilateral approvals requiring more than nine weeks to conduct. Second, participant observation was neither applicable nor permissible within constructs of military duties and responsibilities. Therefore, the only applicable method was to analyze existing data from past predictions and current events as the war unfolds absent of retrospect.[14] The scope of materials excludes interviews and direct participation but includes observations and interactions from existing sources, experts, and current events.

The reliability and validity criteria of researching prioritized four main characteristics when selecting sources: proximity, focus, currency, and scholarliness. Proximity assessed the subjective value of each source in terms of its immediacy to the theme in question. The focus categorized data in terms of history, technological applications, and ethics; materials rarely addressed all three. The date that the research was published was assessed to capture accurately the perceptions surrounding Russia in each time frame without the context of the Ukrainian invasion in mind. Scholarliness was the most objective criterion that prioritized peer-reviewed, expert articles from scholarly journals. Materials used included books, scholarly articles, videos, news articles, and policy papers.

Procedure

Various research materials were considered and required differing degrees of each of the criteria depending on the themes being researched. Sources with the least proximity were those that observed Russian history as early as the 18th century. Russian imperial culture is not a groundbreaking concept and literature establishing these patterns by historical experts was widely available. It was not necessary to obtain primary sources when peer-reviewed articles established this concept. The most proximate sources consisted of current policies, regulations, and proposals published by key stakeholders in the Russo-Ukrainian war or research which used primary sources from the conflict such as Microsoft's proposed Digital Geneva Conventions[15] and data points on public opinion concerning the Russo-Ukrainian war made available by Chinese data scientists.[16]

Data focuses were organized chronologically but categorized to cover the topics of history, technological applications, and ethics. Materials that covered narrow scopes to capture more details among the focuses were of higher priority than materials that considered these subjects only on their periphery. If available, perspectives which argued contradicting positions on each focus provided valuable insight. Some of the articles that argued opposing views concerning Russian historical prowess and technological applications resulting in a competitive advantage greatly assisted in identifying the factors that contributed toward Russian and Ukrainian performance in the ongoing war.

The currency of the data did not hold objective value; more recent data were not always prioritized over other sources. When analyzing data from before the annexation of Crimea, after the invasion of Ukraine, and the period in between, it was important to prioritize data published within those respective periods to capture accurate perceptions and sentiments surrounding Russian hybrid warfare relative to NATO and the European Union.

Finally, scholarliness varied across periods and focuses. More proximate sources were inherently less scholarly but more current. However, more current sources did not always imply proximity or scholarliness. Despite scholarliness having a value that was lower relative to when it was applied to older time frames, it still retained a higher value over all other materials reflecting analysis and drew conclusions but were not peer-reviewed such as blogs and opinion news articles. Non-peer-reviewed news articles addressing the Russo-Ukrainian war retained value due to a large gap in the body of literature; there was significant value in scanning for data points and empirical statistics from that material. Additionally, policy papers and other such materials were inherently not scholarly but highly valuable in formulating ethical implications.

The outcomes of the procedures provided the basis for which the research was organized and identified the key themes and factors that required further research and analysis. Because the challenge in identifying themes is that they were abstract and difficult to identify,[17] selecting a historical approach identified the themes of perceived Russian strength and how history applied to the technological competitive advantage they have projected since the annexation of Crimea. The case study approach identified additional categories of Ukrainian technological advantage within the latter theme and delineated the ethical theme that uniquely applies to the Russo-Ukrainian war.

Justification and Limitations

To summarize methodology selection, a hybrid approach accurately captured NATO and EU perceptions of Russian strength in information warfare before and after the annexation of Crimea. The historical approach rendered the identification of two of the three key themes and helped formulate causal theories of the ways Ukraine may be gaining a technological competitive advantage in the war. The case study approach contributed to the technological competitive advantage theme of "the first major conflict involving large-scale cyber operations."[18] These methodologies were best suited for typically qualitative data. However, both methods were limited in primary sources due to restrictions that prevent direct involvement in the conflict to study. Additionally, qualitative data analysis is inherently subject to human error in thematic abstraction as well as content interpretation.[19]

