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

Juha Kai Mattila
Aalto University, Espoo, Finland

Juhakaimattila24@gmail.com

Abstract: The artificial cyber environment has reached national security interest and emerged as the fourth domain of battle in the military concept of all-domain operations in most Western armed forces and coalitions in the past 30 years. Currently, militaries are struggling to keep up with cybercriminals and advanced persistent actors while trying to gain an advantage of their data and digital infrastructure. The paper focuses on military affairs' ways and means to address the need for cyber warriors operating in friendly, neutral, and hostile cyber environments integrated under Multi-Domain Operations. The paper uses design research methodology to create and test a model for cyber defence capabilities generation and utilisation. The theoretical reference to military affairs is based on Beer's Viable System Model and previous studies of military organisations' evolution as capability generators. The military and societal cyber environment evolution model is based on industrial revolutions and current tendencies. These approaches define a hypothetical model for two main functions of military affairs (force generation and utilisation) concerning cyber defence capabilities. The fast evolution of cyber threats sets unique requirements for cyber force utilisation and generation structures. This difference has culminated in a recent war between Russia and Ukraine, and data from that conflict is used to test the hypothetical model. The rapid evolution of the cyber environment and its weaponisation establish different requirements for military cyber capabilities compared to any other operational dimension or capability (space, air, land, or maritime). The difference is evident in sourcing resources, generating capabilities, and using them in Multi-Domain Operations. The paper provides a tested model for generating cyber defence capabilities at a strategic level and an operation model for cyber defence at a tactical and operational level. The designed model extends the technically oriented cybersecurity thinking with operational and strategic levels. Furthermore, the model introduces the value stream behind the cyber capability acquisition and supports strategic designers in national and military analysis.

Keywords: Cyber Defence, Multi-Domain Battle, Cyber Conflict, Military Affairs, Cyber Operations

1. Introduction

Within the previous two decades, the cyber environment has become the fourth military domain (NATO, 2023). However, its nature as an artificial, continuously evolving environment establishes an unprecedented challenge to military operators and force generators in fulfilling the joint operation needs alongside other domains (space/air, land, and maritime). Contemporary military operations require multi-domain, coalition, and inter-agency interoperability. Therefore, one separately well-secured and monitored Information and Telecommunications Technology (ICT) domain needs to be connected to other domains, which may not be as well-secured. Every cross-domain gateway in the defence network will increase the vulnerable surface and the adversary's attack options. (Tidjon, et al., 2019) Any breach of trust between domains will halt the cooperation and lower the operational performance. Therefore, trust relationships are lucrative targets for advanced adversaries. (NATO, 2021)

Cyberspace is an artificial, evolutionary environment that needs to be defined from popular, governmental, and military viewpoints in this research. The core definition, according to Wikipedia, is "Cyberspace is an interconnected digital environment." (Wikipedia, 2023) From the military approach, the previous artificial technical environment may seem like "Cyberspace is contested at all times as malign actors increasingly seek to destabilise the Alliance by employing malicious cyber activities and campaigns. Potential adversaries seek to degrade our critical infrastructure, interfere with our government services, extract intelligence, steal intellectual property and impede our military activities." (NATO, 2023)

From different viewpoints, the same environment may be perceived as a risk source for business. For instance, the NIST Cybersecurity Framework aims for a "systematic process for identifying, assessing, and managing cybersecurity risk." (NIST, 2018) Cyber defence is the same operational level approach in the military: "to protect its networks, operate in cyberspace (including through the Alliance's operations and missions), help Allies to enhance their national resilience and provide a platform for political consultation and collective action." (NATO, 2023)

Furthermore, in contemporary military operational art, the Multi-Domain Operations recognise Cyberspace as one of the five areas of operation: "Within NATO's structure, there are five areas of operations: Maritime, Land, Air, Space and Cyberspace. Given the speed of information, data flows, and adversarial capabilities, orchestrating military activities across all domains as a single force is crucial for long-term defence and deterrence initiatives within NATO." (NATO, 2023) Hence, the convergence or at least the orchestration of action over several operation areas is crucial. Other military establishments perceive added value from a multi-domain approach but in different combinations. Russia continues its successful information operation line with technical support from Cyberspace. (Mattila, 2022) On the other hand, the Chinese military seeks to conduct complex information operations using space, electromagnetic, cyber, and cognitive areas to gain information dominance. (CSIS, 2019)

Military generate their cyber capabilities differently than force elements for the other domains. (Mattila, 2022) U.S. DoD sources its defence industrial network to educate cyber teams for the Services and Cyber Command. Russia started its cyber capability development by exploiting cybercriminal organisations enjoying sanctuary in the nation. Iran uses an ideological base for motivation and cultivates digital competencies in universities, para-military organisations, and educating selected individuals abroad. Ukraine recruited their I.T. Army of Ukraine based on patriot citizens' willingness to contribute to national cyber actions using easy tools available on the Internet.

