# A Model for State Cyber Power: Case Study of Russian Behaviour

**Juha Kai Mattila**
**Aalto University, Helsinki, Finland**
juha.mattila@aalto.fi

**Abstract:** The emerging cyber environment with new information channels provides a novel avenue for states to project their powers to govern their residents and fulfil their international ambitions. The recent manipulation of elections, coercing companies, blackmailing citizens, and suppressing essential infrastructure services reflects an increased activity and development both by state and non-state entities in the cyber environment. Several models for inter-state power projection are created in studies of international relationships, military strategy, and, recently, hybrid warfare. Do these models recognise the foundational transformation in international power projection? Do they explain the current national cyber strategies? Can they help foresee the possible developments of power projection in international confrontations? The paper seeks a bigger picture from other power strategies in fulfilling the state's political ambitions. Furthermore, the paper explores the evolution of the cyber environment and its possible emerging features for international power projection. A constructive research method builds a multiple domain power projection model by combining systems thinking with various models from international relationships, military strategies, business strategies to classical decision making. Finally, the feasibility of the model is tested in a case study of Russian cyber strategies and actions between 2007-2020 from a positivistic approach. As a result, the model seems to help explain the past cyber power-wielding and provide insights into current national cyber policies. Further testing is required to evaluate the model's feasibility in creating a foresight. Nevertheless, the proposed state-level cyber power projection model extends the existing models with a system dynamics viewpoint. Additionally, it adds the dimension of evolution to consider the future changes of international power projections in the information realm. Hence, the model improves the ability of national defence planners to study cyber strategies and estimate the lines of operation and impact of cyber operations.

**Keywords:** cyber domain, state power, international relationships, modelling, cyber strategy, and cyber operations

## 1. Introduction

In the early 1990s, an imagined cyberwar was perceived as a culmination of non-kinetic wars that would disarm and disable a whole society without killing masses of people. (Arquilla & Ronfeldt, 1993) That has not been the reality yet. (Rid, 2013) Nevertheless, technology and digitalisation are transforming the ways of politics (Cederberg, 2020), economy (Zuboff, 2019), social life (Dwyer & Kreier, 2015), education (McCamey, Wilson, & Shaw, 2015), industry (Schwab, 2016), and eventually also military (Fiott, 2020). For example, Russia has used cyber power as part of its operations in Estonia 2007, Georgia 2008, and Ukraine 2014. (Clark, 2020) How can one understand novel avenues of impact emerging from the seemingly volatile, uncertain, complex, and ambiguous (VUCA) (Scherrer & Grund, 2009) digital landscape?

Besides the multiple models for power in international relations, the RAND model on assessing risks of cyber terrorism Risk = Threat x Vulnerability x Consequence (Willis, 2006) may still work for the essential risk assessment. The comprehensive model for the national cyber power index, which sums and normalises the outcome of capability and intention, may provide a quantified model to compare state-level cyber powers. (Voo, Hemani, DeSombre, Cassidy, & Schwarzenbach, 2020) Estimating the relative cyber strengths of each nation by considering their cyber defence, dependence, and offence (Clarke & Knake, 2010) features may provide a strategic viewpoint to the question. Nevertheless, it is worth reviewing the model for state-level cyber power in parallel with some ongoing research projects (Tabansky, 2021), (International Institute for Strategic Studies, 2021), (Massachusetts Institute of Technology, 2020), especially when the cyber environment gains space in other realms, relationships become more complicated, the understanding of war and peace is changing, and causality between sensemaking-act-outcome becomes blurred.

The sovereign state has been the dominant global institution since the Peace of Westphalia in 1648. (Nye, 2011) Since then, the transactional relationship between states and wielding diplomatic, trade, and military power has transformed into a globalised network of interrelationships where finance, trade, transportation, manufacturing, energy, and even military cooperation is primarily driving the relationships between contemporary states. (Toffler, 1981) The last decades have seen the most improvement in global living conditions (Roser, 2020) and the least amount of militarised violence being wielded between states since 1648. (Rossling, Rossling Rönnlund, & Rossling, 2018) What kind of hard and soft powers do states wield in trying to affect the behaviour of other states in the era when military power is the least preferred mean?

On the other hand, non-state actors have been actively growing their influence at the international level. In the western hemisphere, the five most significant technology companies, Alphabet, Amazon, Facebook, Apple, and Microsoft (GAFAM) (Wikipedia, 2021), are among the most valuable public companies (Randewich & Ahmed, 2022). They play a significant role in the digital economy (Miguel de Bustos & Izquierdo-Castillo, 2019), social relationships, and so-called surveillance capitalism (Zuboff, 2019). The GAFAM and their Chinese competitors BATX (Baidu, Alibaba, Tencent, and Xiaomi) run platform ecosystems that revolutionise business-to-consumer and business-to-business trade while implementing new technologies like artificial intelligence, big data, on-line-gaming, and payment systems. (Mulrenan, 2020) They build a global cyber environment and wield powers of big data, ecosystems, R&D and end-to-end digitalisation to change the behaviour of individuals, societies, and states. How will these international organisations change the cyber realm and open or close avenues of approach at the data or information level?