FINDINGS AND DISCUSSION

Three themes stood out while conducting research. First, the perception of Russia's power projection is not a phenomenon of recent history, i.e., within the last 100 years. Russa has an

established expansionist pattern and conducts strategic messaging to create the perception of strength and to bolster the notion that it is more powerful than it is. Every instance of a cyber-attack between 2014 and 2022 became a cause for significant concern, and Russia's impunity further inflated that image. Second, world powers did not anticipate Ukraine's collective technological benefactors resulting from public opinion, both commercially and militarily, that would affect the tide of war in their favor. Finally, the application of Porter's five forces model, one that is traditionally used to explain factors that contribute to competitive advantage in business,[20] adds clarity to understanding the factors contributing to competitive advantage and strategy.

Perception of Russian Cyber Domain and Hybrid Prowess

Research trends surrounding Russian cyber and information warfare established the notion that Russia could do whatever it wanted to other nations' systems without regard for common, yet unwritten, decency. Russia's perceived prowess before 2014 resulted in limited sanctions for its actions from NATO and the EU, further bolstering its impunity. Comparatively, its system of government and policies were more consolidated and unified than NATO's to execute offensive cyber operations and defend against attacks.[21] Adding to external misperceptions, Russia was transparent about how it prioritized the information sphere and non-military tactics. Not only did Russia seem better rehearsed in the cyber domain with more effective policies, but it also messaged proactivity, aggression, and impunity so that other countries would not interfere for fear of repercussion. The NATO unity of command in a ground attack is very clear[22] because it has a legal direction to act as one. Cyber-attacks are not covered in the same unified and tangible manner, leading NATO to perceive itself as weaker in this domain despite being wealthier and larger overall.[23] However, Swedish cyber defense exercises (CDXs)[24] may provide a blueprint for integrating industry allies into NATO's Cyber Coalition Exercises[25] to build unity of command and collaborative solutions against threats to the private sector. Russia's numerous transgressions, impunity, and overt messaging, plus NATO's limited cyber-unity, are the established factors that perpetuated Russia's image. Putin's actions proved counterproductive and entrenched Ukraine deeper in the West,[26] leading to Russia's miscalculation of Ukrainian identity and degree of support.

Technological Aid and Support from Outside Ukraine

The commercial technological support from outside Ukraine is well documented but poorly consolidated because the conflict is ongoing. The volume of financial and military aid has fluctuated with subjective popular opinion worldwide. This kind of collaborative global indirect support is unprecedented and largely unofficial. Leaders did not anticipate this situation due to the lack of official policies and procedures in effect regarding Ukraine as a non-NATO nation.[27] The cyber domain has no borders and limited governance in wartime conditions, yet Ukraine was able to gain and maintain a competitive advantage through technology and public opinion against Russia.

COMPETITIVE ADVANTAGE: FIVE FORCES APPLIED

Though Porter's five forces model is traditionally used to explain factors that contribute to competitive advantage in business,[28] it can be reframed to describe and conceptualize the commercial technological factors that play a strategic supporting role in military efforts. The five forces discussed and renamed in this study are the bargaining power of suppliers, the threat of substitute products, the bargaining power of buyers, the threat of new entrants, and rivalry among existing competitors.[29] In this article they are applied to Russia and Ukraine as business competitors to account for the tangible and intangible factors that were attributed to Ukraine's unanticipated success. Benefactors to either country are considered suppliers and buyers depending on their type of support. The product each country provides in this hypothetical market is national security, interests, and ideologies for their domestic consumer populations and financial benefactors. Consider that each factor is bolstered by public opinion, and analogous to brand loyalty.