The paper provides a framework and an operation model to support military affairs addressing the fast-evolving technical competition, information contest, and state-level conflict in Cyberspace. Because there are various approaches to utilise and generate military capabilities in cyber environments, most defence strategy planners are seeking the best approach for their nation. Naturally, the approach depends on available resources, population, culture, motivation, the surface of national digital infrastructure, and available tools. A typical multi-variable problem needs a model for understanding the phenomena and design. Hence, the **Research question** is: How should military affairs address the generation and utilisation of cyber defence capabilities in a current cyber environment in the context of state-level defence strategy?

2. Understanding the Problem and Creating a Tentative Design

The paper uses some principles of Capability-Based Planning (CBP) (Despont, 2022) that have been used widely. Hence, the research first compares the cyber domain to other military domains, trying to identify differences that may impact the ways of utilising, generating, and sustaining cyber force. Secondly, the research addresses these differences while creating a high-level design of cyber force based on generic system models, military enterprise evolution models and industrial revolution generations. Finally, the research tests the concept design against three adversarial cyber strategies: operations, capabilities, and generation.

2.1 Why is the Cyber Domain Different From Other Military Domains?

With the rapid digitalisation of critical infrastructure, military systems, governance, public services, and cyber criminality, states have recognised the extended attack surface of their cyber environment. (Ciepiela & Venkateshwaran, 2017) The first task of the research is to identify the differences in the cyber domain, network operations, cyber environment, attack vectors, and adversaries' potential at tactical, operational, and strategic levels compared to other military domains. Table 1 details the comparison and differences between the domains.

Table 1: Comparison between cyber-electromagnetic domain and legacy (Land, Air, Maritime) military domains

Domain/ Level of Warfare	Cyber/Electromagnetic Environment Features	Legacy Military Domains (Air, Land, Maritime) Features	Tenets that may impact the Cyber Force utilisation, generation, and sustainment
Strategic	Volatile and abstract offensive capabilities in everchanging target surface. (Clarke & Knake, 2019) Adversary attribution remains unclear. (Gayde & Neuhaus, 2020)	Credible coercion with tangible force elements against known armament. (Clausewitz, 1984) Attribution of forces and their use is primarily evident; hence, the retaliation has a clear target. (Libicki, 2009)	a)Attackers' advantage and ambiguity expose to strategic surprise. b)Strategic armament stockpiles are volatile as weapons are one-time, and their capability for effect evolves as the environment changes.

Domain/ Level of Warfare	Cyber/Electromagnetic Environment Features	Legacy Military Domains (Air, Land, Maritime) Features	Tenets that may impact the Cyber Force utilisation, generation, and sustainment
Opera-tional	Cyber force is not necessarily organised or has identifiable insignia. (Clarke & Knake, 2010) The impacts of cyber offence operations are not necessarily detectable. (Libicki, 2009) Cyber competencies retention requires continuous training. (NATO, 2019)	Since the Peace of Westphalia, sovereignty has defined the terms for projecting military force. (Kaldor, 2012) The impact of force utilisation is evident.	c)Operating under the threshold of war is a contemporary norm. d)Capability – Impact – Effect causality is nonlinear. e)The operational range is extended, and the attack path is less evident. f)Sourcing cyber force is not constrained to military institutes, on the contrary. g)Retention of cyber competencies requires effort.
Tactical	Navigation in the cyber realm is challenging as reference points for measuring progress are few. (Clarke & Knake, 2019) Errors and mistakes are less distinguishable from intended action. (Libicki, 2009) Malevolent software often spreads wider than the targeted system. (Malwarebytes, 2024)	Navigation and manoeuvring can be referenced with a variety of orienteering means. Massing kinetic force is evident, and crossing state borders is detected. (Friedman, 2017) Command and control of weapons is straightforward. (Creveld, 1987)	h) The Observe – Orient – Decision – Action loop is much faster and more evolutionary. i)Automation and artificial intelligence actors are adopted faster. j)The impact may cause tactical, operational, and strategic effects, so decision-making is ambiguous. k)Collateral damage is more probable.

The differences indicated in the above matrix mean that at least the strategic posture and processes (Mattila & Parkinson, 2018) of military enterprises may need different approaches in cyber force utilisation, generation, and sustainment.

