Wargaming Design for Cyber Warfare

Dong Wang
New York Institute of Technology, Vancouver campus, Canada

dwang52@nyit.edu

Abstract: Wargaming design serves as a critical tool for military simulation, analysis, training, and strategic planning. Throughout history, innovations in wargaming have paralleled the introduction of new weapons and technologies. As information technology advances rapidly, cyber warfare has emerged as a fundamental component of modern conflicts. However, systematic studies of cyber warfare wargaming design remain inadequate compared to conventional kinetic warfare simulations. The cyber domain has not received appropriate attention within wargaming design frameworks, leading to conceptual confusion among terms such as "Cyber Warfare," "Cyberwar," and "Information War." This paper addresses this imbalance by synthesizing insights from traditional wargaming design and cyber warfare analysis. After examining the basic structure of traditional wargaming and assessing its adaptability to cyber warfare scenarios, this paper identified fundamental design challenges specific to cyber warfare wargaming. This research proposed an original framework based on analysis of real-world wargaming activities, particularly drawing from China's national wargaming competitions hosted by the Chinese Institute of Command and Control (CICC). The primary contributions of this research include: (1) summary and analysis of traditional wargaming structures, (2) integration of classic models with cyber warfare's unique natures, and (3) identification of key design questions requiring further studies.

Keywords: Wargaming, Cyber warfare, Wargaming design, Cybersecurity, Military simulation

1. Introduction to Wargames and Wargaming Design

Modern wargaming traces its origins to 19th century European military innovations, particularly Prussia's Kriegsspiel system. However, the fundamental philosophy underlying wargaming extends to ancient strategy games like Go and Chess, which share common principles: abstracting complex military realities into controllable simulation environments, focusing on core factors that could influence warfare outcomes, and providing insights into strategic decision-making and operational planning effectiveness, as Perla (1990) and Dunnigan (1992) stated.

Contemporary wargaming and its design methodologies rely primarily on quantitative comparisons of weapons' lethality. Carl von Clausewitz's emphasis on force concentration and massed effects in his work *On War* was reflected in modern attrition models such as Lanchester's Laws, which provide mathematical justification for firepower concentration principles through differential equations relating force size and firepower to combat outcomes. Perla (2016) discussed that in his research. These foundational concepts have guided manual and digital wargaming development for over a century.

Modern wargames are structured conflict simulations designed to train commanders, test strategies and tactics, enhance cross-service coordination, and evaluate decision-making processes within controlled environments. Their application has expanded throughout major military institutions worldwide. Several authoritative definitions of wargames exist in the literature:

In *The Complete Wargames Handbook*, Dunnigan (1992) described wargames as combining elements of gaming, history, and science, characterizing them as "glorified chess" with more complex boards and movement rules. He emphasized that wargames typically combine maps, pieces representing historical figures or military units, and rule sets governing permissible actions. Crucially, Dunnigan insisted on realism as a defining characteristic, viewing wargames as attempts to understand future possibilities through better comprehension of historical patterns.

The U.S. Department of Defense (2017) defined wargames as simulations of military operations involving opposing forces, conducted according to prescribed rules, data, and procedures for testing plans, training personnel, or developing new operational concepts in *Dictionary of Military and Associated Terms*.

In *The Art of Wargaming*, Perla (1990) defined wargames as warfare models or simulations where event flow both shapes and is shaped by human player decisions throughout the exercise. He distinguished wargames from training exercises and operations research by emphasizing humans' decision-making under uncertainty and imperfect information conditions.