1. Bargaining Power of Supporters. In business, the bargaining power of suppliers refers to the number and size of suppliers, the uniqueness of each supplier's product, and the company's ability to substitute.[30] In the Russo-Ukrainian war, the number and size of suppliers are the tech supporters, whereas Russia has fewer suppliers in technological aid. Though the IT suppliers do not offer unique products, Ukraine enjoys exclusive IT and cyber defense support from larger commercial assets like Microsoft and Starlink that Russia does not.[31] Starlink support raised SpaceX valuation to $127 billion in 2022, increasing its status among tech giants.[32] Conversely, China continues to maintain an openly neutral sentiment that advocates for peace and sending Chinese representatives to Russia, Ukraine, and many other countries to support conflict resolution.[33] In addition to actively supporting Ukraine with IT, many countries, primarily the U.S., have implemented restrictions on technology to undermine Russia's industries.[34] Where Ukraine reaps the benefits of various technological supporters, military and commercial, for a competitive advantage, Russia relies mostly on itself.

2. Threat of Substitute Security Measures. The threat of substitute products refers to the number of substitute products, the buyer's propensity to substitute, and relative price performance.[35] In the national security context, this is reframed as the threat of substitute security measures. There are no substitute national defense agencies for either country, short of the U.S. or China's militaries stepping in to defend either one in a higher-impact conflict if its forces are decimated. The buyer's propensity to substitute refers to the benefactor's propensity to substitute indirect financial and technological aid with direct combat support; the latter is not consistent with global interests to maintain physical national security.[36] The threat of global powers substituting indirect technological support for direct high-impact warfare as a national security measure is low.

3. Bargaining Power of Benefactors. The bargaining power of buyers is the number of customers, differences between competitors, and the buyer's information ability.[37] The buyers are the benefactors that are contributing monetary aid to Ukraine in exchange for their sovereignty, which represents Western democracies and the opportunity to stay out of direct combat. From January 23, 2022, to October 3, 2022, Western countries, Japan, and Taiwan sent Ukraine over 90 billion euros in financial, humanitarian, and military aid.[38] The difference between the competitors is defined by their views on sovereignty and their respective levels of positive public opinion. The buyer's information availability is characterized by open-source interpretations of the current events in Ukraine. Russian policies align better with its internal state media to control its internal messaging[39] but have little effect outside of its borders. "The COVID-19 pandemic promoted collaborative fact-checking on an international scale."[40] Lessons learned from the Russian cyber-attacks, along with COVID-19 and political misinformation efforts became case studies that allowed agencies to refine their practices. Ukraine holds a relative advantage in the number of supporters and benefactors to its national security and ideology. The collective effectiveness of commercial and government agencies fighting against Russian misinformation efforts in the cyber domain is evidence of their advantage.

4. Threat of New Adversaries. The threat of new entrants refers to cumulative experience, government policies, brand loyalty, and capital requirements.[41] Russia alone has more experience in hybrid warfare than Ukraine but, in a cyber war involving private and public supporters on either side of the cyber conflict, Russia is outmatched as well as any other potential adversary that has not already aligned itself with a side. Government policies do not exclude commercial IT supporters, which are encouraged by public opinion, from helping Ukraine. The predicted human, technological, and financial capital to join a high-impact war against Russia or Ukraine exceeds the capital to remain a peripheral supporter. The threat of new adversaries that would compromise Ukraine's sovereignty and undermine autonomy is low.

5. Rivalry Among Existing Competitors. Finally, rivalry among existing competitors is the central factor that is impacted by the other four. It refers to the number of competitors, brand loyalty, and quality differences.[42] Ukraine has only one country to compete against. Brand loyalty is comparable to the rates at which public opinion affects domestic support for each country's efforts, also heavily affecting external aid to their causes. The quality of Ukraine's and Russia's national security forces depends on the bargaining power of supporters, the threat of substitute security measures, the bargaining power of benefactors, and the threat of new adversaries. Russia's underwhelming cyber effects are attributed to Ukraine's benefactors, both commercial and military, protecting its cyber sovereignty.[43] So long as Ukraine leverages the five factors, it can gain and maintain a competitive advantage over Russia, despite its relatively smaller size and limited internal assets.