2.2 Creating a Tentative Design or Concept of Operation

Contemporary Military Affairs consist of force utilisation, generation, and support. (Smith, 2005) These three functions may be defined as per military domain, orchestrated at the joint operations level, and governed at the strategic level. Therefore, Beer's Viable System Model (VSM) (Rios, 2012) may be used to illustrate a generic approach to Military Affairs in Figure 1. The cyber domain is included as one of the tactical engagement areas. Tactical cyber activities are orchestrated from the Joint Operations level in concert with other domain activities, and future capability generation is governed from the Military Strategic level using capability portfolios. (U.S. DoD, 2023)

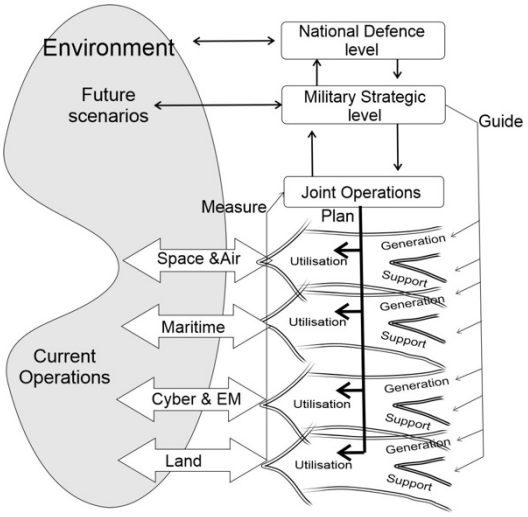

Figure 1: Military Affairs outlined using the Viable System Model

Nevertheless, the above model is not the most feasible or probable way to arrange cyber operations capability within military affairs. Firstly, the socio-technical nature of the cyber environment will impact the arrangements. Secondly, the evolution of military capabilities also introduces power vectors to the evolution of cyber operations. Thirdly, information security creates the foundation for cyber defence and impacts its arrangements.

Since the cyber environment is a Socio-technical system (Pasmore, 1995) and the Internet is also almost an open system, the structure and evolution of cyber operations capability will be defined by the elements: social relations, human cognition, processes, applications and information, machine cognition and hardware. For example, the Russian war against Ukraine has accelerated the use of commercial, cyber-physical devices at the tactical level. Previously, the Armed Forces were slow to adapt to small drones at patrol level. (O'Brien, 2022) Technological development does not solely define the evolution of the cyber environment.

Mattila & Parkinson have studied the evolution of military enterprises using enterprise architecture views and recognise four evolutionary paths for military development (Mattila & Parkinson, 2018):

1. Diversification is typical for newly established capabilities, but gradually, adversaries may drive separate capabilities for more coordinated operations.
2. Coordination seeks combined arms effect and joint operations resource optimisation.
3. Unification happens when unique capabilities are used under the joint task force or command.
4. Replication is critical for generating masses of "citizen armies", and peacetime garrison/base structures prefer replication within the force or branch.

Based on the above evolutionary paths, Cyber operations capability may evolve in military enterprises from diversified units towards coordinated impact and, with sufficient maturity, to unified effects. However, since the omnipresent nature of information technology gave birth to information security and cybersecurity (Lal, 2023), other evolutionary paths are also viable.

Cyber defence operations occur in cyber environments, defined by architecture, controls, network operation, and information security policies. Therefore, the evolution of military information security may have the most decisive impact on defence. The roadmap for military information security (Mattila, 2020) identifies a common evolutionary path from vault/building/site-based mainly physical security to domain-based solutions where connections between sites are encrypted. From domain security, the path proceeds to host-based security, where all actors and their behaviour are monitored. From the host, the path continues towards the service level, currently called the Zero-trust model. The content-based security model is the furthest visible stage. Naturally, the tactical level defence of the cyber environment is differently arranged in each of the above stages.

As a summary, this section outlines a generic model for military affairs, including the cyber dimension, but recognises the volatility of the cyber environment and possible constraints for the design from four viewpoints: 1. constantly evolving, open socio-technical systems; 2. past evolutionary paths for military enterprises defined by strategy, culture, and competencies; and 3. information security strategy and policies of critical cyber environment. The outlined model is projected for different cybersecurity strategies in the next section.