By synthesizing these perspectives, this paper takes the wargame as a confrontational military simulation exercise where participants' decisions serve as the primary driving force. Well-designed wargaming possesses

predictive capabilities regarding warfare outcomes and strategic developments. Based on this understanding, wargaming design encompasses:

- Extracting and selecting key elements from real-world for scenario simulation
- Collecting and quantifying objective dynamic information, including weapons lethality, destructive capabilities, and troop movements
- Designing mechanisms that demonstrate causal relationships between decisions and outcomes

In the U.S., wargames are deeply integrated into military institutional culture and curricula. U.S. Naval War College, pioneering sophisticated manual wargames since the late 19th century, continues employing wargames as foundational tools for educating future commanders on naval strategy, operational art, and joint operations complexity, as Perla (1990) recorded. Dunnigan (1992) stated that the U.S. Army and Air Force similarly incorporate extensive wargaming, from tactical-level exercises using sand tables and computer simulations to strategy games conducted at respective war colleges.

In *Wargaming for Leaders*, Herman, Frost and Kurz (2009) viewed that regular joint wargaming activities, which involve multiple branches and international partners, are of great benefit to test joint doctrine, improve interoperability, and analyze responses to multi-domain threats. This pervasive application demonstrates U.S. military recognition of wargames as essential tools for analytical rigor, experiential learning, and adaptation to evolving operational environments.

The People's Liberation Army (PLA) of China, one of the main counterparts to the U.S. military, similarly emphasizes wargaming design as part of comprehensive military modernization. According to the U.S. Department of Defense (2023), PLA military academies and research institutions actively develop and employ advanced wargaming methodologies, recognizing demands of "intelligentized" warfare and enhanced joint operational capabilities.

The significant institutional investment in wargames by both the U.S. and China highlights their perceived critical role in preparing for modern multi-domain conflicts.

2. Cyber Warfare Conceptual Issues

2.1 Definitional Clarification

The widespread adoption of wargaming in traditional military contexts provides crucial background for understanding challenges and needs for dedicated design methodologies when applying wargaming to the characteristics of cyber warfare.

Before examining wargaming design issues, clarifying distinctions among "Cyber Warfare," "Information War," and "Cyberwar" is essential for accurate discourse and effective wargaming design in the cyber domain.

- Cyber Warfare: The U.S. Department of Defense (2017) defined this concept as the application of military force in or through cyberspace, focused on using cyber capabilities to achieve military objectives by directly affecting computer networks and systems. This represents a distinct warfare form conducted within the information domain.
- Information War (Information Operations, IO): Courterm (2024) defined IO as a broader concept than cyber warfare. In his thoughts, IO involves integrated employment of capabilities to influence, disrupt, corrupt, or usurp adversary decision-making while protecting friendly information and information systems. IO's primary objective is cognitive and behavioral influence, using various means to control or manipulate the information environment.
- Cyberwar: Hughes and Colarik (2017) found that, among 159 examined articles, only 56 provided explicit definitions of cyber war or warfare, while 103 relied on weaker implicit ones. Ashraf (2021) similarly noted the abundance of contradictory definitions—from claims of cyberwar's non-existence to warnings of its imminent threat—and proposed instead a flexible framework based on three core themes and five variables drawn from an interdisciplinary literature review. Dyer-Witheford and Matviyenko (2019) stated that cyberwar is often used imprecisely in public and media contexts to describe significant hostile cyber activity between states. This encompasses various actions, including espionage, sabotage, and disruption.

2.2 The Gap in Cyber Warfare Wargaming Design

After clarifying cyber warfare scope, a significant gap emerges: few wargames focus primarily on cyber warfare. Most existing military exercises treat cyber as service or support elements rather than primary focus areas. Several factors contribute to this deficiency:

- Abstract and Intangible: Unlike physical assets such as vehicles or weapons, cyber "assets" and "casualties" lack physical form. Traditional wargames employ quantitative models to measure force exchange; however, no analogous, agreed-upon metrics exist for cyber effects. The absence of clear attrition ratios for cyber forces complicates deterministic outcome assignment to cyber engagements.
- Organizational Integration: Cyber units are often organized as support elements for conventional forces, with roles that may not be independently modelled.
- Lack of Assessment Consensus: Cyber warfare commentators range from viewing cyber weapons as strategic nuclear threat equivalents requiring extreme caution to dismissing them as minor nuisances if physical infrastructure can be isolated, as reported in *War in the Fifth Domain* (2010). This divergence between "cyber hype" and "cyber scepticism" complicates scenario design.

