Expanding Tactical Cyber Operations for Information-Age Warfare

Archie Bass and Timothy Shives
Naval Postgraduate School, Monterey, California, USA

archie.bass@nps.edu
timothy.shives@nps.edu

Abstract: The proliferation of information through cyberspace has reshaped the character of modern warfare and altered how power is generated and exercised. Digital systems now underpin intelligence collection, operational coordination, and influence activities across instruments of national power. This dependence creates a persistent capability–vulnerability paradox in which the same networked systems that provide operational advantage also introduce exploitable weaknesses. Although the United States has developed significant strategic cyber capabilities, operational authorities and execution remain largely centralized. Incident data show that espionage, access operations, and information manipulation dominate cyber-conflict patterns, while bespoke cyber tools remain constrained by access requirements, target specificity, and limited reuse. This paper argues that maintaining an advantage in the information age requires expanding cyber execution capability and selected authorities to operational and tactical levels. It examines how cyber power's low barrier to entry enables both state and non-state actors to generate disproportionate effects and how cyberspace, as a human-built domain, often favors offense over defense. The study outlines limits on the employment of strategic cyber tools, including tradeoffs among speed, intensity, and control, as well as the single-use nature of exposed exploits. The paper proposes a tactical cyber operations framework built on dispersed, hyper-enabled units operating under decentralized command and supported by operational-level artificial intelligence processing and human–machine teaming. The framework integrates distributed intelligence validation, signature reduction, deception and decoy practices, and ambiguity operations designed to slow adversary decision cycles and increase targeting uncertainty. The paper concludes that doctrinal and authority structures should evolve to support delegated cyber action aligned with the commander's intent in persistent cyber competition.

Keywords*:* Tactical cyber operations, Cyber power, Decentralized command, Human–machine teaming, Cyber deception, Distributed operations

1. History of Information and the Importance of Cyberspace

The proliferation of information through cyberspace has fundamentally reshaped the character of modern warfare. Cyberspace expands information access to remote users and "may prove as valuable and influential in the post-industrial era as capital and labor have been in the industrial age" (Arquilla and Ronfeldt, 1993). Information technology, which enables access to information through cyberspace, is inseparable from modern warfare and generates a persistent capability/vulnerability paradox (Schneider, 2019). This paradox, combined with the inherent security weaknesses of cyberspace, creates enduring opportunities for exploitation across strategic, operational, and tactical levels of warfare. The United States has leveraged these opportunities through cyber operations; however, early efforts remained primarily confined to the strategic level due to personnel and equipment constraints. Over time, the sophistication and quantity of trained personnel and equipment have increased, yet cyber operational authorities have largely remained centralized at the strategic level. Cyber actors rely on cyberspace to rapidly transfer, aggregate, and collect information. The adversary's dependence on cyberspace to conduct operations, coupled with cyberspace's inherent characteristics and security weaknesses, necessitates that the United States delegate cyber authorities and operational approval down to the operational and tactical levels to maintain an advantage in this dynamic, evolving domain.

Organizations, whether nation-states or non-state actors, invest their limited resources to increase their relative power and to exert influence on external actors to secure resources and achieve their organizational goals (Nye Jr., 2010). Cyberspace enables access to and exploitation of information, both of which are fundamental to the use of power (Nye Jr., 2010). Organizations utilize cyberspace as a unique opportunity to rebalance power and increase influence in the information age.

Cyber power—"the ability to use cyberspace to create advantages and influence events in all operational environments and across the instruments of power"—has a relatively low barrier to entry because the required assets and training are readily available on the open market (Kramer, Starr and Wentz, 2009). Moreover, cyber power requires significantly fewer resources than developing other types of power, such as a naval fleet or a nuclear weapons capability. This smaller resource requirement allows nearly any organization to wield substantial cyber power worldwide. Cyber power is distinctive because actors can use it across the spectrum of diplomatic, informational, military, economic, financial, intelligence, and law-enforcement (DIME-FIL) domains. This unique ability to produce widespread effects stems from each DIME-FIL instrument's dependence on cyberspace. As a result, organizations can acquire and project extensive cyber power with relatively modest

investments. This incentive has flooded cyberspace with a variety of actors, leading to a broad distribution of power, although not absolute equality. Such a distribution diminishes the control traditionally held by superpowers over domains like the air and the sea. The increasing use of cyberspace also introduces a capability/vulnerability paradox, which makes exploitation across different levels of warfare more possible. (Schneider, 2019).