Terrorists are using calculated unlawful violence or threat of violence to inculcate fear, intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological. (Theohary & Rollins, 2015) Transnational terrorist organisations, insurgents, and jihadists have used the Internet as a tool for planning attacks, radicalisation and recruitment, a method of propaganda distribution, and a means of communication, and for disruptive purposes. (Rollins & Wilson, 2007) Furthermore, Internet memes (Merriam-Webster, 2022), conspiracy theories (Oliver & Wood, 2014), and other social media-enabled avenues to social behaviour (Amedie, 2015) are opening new approaches to a variety of agents trying to manipulate crowds. What of these emerging abilities states will adopt to their box of international power-wielding tools?

Rather than diving deep into contemporary power-wielding observed in cyberspace, the research aims to approach the phenomena comprehensively. Accordingly, the hypothesis is that a state modelled as a viable system extended with the Clausewitz triangle relationship creates a better artefact to study the interrelationships and fragility of the state structure. Furthermore, the combination of international relation models and doctrines of military power explain the avenues and levels of effort. In addition, the technical and business evolution in the cyber environment needs to be included in the model. Finally, the research tests the created hypothetical model against some factual data gathered from Russian strategies and operations in the cyber environment, i.e., operations against Estonia 2007, Georgia 2008, and Ukraine 2014 (Freedman, 2017) to measure its feasibility.

The paper analyses the features of current models and provides a theoretical foundation for the hypothetical model in section 2, documents the case study of Russian behaviour in a cyber environment in section 3, explains the feasibility of the proposed model in section 4, and concludes the research in section 5.

## 2. Literature research

### 2.1 Existing models and gaps in their perception

The current knowledge base concerning the models for cyber powers, capabilities, or systems includes military, international relations, quantitative indexes, and cybercrime or security viewpoints. (van Haaster, 2016) They have all established their position over the years. However, they seem to exclude some system dynamic (Jackson, 2019, pp. 229–259) features that could explain causalities in VUCA cyberspace and its evolving role as a line of operation or domain between two states, as summarised in Table1.

**Table 1**: Categorising contemporary models for cyber power according to selected components of dynamic system

| Contemporary models for cyber power | Source | Medium | Target | Remarks |
|---|---|---|---|---|
| DIMEFIL lines of operation (Armstrong, 2019) | Assumes a simple source | Primarily categorises the instruments of national power to Diplomatic, Information, Military, Economic, Finance, Intelligence, and Law enforcement. | Assumes a linear impact | A military approach to lines of operation between two states can be used as a context to the cyber realm. |

| Contemporary models for cyber power | Source | Medium | Target | Remarks |
|---|---|---|---|---|
| Betz & Stevens IR model applied to cyberspace (Betz & Stevens, 2011) | Assumes as an unvarying entity | Extends the interstate power relations with ways of Compulsory, Institutional, Structural and Productive ways of wielding power. | Assumes as an unvarying entity | The IR taxonomy of power to analyse cyber power may extend the DIMEFIL. |
| Nye's hard and soft power model for cyberspace (Nye, 2010) | Recognises intra cyberspace where state wields both hard and soft power. Recognises a variety of actors related to cyberspace. | Recognises escalation in relations through cyberspace: shape, create agenda, and confront. | Uses case examples of cyberspace enabling effect in other realms. | Uses both information and physical instruments to cyber power and describes the escalation model. |
| Belfer Center's National Cyber power index (Voo et al., 2020) | Recognises cyber-related infrastructure, public and private behaviour, and assets. | Measures 27 national cyber capabilities against 32 intents. | Recognises seven national objectives that countries pursue using cyber means. | Quantitative approach summing the product of intent and capability over 7 strategic objectives. The strategic approach may be used further. |
| Cyber security (Zaballos & Herranz, 2013) and crime (Mandelcorn, 2013) models | Recognises cognitive and social motivation for actors to engage in cybercrimes. | Recognises the ecosystem that operates and secures cyberspace. | Recognises preparedness and prevention, detection, and reaction processes in defending against the cyber offence. | Models for cyber security and crime prevention may be used as sub-systems. |
| Various cyber strategy analyses (Mattila, 2014) (Lilly & Cheravitch, 2020) | Recognises the national strategic approach related to defensive or offensive cyber activity. | Understands cyber as a part of the information domain and type of warfare. | Introduces views on how a state may perceive cyber-related threats. | Uses, e.g., Nash equilibrium or Russian military studies to make sense of some events in the real world. |

It is evident that the above-reviewed models for cyber power all approach the same subject from a different viewpoint and, thus, fall short to explain the entirety of the phenomena. Therefore, the research approaches contemporary models from system science as the following gaps were recognised:

- 1. Emerging nature of cyberspace concerning time and other realms,
- 2. Dynamics of a state as a system, and
- 3. Different levels of vulnerability and maturity of abilities are available for either of the state entities.