The shortage of dedicated cyber wargaming design matters because modern conflicts already incorporate cyber dimensions. For non-state actors or rogue state, cyber warfare offers excellent cost-effectiveness ratios. These actors can conduct cyberattacks without physical exposure, explaining why certain authoritarian states invest heavily in cyber warfare technologies. The complexity, persistence, and concealment characteristics of cyber warfare mean that discovery of cyberattacks often occurs too late for effective response, necessitating advance consideration and response planning.

3. Integrating Cyber Warfare into Wargaming Design Paradigms

Traditional wargaming frameworks provide valuable structural foundations, but their components require thoughtful adaptation to effectively represent cyber warfare's characteristics.

3.1 Structural Adaptations

3.1.1 Scenario

Scenarios should represent realistic cyber warfare situations, drawing inspiration from historical cyber conflicts, anticipated future threats, or specific operational plans. Traditional wargaming scenarios require modification to represent multi-faceted cyber warfare, which may involve system degradation, data compromise, information manipulation, or service denial rather than purely physical destruction.

3.1.2 Map/board representation

Traditional wargaming philosophy stimulates real battle situations in controlled environments, typically represented as "maps" or "boards." In contrast, cyber warfare wargaming "maps" represent complex, interconnected network landscapes including:

- End users (laptops, servers, drones, mobile devices)
- Protection measures (firewalls, intrusion detection systems, security policies)
- Critical infrastructures (channels, cables, power grids, financial networks, communication systems)
- Service providers (data centres, cloud computing platforms)
- Emerging AI infrastructures

3.1.3 Units/pieces

Traditional wargaming "pieces" represent weapon units or battlefield events. Quantified points assigned to these pieces provide fundamental elements for evaluating battle outcomes.

In cyber warfare wargaming, each “unit” should be defined by specific capabilities, limitations, and potential rule-based interactions, representing various entities impacting cyber environments:

- Offensive cyber units (network attack technologies and exploitation capabilities)
- Defensive cyber units (network defense systems, incident responses, and resilience capabilities)
- Critical infrastructures (modelled with specific vulnerabilities and dependencies)
- Data assets (with varying sensitivity and value levels)
- Representations of non-state actors or individual users serving as attack vectors or influence targets

3.1.4 Turn sequence/rounds

Sequential turn structure in traditional wargaming is a necessary trade-off between reality and time management practicality. However, it is inadequate in the context of rapid and simultaneous cyber warfare scenarios. The design of turn sequences of cyber warfare wargaming must account for speed and concurrency of events across distributed networks. Options include highly abstracted simultaneous turns, discrete phases allowing specific action types, or real-time/near-real-time adjudication facilitated by control teams or automated mechanisms.

3.1.5 Force status

In cyber warfare scenarios, cyberattack weapons achieve maximum effectiveness when unveiled to opponents (e.g., Zero-day exploits, Advanced Persistent Threats, System backdoors). Once deployed, the openness and versatility of cyberattacks enable opponents to quickly patch or address vulnerabilities. This characteristic necessitates rapidly changing parameter settings in the design of force status.

Cyber warfare wargaming's force tracking must watch not just physical loss, but whether critical nodes are exploited, controlled or denied, and how C.I.A. triad (Confidentiality, Integrity and Availability) degrades. It also has to keep an eye on network performance, defensive-tool readiness and the cascading side-effects that flash through linked systems in seconds.

3.2 Key Questions for Designing

3.2.1 What are the cyber warfare wargaming's objectives?

The foundational question for any wargaming design concerns its purpose. In cyber warfare, objectives are particularly diverse, ranging from technical training to strategic analysis. Chosen objectives dictate required technical fidelity levels, simulated environment scale, game duration, and participant expertise requirements. Clearly defining analytical or training objectives is paramount before other design decisions.