In the early 2010s, terrorist organizations quickly adapted to the changing information environment, gaining significant cyber power with minimal investment. In July 2015, Ayman Al Zawahiri stated that al-Qaeda was in a "battle and more than half of this battle is taking place in the battlefield of the media" (Kapsokoli, 2019). Terrorist organizations like al-Qaeda understood that this new cyberspace environment was critical to controlling the narrative and influencing the population. Terrorist organizations also use the fast, reliable, and ambiguous nature of cyberspace to conduct mission planning and coordination. (Kapsokoli, 2019). These communication pathways also assist with identifying, radicalizing, and recruiting susceptible individuals (Kapsokoli, 2019). Terrorist organizations then instruct recruits through a virtual training camp that teaches them how to plan, prepare, and conduct terror attacks (Kapsokoli, 2019). Terrorist organizations also use cyberspace and cryptocurrencies to collect and transfer funds without interference from organizations like the FBI. Finally, cyberspace allows terrorists to spread terror through the amplification of their desired narrative to a level that was unimaginable before social media. Because of their limited resources and high adaptability, terrorist organizations were among the earliest adopters of cyberspace and have leveraged it to exert disproportionate influence.

Cyberspace is a unique domain, as it is a "flexible, human-built, institutionally governed, sociotechnical infrastructure" that favors offensive actions over defensive posture (Lindsay and Gartzke, 2022). Being the only human-built domain (the other domains are maritime, land, air, and space), cyberspace presents distinct opportunities for users. For example, cyber operators can exert cyber power to "produce preferred outcomes within cyberspace, or [they] can use cyber instruments to produce preferred outcomes in other domains outside cyberspace" (Nye Jr., 2010). These subsets are referred to as intra-cyberspace power and extra-cyberspace power, respectively (Nye Jr., 2010). Both of these subsets favor offensive over defensive cyber power (Arquilla, 2021). This offensive advantage is rare within warfare, where defense is typically the dominant form. These conditions enable the evolution of cyberspace attacks from isolated incidents to "coordinated, multi-domain military operations" (Devanny, Goldoni and Medeiros, 2022).

The integration of artificial intelligence (AI) into cyberspace will improve both offensive and defensive cyber capabilities. However, AI is likely to further enhance offensive advantages. Cyber actors use AI to amplify their effects both within and outside cyberspace. In 2022, a U.S. intelligence review found that Russia had invested over $300 million in foreign influence campaigns over the past eight years. Although the success of these investments varies, the substantial Russian investment highlights the strong link between cyberspace, artificial intelligence, and information operations. Russia also employs cyber operations against targets beyond cyberspace. In December 2015, the BlackEnergy malware caused power outages that affected over 230,000 people in Ukraine. Additionally, in 2017, the NotPetya attack on a Ukrainian bank spread worldwide and caused roughly $10 billion in damages. These attacks demonstrate the destructive potential of cyber operations that extend beyond cyberspace, butactors planning to seize infrastructure should avoid causing irreversible damage. For example, when Russia invaded Ukraine in 2022, the aim was to seize critical infrastructure intact, particularly the communications network, to ensure its continued usefulness for the invaders. Destroying the communications network would aid current military operations, but it would also require additional effort and money to restore it afterward. On the other hand, this choice to limit attacks on critical infrastructure allowed Ukrainian forces to keep using it for defense. When choosing cyber targets that extend beyond cyberspace, actors must balance the immediate military benefits against possible long-term effects. These structural dynamics shape not only the strategic environment but also the operational constraints under which cyber power is developed and employed.

2. Cyber Tool Constraints and Strategic–Operational Imbalance

Cyberspace also presents distinct challenges because three key variables—speed, intensity, and control—negatively correlate with one another, and cyber tools lack universal effectiveness (Maschmeyer, 2021). Both intra- and extra-cyberspace powers depend on access and require a bespoke cyber tool tailored to the specific target (Borghard and Lonergan, 2019). This access, along with the tool's required specificity, limits its fungibility. This limitation is compounded at the strategic level because access is drastically more resource-intensive to gain and maintain. Additionally, the time required to develop the cyber tool, the extent of its impact, and the ability

to control its effects once deployed are in direct competition with one another, creating the "subversive trilemma" (Maschmeyer, 2021). Finally, once organizations develop a strategic tool and the opportunity to employ it arises, commanders face the reality that "cyber operations have a 'use it and lose it' quality" (Borghard and Lonergan, 2019). This single-use nature of the cyber tool stems from its bespoke design. Once the exploit is exposed, it can be patched with relative ease. The United States' decision-makers have seldom employed strategic cyber power because it has limited applicability, and they are reluctant to expend a capability they may need in the future.