CONCLUSION

Despite reluctance to act against Russian aggression that emboldened the Kremlin to overstep physical and ethical boundaries, formal and informal cyber-defense agencies worldwide were able to take advantage of Russian transgressions as case studies to analyze them and build effective defenses. Worldwide popular opinion reinforced Ukraine's ability to compete with Russia on the world stage despite its original disadvantages. While the unprecedented benefits of commercial IT benefactors significantly aided government efforts against Russian cyber-attacks and misinformation in a hybrid war, commercial IT support raises concern and urgency to establish international policies that define and protect non-combatants in cyberspace; though SpaceX restricted Starlink from being used in offensive operations as recently as February 2023, its involvement in the war continues to initiate debate and garner support for stronger public-private relationships with rising tech companies.[44]

Future Direction

As the war unfolds and someday concludes, a deeper study should be conducted with qualitative and quantitative feedback from those involved. In China, researchers applied a quantitative approach toward public opinion for or against the war. More research is required to understand the accuracy, feasibility, and ethics of applying business intelligence to international policy and decision-making. If NATO integrates private actors into CDXs with the five forces model used as a common language, researchers can assess the applicability and propose refinements to subcomponents from an empirical system dynamics perspective. Research providing a detailed approach toward rules of engagement must be conducted if private actors are formally introduced to cyber operations.

DISCLAIMER

The views expressed in this work are those of the author and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, or the Department of Defense.

APPENDIX

Figure 1: Reframed Five Forces Model.

NOTES

1. Sascha Dov Bachmann and Hakan Gunneriusson, "Russia's hybrid warfare in the east: The integral nature of the information sphere." *Georgetown Journal of International Affairs* (Johns Hopkins University Press, 2015) 16: 198+. Accessed November 5, 2022, https://go-gale-com.ezproxy.libproxy.db.erau.edu/ps/retrieve.do?tabID=T002&resultListType=RESULT_LIST&searchResultsType=SingleTab&hitCount=365&searchType=BasicSearchForm&currentPosition=17&docId=GALE%7CA474768082&docType=Essay&sort=Relevance&contentSegmen.
2. Jefferey Mankoff, *Russia's War in Ukraine: Identity, History, and Conflict*. Center for Strategic International Studies (2022). Accessed November 4, 2022, https://www.jstor.org/stable/resrep40567.
3. Joshua A. Sanborn, "RUSSIAN IMPERIALISM, 1914-2014: ANNEXATIONIST, ADVENTURIST, OR ANXIOUS?" *Revolutionary Russia* 27, no 5 (2014): 92-108, https://doi.org /10.1080/09546545.2014.973677.
4. Abishur Prakash, "How Technology Companies Are Shaping the Ukraine Conflict," last modified October 28, 2022, https://www.scientificamerican.com/article/how-technology-companies-are-shaping-the-ukraine-conflict/.
5. Jefferey Mankoff, *Russia's War in Ukraine: Identity, History, and Conflict*. Center for Strategic International Studies (2022). Accessed November 4, 2022, https://www.jstor.org/stable/resrep40567.
6. Andrew Radin, Alyssa Demus, and Krystyna Marcinek, *Understanding Russian Subversion: Patterns, Threats, and Responses*, RAND Corporation (2020): 6, https://www.jstor.org/stable/resrep26519.