3.2.2 How is victory determined?

Defining victory in cyber warfare poses significant challenges compared to traditional kinetic conflicts. Whyte and Mazanec (2019) highlighted that cyber attacks' outcomes are often intangible, delayed, indirect, and difficult to attribute definitively. Successful attacks typically yield data exfiltration, system degradation, or information manipulation rather than physical destruction. This renders conventional metrics like attrition or territorial gains largely inapplicable. The paper discusses combined victory criteria tailored to cyber warfare.

3.2.3 How to model cyber domains?

Unlike relatively stable physical wargame terrain, cyber domains are constantly in flux. New vulnerabilities are discovered, exploits are developed, patches are released, and technologies rapidly evolve. Cyber warfare wargaming design should realistically represent this dynamism through the control team's intervention or AI-powered automated mechanisms.

3.2.4 How to represent third-party participants?

Cyber warfare involves diverse actors beyond traditional state militaries, including intelligence agencies, non-state proxies, criminal organizations, and ideologically motivated groups. These actors possess varying capabilities, motivations. Effective wargaming design should represent this complex ecosystem accurately.

3.2.5 How to incorporate legal and policy constraints?

Cyber warfare occurs within complex and ambiguous legal and policy frameworks, including international laws, national rules of engagement, and evolving international cyberspace behavioral norms. Modelling and designing these non-technical factors are essential for strategy wargaming because they can authentically reflect the complexities of real-world decision-making procedures.

4. Case Study: Chinese Modern Wargaming Design

4.1 CICC 2025 Wargaming Competition

Since 2016, the Chinese Institute of Command and Control (CICC) has hosted annual national wargaming competitions from May to December, with participants primarily from military academies and research institutions. The ongoing 2025 competition comprises five events:

Table 1: Basic Information about 2025 CICC Wargaming Competitions

Competition Category	Wargaming Level	Platform Used	Branches Involved	Wargaming Design Focuses On
People vs. People Wargaming Match	Strategy joint operation	"Mozi Future Commander" wargaming system	All military branches	Joint confrontation across land, sea, air, and cyber-electronic warfare domains based on geopolitical conflicts
Joint Operations People-System Collaborative Challenge	Campaign-level joint operations	"Lingyi (Smart Gaming)" intelligent wargaming platform	All military branches	People-System collaboration models and decision-making technologies in large-scale, complex confrontations
Intelligent Air Combat Algorithm Challenge	Action-level	"Zhikong (Seize Sky)" air combat wargaming platform	Air force	Intelligent gaming algorithms for unmanned systems
Urban Operations Algorithm Challenge	Action-level	"Chengchi Gonglue (City Capture)" wargaming platform	Army	Decision-making assistance and gaming confrontation technologies
Long-Range Collaborative Strike Offensive and Defensive Challenge	Campaign-level joint operations	"Juesheng Qianli" (Winning From a Thousand Miles Away) intelligent wargaming platform	Navy	Large model intelligent cognition and dynamic gaming in full-process, long-range collaborative strike scenarios
Traditional Board Wargaming Contest	Educational event	"Red Classics" board-and-turn-based wargames	Army	Historical battles on Chinese front during World War II

The nine-year-old competitions have significantly supported Chinese military development, including the formations of Chinese Cyberspace Force and Information Support Force, which have made their debuts in September's V-Day military parade through Tian'anmen Square.

Except for the educational "Traditional Board Wargaming Contest," all competitions utilize specially designed network platforms with client-server architecture, on which software platforms are deployed and operated. These platforms support daily training and exercises.

4.2 CICC 2024 Competition Example

Using CICC 2024 final competition as an example, typical turn-based wargaming processes include the following components.

