Security and Defence Quarterly
ISSN 2300-8741 eISSN 2544-994X
2019 June Volume 24 Number 2
https://doi.org/10.35467/sdq/103346

WARGAMING THE CYBER RESILIENCE OF STRUCTURALLY AND TECHNOLOGICALLY DIFFERENT NETWORKS

Heikki LANTTO[1*], Simo HUOPIO[2], Bernt ÅKESSON[2], Juha-Pekka NIKKARILA[2], Marko SUOJANEN[2], Mari RISTOLAINEN[2], Topi TUUKKANEN[2]
[1] *Finnish National Defence University, Helsinki, Finland*
[2] *Finnish Defence Research Agency, Riihimäki, Finland*

Abstract

Based on a review of different analytical frameworks, it is suggested to run a table top cyber wargame when trying to analyse the effects of closed national networks being imposed in the near future. The scope of the wargame is to extract results to show how the resilience of an open national network differs from a closed national network. It is self-evident that the formation process of resilience is different between the diverse systems. The proposed wargame is a two-sided cyber table top wargame. The wargame is based on at least two blue teams, at least one red team and a control team (namely a white team). One blue team is located in the closed national networks and its system relies on closed national network infrastructure. The other blue team operates its system within open network society. By designing, constructing and executing the proposed cyber wargame we argue it is possible to find these differences and similarities as well. Current research improves cyber situation awareness and proposes a direction to be followed when trying to understand the changing circumstances of the cyber space. It also suggests how the research resources could be directed when trying to improve the situation awareness of the closing process.

Keywords: Cyber Defence, Cyber resilience, Wargaming, Closed national network, Russia

* Corresponding author: heikki.lantto@mil.fi

Introduction

It was revealed earlier that Russia has initiated a network closing process that aims to improve its cyber capabilities when compared to its adversaries. Essentially, by 2020, Russia aims to achieve the capability to monitor, control, restrict, and if necessary close the Russian segment of the Internet. If the closing process is successful in its technical groundings, this would cause significant structural changes in cyberspace and create an asymmetric advantage (Kukkola et al. 2017b). Allegedly, the cyber resilience of a closed national network[1, 2] (Kukkola 2018) is different than the remaining open network[3]. Moreover, this resilience may invoke intended or unintended aspirations to shape the cyberspace to their own benefit and could potentially lead to haphazard and even dangerous international political endeavours if unchecked. This paper seeks to develop an analytic approach to evaluate the differences between a closed national network and the open network. Based on our analysis, the initial research could be based on wargaming providing sufficient grounds for later expansion of similar research efforts.

In 2014, the Russian government began to plan for a technical disconnecting of the Russian segment of the Internet (RuNet) from the global Internet (if needed) and conducted a series of exercises to test its feasibility. During summer 2016, Russia declared that RuNet was able to be disconnected from the global Internet by 2020. (Kantyshev Golits'na 2016) Moreover, Russia aims to have technological self-sufficiency and wants to reduce its dependence on imported technology. In addition, there are several countries that wish to question and challenge the US-dominated/led world order, i.e. both structurally and technologically different networks will be emerging in

[1] The concept of a 'closed network nation' is understood in this paper as a nation that is technically able to maintain a closed network, i.e. to operate a nationally governed segment of the Internet that can be technically separated from global Internet. The concept is used without quotation marks hereafter.

[2] The 'closing process' concept refers to the process of establishing standards and developing technology and solutions for the ability to nationally control the reliability, integrity and availability of data transfer, storage and processing. The closing process is related to Internet fragmentation as a phenomenon.