There were other deviations from the system dynamics, but this paper's hypothetical model seeks to address the above gaps in the following subsection.

## 2.2 Hypothetical model

Sub-section generates a hypothetical model addressing the chosen gaps. First, cyberspace needs to be understood as an emerging, man-made realm (Scherrer & Grund, 2009) that is gradually gaining volume through digitalisation, automation, and artificial intelligence. Second, the state needs to be illustrated as a logical system that adjusts to changes in situations, environment, and relationships. Third, the state system's environment needs to be comprehended from existing and emerging threats viewpoints. Fourth, the dynamics of international relations, apparent lines of operation and chosen courses of action between two states or political entities should be considered part of the model.

Cyberspace needs to be understood as an emerging feature in the classical model of the military impact (i.e., physical, information, cognitive and social realms) (Krezer, 2021). Traditionally, militarised violence has changed social behaviour by causing material and human attrition in the physical realm. Survivors of the violence have forwarded information about horrors to other people, whose feelings and beliefs are altered based on the received information. (DoD, 2018 p. 2) When these new feelings and beliefs are confirmed within the social construction, people may change their behaviour. (Zuboff, 2019 p.93-97) That is the simple, linear approach. Whereas, in many revolutions, a force captures control over broadcasting services, starts distributing their information and changes the behaviour of society. Besides, social media has enabled terrorists to distribute videos of their physical violence for a wider audience and thus extending the impact of fear and terror. (Kaldor, 2012) Furthermore, the art of strategy (Sun, 2014, pp. 92–93) aims to conquer or suppress the adversary without fighting by indisposing the adversary's plans and preventing the junction of its forces. The physical attrition on the battlefield, especially against prepared positions, is perceived as the worst scenario. Figure 1 illustrates the cyberspace gradually extending towards the physical, information and cognitive realms and subsequently opening new avenues to create impact and change human behaviour.

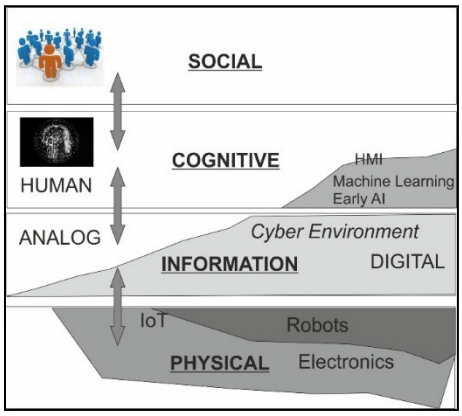


**Figure 1**: A model for evolution and causality in using power to change behaviour, i.e., realms of warfare

The emerging cyber environment in Figure 1 is extending, almost exponentially, both through utilisation and application in most areas of human life (e.g., electronics, robotics, digitalisation, artificial intelligence). The performance of information technology is still improving two times every 18 months (Electrical 4U, 2020). The content of WWW is increasing with over 4 million hours of content every day (Schultz, 2019) which may accumulate human knowledge base at the speed of doubling every 13 months. (Schilling, 2013) The Internet of Things and automation are foreseeing a tenfold expansion during the ongoing decade. (IOT News, 2020)

While improving the model of actor and target, the hypothesis assumes the state as a rational, hierarchical system rather than a network of autonomous nodes. Therefore, it uses Beer's Viable System Model and its improvements (Lowe, Espinosa & Yearworth, 2020) to illustrate the levels of politics, strategy, operations, and tactics as processes to manage action during the confrontation. Besides, the Clausewitz model (Clausewitz, 1984) of state elaborates the VSM with relationships between government, society, and power sources.

Systems thinking sees the open entity constantly interacting with its environment (Arnold & Wade, 2015). Hence, the state should be seen in interrelation with other political entities and threats they perceive against their interests. One of the rights of the sovereign state (Annan, 1999) includes the right to use power to prevent or deter threats to their security. Threats can be perceived differently, but one way to categorise them is existential, global/regional, and intra-state threats, as illustrated in Figure 2.

Naturally, the threat environment is dynamic, but the hypothetic model concentrates, on this occasion, on the interaction between environment and state rather than studying the evolution of threats perceived at a state level.

As a result, the state model is based on VSM (Jackson, 2019, pp. 291-343), illustrating the levels of control (tactical, operational, strategic) and interfaces between organisational bodies and the environment of their viewpoint. The VSM organisation is then elaborated with Clausewitz's state model (Clausewitz, 1984). The triangle relationship between governing entity, society and power institutes explains the lines of interaction within the state itself. It also opens the Centres of Gravity (U.S. DoD, 2015) for the adversary target analysis. The

state uses its powers to impact other states at compulsory, institutional, productive, and structural levels. (Barnett & Duvall, 2005) Furthermore, the previous structure is extended with military levels of interaction in conflict: Political (Vego, 2007), Strategy (Strachan, 2013) (Clausewitz, 1984), Operational art (Strachan, 2013), Tactical (Suvorov, 2015), and Techniques (DoD, 2021, p.214).

