Cyber Defence is More Than Just Cybersecurity

Juha Kai Mattila
Aalto University, Helsinki, Finland

juhakaimattila24@gmail.com

Abstract: Power projection through the cyber environment has become customary in competition, confrontation, and conflict between states. Cyber exploitation is supporting Iranian information warfare against its neighbours and the US. Russia is attacking Ukraine's cyber environment as part of its information and physical operations. The US and China wield cyber means as part of their strategic competition. Information security and cybersecurity, as part of it, focus on technical and procedural areas of cyber defence but miss the tactical, operational, and strategic levels required for national defence. Cybersecurity experts may recognise the technical and strategic layers of Cyber Defence. On the other hand, military officers approach warfare with three layers: tactical, operational, and strategic. These two world views seldom meet to generate and operate Cyber Defence. Therefore, this paper designs a model for Cyber Defence, bringing together information security and military experts from the strategic down to the technical level for capability generation and cyber force projection. The research approaches the topic from a relativist viewpoint, understanding the boundaries of Western cultural thinking and recognising the interplay between subject and object and between the nodes of the sociotechnical system. The research uses the standard research process of design sciences. The cyber defence model is built based on information and cybersecurity practices at a technical level, and on top of those, military tactical, operational, and strategic practices are applied. Selected use cases test the integrated model at each level. The paper tests the feasibility of the Cyber Defence Model with three scenarios, and the results show that the model addresses the essential tenets in tactical, operational, and strategic cases. The model recognises the different nature of the cyber environment compared to traditional domains, illustrates a collaboration model between layers of warfare, and emphasises the different nature of functions at each layer. The model and findings of the research may support establishing collaboration between stakeholders in creating national defence and military strategies, building cyber defence doctrines, and training cyber defence for planners and executors of operations and missions.

Keywords: Cyber defence, Information dimension, National defence, Military defence, Design science

1. Introduction

Power projection through the cyber environment has become customary in competition, confrontation and conflict between states. For example, cyber exploitation is supporting Iranian information warfare against the US and against its neighbours. Russia is attacking Ukraine's cyber environment as part of its information and physical operations. The US and China wield cyber means as part of their strategic competition, and defence is struggling to address issues with information security only, as in the case of ¨Salt Typhoon¨ attack (Kirby, 2024). Hence, this paper intends to provide a more holistic approach to Cyber Defence from a military force projection viewpoint than existing cybersecurity models seem to capture.

This paper designs the Cyber Defence model based on the fundamental frameworks of the Viable System Model (VSM) (Beer, 1995). It extends the VSM with strategic, operational, and tactical details from military force projection (Liddell Hart, 1991). The design benefits from research on the state-level cyber confrontation model (Mattila, 2022) and cyber force generation (Mattila, 2024).

Adversaries (RED) currently use the cyber domain to impact the physical sphere by combining kinetic and cyber strikes to target the defenders' (BLUE) physical systems through the spectrum of confrontation and conflict. Simultaneously, RED uses kinetic and cyber strikes to create fear and confusion in BLUE's cognitive and social spheres. So, with the introduction of the cyber environment, the military faces a more complex theatre than the traditional physical sphere where space, air, land and maritime operations take place (Vego, 2007).

Information security promotes governance, controls, and procedures (e.g., ISO/IEC 27 000 or NIST 800 series), and cybersecurity provides some processes or management models (e.g., NIST Cybersecurity Framework, ITIL, COBIT, ISO 38500). These leave the military short at higher levels of force projection in confrontation and national security constrained with means and ways.

Therefore, this paper aims to build the cyber defence capability generation and force projection models from technical levels defined by information and cybersecurity towards military tactical, operational and strategic levels. This research aims to create a model that cyber defence strategists, capability planners, operational planners and cyber warriors may use in planning and conducting challenges. The model is designed using methods of design sciences, and its feasibility is verified through case studies. In the following section, this

paper builds the model for more holistic Cyber Defence, explains the research methodology, provides results with further discussion, and concludes with conclusions.