Table 2: The Final Competition Scenario of CICC 2024 is Named "Pincer Movements at Kalinin"

Components	Main Contents/Purposes	Scenario Description
Wargaming Purpose	Outlines principal assessment criteria, design features, core contested issues, and weapons peculiarities, enabling the control team to evaluate participants' strategic planning performance	Exercise enabling commanders to conduct strategic planning within multi-domain joint operations, integrating land, maritime, air, and cyber-electronic warfare assets
Participants	In competitive wargaming, Red and Blue cells form small teams; each designates one overall commander while others serve as operators executing orders and managing force allocation	Red cell and Blue cell (three personnel each); A control team serves as coordinator and adjudicator
Wargaming Background	To maximize real-world utility, wargaming focuses on current hot-spot regions and ongoing crises, testing participants' strategic decision-making in authentic conflicts	Y2028: Buffer-state B tilts to R-State; Atlantic-led Alliance strikes first to keep the east out of Europe's doorstep, yet its own northern door is ajar
Wargaming Period	Select plausible conflict scenarios emerging in near-future timeframes	04 OCT 2028, 10:00:00–12:30:00 Zulu
Win/Loss Conditions	Victory assessed by quantified points only—destroy opponent's weapon power and minimize own losses; personnel casualties not factored	Destroy key target: attacker gains points, defender loses; highest point at end wins
Map	Interactive digital maps of physical battlefields	European-Russian border area, annotated per scripted force lay-down and territorial ownership

Components	Main Contents/Purposes	Scenario Description
Force Status	Provide separate Red and Blue weapon equipment lists with assigned power points	Total points for each side balanced within ±1.5%
Mission Briefings	Primary directive for joint-force exercise; each participant's deployments and strategic planning are solely under its authority	By order of Red/Blue Combined Joint Force HQ, the operational directives outlined the mission background, opponent's situation, assigned tasks, and timing requirements

5. Wargaming Design Framework for Cyber Warfare

Based on CICC past year's wargaming analysis, a framework for cyber warfare wargaming design can be proposed. The framework addresses the unique characteristics of cyber warfare while maintaining the proven structure of traditional classic wargaming methodology.

5.1 Scenario Design

Given the rapid iteration of cyber technologies, the time span of a wargaming should not be too long, preferably measured in monthly units, with the scenario set for a few months into the future. This timeframe allows for realistic technological evolution while avoiding speculation about distant future capabilities. The introduction of third-party variables can reflect the complexity of cyber warfare, including the actions of non-state actors, criminal organizations, and proxy groups that often complicate real-world cyber conflicts.

Scenarios should be grounded in current threat landscapes and emerging technological trends. They should incorporate realistic geopolitical tensions and reflect the interconnected nature of global information infrastructure. The scenario should also account for the civilian nature of much cyber infrastructure, including the role of private companies as both targets and defenders.

5.2 Map Design

Instead of a physical battlefield, a network topology map should be the primary medium to reflect the unique characteristics of cyber warfare. This map should represent:

- Critical infrastructure nodes (power grids, financial systems, communications networks)
- Government and military networks with varying classification levels
- Commercial networks and cloud service providers
- Internet service providers and routing infrastructure
- Mobile and IoT device networks
- International connections and undersea cables

The map should be dynamic, allowing for changes in network topology as systems are compromised, isolated, or restored. It should also represent logical connections rather than just physical geography, showing data flows and trust relationships between different network segments.

5.3 Parallel Operations Design

To address the problem of synchronized realism, many cyber exercises shorten the time slices of each turn to simulate real-time synchronization, but they are fundamentally still asynchronous and turn-based. However, cyber warfare wargaming design should be strategically and tactically oriented rather than technically driven. It's recommended to introduce a comprehensive adjudication mechanism in the figure below.