2.3 A Short Analysis of Defence Against Sample Adversarial Strategies

Ultimately, the adversarial resources, capabilities, and intentions define how cyber defence should be arranged. State cyber strategies usually outline the ends, ways, and means for a state to generate and utilise its cyber force. (Eikmeier, 2007). The research chooses three active adversary approaches and analyses their impact on cyber defence (Mattila, 2015):

i. Active defence (NATO), where the actor aims to build a robust domestic cyber environment and does not invest in building offensive cyber capabilities, prefers asymmetric (DIME) counteractions. Defenders benefit from a unified approach over the DIMEFIL dimensions but do not require strong cyber defence capability. (NATO, 2023) (Burton, 2015)
ii. In proactive defence (China), the actor runs a highly controlled and monitored domestic cyber environment. Furthermore, the actor actively exploits and attacks in international and adversary environments as part of joint information operations while staying under the war threshold. Defender faces the race in cyber capabilities and must invest heavily in defensive capabilities. (Baughman & Singer, 2023) (Johnson, 2018) (Saalman, et al., 2022)
iii. In the information war (Iran), the actor exploits the open information space for cognitive impacts and supports information operations with cyber capabilities. Defenders will be manipulated and harassed

until the domestic cyber environment is robust enough. Investment in offensive capabilities may have a systemic effect in conflict situations. (Rubin, 2019) (Erfourth & Bazin, 2020)

The above three scenarios provide the strategic horizon for the research.

3. Research Design

The research approaches the question of "How military affairs should address the generation and utilisation of cyber defence capabilities in the current threat landscape?" from the design science viewpoint since the outcome will be an operation model, i.e., a design of an artificial socio-technical system (Trist, 1981). Hence, the research design follows the sequence of 1. Understanding the problem, 2. Suggesting a tentative design, 3. Developing an artifact, 4. Evaluation performance of the artefact, and 5. Concluding. (Dresch & Anatunes, 2015)

Since the military tends to design the new capability development organisation first (Farrell & Terriff, 2002), the system design approach promotes an alternative toolbox for military transformation planners. The method also aims to show how industrial engineering and management principles can be used in the planning of military socio-technical systems as well as in military-industrial products (Badiru & Thomas, 2009) or health services (Sharma, et al., 2021). The MITRE enterprise system engineering practice (MITRE, 2022) promotes some approaches but does not recognise, for example, the adversarial analysis, evolutionary analysis, or affairs cultural analysis applied in this research.

Naturally, the design science approach has an engineering flavour and may bypass the cognitive and social aspects of the military enterprise system. To compensate for these biases, the research chose Viable system (Espejo, 1990), Military evolution (Mattila, 2020), and Socio-technical system evolution (Trist, 1981) models for the high-level design.

4. Development, Evaluation, and Discussion on Design

Firstly, the section details the cyber affairs model design using the previous sections' tenets, variants, and principal dimensions. Secondly, the section applies the model in analysing the Russia – Ukraine war in 2022. Thirdly, the section assesses the quality and feasibility of the design.

4.1 Detailed Design of Cyber Affairs as Part of Military Enterprise

The Model for Cyber Affairs (CAM) in Figure 2 presents two parties, Blue and Red, in the confrontation in the cyber environment. Red party varies between three sample strategies: Active defence (NATO), Proactive defence (China) and Information Warfare (Iran). Both parties utilise the Internet but also have separate Intranets as part of their Cyberspace. The position of information security in the evolutionary roadmap define mainly the tactical level defensive cyber actions. The combination and complexity of connected cyberspaces define the operational art. The three levels of military affairs culminate in tenets defined in Table 1. The strategic and operational features of the Blue party are categorised in the quad chart, which is composed of Diversified, Coordinated, Replicated, and Unified postures. This version of the model illustrates the cyber value stream through force generation and resource sourcing but excludes sustainment and governance functions for simplification purposes. (Mattila & Parkinson, 2018)

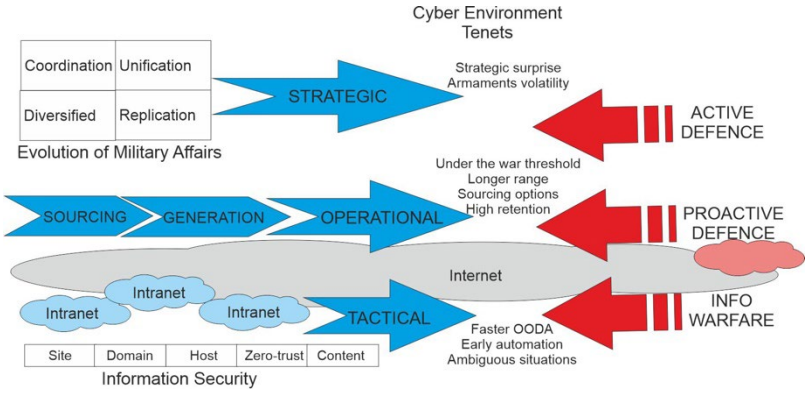

Figure 2: The Model for Cyber Affairs as part of Military Enterprise

The simplification aims to make the model feasible for analysts. Hence, it leaves out other possible strategic postures or variations in confrontation. (Mattila, 2015) It does not include the complexity and dynamics of military enterprise architecture or systems. (Mattila, 2020) Furthermore, the model neglects different sourcing models and their effect on cyber capabilities. (Mattila, 2022) The following step tests how this simplified model works in a complex situation.