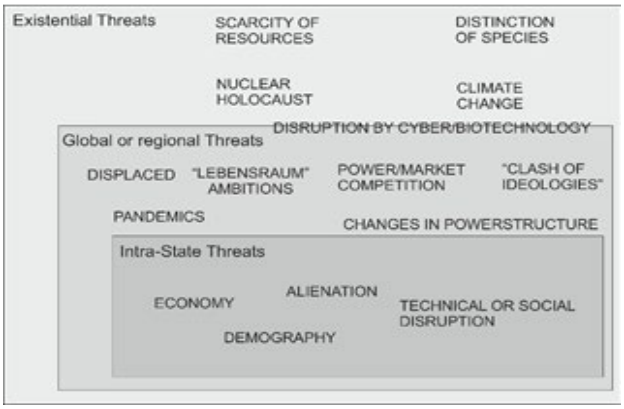


**Figure 2:** An example of threat environment possibly perceived by a state

In conclusion, the hypothetical model illustrates a confrontation between blue and red states using the means of DIMEFIL in the ways of compulsory, institutional, productive, or structural to create impact through evolving cyberspace that exponentially extends its range over physical, information, and cognitive realms. The means are used in ways over the medium to change the adversary's behaviour in the cognitive and social realms. The control of the applied powers follows the hierarchy of political, strategic, operational, tactical, and technics, as illustrated in Figure 3.

The model excludes grand strategy (Liddle Hart, 1991) from the control hierarchy to not open the model towards the sub-system of preparation, building, and directing of all means and ways of state powers. Subsequently, the model does not consider the escalation (Joint Chiefs of Staff, 2015) (Nye, 2010) of international relationships as it would increase the complexity of the model at this stage. Also, the current version of the model excludes individuals' perceptions and formative experiences at political decision making to allow iterative and coherent build-up. (Fuerth, 2009) The following sections will explain how the hypothetical model was tested using a case study of contemporary Russian operations in cyberspace.

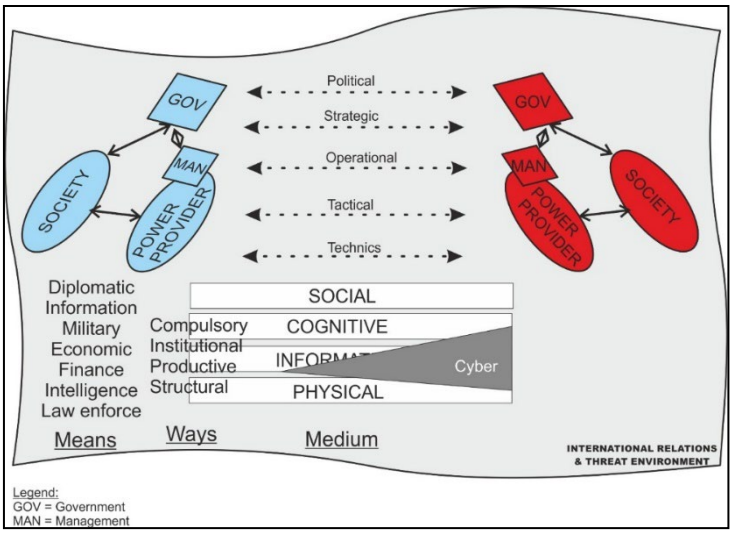


**Figure 3:** Hypothetical model for state-level power system using cyber domain

## 3. Research design

The research process follows the approach of case theory as a process of gap analysis, hypothesis, evidence collection, hypothesis testing and interpretation of results. (Gummersson, 2017, pp. 195–196) The research aims to improve the model of understanding the state-level cyber powers utilisation in a context of the broader spectrum of international relations and focus on a turbulent, man-made domain called cyberspace. The research

approach is pragmatic (Creswell, 2014, pp. 10-11) to create an artefact to model the cyber domain's complex and emerging nature. The viewpoint is more from complexity than positivist posture (Gummersson, 2017 pp. 49-56). Nevertheless, the pragmatic aim requires a model that reflects meaningful simplicity amid apparent disorderly complexity (Simon, 1957).

The model of wielding state-level cyber power is assessed in a case study. Data is a sample of the latest Russian operations, especially from the action along the lines of cyber domain as part of their overall operational behaviour. Russians have used the cyber domain as one line of operation to change the behaviour of Estonian, Georgian, and Ukrainian societies. The cyber incident data should provide evidence of tactical level action. The overall conduction of hybrid operation should provide evidence on thinking at the level of operational art. Finally, the historical and contemporary strategic data should indicate the Russian approach at the strategical level of cyber policies.