The discussion of the importance of cyber access for power projection gave rise to cyber persistence theory (CPT). CPT posits that for a state to achieve security in the cyber strategic environment, it must maintain constant contact with the adversary (Fischerkeller *et al.*, 2022). This differs from traditional international relations (IR) theory, in which physical barriers limit the projection of power, and peace is the absence of interaction (Akdağ, 2025). CPT provides an alternative approach to deterrence that does not require confrontation in the physical domain and limits the risk of escalation in the nuclear environment (Fischerkeller *et al.*, 2022).

Although the United States focuses on strategic cyber operations, the Dyadic Cyber Incident and Campaign (DCID) dataset 2.0 found that 61% of cyber incidents since 2000 have been cyber espionage operations (Maness *et al.*, 2023). This emphasis on cyber espionage also bears true during full-scale conflict. Between January 2022 and August 2023, the two most common categories of cyber incidents in Ukraine were malicious code (11%) and espionage (7%) ("A Decade in the Trenches of Cyberwarfare: Ukraine's Story of Resilience," 2024). Additionally, the premier Russian cyber operators work within departments that specialize in intelligence and subversion (Giles, 2023). The United States will continue to cede power and influence if it does not begin to prioritize the ongoing cyber competition for the collection and manipulation of information and data (Cristiano *et al.*, 2023).

Russia does not distinguish between the information domain and information operations; instead, it considers information as "the tool, the environment, and the target" (Giles, 2023). Between 2013 and 2021, this integrated understanding allowed Russian cyber operations to experience a "strategic shift from opportunistic disruption to calculated, long-term planning," aligning with Russia's broader geopolitical strategy ("A Decade in the Trenches of Cyberwarfare: Ukraine's Story of Resilience," 2024). Russia has also effectively integrated cyberspace into its long-standing Soviet-era doctrine of disinformation tactics and manipulation of public perception, yielding significant effects in the information environment ("A Decade in the Trenches of Cyberwarfare: Ukraine's Story of Resilience," 2024). Russia uses its Internet Research Agency, also known as a "troll farm," to further its information campaign by disseminating disinformation and manipulating the narrative ("A Decade in the Trenches of Cyberwarfare: Ukraine's Story of Resilience," 2024). Russia also tolerates pro-Russian hacktivist groups, such as Killnet, Xaknet, and NoName057, to conduct distributed denial-of-service (DDoS) attacks, thereby removing direct attribution ("Chronology of Cyber Aspects of the war in Ukraine 2022–Present," 2024). Additionally, Russia conducts cyber espionage operations on Western countries to gather information related to the Ukrainian security assistance strategy. ("Chronology of Cyber Aspects of the war in Ukraine 2022 – Present," 2024). Lastly, Russia often employs cyber to shape the physical and information environment for future kinetic operations ("Chronology of Cyber Aspects of the war in Ukraine 2022–Present," 2024; "A Decade in the Trenches of Cyberwarfare: Ukraine's Story of Resilience," 2024). These various tactics are subsets of a coordinated and integrated approach that is only possible because of Russia's comprehensive understanding of cyberspace, information, psychological operations, and narrative control.

Although Russia has taken a comprehensive approach to cyber operations, its efforts have often been countered effectively by Ukrainian civilian and government countermeasures supported by an international coalition. On February 26, 2022, two days after Russia's invasion, Ukraine announced the formation of an "IT Army" and called for talented applicants to join. That same day, Ukraine assigned initial tasks to this group to carry out a DDoS attack on selected Russian commercial and government websites. The Ukrainian IT Army quickly gained hundreds of thousands of followers worldwide, making it resilient to attacks. Molfar, a private Ukrainian company, uses open-source intelligence to collect target-quality data from social media posts and supplies it to Ukrainian Intelligence for operational use. Ukraine's cyber defenses have received international support through direct cybersecurity assistance and cyber intrusion alerts. The combination of civilian and government capabilities, bolstered by international advice and aid, has enabled Ukraine to neutralize Russia's credible cyber threats and directly support its kinetic defense operations.