4.2 Evaluation of the Cyber Affairs Model Against Observed Data from Russia – Ukraine War

The war between Russia and Ukraine has been ongoing since 2016. However, the 2022 Russian intent to capture the Ukraine capital and replace the democratic regime sets a model for contemporary campaigns where political intent defines military strategy, which is implemented through operations using available military tactical capabilities. (Liddell Hart, 1991) The build-up of the 2022 February offence provided insights into how both parties of war prepared themselves for engagement in the cyber environment and how the offensive proceeded at all three levels of warfare and through four dimensions of tactical engagement. Therefore, the Russo-Ukraine War provides a usable number of data points to test the Cyber Affairs Model.

The confrontation matrix between Ukraine (blue) and Russia (red) in Table 2 illustrates the Cyber Affairs Model in two dimensions: levels of warfare and depth of force value chain. The analysis of confrontation uses the tenets and postures defined in Figure 2. It documents them through the two-dimensional matrix in Table 2 to emphasise the confrontation of two intentions, wills, and capabilities (Oliviero, 2022), often neglected in contemporary cyber operations analysis. The data points are collected from open-source feeds and early analysis published in 2022. (Mattila, A Model for State Cyber Power: Case Study of Russian Behaviour, 2022) (Mattila, Ways to generate a military cyber capability - A review of three countries, 2022)

Table 2: Application example of the Cyber Affairs Model in Russian – Ukraine War during 2022

	UKRAINE		**RUSSIA**	
	GENERATION OF FORCE	**UTILISATION OF FORCE**	**UTILISATION OF FORCE**	**GENERATION OF FORCE**
Strategic	Sourcing of competencies and security services internationally. Information security-based preparedness.	Active Defence Strategy at best: • Passive risk-averse security preparations • Relying on tactical-level partner support • Finally, successful defence is achieved by ad-hoc creativity and coordinated cooperation.	Proactive Defence Strategy: • Strategic shock during the first attack • Terrorising society with info and cyber operations • Breaking trust between government and population with cyber and kinetic operations against critical infrastructure.	FSB and GRU force generation since 2003. Source competencies from private and criminal business. Exploit cyber criminals created open armament and weaponised vulnerabilities.
Opera-tional	Cyber competency sourcing from partners. Quick employment of Cyber Army. Preparations to move critical assets to global clouds.	• Diversified and domain-based reactive cyber defence. • Transfer of critical assets to more protected cloud services. • Use no-trust Internet with global support.	• Coordinated all-domain operations in the beginning. • Afterwards, some planned joint information and kinetic operations. • Later, mainly diversified cyberattack efforts.	Government competition and variety in sourcing end up with sub-optimised resource utilisation at national and battlefield levels.
Tactical	U.S. DoD and Microsoft technical and tactical support. Crowd-sourced information operations and cyber harassment.	Cyber defence is defined by information security based on domain boundaries and host-based monitoring.	Site- or domain-based information security exposes its cyber environment to harassment, but societal functions seem resilient enough to sustain it long-term.	The mass flee of international-level cyber competency may have impacted defensive and offensive capabilities.

The VSM model includes four central systems and their cooperation (Jackson, 2019). The levels of warfare comply with three of them, leaving the audit or lessons identified system out. The lack of inside data prevents the analysis of viability within each system. However, some cooperation features between vertical (strategic-operational-tactical) and horizontal (generate–utilise) systems can be concluded based on impact data and, therefore, test the viability of the CAM. (Schwaninger & Scheef, 2016) The Russian strategic intentions seem to

guide their cyber force generation well, enabling tactical capabilities and linking to force utilisation to achieve strategic surprise and operational shock at the beginning of the offensive. The model also explains the emerging friction between vertical Russian systems when the tactical level failed in the first offensive. However, the strategic level pushed the tactical level for more effort without impacting the operational level.