[3] An open network (i.e. global Internet) is defined in this paper as a network based on a multi stakeholder process, non-nation based governance, public-private partnerships, open access and global connectivity. The open network represents part of the global commons – a collective asset that secures freedom of expression, media pluralism, and equal access to knowledge etc. (Choucri 2012, pp. 221-238). Open network nations share the values of open networks and their segment of the Internet is built on those principles. The open network society is a collection of the above defined nations. The concepts open network, open network nation and open network society are used without quotation marks hereafter.

the future. Consequently, it is important to analyse how the features of closed national networks differ from the open society networks at technical, tactical, operational and strategic levels (Kukkola et al. 2017a).

Starting from the application of versatile technologies, the actor that owns closed national network has had many alternatives for implementing the network. Since security and isolation of the network has been the primary design driver, excessive expenses for building proprietary networks of domestic origin is only a secondary factor. For other actors relying on open network technologies, technology selection and building of network-centric and command & control capabilities is hindered by the requirements on the need to connect everything, interoperability, limited technology alternatives from major communications technology providers and all other consequences that follow from picking up those technologies e.g. operating systems, application interfaces and connection alternatives. Using open source software and open architectures improves interoperability and communities of active cyber experts may improve cyber security of those systems by seeking and advertising cyber vulnerabilities but at the same time, key elements of these open networks are available on the Internet to all actors. Therefore, the actor that owns the closed national network has an upper hand on the other who relies on open network, since similar access points as an open network has may not exist. Also, as the network structure, technologies, redundancies, encryption, use cases, procedures and even actors that may be unknown beforehand, the owner of a closed network is many steps ahead in protection of the network in contrast to the owner of an open network. Initial steps for finding out the first access point requires extensive pre-analysis based on information that may not be collected in any other way than getting physically close to the network. Even though part of the network would be investigated physically, the whole closed network might still be built on versatile technologies and different procedures to access services that would complicate adversaries from carrying out cyber activities in this unknown network (Kukkola et al. 2017b).

Analytical Frameworks

As researchers (Kukkola et al. 2017b) allude to, the Russian initiatives, inter alia the Runet 2020, may have, at least in the background, aspirations which can easily be framed under the concept of cyber power (Nye 2011). Within cyberspace, the relative low costs involved, challenges of attribution and inherent asymmetries due to vulnerabilities have led to a situation where ever smaller belligerents have the potential to exercise tools and leverages related to the notion of cyber power. The notion of power itself, however, has been challenged. The interpretations of the definition and constituent elements differ from one stakeholder to another based on their interests and values. Moreover, the notion is highly dependent on the context. However, in order to direct our focus, we shall adopt the following definition (Kuehl 2009, in Kramer et al. 2009):

> *"Cyber power is the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power."*

This definition is most appropriate for our purposes of considering how the Russian initiatives are about to change cyberspace and to influence potential future events. However, with the potential evolution of these, we do not yet have clearly defined context. Therefore, the concept of cyber power would, at the moment, be overkill for our academic scrutiny exploring the potential outcomes of these Russian initiatives being implemented.

Another avenue we could approach when analysing the Russian initiatives could be through the notion of national cyber security, which is widely used in contemporary policy discussions, yet is partly undefined and significantly influenced by individual national context. Klimburg (2012) starts with the notion of national cyber security as:

> *"National Cyber Security is the focused application of specific governmental levers and information assurance principles to public, private and relevant international ICT systems, and their associated content, where these systems directly pertain to national security."*

Based on this definition, he further presents a theoretical framework to analyse national cyber security consisting of:

1. The five mandates: military, intelligence, counter cybercrime, critical infrastructure protection, and cyber diplomacy
2. The three dimensions: governmental, national, international
3. The five dilemmas: economy vs. security, modernization vs. protection, private vs. public sector, data protection vs. information sharing, freedom of expression vs. political stability.

We recognise that the Russian initiatives could well be analysed through this theoretical framework. However, to do so would involve a much more elaborate research programme than currently available to the authors.