As cyberspace becomes increasingly integrated into daily life, its prominence and society's reliance on information will continue to grow. The organizations that can rapidly adapt and gain relative cyber power will exert unmatched dominance across all warfighting domains and instruments of power. The deterrent role of

strategic cyber power is essential and should be maintained. However, limiting cyber capabilities to the strategic level unnecessarily constrains the United States. Therefore, the United States should expand the employment of cyber power to the operational and tactical levels to increase tempo and gain a significant advantage over threat actors.

3. Tactical Cyber Operations and Distributed Execution

The information revolution will continue to expand cyberspace's availability to more organizations, groups, and people. As cyberspace becomes increasingly integrated into daily life, organizations will become increasingly dependent on it (Mbanaso and Dandaura, 2015). This dependence spans the range from daily administrative tasks to the development and employment of the most exquisite instruments of national power. This reliance intensifies the capability/vulnerability paradox and creates expansive opportunities for exploitation (Schneider, 2019). The United States should employ dispersed, hyper-enabled teams with the necessary authorities and permissions to leverage tactical cyber operations to "swarm" adversary threats, thereby meeting the commander's intent through decentralized command (Arquilla, 2021).

Successful military operations have always relied upon developing trustworthy information into actionable intelligence. To complete this, analysts gather information through the seven intelligence disciplines: human intelligence (HUMINT), geospatial intelligence, signals intelligence, measurement and signature intelligence, open-source intelligence, technical intelligence, and counterintelligence (U.S. Joint Chiefs of Staff, 2013). Following the collection, this information is synthesized and published as intelligence for further use. Beyond HUMINT, each of these disciplines relies heavily on capabilities that reside in cyberspace. Therefore, the actual battle is a fight for critical pieces of information in cyberspace. In the information age, more information is available than can be analyzed, which is where the need for dispersed, hyper-enabled teams emerges. To succeed in information warfare, tactical units must possess both the capability and authority to rapidly transition from gathering information to executing operations, thereby ensuring they capitalize on the information advantage before it becomes obsolete.

Cyberspace has, however, also expanded the availability of fake and misleading information. Cyberspace enables actors to fabricate massive amounts of information, thereby decreasing the reliability of various sources and source types. This concern has altered the intelligence cycle and increased the quantity of analysis required. To validate the integrity of the information, analysts must understand the reliability of the data source and verify its authenticity by corroborating it across multiple sources and over time. Additionally, the time required to make this interpretation increases as the analyst becomes further removed from the source. Accordingly, the United States must deploy the appropriate personnel at the appropriate echelon to conduct this analysis in close proximity to the information source. Expanding tactical cyber capacity, however, requires analytic scalability to manage the volume and velocity of contested information.

4. Artificial Intelligence and Human–Machine Teaming

The information access provided by cyberspace, coupled with advanced information technologies, has inundated analysts with an abundance of available information. Although human input will always be necessary, analysts should deliberately shift a portion of this analysis to AI engines; this pairing of AI models with humans is often referred to as a human-machine team (HMT). AI systems can efficiently ingest, categorize, and structure large-scale data streams, ensuring that "information is made swiftly available to forces operating at the leading edge of battle" (Arquilla, 2021). However, as these AI models develop through machine learning, they will inherently absorb biases and begin improperly connecting information to create a narrative. Analysts should transition from brute-force analysis of raw data to dissecting and validating the narrative generated by the AI engine. This verification process will ensure that the AI models do not devalue or over-rely on critical pieces of intelligence. Operational-level commands should conduct AI processing because they possess the required power, connectivity, and force protection measures. Additionally, operational-level commands have access to additional information systems. The operational commands can transmit the parsed intelligence to the tactical level for verification and immediate operational use. The employment of HMTs, combined with task delineation across command echelons, will expedite analysis and ensure the prompt execution of actionable intelligence.

Machine learning models, a subcategory of artificial intelligence, predict outcomes by learning from data and building synthetic models. These models perform best when employed in the same context in which they were trained. After training, they cannot operate independently and are most effective with human oversight. At the operational level, these models can be integrated with analysis teams to expedite the process and reduce the time required to produce each intelligence report. These reports can then be distilled and communicated to

tactical forces for implementation. The military's use of AI must account for increased risks and changing operational dynamics. For instance, Denise Garcia and the Committee on Human-System Integration at the Air Force Research Lab have warned that AI models can produce unpredictable and sometimes misleading results, posing significant concerns for the military. Another key consideration is that adversaries can manipulate the data used for training and analysis to deceive or confuse the models. This vulnerability means the models must be safeguarded against external influences and be completely transparent about how and why they arrived at their outcomes. The military's deployment of AI naturally extends its capabilities and can support cyber operations when used responsibly to augment, not replace, human decision-makers. The integration of AI-enabled analysis must therefore be paired with force architectures designed for survivability and resilience.