2. Design of a Model

Cyber warfare refers to nation-states or non-states using digital attacks to disrupt, damage, or destroy computer systems and networks to achieve strategic objectives. The attacks encompass hacking, information manipulation, sabotage, and espionage within cyberspace. (Whyte & Mazanec, 2023) Hence, offensive and defensive actions in cyberspace have national, military, and law enforcement viewpoints. Therefore, the model must acknowledge further levels on top of the technical cybersecurity layer.

Cyberspace is an emergent domain of conflict parallel to the primary domains of land, sea, air, and space (Clarke & Knake, 2020). Unlike other domains, cyber domains are artificial and can be changed once a cyber weapon is discovered. On the other hand, the attacker has an advantage because cyberspace has plenty of artificial vulnerabilities, and increasingly automated cyberattack-related intelligence, programming, and exploitation produce many new attack vectors and means daily (Libicki, 2021). Hence, the volatility of cyberspace differs from the other domains where laws of physics prevail.

The model needs to recognise the volatile cyberspace and adjust to the evolution speed of defensive and offensive technologies and tactics. The Viable System Model interfaces with the environment at the management and operations levels and recognises the competition, regulation, and supply chain of support and sourcing (Beer, 1995).

Competition, confrontation, and conflict are more evident within the Cyber domain than in other traditional domains. The US feels that China and Russia are exploiting the cyberspace and digital highways that the US has been taking the lead in building (McLaughlin & Holstein, 2023). Hence, the model must focus on evolving escalation from competition to conflict that does not comply with Geneva or Hague rules of war (The Law Institute, 2023).

The effects of attack in cyberspace vary between disruption (Russian suppressing European VSAT communications during the invasion in Ukraine (O'Neill, 2022)), corruption (Russian attacker infiltrated the SolarWinds software and embedded a malicious code (Williams, 2020)), eruption (Ukrainian Cyber Army located Russian soldiers through their social media accounts (Mighty staff, 2023)), and interception (It took Equifax 76 days to detect the breach, allowing the attackers ample time to steal data of 147 million Americans (Tuned into Security, 2024))

Cyberspace evolves fast with emerging technology, and boundaries between physical, digital, and cognitive realms are crossed. National security worries that creating a fully immersive biophysical and psychological environment with cyber vulnerabilities and access will open nations to individual-level profiling, manipulated at an emotional level, and exploited en masse (McLaughlin & Holstein, 2023). Hence, the model must recognise the speed of technical evolution that may lead to a revolution in business, government, and private life.

Considering the above requirements, the Cyber Defence Model, as outlined in Figure 1, needs to address the following features:

- Illustrate the levels of confrontation from technical to strategic
- Explain the integration and different dependencies between the force entity and environment considering both adversarial and coalition/support relationships
- Explain the command-and-control connections from the strategic level down to the technical level within the force entity
- Enable the evolution and revolution of fast-developing artificial cyberspace
- Include the functions of development in both the defender's and offender’s viewpoint
- Understand the grey areas in competition – conflict spectrum and lack of international regulation
- Understand the evolving connection between cyberspace, the physical realm, and the cognitive realm, where surprising vulnerabilities or attack vectors may emerge as societies undergo digital transformations.