7. Marcus Willet, "The Cyber Dimension of the Russia-Ukraine War," *Survival* 64, no.5 (2022): 7-26, https://doi.org/10.1080/00396338.2022.2126193.
8. Nicholas S. Argyres, Alfredo De Massis, Nicolai J. Foss, Federico Frattini, Geoffrey Jones, and Brian S. Silverman, "History-informed strategy research: The promise of history and historical research methods in advancing strategy scholarship," *Strategic Management Journal* 41, no. 3 (2019): 343-368, https://doi.org /10.1002/smj.3118.
9. Ibid.
10. Emad Yaghmaei and Alexander Brem, "Case study research to reflect societal and ethical issues: Introduction of a research implementation plan for ICTs." *Computers & society*,45 no. 3 (2016): 306-312, https://doi.org/10.1145/2874239.2874284.
11. Nova Allison, *Types Of Qualitative Research – Overview & Examples*, accessed December 2, 2022, https://www.myperfectwords.com/blog/research-paper-guide/types-of-qualitative-research.
12. Stephen Kotkin, "Russia's Perpetual Geopolitics: Putin Returns to the Historical Pattern," *Foreign Affairs* 95, no. 3 (2016): 2-9.
13. Abishur Prakash, "How Technology Companies Are Shaping the Ukraine Conflict," last modified October 28, 2022, https://www.scientificamerican.com/article/how-technology-companies-are-shaping-the-ukraine-conflict/.
14. Nova Allison, *Types Of Qualitative Research – Overview & Examples*, accessed December 2, 2022, https://www.myperfectwords.com/blog/research-paper-guide/types-of-qualitative-research.
15. "A Digital Geneva Convention to protect cyberspace, Microsoft Policy Papers," Microsoft, accessed November 20, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH.
16. Bingyang Chen, Xiao Wang, Weishan Zhang, Tao Chen, Chenyu Sun, Zhenqi Wang, and Fei-Yue Wang, "Public Opinion Dynamics in Cyberspace on Russia-Ukraine War: A Case Analysis With Chinese Weibo," *IEEE Transactions on Computational Social Systems* 9, no.3 (2022): 948-958, https://doi.org /10.1109/TCSS.2022.3169332.
17. Ulla H. Graneheim, Britt-Marie Lindgren, and Berit Lundman, "Methodological challenges in qualitative content analysis: A discussion paper," *Nurse Education Today* 56 (2017): 29-34, https://doi.org/10.1016/j.nedt.2017.06.002.
18. Lewis, A. J. (2022). Cyber War and Ukraine. Strategic Technologies Program. Washington D.C.: Center For Strategic & International Studies. Retrieved October 13, 2023, from https://www.csis.org/analysis/cyber-war-and-ukraine.
19. Ibid.
20. "The Five Competitive Forces That Shape Strategy," *Harvard Business Review*, filmed June 30 2008, video, accessed November 1, 2022, https://www.youtube.com/watch?v=mYF2_FBCvXw.
21. Kimberly Lukin, "Russian Cyberwarfare Taxonomy and Cybersecurity Contradictions between Russia and EU: An Analysis of Management, Strategies, Standards, and Legal Aspects." *Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare*, (IGI Global, 2015), https://search-credoreference-com.ezproxy.libproxy.db.erau.edu/content/entry/igitkws/russian_cyberwarfare_taxonomy_and_cybersecurity_contradictions_between_russia_and_eu_an_analysis_of_management_strategies_standards_and_legal_aspects/0.
22. Marcus Willet, "The Cyber Dimension of the Russia-Ukraine War," *Survival* 64, no. 5 (2022): 7-26, https://doi.org/10.1080/00396338.2022.2126193.
23. Alba Iulia Catrinel Popescu, "OBSERVATIONS REGARDING THE ACTUALITY OF THE HYBRID WAR. CASE STUDY: UKRAINE," *Strategic Impact* 53 (2014): 124, https://www.proquest.com/docview/1692921972?pq-origsite=primo.