4.3 Discussion on the Quality and Feasibility of the CAM

The three vertical levels (strategic, operational, and tactical) and three steps in horizontal depth (sourcing, generation, and utilisation) perception in military confrontation provide enough VSM viewpoints for cyber affairs analysis. The two-dimensional CAM improves the thinking behind current tactical-level cybersecurity and risk management standards (NIST, 2018). Furthermore, the CAM may elaborate some national cybersecurity policy approaches that focus narrowly on risk avoidance, compliance, and governance viewpoints. (NSA of Finland, 2021) (NCA KSA, 2018) Naturally, the CAM elaborates on the current event, incident and reactive approach widely provided in the contemporary cybersecurity consultation market (Aiyer, et al., 2022) with operational art and strategic analysis. The CAM may mitigate the challenges the U.S. DoD experienced in fighting against ISIS, and other insurgent groups between 2015 – 2022. (Carter, 2017) Finally, the CAM includes event- and presence-based cyber operations but establishes a broader context for the approach presented by Daniel Moore (Moore, 2022).

The CAM does not capture the differences between NATO's and Russia's thinking on cyber capabilities and their utilisation. NATO perceives cyber as one of the four tactical level dimensions, and the U.K. even pairs it with electronic warfare. However, Russia's operational art sees cyber as a technical multiplier of Information Operations Effects directly supporting their cognitive level warfare. Despite the two dimensions, the art of operation is missed when using the CAM unless this insight guides the analysis.

The CAM helps to illustrate and analyse the challenges in sourcing competent cyber forces, which drive towards different force generation approaches compared to air, land, or maritime domains. The cyber force sourcing variations Ukraine and Russia have used during the ongoing war should open the traditional defence planners' thinking.

5. Conclusions

From the military affairs viewpoint, there is a wide gap between security controls and strategy. Hence, an analysis model is needed to cover all vertical levels of warfare and essential horizontal dimensions of military affairs. Meanwhile, the cyber environment differs from other military domains, so traditional power and engagement models do not necessarily apply to the cyber domain. The paper aims to design a framework and an operation model to support military analysis of the fast-evolving technical competition, information contest, and state-level conflict in Cyberspace.

The paper designs the Cyber Affairs Model (CAM). The paper applies the model in one use case to assess the model's viability. The CAM provides a confrontational operational view to define the story and a matrix to capture the analysis. Based on the test case, the CAM opens the cyber operations thinking, fills the gap between strategies and security controls, and closes the guidance loop between strategic, operational, and tactical levels, which is sometimes missed in national security strategies.

The Cyber Affairs Model provides a framework for strategic analysis and planning concerning state and military-level engagement in the cyber environment. It may reveal significant gaps in existing strategies and help prepare more systematic approaches for future competition or clashes of national interests.

The Cyber Affairs Model presented in this paper leaves out many dimensions from state-level confrontation, provides only a few samples of possible strategies, illustrates military affairs in one snapshot, neglects the evolution and dynamics of the system, and simplifies the model to gain more usability.

Further research should test the model's viability with other case studies, including varying strategies, art of operation, and tactical capabilities. The falsification of the model remains thin in this paper, so further testing should improve the existing approach. The model could use more extensive testing with a higher number of strategic analysts to improve its usability.

References

Aiyer, B., Caso, J., Russell, P., & Sorel, M. (2022). New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers. McKinsey & Company.

Annenko, O. (2022, April 01). 12 New Application Integration Statistics and Trends for 2022. Retrieved from elastic.io: https://www.elastic.io/enterprise-application-integration/application-integration-statistics/

Badiru, A. B., & Thomas, M. U. (2009). Handbook of Military industrial engineering. Boca Raton: CRC Press.

Baughman, J., & Singer, P. W. (2023, April 7). China gears up for cognitive warfare. Defense One.

Burton, J. (2015). NATO's cyber defence: strategic challenges and institutional adaptation. Defence Studies.

Carter, A. (2017). A Lasting Defeat: The Campaign to Destroy ISIS. Cambridge: The Belfer Center.

Ciepiela, P., & Venkateshwaran, B. V. (2017). Evolution of Cyber Threats and the Development of New Security Architecture. 22nd World Petroleum Congress. Istanbul: World Petroleum Council.

Clarke, R. A., & Knake, R. K. (2010). Cyber war. New York: HarperCollins.

Clarke, R. A., & Knake, R. K. (2019). The fifth domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats. London: Penguin Press.

Clausewitz, C. v. (1984). On War. (M. Howard, & P. Paret, Trans.) Princeton: Princeton University Press.

Creveld, M. v. (1987). Command in War (Revised ed.). Harvard University Press.

CSIS. (2019). Advanced Modernisation and Preparation for War: Informatized Warfare, New Force Elements, Cyber, Space, Logistics. Center for Strategic and International Studies.