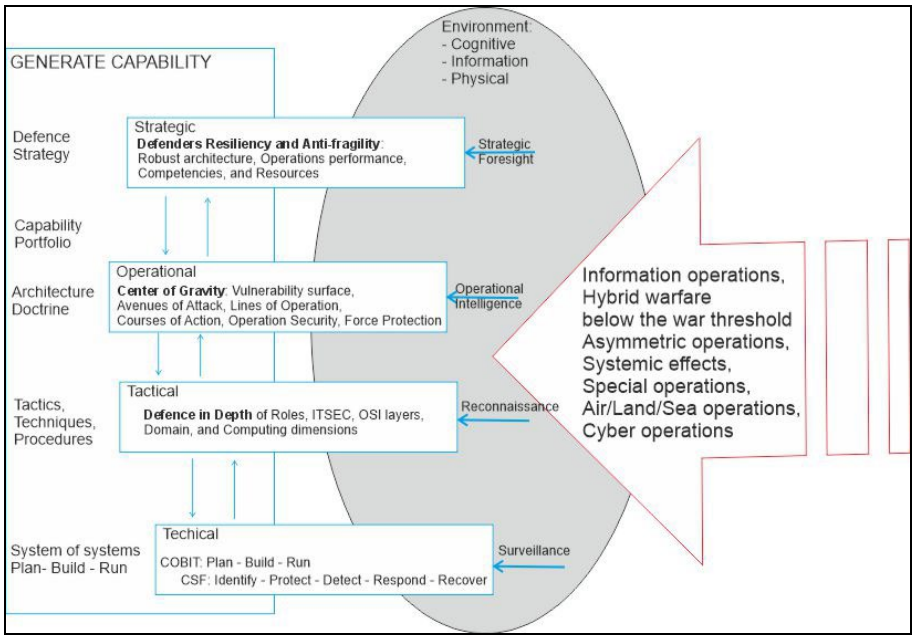

Figure 1: A View of the Cyber Defence Model

2.1 Technical-Level Cyber Defence

The NIST Cybersecurity Framework (NIST, 2024) recognises five functional areas at the technical level of cybersecurity, namely:

- Identifying assets, threat environment, risks, and options for remediation
- Protecting critical assets and services through access control, training, security, controls, maintenance and using protective technology
- Detecting anomalies and incidents
- Responding to incidents with analysis, mitigation, and continuous improvement
- Recovering from the attack as per the planned recovery and continuously improving the cyber environment's resiliency and availability.

The ISO/IEC 27000 -series (ISO/IEC, 2022) and NIST 800-series (NIST, 2025) standards provide good practices and controls for protection, detection, recovery, and information security, as illustrated in Figure 1. The technical structure providing services needs to recognise domain-specific information technology, information security, and cyber monitoring functions closely integrated with network operations. As the change management reaches out to the primary tactical decision maker, the cyber incident needs to follow the same line of support. Since cyberspace is considered an enabler in every military domain and creates a separate battlespace at a joint level, the technical cyber defence must support operational and tactical levels.

2.2 Tactical-Level Cyber Defence

Military tactics encompass "the art of organising and employing fighting forces on or near the battlefield" (Wikipedia, 2024). Applying the tactics for the defence of the cyber environment, the following functions may be included (as illustrated in Figure 1):

- Establishing a doctrine that would nullify the adversary's most probable attack techniques and vectors (IT- and security architectures),
- *Construct BLUE domain defence against RED attack vectors (e.g., MITRE Att@ck) based on the posture of information security*
- Prepare the area of cyber operation (artificial cyberspace),
- *Stabilise BLUE baseline of protocols and behavioural patterns to improve the probability of detecting anomalies*
- *Establish security at least at emission, transmission, communications and session levels in the Open Systems Interconnection (ISO/OSI) model*
- *Test the domain integrity continuously with penetration testing, black box testing, and vulnerability hunting*

- Dig defensive positions (defence-in-depth) and define the areas of fire (sandboxes, honey pots),
- *Prepare the BLUE domain using the dimensions of depth*
- *Establish kill zones with honey pots and abilities to create virtual sandboxes within the domain*
- Set tripwires and reconnoitre (vulnerability hunting, monitoring and threat intelligence),
- *deploy intrusion detection, segmentation, and zero-trust policies*
- *fuse different threat intelligence sources and apply knowledge in each domain specifically*
- *actively hunt vulnerabilities, apply penetration testing in each entity before migration and fuzz test entities for unknown vulnerabilities*
- 24/7 Surveillance of cyberspace and detecting anomalies and possible adversary deployments
- *establish 24/7 monitoring of Security Incident and Event Management*
- *use Artificial Intelligence to enhance pattern recognition,*
- *automate some of the basic response actions for faster reaction.*
- Prepare alternative positions (continuation and recovery)
- *use strategic diversification to minimise single points of failure*
- *distribute critical computing and storage geographically while centralising virtually*
- *configure the recovery of processing, storage and data to meet the operational availability* requirements
- Exercise the fire and position changes drill day and night (incident, problem, change management and red teams).
- *Exercise BLUE detection, response and recovery with red teaming in live domains.*
- *Exercise with partners in a cyber environment (inter-agency, inter-operator, coalition).*