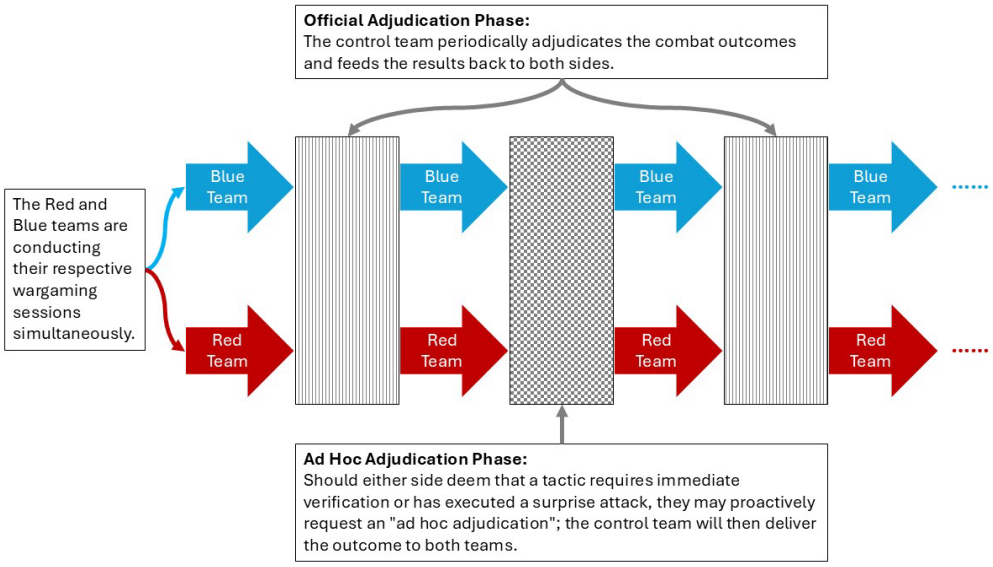

Figure 1: A New Design Adjudication Mechanism for Cyber Warfare Wargaming

This mechanism foregrounds the function of the control team, integrating it into the wargaming process. It safeguards the uninterrupted continuity of Red and Blue cells' strategic planning while simultaneously accommodating flexibility and complexity. The mechanism includes the following main phases:

- Planning and Execution Phase: Red and Blue teams carry out their moves simultaneously, guided by their mission orders and their interpretation of the wargame settings.
- Official Adjudication Phase: At intervals defined by the scenario, the control team assesses the battlefield situation and feeds the results back to all parties. Note that the time between two adjudications is not fixed—the unit of time is variable and may be denominated in hours, days, or even in seconds and milliseconds.
- Ad-Hoc Adjudication Phase: At any moment, either side may request the control team to intervene based on its strategy or operational developments; the ruling is then relayed to all parties.

5.4 Win/Loss Conditions Design

Cyber warfare wargames differ significantly due to the existence of sudden-death nodes. The destruction of certain nodes, such as undersea cables or major data centres, can cause entire networks to collapse. Therefore, the win/loss conditions should include both the cumulative calculation of destroyed enemy cyber forces and the potential for a sudden-death attack.

This design forces decision-makers to train under the pressure of a sudden-death threat while balancing multiple competing objectives, further highlighting the wargaming training value.

5.5 Force Status Design

In traditional wargaming, the quantitative points of weapons are often fixed. However, in cyber warfare wargaming, the power of a cyberattack weapon and the resilience value of a cyber-defense weapon are variable. Since a change at one node can alter the entire network topology, the force status should change dynamically under different offensive and defensive conditions. The force status system should track:

- Offensive powers' changing status (e.g., Zero-day exploits and their degradation after disclosure)
- Defensive capabilities and their effectiveness against known attack vectors
- System compromise levels (ranging from reconnaissance to full control)
- Network robustness
- Attribution confidence levels for observed activities

5.6 Third-Party Participants Design

In addition to the standard Red vs. Blue cells confrontation, the introduction of third-party participants increases the diversity and randomness of the wargame. These third parties might include:

- Criminal organizations conducting attacks for financial/political rewards
- Hacktivist with ideological motivations
- Private companies providing cyber defense services
- Allied nations with their own cyber capabilities and objectives
- International organizations attempting to mediate or investigate

5.7 AI Integration Design

AI itself is part of the substance of cyber warfare wargaming. Whether the models are secure, reliable and controllable constitutes an unknown risk for every participant. Learning to strike the right balance in employing AI tools is a training objective in the wargaming context.