Dahlqvist, F., Patel, M., Rajko, A., & Schulman, J. (2019, July 22). Growing opportunities in the Internet of Things. Retrieved from McKinsey & Company: https://www.mckinsey.com/industries/private-equity-and-principal-investors/our-insights/growing-opportunities-in-the-internet-of-things

Despont, C. (2022). Understanding CapabilityBased Planning. CSS Analyses in Security Policy, 1-4. Retrieved from https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse298-EN.pdf

Dresch, A., & Anatunes, J. (2015). Design science research. Geneve: Springer International Publishing.

Drinhausen, K., & Legarda, H. (2022). Confident paranoia: Xi’s "comprehensive national security" framework shapes China’s behavior at home and abroad. Berlin: Mercator Institute for China Studies.

Eikmeier, D. C. (2007). A logical method for center of gravity analysis. Military Review, 62-66.

Erfourth, M., & Bazin, A. (2020). The Iranian Pursuit of Military Advantage: A Forecast for the Next Seven Years. Mad Scientist Laboratory. Retrieved from https://madsciblog.tradoc.army.mil/241-the-iranian-pursuit-of-military-advantage-a-forecast-for-the-next-seven-years/

Espejo, R. (1990). The Viable System Model. Systemic Practice and Action Research 3(3), 219-221. Retrieved from https://www.researchgate.net/publication/225863384_The_Viable_System_Model

Farrell, T., & Terriff, T. (2002). The sources of military change: Culture, politics, technology. Boulder: Lynne Rienner.

Fernandes, T., & Ackerson, D. (2022, June 02). 5 Ways to Run Faster CI/CD Builds. Retrieved from Semaphore: https://semaphoreci.com/blog/run-faster-ci-cd-builds

Forrester. (2019). Why Faster Refresh Cycles And Modern Infrastructure Management Are Critical To Business Success. Forrester Consulting.

Friedman, B. A. (2017). On Tactics: A Theory of Victory in Battle. Annapolis: Naval Institute Press.

Gambrell, J. (2018). Iran deploys 'halal' Internet in latest bid to rein in citizens' web freedoms. Independent.

Gayde, A., & Neuhaus, J. (2020, August 12). Five critical data source considerations for adversary attribution. Retrieved from NISOS - Managed Intelligence company: https://www.nisos.com/blog/5-adversary-attribution-tips/

Gilles, K. (2017). Assessing Russia's reorganised and rearmed military. Washington, DC: Carnegie. Retrieved from https://carnegieendowment.org/2017/05/03/assessing-russia-s-reorganized-and-rearmed-military-pub-69853

Hofstede, G., Hofstede, G. J., & Minkov, M. (2010). Cultures and Organisations: Software of the Mind. 3rd Edition. McGraw-Hill.

Jackson, M. C. (2019). Critical Systems Thinking and the Management of Complexity. Wiley.

Johnson, J. S. (2018). China's vision of the future is network-centric. Comparative Strategy, 373-390.

Kaldor, M. (2012). New and Old Wars 3.Ed. Cambridge: Polity Press.

Lal, A. (2023, August 14). The Evolution Of Cybersecurity And How Businesses Can Prepare For The Future. Retrieved from Forbes: https://www.forbes.com/sites/forbesbusinesscouncil/2023/08/14/the-evolution-of-cybersecurity-and-how-businesses-can-prepare-for-the-future/

Libicki, M. C. (2009). Why the Purpose of the Original Cyberattack Matters. In M. C. Libicki, Cyberdeterrence and Cyberwar (pp. 75-89). Santa Monica: RAND Corporation.

Liddell Hart, B. H. (1991). Strategy, 2nd Revision. London: Plume.

Malwarebytes. (2024). What are Petya and NotPetya ransomware? Retrieved from Malwarebytes: https://www.malwarebytes.com/petya-and-notpetya

Mattila, J. K. (2015). Protecting national assets against Information Operations in Post-modern world. 2nd BCS International I.T. conference. Abu Dhabi.

Mattila, J. K. (2020). Engaging a Moving Organisation - Modelling a military enterprise with architecture tools. Helsinki: Aalto University. doi:10.13140/RG.2.2.10167.85927

Mattila, J. K. (2022). A Model for State Cyber Power: Case Study of Russian Behaviour. In T. Eze, N. Khan, & C. Onwubiko, Proceedings of the 21st European Conference on Cyber Warfare and Security (pp. 188-197). Reading, U.K.: Academic Conferences International Ltd.

Mattila, J. K. (2022). Ways to generate a military cyber capability - A review of three countries. In C. Fachada, C. Gil, & R. Marreiros, Conference of the International Society of Military Sciences 2022 - Book of Abstracts (pp. 81-82). Lisbon: Military University Institute of Portugal.