2.3 Operational-Level Cyber Defence

Operational represents the level of command that connects the details of tactics with the strategy goals. (Vego, 2007) Operational art may be based on Sun Tzu's (Know Yourself and Your Enemy) (Sun, 2014) and Clausewitz's (Center of Gravity) (von Clausewitz, 1984) models. BLUE recognises their power sources and considers them possible Centres of Gravity (CoG) for the RED, as illustrated in Figure 1. Each CoG needs to be assessed from the RED viewpoint, considering different Lines of Operation (LoO) for effecting the CoG and variation of Courses of Action (CoA) needed to achieve the impact in the most beneficial CoG. From all the feasible CoA variations, BLUE estimates the most probable to be considered from the RED viewpoint based on their doctrine, previous behaviour and available resources in each situation.

Applying operational art for Cyber Defence provides the following sequence of BLUE operational planning:

- Recognise lucrative CoGs in the BLUE system of systems: essential operations, critical data assets, critical sites as single points of failure, critical services that are not replaceable, critical gateways that will prevent information flows or suppresses systems that cyberspace is dependent (e.g., telecommunications, power distribution, cooling, fuel distribution, garbage collection)
- Innovate potential lines of operation to access the beneficial CoGs through humans, kinetic ways, cyber-attack vectors, supply chains, or utilising dependencies and peripherals.
- Assess each Center of Gravity against a potential Line of Operation (e.g., kinetic, electromagnetic, cyber, economy, law enforcement) and try to optimise available RED resources, cost of attack, and benefit of the impact.
- Vary vulnerabilities, costs of attack, and possible benefits in different scenarios and develop probable courses of action available to the RED.
- Wargame scenarios to find the most probable CoAs RED executing in a given situation.
- Deploy different tactics to defend the potential BLUE CoGs and find ways and means to prevent or nullify the RED CoAs until only the most probable remain. Consider active (e.g., kinetic, electromagnetic, cyber, financial) and passive (e.g., information security, cybersecurity, recoverability, availability) means and ways to address most RED CoAs.
- Arrange the concealment, mock-ups, and hardening of BLUE's critical assets. Along the most probable attack vectors, BLUE sets digital sandboxes and honey pots together with physical engagement zones and counter agents.
- Establish reconnaissance, anomaly pattern recognition, movement detectors, and thresholds to detect RED manoeuvre in physical, cyber, and information spheres against the most vulnerable BLUE COGs.

2.4 Strategic-Level Cyber Defence

Military strategy is "the art of distributing and applying military means to fulfil the ends of policy" (Liddell Hart, 1991). Policy in this context usually refers to national-level security strategy, which defines the main threat scenarios against the state, its sovereignty, and interests. The model for strategic thinking in a cyber environment is based on a technological approach among the five dimensions of military strategy defined by Atkeson (Atkeson, 1977). The technological approach to strategy assesses the technical innovation and ability to render obsolete adversary effectors. In a conflict of system of systems, the strategic advantage can be achieved in three ways, as illustrated in Figure 1, applied in a cyber domain:

- The adversary achieves a strategic surprise by launching a strike at an unexpected time or place from the Defender's viewpoint (Cancian, 2018).
- Systemic effects are "those indirect effects aimed at affecting or disrupting the operation of a specific system or set of systems" (Man III, Endersby, & Searle, 2002).
- Strategic advantage may be achieved through technological innovation and deployment of capabilities multiplied by emerging technologies, providing strategic dominance over the other party (Raska, 2020).