Furthermore, the period from 2007 to 2014 provides a view of how cyberspace is extending and how power utilisation is evolving and exploiting the emerging features of information technology on the Internet. The span of data should ensure a sufficient longitudinal line of research to the dynamic nature of cyber operations. However, the time span also increases the complexity of the model and exposes it to ambiguities of system dynamics (Jackson, 2019, pp. 233-240).

The model attempts to meet the system dynamics' expectations by recognising the structure's four hierarchies (Forrester, 1969): boundary around the system, feedback loops within the boundary, level variables representing accumulations and rate variables representing activity within the feedback loops. Naturally, the paper is not aiming to create a holistic system model but a simplified understanding of possible real-life phenomena. The benefits of simplicity include the relations between the organisation and its environment together with sub-systems and their relations with the environment. Naturally, the thinking organisation view does not necessarily illustrate the features of society as living holacracy (Robertson, 2015). For example, it does not reflect well the confrontation between two political entities (Wittes & Blum, 2015) nor the causalities in the case of a failing nation (Acemoglu & Robinson, 2013). Moreover, data has been collected from English sources only and, therefore, possess a bias of western cyber thinking. The bias is recognised, and research tries to remedy it by sourcing from a broader selection of English publications.

## 4. Results and discussion

The case study of how well Russian cyber behaviour can be explained by using the features of the hypothetic model is presented in Table 2. The analysis is a sample of results focusing only on the outstanding features of the model from section 2.1 and their support in rationalising Russian behaviour. The aim is to prove the feasibility of the hypothetical power model.

**Table 2**: Using the hypothetical power model to explain Russian action in cyberspace

| Outstanding features of the power model | Documented Russian behaviour | Explanation based on the model |
|---|---|---|
| A. Emerging cyberspace | 1.2007 combines traditional disinformation operation with DDoS attack in Estonia. | Russia utilises emerging opportunities to divide the opponent's government from its society and create unrest. => Quick exploitation of novel avenues of attack while using criminal hackers as a power provider. |
| | 2.2011 "Under today's conditions, means of information influence have reached a level of development such that they are capable of resolving strategic tasks." (Giles, 2016) | Indicating the strategic role, Russians see how cyberspace opens the avenues of impact to state decision making and public opinion. => Evolution of realms |
| | 3.2011 "Disinformation is a Russian technique to manipulate perceptions and information of people." (Thomas, 2011) | Societies that use extensively social media platforms are exposed to Russian disinformation operations via troll factories. => Digitalisation of information |

| Outstanding features of the power model | Documented Russian behaviour | Explanation based on the model |
|---|---|---|
| | 4.2016 Russian Information Security Doctrine defined the information sphere that includes the technical and cognitive components. (Lilly & Cheravitch, 2020) | Russia recognises a broader sphere of an effect than just the technical layer of cyberspace. => both offensive and defensive cyber power providers. |
| B. Dynamics of state | 1. Information war aims "causing damage to information systems, processes and resources, critically important and other structures, subverting the political, economic and social systems, mass psychological work on the population to destabilise society and state, and coercing the government to take decisions in the interest of opposing side." (Giles, 2012)<br><br>2.1990 – early 2000's FSB employed illegal hackers to attack financial actors in the US and Europe. Since 2013 the GRU has been building a militarily organised information operations force. (Lilly & Cheravitch, 2020)<br><br>3.2008 Georgian operation included a reflexive control through a combination of the pressure of force, opponent's formulation of the initial situation, shaping opponent's objectives, shaping opponent's decision making and the choice of the decision-making moment. (Blandy, 2009)<br><br>4.2014 Russia established the National Defence Control Centre for central planning, coordination and command of all government agencies, state corporations and military commands. It was used to manage Russian involvement in the Syrian Civil War. (Clark, 2020)<br><br>5. As observed in the 2020s: "But its intensive focus on asymmetric measures, and in particular the utility of information warfare for exerting control without the need for overt military intervention, means that the threat from Russian expansionism is far more diverse and nuanced." (Giles, 2021) | Since the 2011 doctrine release, Russia has understood the information layer as a medium to impact the social and decision-making behaviour of the opposing side. => Medium They deem cyberspace part of the information realm (information systems) and extends to the physical realm (critical structures). =>Cyber<br><br>As Internet dependability has evolved, Russia has built a professional force to run offensive operations on the cyber domain. => Initial operational capability achieved with available assets following the build-up of organised full operational capabilities.<br><br>Impact through cyberspace was used as one avenue to manipulate opponent's operational level sense- and decision making. => operational course of action included actions along the cyber line of operation.<br><br>Russia improves its coordination of actions through all lines of operation and shortens the feedback loop between tactical-operational-strategic levels of command. => Improving the orchestration of power provider networks in their particular lines of operation.<br><br>International effect using means and ways suitable for a cyber domain are frequently applied at strategic, operational, and tactical levels. => Cyber is one domain, but the effect is created through courses of action overall domains and lines of operation. |
| C. Vulnerabilities and maturities of cyber-related abilities | 1. "How can you successfully wage an information struggle if during Chechnya a significant part of the mass media is taking the side of the specialists? We need a law on information security." (Giles, 2012)<br><br>2. In the 2014 Ukraine operation Russia was using three different metanarratives distributed through social media, websites, and mass media in coordination with cyber suppression of opposite sources. (Pynnöniemi & Racz, 2016) | The Russian leadership is securing their control over domestic mass media while suppressing the foreign-owned social media to maintain the lines of control over Russian society. => Means & State as system<br><br>Russia used open western social media to promote their narratives while suppressing Ukrainian sources through cyber means. => Exploitation of opportunities and vulnerabilities of international cyberspace |