5. Dispersed Units, Signature Reduction, and Survivability

The information age has also created a dependence on rapid, reliable communication and connectivity. This reliance has amplified the technical signature of tactical units and decreased their survivability. To counter this phenomenon and reduce this vulnerability, the United States should employ small, dispersed units of action capable of coordinating and massing fires against the enemy (Arquilla, 2021). The decrease in unit size will reduce external communication and allow for tightly controlled internal networks. Reducing the size of each unit diminishes its technical signature and enhances cybersecurity by limiting the number of users who require network access. These units' reduced physical and technical signatures mitigate initial force protection concerns associated with their smaller size. The reduced user demand per location also enables enhanced cybersecurity measures, thereby reducing the threat of cyber infiltration and exploitation. Additionally, the dispersed units provide additional collection opportunities from their distributed locations. This approach should serve as the primary method of employment until the next significant disruption to the information environment. The integration of AI-enabled analysis must therefore be paired with force architectures designed for survivability and resilience.

6. Deception, Decoys, and Ambiguity Operations

An additional mechanism to mitigate force-protection concerns for small, dispersed units is to employ deception tactics. For example, through an in-depth understanding of Russian targeting, Ukraine has employed decoys, such as inflatable tanks and flat-pack artillery, to mimic high-value targets that then received live Russian ordnance (Shevchenko, 2025). With minimal investment, this tactic can drastically increase the cost for an adversary and erode trust in its intelligence reports, thereby slowing the targeting cycle (Fowler and Nesbit, 2013). Finally, the use of decoys can mislead foreign intelligence to the location of pending attacks, thereby increasing operational success. In an era where being sensed is tantamount to being targeted, the United States should invest in a similar decoy capability to deceive the enemy of our intentions and enhance the survivability of tactical units.

Although the physical deception tactics described above are valuable in the physical domain, they do not reflect the intricacies of deception in the virtual environment. Due to the interconnectedness of today’s operating environment, a recent emphasis in military practices has been on synchronizing effects across domains. Multi-Domain Operations requires the orchestration of military and non-military activities across all domains (Land, Sea, Air, Space, Cyber) to create desired outcomes in space and time (NATO’s Strategic Warfare Development Command, 2023). Current deception theories, however, lack the complete integration of the cognitive, physical, and virtual dimensions, with many describing the virtual as merely a channel rather than a core component (Grant and Henderson, 2025). Even newer cyber-specific deception theories, such as those of Rowe and Rrushi (2016), misidentify the target as the machine and lack the evaluation required to holistically determine the effects of deception in an MDO context. Finally, further research is required to determine appropriate measures of effectiveness for virtual deception operations.

Another method for reducing force protection concerns is by dispersing units of action across the battlespace. This tactic also enables the rapid dissemination and execution of critical intelligence across both physical and cyberspace domains. These units can analyze AI-derived information and share key intelligence via low-probability-of-intercept and low-probability-of-detection communications with lateral units. This form of communication is preferred for its reduced signature, though it is constrained by limited data transmission capacity. However, each unit's intelligence and cyber personnel can address this limitation by distilling the data before transmission. This low-signature tactical communication and coordination technique, coupled with each unit's ability to conduct physical and cyberspace operations, will considerably increase force protection.

The United States also needs to take specific actions inside and outside cyberspace to increase ambiguity for an enemy decision-maker or reduce ambiguity by misleading their decision-making process into a favorable outcome (Daniel and Herbig, 1982). To increase ambiguity, the United States should vary the technical signatures of its locations and deploy decoy emulators at unused sites. These emulators are most effective when used in conjunction with visible decoys to further deceive adversarial sensors. AI bots at these sites could simulate electronic communications by emitting appropriate signatures. By increasing ambiguity (A-type), the United States will confuse the enemy about the location of its actual forces, requiring the adversary to spend time and resources confirming each location (Daniel and Herbig, 1982). These actions will also enhance force protection at each active site. Additionally, the tactical units should decrease ambiguity and mislead the adversary (M-type) by seeding misinformation about their intent and capabilities (Daniel and Herbig, 1982). These actions should be controlled and approved at the tactical level to increase their tempo and decrease communications with higher commands. By varying the level of ambiguity, these dispersed units can immobilize the adversary decision-maker and increase operational effects across the battlespace. The resulting surprise has been shown to increase casualties for the adversary while decreasing casualties for the initiator (Whaley, 2007). Operationalizing these capabilities at scale ultimately requires institutional adaptation in doctrine, authority structures, and campaign design.