Principles of strategic level cyber defence may include:

- An attacker has an advantage in their cyber environment and freedom of manoeuvre on the Internet. The Defender has an advantage in cyber environments under their control. Hence, Defender should build technological advantage and maintain dominance in their cyber environments (Total Military Insight, 2024).
- Defender's cyber architecture includes redundant and robust means for communications, computing, and storage, so even with 50% infrastructure losses, the essential services and processes run sufficiently, and data remains accessible (Clarke & Knake, 2020).
- Defender raises a threshold against cyber-attacks, declaring assured retaliation with weapons of mass destruction (De Haas, 2011).
- Defender prepares to cut their domestic Internet domain from the international Internet to diminish vulnerable surfaces and minimise options for direct attack vectors (Wolff, 2021).
- Defender builds their national Internet domain based on different programming languages, communications protocols, and integrated circuits. It effectively filters all traffic in and out of their national domain (Candelon, Chenao, & Jun, 2019).
- The Attacker builds and prepares strong offensive cyber capability against the weakly prepared Defender, which deters other power projections.
- Attacker sources their cyber warriors from industry or cyber-criminal gangs to accelerate offensive cyber capabilities and gain a possibility of strategic surprise (Lopez, 2024).
- Defender advances the information security architecture (Domain-defined—> Service–defined—> Zero–trust—> Content–defined) of their cyber environment, maintaining security controls and monitoring resistance against potential adversary attack vectors (Mattila & Parkinson, 2017).
- The Defender uses global dominance in economy, trade, science and technology, and cyber-physical manufacturing to slow the Attacker's ability to build a more effective cyber arsenal (Allison, Klyman, Barbesino, & Yan, 2021).

3. Research Method

The research approaches the topic from a relativist viewpoint (Moon & Blackman, 2017), trying to illustrate interdependencies between social and technological realms (Wilson, 2001) where human behaviour and technical functions create a system of systems (Systems Engineering Body of Knowledge, 2024). Moreover, it fosters the interaction between different layers of thinking in cyber defence, mainly at technological, tactical, operational, and strategic levels (Liddell Hart, 1991). Furthermore, it recognises the boundaries of Western Military culture, thinking, and values concerning competition, confrontation, conflict, and war (Fox, 2023).

Since the research aims to develop a model and test its viability, the epistemological approach is knowing through making. Hence, the research method uses the standard research process of design sciences, i.e., recognising the problem, surveying optional solutions, developing a solution, and evaluating the solution's feasibility (Shuttleworth, 2008). Finally, the feasibility testing of the created model follows the systems analysis methods (Mobus & Kalton, 2015).

The design architecture for the model uses Beer's cybernetical approach to the Viable Systems Model, VSM (Beer, 1995), to set the foundational business strategic and operations levels and their interfaces aiming for the organisation to survive in a military environment (Beer, 1981). Furthermore, the VSM sets essential control and information channels between the strategic and operational functions supporting a dynamic organisation (Jackson, 2019). The security political (Lowe, Espinosa, & Yearworth, 2020) and defence strategic (Liddell Hart, 1991) structures amend the VSM model and link organisations to broader society and state context. The operation of the VSM model is replaced with a concept of joint operations (Vego, 2007) to gain a force utilisation approach and tactics (Friedman, 2017) to reflect the combined arms nature of confrontation in cyberspace. The technical level construction follows the established standards for governance of information technology ISO 38500 (ISO/IEC, 2024), information security ISO 27001 (ISO/IEC, 2022) and cybersecurity framework (NIST, 2024).

4. Results and Discussion

The research tested the Cyber Defence Model with three use cases for feasibility in real-world events. The technical/tactical test case follows common military tactical practices applied in the cyber domain (Oliviero, 2021). Operational testing follows operational art disciplines (Friedman, 2021). Strategic testing criteria are deduced from common military-strategic approaches (Oliviero, 2022). Table 1 summarises the test cases, assumed behaviour per the model, and results against the criteria.

Table 1: Testing the feasibility of the Cyber Defence Model with three test cases