Mattila, J. K., & Parkinson, S. (2018). Quo Vadis, Militare? Evolution of Military Affairs from a Business Architecture Viewpoint. Kungliga Krigsvetenskapsakademien Hanglingar och Tidskrift, 151-172.

MITRE. (2022, April 28). Enterprise engineering. Retrieved from MITRE Publications: https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering

MITRE. (2023, December). MITRE ATT&CK. Retrieved from https://attack.mitre.org/

Moore, D. (2022). Offensive Cyber Operations. London: Hurst & Company.

NATO. (2019, February 12). North Atlantic Treaty Organization. Retrieved from New NATO hub will gather the Alliance's cyber defenders: https://www.nato.int/cps/en/natolive/news_163358.htm

NATO. (2021, November 4). REQUEST FOR INNOVATIVE PARTICIPATION (RFIP). Retrieved from Countering Cognitive Warfare: https://www.act.nato.int/wp-content/uploads/2023/05/rfip021109_amdt1.pdf

NATO. (2023, September 14). Cyber defence. Retrieved from https://www.nato.int/cps/en/natohq/topics_78170.htm

NATO. (2023, October 5). Multi-Domain operations in NATO - Explained. Retrieved from https://www.act.nato.int/article/mdo-in-nato-explained/

NCA KSA. (2018). Essential Cybersecurity Controls – 1. Riyadh: National Cybersecurity Authority of KSA.

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity 1.1. National Institute of Standards and Technology .

NSA of Finland. (2021). Information Security Audit Tool. Helsinki: Traficom publication series.

O'Brien, P. P. (2022). The Future of American Warfare Is Unfolding in Ukraine. The Atlantic.

Oliviero, C. S. (2022). Strategia - A primer on theory and strategy for students of war. Toronto: Double Dagger Books.

Pasmore, W. (1995). Social science transformed - the socio-technical perspective. Human Relations, 48(1), 1-21.

Rios, J. P. (2012). Design and Diagnosis for Sustainable Organisations: The Viable System Method. Verlag: Springer.

Rubin, M. (2019, Agust 08). Iran's Military Is Making Strides into Twenty-first Century Technology. Retrieved from American Enterprise Institute: https://www.aei.org/articles/irans-military-twenty-first-century-technology/

Saalman, L., Su, F., & Dovgal, L. S. (2022). Cyber posture trends in China, Russia, The United States and the European Union. Solna: Stockholm International Pease Reserach Institute.

Schwaninger, M., & Scheef, C. (2016). A Test of the Viable System Model: Theoretical Claim vs. Empirical Evidence. Cybernetics and Systems. doi:10.1080/01969722.2016.1209375

Scwaninger, M. (2006). Design for viable organisations. Kybernetes, 955-966. Retrieved from https://www.alexandria.unisg.ch/31940/1/Design%20for%20Viable%20Organizations_06.pdf

Sharma, G., Prasan, C., & Srinivasa Rao, M. (2021). Industrial engineering into healthcare – A comprehensive review. International Journal of Healthcare Management, 1288-1302.

Smith, R. (2005). The Utility of Force: The Art of War in the Modern World. London: Allen Lane.

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

Tidjon, L. N., Frappier, M., & Mammar, A. (2019). Intrusion Detection Systems: A Cross-Domain Overview. IEEE Communications Surveys & Tutorials, vol 21, 3639-3681.

Traore, Y. (2017, November 17). The utility of military force. Retrieved from War Room online journal: https://warroom.armywarcollege.edu/articles/utility-military-force/

Trist, E. (1981). The evolution of socio-technical systems. Perspectives on Organisational Design and Behaviour(August).

U.S. Army. (2010, July 19). Army force generation. Retrieved from U.S. Army: https://www.army.mil/article/42519/army_force_generation

U.S. DoD. (2023). DOD Directive 7045.20 Capability Portfolio Management. Office of the Under Secretary of Defense for Acquisition and Sustainment .

Vaishnavi, M., & Vineet, K. (2023, July). Operational Technologies Market 2023 - 2032. Retrieved from Allied Market Research: https://www.alliedmarketresearch.com/operational-technologies-market-A136138

Wiki. (2024). Wikipedia. Retrieved from Russian_invasion_of_Ukraine: https://en.wikipedia.org/wiki/Russian_invasion_of_Ukraine

Wikipedia. (2023, December 07). Cyberspace. Retrieved from https://en.wikipedia.org/wiki/Cyberspace

Zhao, P. (2023). Chinese Political Warfare: A Strategic Tautology? The Three Warfares and the Centrality of Political Warfare within Chinese Strategy. The Strategy Bridge.