7. Conclusion - Doctrine, Authority, and Implementation Implications

In conclusion, information will continue to play a vital role in military operations throughout the 21st century as more daily activities become dependent on cyberspace. Cyberspace has dramatically transformed modern warfare, and rapid adaptations are necessary to maintain the United States' military dominance. The United States has become increasingly reliant on large bases with extensive personnel and communications equipment, which enable real-time, direct links to tactical units. The United States must rethink how it conducts warfare and become comfortable with limited communications, giving tactical commanders the decision-making space to seize real-time opportunities. The United States should employ AI-enabled operational commands and deploy small, dispersed, hyper-enabled tactical units. These commands will quickly process vast amounts of information and deliver actionable intelligence to tactical units. The tactical units will stay below detection thresholds while validating intelligence and executing operations swiftly and efficiently. These strategies incorporate ten principles from Arthur Buckley's book, "Principles and Deceptions," and complicate the adversary's decision-making process. As AI advances, it will deepen human reliance on cyberspace. Commanders should leverage this dependency by deploying tactical units with the necessary authorities to address vulnerabilities and align with strategic objectives, ensuring operational success in the information age. The United States Department of War must update its joint doctrine to implement these techniques effectively. This revision must consider how cyberspace has altered traditional views of the competition continuum. A conventional framework that classifies interactions between states as cooperation, competition, or conflict no longer fully captures the kinds of hybrid and information warfare tactics that Russia has effectively utilized throughout the 21st century. Armed with this perspective and the outlined techniques, the United States strengthens its ability to maintain military advantage in the information age.

Ethics Declaration: This research did not involve human subjects, the collection of personal data, or experimental intervention. The study is based entirely on published literature, doctrine, and publicly available sources. No ethical approval was required.

AI Declaration: Open-source artificial intelligence tools were used solely for proofreading. All analyses, arguments, and conclusions presented in this paper are the original work of the authors or are derived from appropriately cited sources.

Disclaimer: The views expressed here are those of the authors and do not necessarily represent the views of the Naval Postgraduate School, the Department of War, or the U.S. Government.

References

"A Decade in the Trenches of Cyberwarfare: Ukraine's Story of Resilience" (2024). Cyber DIIA Platform. Available at: https://nsarchive.gwu.edu/sites/default/files/documents/semon9-ryglx/2024-02-02-Cyber-Diia-A-Decade-in-the-Trenches-of-Cyberwarfare.pdf (Accessed: September 6, 2025).

Akdağ, Y. (2025) "Great Power Cyberpolitics and Global Cyberhegemony," *Perspectives on Politics*. 2025/03/31 ed, pp. 1–22. Available at: https://doi.org/10.1017/S1537592725000040.

Arquilla, J. (2021) *Bitskrieg: the new challenge of cyberwarfare*. Cambridge: Polity Press.

Arquilla, J. and Ronfeldt, D. (1993) *Cyberwar is Coming!* Available at: https://www.rand.org/pubs/reprints/RP223.html (Accessed: July 9, 2025).

Borghard, E.D. and Lonergan, S.W. (2019) "Cyber Operations as Imperfect Tools of Escalation," *Strategic Studies Quarterly*, 13(3), pp. 122–145. Available at: https://www.jstor.org/stable/26760131 (Accessed: February 18, 2026).

"Chronology of Cyber Aspects of the war in Ukraine 2022 – Present" (2024). The George Washington University: National Security Archive Cyber Vault. Available at: https://nsarchive.gwu.edu/document/29562-cyber-vault-ukraine-timeline.

Cristiano, F. *et al.* (2023) "Artificial intelligence and international conflict in cyberspace," in D. Broeders et al., *Artificial Intelligence and International Conflict in Cyberspace*. 1st ed. London: Routledge, pp. 1–15. Available at: https://doi.org/10.4324/9781003284093-1.