Test case	Action per Model	Results
The Cybersecurity Operation Centre (CSOC) does not receive log data from servers, firewalls, IDS, switches, or routers. The Network Operation Centre (NOC) indicates it has lost connection to several servers, switches and routers. The physical Security Operation Centre (PSOC) has lost all video and sensor feeds from Data Center A.	Tactical and technical level Operation Centres may take the following actions: Confirm the possible loss of an entire Data Centre from other sources Assess the gravity of the situation and draft Courses of Action (CoA) for remedy and communicate them to Operation Control Monitor the process of automated recovery of data and services and launch possible manual remedies Get recovery priorities and decide on CoA from Operation Control Launch required additional remedies to recover and restore data and services based on agreed CoA and priorities. Inform Operation Control and end users of the recovery progress.	**Situational Awareness**: A fused and shared situational picture at the technical and tactical level provides higher-quality sense-making with more information. **Pace of OODA**[1]: The model follows common lines of C3 without additional delays. **Cooperation**: Horizontal cooperation and data transfer between CSOC, NOC, and PSOC facilitates swift tactical action. **Time to recover**: Preplanned and exercised ways of recovery shorten the suppression time.
BLUE information exchange and cooperation between government agencies are harassed by continuous spear-phishing through the Internet email system. After some dignitaries become victims of phishing and have their data wiped, users are afraid to open attachments, even from known senders, and quickly lose their trust in the email system.	BLUE Cyber Defence Operation planning may come up with the following means to mitigate the quickly escalating situation: Launch awareness campaign Lessen the probability of opening malevolent attachments by encrypting all official emails and attached files. Only encrypted emails are safe. Replace email with a cloud-based	**Administration**: Includes recovering the cognitive and social structures **Information**: Ensures the integrity of information as soon as possible **Coordination**: Uses several tactical actions to recover from attack **Fire/Support**: Considers ways to impact the attacker through various domains and means **Command and Control**: Ability to command and coordinate the tactical action

[1] OODA = Observe, Orient, Decide and Act -loop model illustrating the military sensor-commander-shooter process at battle technics and tactics

Test case	Action per Model	Results
	digital workspace and establish users' access to this service through encrypted sessions. Bypass the Internet-based information exchange by extending and sharing existing intranet services between government agencies. Starts target acquisition and considers suppressing the spear-phisher	of several governmental agencies and service providers
There are indications that RED aims to use artificial intelligence to automate and multiply its exploitation arms, achieving attack vectors that are ten times faster within the next ten years.	BLUE strategic planning may conclude the following actions: Accelerate BLUE's development and innovation for a more resilient cyber environment and countermeasure tools Eliminate RED's ability to execute the disruptive leap in offensive capabilities Build BLUE's target acquisition and attacking tools and strike the strikers Change the architecture of BLUE's cyber environment so it will nullify RED's higher performance Build a more robust and redundant cyber environment that could absorb ten times more Attacker's attempts. Train the nation to be non-fragile and more resilient as a society. Consider isolation from the Internet to prevent adversary freedom of movement	**Social/Cultural**: recognises the dimension in strategic enablers **Cognitive/Competency:** considers innovation acceleration in competition **Technology/Industry**: considers national and partner assets in industrial development **Force Generation**: considers building more offensive force to counter adversarial developments **Endurance of resources**: considers society's endurance during extended military and cyber offensive

5. Conclusion

Cybersecurity experts seldom understand the higher levels of cyber defence planning and execution. On the other hand, military officers do not understand the difference between the cyber environment and the operational domain. Therefore, this paper designs a layered Cyber Defence model and proves its viability with use cases.

This paper approaches the differences between cyberspace and other military domains. In designing the cyber defence model, it considers different dependencies between entities and the environment, different paces of evolution and possible revolutions, a broader spectrum of engagement, and a close connection to physical and cognitive realms. The overall framework for the model fuses various approaches from general systems design, business structures, and military tenets and principles.

The Cyber Defence Model's technical level is based on good practices but recognises the close connection between information security, cybersecurity, network operations, and tactical mission command. Tactical-level Cyber Defence combines practices from cybersecurity and military tactics. The Model illustrates improved situational awareness, faster OODA, horizontal cooperation, and faster recovery time.

The operational-level Cyber Defence Model combines the contemporary art of war at physical, information, and cognitive levels of confrontation. It illustrates improved administrative, information, coordination, fire support, and Command and Control features. The strategic-level Cyber Defence Model is based on the competition of cyber powers and introduces a broader spectrum of strategic means and ways to achieve the end state. The Model recognises social, cognitive, industrial, force, and strategic endurance dimensions in strategic planning and preparation.