On the other hand, the integration of AI into cyber warfare wargaming could reduce the calculation burden on the control team. AI can perform as third-party participants with realistic but unpredictable behavior patterns. Furthermore, AI can dynamically adjust force status points according to the always-changing network topology, which can enrich the scenario and bring more flexibility.

AI-integration is the issue that needs careful reflection and cautious handling. The author is also investigating the root causes of so-called AI "ghost answers" or fabricated responses. One potential factor is contamination in the datasets used to train these models. For example, a study led by Alexandra Souly (2025) demonstrates that Poisoning Attacks, in which adversaries inject malicious documents into training datasets, can undermine the safety and reliability of large language models.

6. In Conclusion

This paper sets out a cyber warfare wargaming design framework that mirrors cyber domain's special traits. It tries to make breakthroughs and innovations in four aspects. First, introducing third-party participants multiplies the complexity of strategic planning. Second, a parallel operation mechanism allows any participant to call for ad-hoc adjudication at certain moments, and this design can simulate real situations as much as possible. Third, a sudden-death mechanism widens victory beyond simple point calculation to a triad: destroy enemy capabilities, protect critical assets, and create windows for surprise cyber strikes. Fourth, network-topology maps replace physical battlefield charts, presenting cyber warfare features more scientifically.

Future work should proceed along three main directions: (1) Empirical validation involves systematically collecting and analyzing winning CICC wargaming after-action reports. (2) Comparable archives from other wargaming events, to assess the effectiveness of the proposed design. (3) Building on the ideas presented in this paper, the author is currently developing a cyber warfare wargaming platform that applies these design principles in practice, aiming to enhance experiential learning and operational understanding in cyber warfare, cybersecurity, and broader network-based operations.

In the context of cyber warfare wargaming, humans' decision-making remains irreplaceable; AI should only be assigned narrow, tightly controlled tasks—such as acting as third-party participants, supporting the control team's adjudications or enriching wargaming scenarios—and must never be allowed to encroach on strategic planning.

AI Declaration: No AI tools were used in the development of this paper.

Ethics Declaration: This research did not require ethical approval.

References

Ashraf, C. (2021) 'Defining cyberwar: towards a definitional framework', Defense & Security Analysis, 37(3), pp. 274–294. doi:10.1080/14751798.2021.1959141.

Boer, L.J.M. (2021) International law as we know it: cyberwar discourse and the construction of knowledge in international legal scholarship, Cambridge: Cambridge University Press.

Carr, J. and Shepherd, L. (2010) Inside cyber warfare, Sebastopol, CA: O'Reilly.

CICC Organizing Committee (2024) "**关于**组织全国兵棋推演大赛人人对抗主体赛比赛平台公测的通知 [Notice on the Public Testing of the Wargaming Platform for the People vs. People Wargaming Match of the National Wargaming Competitions]" (in Chinese), [online], Beijing: CICC, https://www.ciccwargame.com/h-nd-135.html (Accessed: 18 September 2025).

CICC Organizing Committee (2024) "**关于**举办 2024 **第八届全国兵棋推演大**赛 **人机混合决策**专项赛的通知 [Notice on the 8th National Wargaming Competitions 2024 – People-system Hybrid Decision-Making Special Competitions]" (in Chinese), [online], Beijing: CICC, https://www.ciccwargame.com/h-nd-141.html (Accessed: 18 September 2025).

CICC Organizing Committee (2025) "**关于**举办 2025 **第九届全国兵棋推演大**赛的通知 [Notice on the 9th CICC National Wargaming Competitions 2025]" (in Chinese), [online], Beijing: CICC, https://www.ciccwargame.com/h-nd-146.html (Accessed: 18 September 2025).