| Outstanding features of the power model | Documented Russian behaviour | Explanation based on the model |
|---|---|---|
| | 3.2015 Russian military scientists expounded that cyber weapons could endanger not only critical infrastructure but also military systems. (Lilly & Cheravitch, 2020) | Russia recognises the expansion of digitalisation both in the state's critical infrastructure and in military systems. => Digitalisation |

The conclusions in Table 2 indicate that the hypothetical power model can assist in the post-analysis of cyber-related strategies and operations, at least in the case of contemporary Russian behaviour. First, understanding the emergent nature of cyberspace supported the recognition of Russian readiness to use novel ways even when it is not organised by the government but leased from the public sector. However, the agile adaptation happened within the traditional Russian doctrine in joint information and kinetic operations. Hence, the understanding of operational level action requires strategic and policy level foundation and shows that focusing only on cyber technical incidents does not provide foresight because it is not reflected in the broader picture of force projection.

Second, the long period revealed the evolution in the structure of the state concerning cyber capabilities. Russians have been building up their cyber capabilities via organising, recruiting, R&D and improving the control of joint operations. Therefore, the model needs to support the dynamics of the state system over time. Meanwhile, the political and strategical agenda has not evolved that much. On the contrary, there are some similarities in the USSR era policies excluding cyber capabilities. Hence, the model needs to understand the hierarchy of control of the emerging ways as part of the legacy means of projecting international force.

Third, the model needs to illustrate the state as an actor and a target since the case of Russia shows how they, while realising their vulnerabilities and commenced mitigation, exploited cyber vulnerabilities in other countries and the international environment. The effort Russia invested in research and development in cyber-related capabilities also indicate the need for modelling the evolution of cyber vulnerability. In conclusion, the main argument is that cyberspace should not be considered an isolated domain or line of operation. Evidently, a state-level actor like Russia uses emerging cyberspace to manipulate the opponent's behaviour as part of other means and ways.

## 5. Conclusion

The paper presents and validates a model to improve the understanding of state-level use of cyber power in the context of international confrontation. Since the existing models approach the topic from narrower views, the research creates a hypothetical model based on system dynamics to improve understanding in a broader context. Therefore, the model focuses on essential components of a system: state as an actor, environment, the medium that provides the lines of operation and levels of control. Once composed, the model is tested with cyber activity data of Russia spanning over the time of 2007 – 2014 to reflect the evolving nature of cyberspace.

Assessing the feasibility of the proposed model concentrates on three system dynamic features:

- 1. The emergent nature of cyberspace is essential to understand since Russia has been ready to use novel ways even when the capability is not organised but leased. However, since Russia has quickly adapted new ways as part of its traditional doctrine in joint information and kinetic operations, a narrow focus on cyber behaviour does not provide foresight because it is not reflected in the broader picture of force projection.
- 2. Dynamic state features are feasible to model and understand since Russia has been building its cyber capabilities, organising it for greater performance and improved control over joint operations, including action in the cyber domain.
- 3. Vulnerabilities and maturities related to digital capabilities are essential to comprehend as part of the model since case Russia shows how they have realised their vulnerabilities and commenced efforts to mitigate them, exploit them in an international environment and research emerging vulnerabilities.

The proposed model for cyber-related power projection at state-level confrontations is still in its early versions but is already adding value to the existing knowledge base with its system dynamics approach missing from contemporary models. Furthermore, the theoretical approach provides a base for expansion towards capturing more complex dimensions in the equation. Additionally, the benefits for cyber strategy analysts became

concretely evident when analysing the Russian case study. The three system dynamic features of the model opened a more holistic foundation of understanding of each operation.

Naturally, the model and its assessment are in the early phase and have many limitations. First, the case study concerned only one actor and not a typical confrontation of two or more actors. Second, the data may be biased because of English sources. Third, the model is still far from the maturity required for being programmable. Fourth, many dimensions and effectors were left outside this model version, requiring further study. Finally, building on the selected approach and system dynamic foundation requires theoretical research, testing, and evaluation to further mature and extend the model.

## References


Acemoglu, D. & Robinson, J. A., 2013. Why nations fail. 2nd ed. London: Profile Books, Ltd.