Integrating cybersecurity with levels of war and framing it within military affairs, the Cyber Defence Model establishes a foundation for national and military strategic cyber defence planning, doctrine work, campaign planning, and operational execution and connects cybersecurity with military tactical and operational levels.

The proposed Cyber Defence Model reflects a European threat environment based on European military cultural and cognitive traditions. Hence, the Model cannot be applied directly to any military or national Cyber Defence. Each nation is uniquely positioned, and the regional threat environment differs even between neighbouring countries. Further research is required to use the model more widely or in specific situations.

Ethical clearance was not required for this research. Only proofreading with Grammarly may use artificial intelligence support; no other application of AI was used in this research.

References

Allison, G., Klyman, K., Barbesino, K., & Yan, H. (2021, December). *The Great Tech Rivalry: China vs the U.S.* Retrieved from Belfer Center: https://www.belfercenter.org/publication/great-tech-rivalry-china-vs-us

Atkeson, E. (1977). The dimensions of military strategy. *Strategic Studies Institute*.

Beer, S. (1981). *Brain of the Firm.* Chichester: John Wiley & Sons.

Beer, S. (1995). *Diagnosing the System for Organizations.* London: John Wiley.

Cancian, M. F. (2018). Strategic Surprise. In *Avoiding Coping with Surprise in Great Power Conflicts.* Center for Strategic and International Studies.

Candelon, F., Chenao, Y., & Jun, W. (2019, January). *Get Ready for the Chinese Internet's Next Chapter*. Retrieved from BCG: https://www.bcg.com/publications/2019/get-ready-for-chinese-internet-next-chapter

Clarke, R. A., & Knake, R. K. (2020). *The fifth domain.* New York: Penguin Random House.

De Haas, M. (2011). Russia's military doctrine development 2000 - 2010. In S. J. Blank, *Russian military politics and Russia's 2010 defense doctrine* (pp. 1-62). Carlisle: Strategic Studies Institute.

Fox, A. C. (2023). Western Military Thinking and Breaking Free from the Tetrarch of Modern Military Thinking. *Associate of the United States Army*. Retrieved from https://www.ausa.org/publications/western-military-thinking-and-breaking-free-tetrarch-modern-military-thinking

Friedman, B. (2017). *On tactics - Theory and practise.* Annapolis: Naval Institute Press.

Friedman, B. (2021). *On Operations - Operational art and military disciplines.* Annapolis: Naval Institute Press.

ISO/IEC. (2022). *27001 Information security, cybersecurity and privacy protection — Information security management systems — Requirements.* International Standardization Organization.

ISO/IEC. (2024). *Information technology — Governance of IT for the organisation.* International Organization for Standardization.

Jackson, M. C. (2019). *Critical systems thinking and the management of complexity.* Chichester: John Wiley & Sons.

Libicki, M. C. (2021). *Cyberspace in peace and war.* Annapolis: Naval Institute Press.

Liddell Hart, B. H. (1991). *Strategy, second revised edition.* Plume.

Lopez, C. T. (2024, February). *U.S. Can Respond Decisively to Cyber Threat Posed by China*. Retrieved from U.S. Department of Defense: https://www.defense.gov/News/News-Stories/Article/Article/3663799/us-can-respond-decisively-to-cyber-threat-posed-by-china/

Lowe, D., Espinosa, A., & Yearworth, M. (2020). Constitutive rules for guiding the use of the viable system model: Reflections on practice. *European Journal of Operational Research*, 1014-1035.

Man III, E. C., Endersby, G., & Searle, T. A. (2002). *Effects-Based Methodology for Joint Operations.* Air University Press.

Mattila, J. K. (2022). A Model for State Cyber Power: Case Study of Russian Behaviour. *Proceedings of the 21st European Conference on Cyber Warfare and Security* (pp. 188-197). Chester, UK: Academic Conferences International.

Mattila, J. K. (2024). Arranging the Defence of the Cyber Environment as a Part of Military Affairs: Tactical, Operational and Strategic approach in retrospect of The Russian -Ukrainian War 2022. *Proceedings of the 23rd European Conference on Cyber Warfare and Security, Vol. 23 No. 1* (pp. 296 - 304). Jyvaskyla: Academic Conferences International.