Cunningham, C. and Touhill, G. (2020) Cyber warfare: truth, tactics, and strategies – strategic concepts and truths to help you and your organization survive on the battleground of cyber warfare, 1st edn, Birmingham, UK: Packt Publishing.

Death, D. (2017) Information Security Handbook: Develop a Threat Model and Incident Response Strategy to Build a Strong Information Security Framework, Birmingham, UK: Packt Publishing.

Dunnigan, J.F. (1994) "Complete wargames handbook: how to play, design, & find them (rev ed)", Airpower Journal, 8(2), pp. 85–87.

Dyer-Witheford, N. and Matviyenko, S. (2019) Cyberwar and revolution: digital subterfuge in global capitalism, Minneapolis, MN: University of Minnesota Press.

Hughes, D. and Colarik, A. (2017) 'The Hierarchy of Cyber War Definitions', in G. Wang, M. Chau and H. Chen (eds) Intelligence and Security Informatics: PAISI 2017. Lecture Notes in Computer Science, vol. 10241. Cham: Springer, pp. 19–29. doi:10.1007/978-3-319-57463-9_2.

Libicki, M.C. and Project Air Force (2009) Cyberdeterrence and cyberwar, Santa Monica, CA: RAND Corporation.

Lonergan, E.D. and Lonergan, S.W. (2023) Escalation dynamics in cyberspace, New York: Oxford University Press.

Marshall, J. (2009) "Wargaming for Leaders: strategic decision-making from the battlefield to the boardroom", Financial Executive, 1 January.

Office of the Chairman of the Joint Chiefs of Staff (2017) "DOD dictionary of military and associated terms", [online], Washington, DC: The Joint Staff, https://apps.dtic.mil/sti/pdfs/AD1029823.pdf (Accessed: 18 September 2025).

Perla, P.P. (1990) The art of wargaming: a guide for professionals and hobbyists, Annapolis, MD: Naval Institute Press.

Perla, P.P. (2016) "Operations Research, Systems Analysis, and Wargaming: Riding the Cycle of Research", in Harrigan, P. and Kirschenbaum, M.G. (eds.) Zones of control: perspectives on wargaming, Cambridge, MA: MIT Press.

Poindexter, D.F. (2015) The new cyberwar: technology and the redefinition of warfare, Jefferson, NC: McFarland & Company, Inc., Publishers.

Shakarian, P., Shakarian, J. and Ruef, A. (2013) Introduction to cyber-warfare: a multidisciplinary approach, 1st edn, Amsterdam: Morgan Kaufmann Publishers, an imprint of Elsevier.

Souly, A. et al. (2025) 'Poisoning Attacks on LLMs Require a Near-constant Number of Poison Samples'. Available at: https://research.ebsco.com/linkprocessor/plink?id=c10adda0-caaa-3e6a-b9da-1b014b6aadf4 (Accessed: 18 December 2025).

The Economist (2010) "War in the fifth domain: Cyberwar", The Economist, 3 July.

U.S. Department of Defense (2023) "Military and security developments involving the People's Republic of China", [online], Washington, DC: Department of Defense. https://media.defense.gov/2023/Oct/19/2003323409/-1/-1/1/2023-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF (Accessed: 18 September 2025).

Weng, M.-H. and Chang, H.-C. (2019) **兵棋推演**：**意涵**・**模式與操作** [Wargaming: meaning, models, and practice], 1st edn, Taipei: Wu-Nan Book Inc. (in Chinese).

Whyte, C. and Mazanec, B.M. (2023) Understanding cyber warfare: politics, policy and strategy, 2nd edn, London: Routledge, Taylor & Francis Group.

Winterfeld, S. (2013) The basics of cyber warfare: understanding the fundamentals of cyber warfare in theory and practice, Boston: Syngress.

Yang, N. (ed.) (2007) **虚**拟演兵：兵棋、作战模拟与仿真 [Virtual wargaming: wargame, combat simulation and emulation], Beijing: **解放**军出版社 [PLA Publishing House]. (in Chinese).