Daniel, D.C. and Herbig, K.L. (1982) "Propositions on military deception," *Journal of strategic studies*, 5(1), pp. 155–177. Available at: https://doi.org/10.1080/01402398208437105.

Devanny, J., Goldoni, L. and Medeiros, B. (2022) "Strategy in an Uncertain Domain: Threat and Response in Cyberspace," *Journal of Strategic Security*, 15(2), pp. 34–47. Available at: https://doi.org/10.5038/1944-0472.15.2.1954.

Fischerkeller, M.P. *et al.* (2022) *Cyber Persistence Theory: Redefining National Security in Cyberspace*. Oxford University Press. Available at: https://doi.org/10.1093/oso/9780197638255.001.0001.

Fowler, C.A. and Nesbit, R.F. (2013) "Tactical Deception in Air-Land Warfare," *The Art and Science of Military Deception*. Artech House, p. 45*53.

Giles, K. (2023) *Russian cyber and information warfare in practice: Lessons observed from the war on Ukraine*. Royal Institute of International Affairs. Available at: https://doi.org/10.55317/9781784135898.

Grant, T. and Henderson, S. (2025) "Evaluating Deception Theories for Applicability to Cyber Operations," *The Proceedings of the 24th European Conference on Cyber Warfare and Security*. *European Conference on Cyber Warfare and Security*. Available at: https://doi.org/https://doi.org/10.34190/eccws.24.1.3574.

Kapsokoli, E. (2019) "The Transformation of Islamic Terrorism Through Cyberspace: The Case of ISIS," *European Conference on Cyber Warfare and Security*, pp. 677–684.

Kramer, F.D., Starr, S.H. and Wentz, L.K. (eds.) (2009) "From Cyberspace to Cyberpower: Defining the Problem," *Cyberpower and National Security*. 1st ed. Washington, D.C: National Defense University Press. Available at: https://doi.org/10.2307/j.ctt1djmhj1.

Lindsay, J.R. and Gartzke, E. (2022) "Politics by many other means: The comparative strategic advantages of operational domains," *Journal of Strategic Studies*, 45(5), pp. 743–776. Available at: https://doi.org/10.1080/01402390.2020.1768372.

Maness, R.C. *et al.* (2023) "Expanding the Dyadic Cyber Incident and Campaign Dataset (DCID): Cyber Conflict from 2000 to 2020," *The cyber defense review*, 8(2), pp. 65–90.

Maschmeyer, L. (2021) "The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations," *International security*, 46(2), pp. 51–90. Available at: https://doi.org/10.1162/isec_a_00418.

Mbanaso, U.M. and Dandaura, E.S. (2015) "The Cyberspace: Redefining A New World," *IOSR Journal of Computer Engineering*, 17(3, Ver. VI), pp. 17–24. Available at: https://doi.org/10.9790/0661-17361724.

NATO's Strategic Warfare Development Command (2023) "Multi-Domain Operations in NATO - Explained." NATO's Allied Command Transformation. Available at: https://www.act.nato.int/article/mdo-in-nato-explained/.

Nye Jr., J.S. (2010) "Cyber Power," *Harvard Kennedy School - Belfer Center for Science and International Affairs* [Preprint]. Available at: https://apps.dtic.mil/sti/citations/ADA522626 (Accessed: July 18, 2025).

Rowe, N.C. and Rrushi, J. (2016) *Introduction to Cyberdeception*. Cham: Springer (SpringerLink Bücher). Available at: https://doi.org/10.1007/978-3-319-41187-3.

Schneider, J. (2019) "The capability/vulnerability paradox and military revolutions: Implications for computing, cyber, and the onset of war," *Journal of Strategic Studies*, 42(6), pp. 841–863. Available at: https://doi.org/10.1080/01402390.2019.1627209.

Shevchenko, V. (2025) *Inflatable tanks and flat-pack guns - inside Ukraine's decoys war*, *BBC*. Available at: https://www.bbc.com/news/articles/cr4e435x4kqo (Accessed: September 9, 2025).

U.S. Joint Chiefs of Staff (2013) "JP 2-0, Joint Intelligence," *U.S. Joint Publications* [Preprint].

Whaley, B. (2007) *Stratagem: Deception and Surprise in War*. Norwood, MA, UNITED STATES: Artech House. Available at: http://ebookcentral.proquest.com/lib/ebook-nps/detail.action?docID=338750.