Mattila, J. K., & Parkinson, S. (2017). Evolution of Military Information Security, *University College Dublin.* Dublin.

McLaughlin, M. G., & Holstein, W. J. (2023). *Battlefield Cyber.* Lanham: Prometheus Books.

Mighty staff. (2023, March). *Russian soldiers in Ukraine are being hunted using social media*. Retrieved from We are the Mighty: https://www.wearethemighty.com/articles/russian-soldiers-in-ukraine-are-being-hunted-using-social-media/

Mobus, G. E., & Kalton, M. C. (2015). Systems analysis. In G. E. Mobus, & M. C. Kalton, *Principles of systems science.* New York: Springer.

Moon, K., & Blackman, D. (2017, May 2). *A guide to ontology, epistemology, and philosophical perspectives for interdisciplinary researchers*. Retrieved from Integration and Implementation Insights: https://i2insights.org/2017/05/02/philosophy-for-interdisciplinarity/

NIST. (2024). *Cybersecurity Framework v2.0.* National Institute of Standards and Technology.

NIST. (2025, February). *National Institute of Standards and Technology*. Retrieved from NIST Computer Security Resource Center: https://csrc.nist.gov/publications/sp800

Oliviero, C. S. (2021). *Praxis Tacticum.* Montreal: Double Dagger Books.

Oliviero, C. S. (2022). *Strategia - A primer on theory and strategy.* Montreal: Double Dagger Books.

O'Neill, P. H. (2022, May). *Russia hacked an American satellite company one hour before the Ukraine invasion*. Retrieved from MIT Technology Review: https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/

Raska, M. (2020). *Strategic Competition for Emerging Military Technologies: Comparative Paths and Patterns.* National Defense University Press.

Shuttleworth, M. (2008, April 1). *Case Study Research Design*. Retrieved from Explorable: https://explorable.com/case-study-research-design

Sun, T. (2014). *The Art of War, Illustrated Edition.* New York: Fall River Press.

Systems Engineering Body of Knowledge. (2024, November 25). *Types of Systems*. Retrieved from SEBoKwiki: https://sebokwiki.org/wiki/Types_of_Systems#Systems_of_Systems

The Law Institute. (2023, November). *The Convergence of The Hague and Geneva Laws in Modern International Law*. Retrieved from The Law Institute International Humanitarian Law: https://thelaw.institute/understanding-ihl/convergence-hague-geneva-laws-international-law/

Total Military Insight. (2024, June). *The Evolution of Cyber Warfare Tactics: Adaptation and Innovation*. Retrieved from Total Military Insight: https://totalmilitaryinsight.com/evolution-of-cyber-warfare-tactics/

Tuned into Security. (2024, October). *Real-World Case Studies: In-Depth Analyses of Major Cyber Incidents and Their Implications for Security Practices - Tuned into Security*. Retrieved from Tuned into Security: https://www.tunedsecurity.com/real-world-case-studies-in-depth-analyses-of-major-cyber-incidents-and-their-implications-for-security-practices/

Vego, M.N. (2007). *Joint Operational Warfare. Theory and practice.* Newport: Naval War College.

von Clausewitz, C. (1984). *On War.* Princeton: Princeton University Press.

Kirby, J. (2024). *On-the-Record Press Gaggle by White House National Security Communications Advisor John Kirby.* Washington: US Government.

Whyte, C., & Mazanec, B. M. (2023). *Understanding cyber warfare, 2nd edition.* New York: Routledge.

Wikipedia. (2024). *Military Tactics*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Military_tactics

Williams, J. (2020, December). *What You Need to Know About the SolarWinds Supply-Chain Attack*. Retrieved from SANS: https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/

Wilson, J. R. (2001). Fundamentals of Ergonomics in Theory and Practice. *Applied Ergonomics*, 557 - 567.

Wolff, J. (2021, July). *Understanding Russia's cyber strategy*. Retrieved from Foreign Policy Research Institute: https://www.fpri.org/article/2021/07/understanding-russias-cyber-strategy/