NOTES

24. Catherine Stupp, "Sweden tests cyber defenses as war and NATO bid raise security risks; military, government and corporate cyber defense experts participated in an exercise focused on protecting the internet infrastructure," *WSJ Pro, Cyber Security* (2022), http://ezproxy.libproxy.db.erau.edu/login?url=https://www.proquest.com/trade-journals/sweden-tests-cyber-defenses-as-war-nato-bid-raise/docview/2716865468/se-2.
25. Allied Command Transformation, *Exercise Cyber Coalition 2022 Concludes in Estonia*, last modified December 2, 2022, https://act.nato.int/articles/exercise-cyber-coalition-2022-concludes-estonia.
26. Stephen Kotkin, "Russia's Perpetual Geopolitics: Putin Returns to the Historical Pattern," *Foreign Affairs* 95, no. 3 (2016): 2-9.
27. Kimberly Lukin, "Russian Cyberwarfare Taxonomy and Cybersecurity Contradictions between Russia and EU: An Analysis of Management, Strategies, Standards, and Legal Aspects." *Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare* (IGI Global, 2015), https://search-credoreference-com.ezproxy.libproxy.db.erau.edu/content/entry/igitkws/russian_cyberwarfare_taxonomy_and_cybersecurity_contradictions_between_russia_and_eu_an_analysis_of_management_strategies_standards_and_legal_aspects/0.
28. "The Five Competitive Forces That Shape Strategy," *Harvard Business Review*, filmed June 30 2008, video, accessed November 1, 2022, https://www.youtube.com/watch?v=mYF2_FBCvXw.
29. Ibid.
30. Ibid.
31. Abishur Prakash, "How Technology Companies Are Shaping the Ukraine Conflict," last modified October 28, 2022, https://www.scientificamerican.com/article/how-technology-companies-are-shaping-the-ukraine-conflict/.
32. "Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public Purpose?." Belfer Center for Science and International Affairs, Harvard Kennedy School, March 9, 2023.
33. China's Position on Russia's Invasion of Ukraine. U.S.-China Economic and Security Review Commission. Washington D.C.: U.S.-China Commission. Retrieved October 13, 2023, from https://www.uscc.gov/research/chinas-position-russias-invasion-ukraine.
34. Kate O'Keeffe, "The Ukraine Crisis: U.S. Acts to Block Technology, Other Exports to Kremlin," *The Wall Street Journal*, April 8, 2022, Eastern Edtion: A.8, https://www.proquest.com/docview/2647961543?parentSessionId=nsxJeRlagjLJDc4fyEeR6F3H4tCxHSV8e7fUlzP48KU%3D&pq-origsite=primo&accountid=27203.
35. "The Five Competitive Forces That Shape Strategy," *Harvard Business Review*, filmed June 30, 2008, video, accessed November 1, 2022, https://www.youtube.com/watch?v=mYF2_FBCvXw.
36. Kate O'Keeffe, "The Ukraine Crisis: U.S. Acts to Block Technology, Other Exports to Kremlin," *The Wall Street Journal*, April 8 2022, Eastern Edtion ed.: A.8, https://www.proquest.com/docview/2647961543?parentSessionId=nsxJeRlagjLJDc4fyEeR6F3H4tCxHSV8e7fUlzP48KU%3D&pq-origsite=primo&accountid=27203.
37. "The Five Competitive Forces That Shape Strategy," Harvard Business Review, filmed June 30 2008, video, accessed November 1, 2022, https://www.youtube.com/watch?v=mYF2_FBCvXw.
38. "Total bilateral aid commitments to Ukraine 2022, by country and type," *Statista*, Statista Research Department, last modified October 11, 2022, https://www.statista.com/statistics/1303432/total-bilateral-aid-to-ukraine/.
39. Kazimierz Pierzchala, "Information Warfare Between Russia and Ukraine: A Cause of War for the West?" *Polish Political Science* 48, no. 1 (2019): 103-111, http://czasopisma.marszalek.com.pl/images/pliki/ppsy/48-1/ppsy2019106.pdf.
40. Noemí Morejón-Llamas, Pablo Martín-Ramallal, and Juan-Pablo Micaletto-Belda, "Twitter content curation as an antidote to hybrid warfare during Russia's invasion of Ukraine," *Profesional de la información* 31 (2022): e310308, https://doi.org/10.3145/epi.2022.may.08.
41. "The Five Competitive Forces That Shape Strategy," *Harvard Business Review*, filmed June 30, 2008, video, accessed November 1, 2022, https://www.youtube.com/watch?v=mYF2_FBCvXw.
42. Ibid.
43. Marcus Willet, "The Cyber Dimension of the Russia-Ukraine War," *Survival* 64, no. 5 (2022): 19, https://doi.org/10.1080/00396338.2022.2126193.
44. "Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public Purpose?." Belfer Center for Science and International Affairs, Harvard Kennedy School, March 9, 2023.
45. Bingyang Chen, Xiao Wang, Weishan Zhang, Tao Chen, Chenyu Sun, Zhenqi Wang, and Fei-Yue Wang, "Public Opinion Dynamics in Cyberspace on Russia-Ukraine War: A Case Analysis With Chinese Weibo," *IEEE Transactions on Computational Social Systems* 9, no. 3 (2022): 948-958, https://doi.org /10.1109/TCSS.2022.3169332.