Amedie, J., 2015. The impact of social media on society. Advanced Writing: Pop Culture Intersections, Issue 2.

Annan, K., 1999. Two concepts of sovereignty. [Online] Available at: https://www.un.org/sg/en/content/sg/articles/1999-09-18/two-concepts-sovereignty [Retrieved September 2021].

Armstrong, A. H., 2019. Challenges to coordinating the instruments of national power. Baltimore: Johns Hopkins University.

Arnold, R.D., Wade, J.P., 2015. A definition of systems thinking: A systems approach. Procedia Computer Science, 44 pp. 669-678

Arquilla, J. & Ronfeldt, D., 1993. Cyberwar is Coming! Comparative Strategy, Vol 12(2), pp. 141-165.

Barnett, M. & Duvall, R., 2005. Power in International Politics. International Organization, 59(1), pp. 39-75.

Betz, D. J. & Stevens, T., 2011. Cyberspace and the state - toward a strategy for cyber-power. London: Routledge.

Blandy, C., 2009. Provocation, deception, entrapment - The Russo-Georgia five day war. Shrivenham: Defence Academy of the United Kingdom.

Cederberg, A., 2020. A comprehensive cyber security approach - The Finnish model, Helsinki: Cyberwatch Finland.

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

Clark, M., 2020. Russian hybrid warfare. Washington DC: Institute for the Study of War.

Clausewitz, C. v., 1984. On War. New Jersey: Princeton University Press.

Creswell, J. W., 2014. Research design. London: SAGE Publication Inc.

Dwyer, D. S. & Kreier, R., 2015. Internet and Cell Phone Dependence: Too much of a good thing? Melville, NY, Stony Brook.

Electrical 4U, 2020. Moore's Law and The Exponential Growth of Technology. [Online] Available at: https://www.electrical4u.com/moores-law/[Retrieved September 2021].

DoD, 2018. Joint concept for operating in the information environment, JCOIE. Washington DC: The Joint Chiefs of Staff

DoD, 2021. DOD Dictionary of Military and Associated Terms. Washington DC: The Joint Chiefs of Staff

Fiott, D., 2020. Digitalising defence. [Online] Available at: https://www.iss.europa.eu/content/digitalising-defence

Forrester, J. W., 1969. Urban dynamics. Cambridge: MIT Press.

Freedman, L., 2017. The future of war - a history. London: Penguin Books Ltd.

Fuerth, L. 2009 "Cyberpower from the Presidential Perspective." In Cyberpower and National Security, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, 557–62. University of Nebraska Press.

Giles, K., 2012. Russia's public stance on cyberspace issues. Tallinn, NATO CCD COE.

Giles, K., 2016. Handbook of Russian information warfare. Rome: NATO Defense College.

Giles, K., 2021. What deters Russia - Enduring principles for responding to Moscow. London: Chatham House.

Gummersson, E., 2017. Case theory in business and management. London: SAGE Publications Ltd.

International Institute for Strategic Studies, 2021. Cyber capabilities and national power: a net assessment. [Online] Available at: https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power

IOT News, 2020. The IoT in 2030: 24 billion connected things generating $1.5 trillion. [Online] Available at: https://iotbusinessnews.com/2020/05/20/03177-the-iot-in-2030-24-billion-connected-things-generating-1-5-trillion/[Retrieved August 2021].

Jackson, M. C., 2019. Critical systems thinking and the management of complexity. Chichester: Wiley.

Joint Chiefs of Staff, 2015. The national military strategy of the United States of America 2015. Washington D.C.: U.S. DoD

Kaldor, M., 2012. New and old ward. 3rd Edition. Stanford: Stanford University Press.

Krezer, M. P., 2021. Cyberspace is an analogy, not a domain. [Online] Available at: https://thestrategybridge.org/the-bridge/2021/7/8/cyberspace-is-an-analogy-not-a-domain-rethinking-domains-and-layers-of-warfare-for-the-information-age[Accessed September 2021].

Liddle Hart, B. H., 1991. Strategy. 2nd Revised Edition. London: Penguin Books Ltd.

Lilly, B. & Cheravitch, J., 2020. The past, present, and future of Russia's cyber strategy and forces. Tallinn, NATO CCD COE.

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, 287, pp.1014-1035.

Mandelcorn, S. M., 2013. An explanatory model of motivation for cyber-attacks drawn from criminological theories. College Park: University of Maryland.

Massachusetts Institute of Technology, 2020. Cyberpower, Cybersecurity and Cyberconflict. [Online] Available at: https://ecir.mit.edu/research/cyberpower-cybersecurity-and-cyberconflict

Mattila, J. K., 2014. Protecting National Assets against Information Operations in Post-modern World. Abu Dhabi, Proceedings of the 2nd BCS International IT Conference.
McCamey, R., Wilson, B. & Shaw, J., 2015. Internet dependency and academic performance. The Journal of Social Media in Society, pp. 126 - 150.
Merriam-Webster, 2022. Essential meaning of meme. [Online] Available at: https://www.merriam-webster.com/dictionary/meme[Retrieved January 2022].
Miguel de Bustos, J. C. & Izquierdo-Castillo, J., 2019. JC Miguel de Bustos, J Izquierdo-Castillo (2019): "Who will control the media? The impact of GAFAM on the media industries in the digital economy. Revista Latina de Comunicación Social, 74, pp. 803-821.
Mulrenan, S., 2020. China's tech giants take on the FAANGs. [Online] Available at: https://www.ibanet.org/article/D40AD0EC-8C8D-444F-8DB8-431E4F181576
Nye, J. S. J., 2010. Cyber power. Cambridge: Belfer Center for Science and International Affairs.
Nye, J. S. J., 2011. The future of power. New York: Public Affairs.
Oliver, E. J. & Wood, T. J., 2014. Conspiracy theories and the paranoid style of mass opinion. American Journal of Political Science, Vol. 58(4).
Pynnöniemi, K. & Racz, A., 2016. Fog of falsehood - Russian strategy of deception and the conflict in Ukraine. Helsinki: The Finnish Institute of International Affairs.
Randewich, N. & Ahmed, S. I., 2022. Apple's $3 trillion market value follows 5800% gain since iPhone debut. [Online] Available at: https://www.reuters.com./technology/apples-3-trillion-market-value-follows-5800-gain-since-iphone-debut-2022-01-03/[Retrieved January 2022].
Rid, T., 2013. Cyber war will not take place. Oxford: Oxford University Press.
Robertson, B. J., 2015. Holacracy. New York: Henry Holt and Company, LLC.
Rollins, J. & Wilson, C., 2007. Terrorist Capabilities for Cyberattack: Overview and policy issues, Washington DC: Congressional Research Service.
Roser, M., 2020. The short history of global living conditions and why it matters that we know it. [Online] Available at: https://ourworldindata.org/a-history-of-global-living-conditions-in-5-charts
Rossling, H., Rosling Rönnlund, A. & Rosling, O., 2018. Factfulness. Hodder & Stoughton Ltd.
Scherrer, J. H. & Grund, W. C., 2009. A cyberspace command and control model. Maxwell AFB: Air War College.
Schilling, D. R., 2013. Knowledge Doubling Every 12 Months, soon to be Every 12 Hours. [Online] Available at: https://www.industrytap.com/knowledge-doubling-every-12-months-soon-to-be-every-12-hours/3950[Retrieved September 2021].
Schultz, J., 2019. How Much Data is Created on the Internet Each Day? [Online] Available at: https://blog.microfocus.com/how-much-data-is-created-on-the-internet-each-day/[Retrieved August 2021].
Schwab, K., 2016. The fourth industrial revolution. Geneva: World Economic Forum.
Simon, H., 1957. A behavioral model of rational choice. In publication: In models of man, social and rational: Mathematical essays on rational human behaviour in a social setting. New York: Wiley.
Strachan, H., 2013. The direction of war. Cambridge: University Printing House.
Sun, T., 2014. The Art of War - Illustrated edition. New York: Fall River Press.
Suvorov, A., 2015. Voittamisen taito (Art of Winning) Jyväskylä: Docendo Oy.
Tabansky, L., 2021. Towards a theory of cyber power: Security studies, mete-governance, national innovation system. [Online] Available at: https://en-cyber.tau.ac.il/research/theoryofcyberpower
Theohary, C. A. & Rollins, J. W., 2015. Cyberwarfare and Cyberterrorism: In Brief, Washington DC: Congressional Research Service.
Thomas, T. L., 2011. Recasting the red star. Fort Leavenworth: Foreign Military Studies Office.
Toffler, A., 1981. The third wave. New York: Bantam Books.
U.S. DoD, 2015. The center of gravity - systemically understood. Middletown: U.S. Army TRADOC.
Van Haaster, J., 2016. Assessing cyber power. Tallinn, NATO CCD COE Publications.
Vego, M. N., 2007. Joint Operational Warfare. Theory and practice. Newport: Naval War College.
Voo, J. et al., 2020. National cyber power index 2020, Cambridge: Belfer Center for Science and International Affairs.
Wikipedia, 2021. List of public corporations by market capitalisation. [Online] Available at: https://en.wikipedia.org/wiki/List_of_public_corporations_by_market_capitalization
Willis, H. H., 2006. Guiding Resource Allocations Based on Terrorism Risk. [Online] Available at: https://www.rand.org/pubs/working_papers/WR371.html.
Wittes, B. & Blum, G., 2015. The future of violence. New York: Basic Books.
Zaballos, A. G. & Herranz, F. G., 2013. From cybersecurity to cybercrime - a framework for analysis and implementation. Inter-American Development Bank.
Zuboff, S., 2019. The age of surveillance capitalism. New York: Hachette Book Group, Inc.