Within the defence planning domain, the capability based planning has proliferated since the demise of the Cold War. Capability as a term has different definitions and meanings in different contexts, similarly to what we have already seen earlier in this paper. In the military, capability sometimes refers to objectives, tasks needed to achieve these objectives, or the means of conducting these tasks. The concept is used by various stakeholders and at different levels of planning, which has led to the emergence of a number of capability models within the western military context. However, we shall consider adoption of the Comprehensive Capability Meta Model (CCMM) (Anteroinen 2012). The CCMM presents a horizontal definition of the primary application area of the capability perspective, the stakeholders, relevant process, temporal features and the motivation of each capability perspective. Within the model:

1. The CCMM level 1 defines the scope. For our purposes, we shall label this as Cyber Power. At the national level, the cyber capabilities represented by the notion of Russian Information Security are seen as an element and an instrument of foreign policy. Consequently, this capability level is one of the elements in international relations.
2. The CCMM level 2 defines the business model. At this level, the capability is seen as an ability or a capacity to perform a set of tasks, or an ability to achieve a desired effect. This functional, or business, model is used in planning to avoid potential bias to a particular solution and to develop solutions suitable for a wide range of operations.
3. The CCMM level 3 defines the system model. The military acquisition process often sees the capability as systems. In this perspective, the capability is a conceptual system defining the components of the capability. The system model can also be viewed through different capability lines of development known as DOTMLPFI, where D stands for doctrine, O for organisation, T for Training, M for materiel, L for Leadership, P for personnel, F for facilities and I either for information or Interoperability.
4. The CCMM level 4 is defined through a technology model. The capability is typically seen by the system operators and developers as a technical system or a platform. This technology perspective describes the components of capability rather than the capability itself.
5. The CCMM level 5 is a detailed representation of sub-systems. The sub-systems viewpoint is used to decompose the systems or platforms into modules or sub-systems.

Anteroinen (2012) argues that this detailed representation perspective is crucial in the realisation of the aspired capabilities.

6. The CCMM level 6 depicts the functioning enterprise. As probably the most obvious and visible capability viewpoint, this can be viewed as the ability to control the Russian Internet and for federal organisations to manoeuvre in international cyberspace.

These CCMM levels form an interdependent network of capability views where some views may manifest themselves as real life instances, whereas some are more abstract as depicted in Fig. 1. (Koivisto and Tuukkanen 2017)

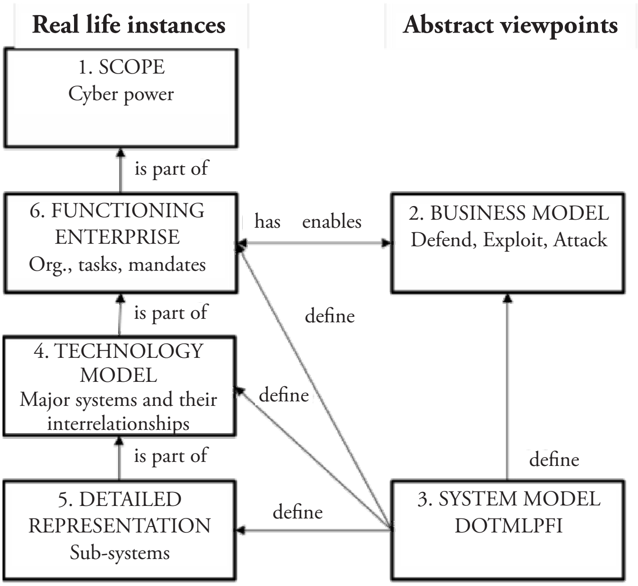

Fig. 1. The CCMM viewpoints arranged into real life and abstract instances (Nye 2011)

Again, we note that the Russian initiatives could well be analysed through the CCMM but, in the absence of resources, we have to seek simpler and more cost effective ways for initial analysis and to provide justification for potential later expansion of such research efforts. Which leads us to the notion of cyber resilience that is relatively well understood within the cyber communities of interest and is, in many ways, considered a central notion. Cyber resilience refers to (Björck et al. 2015)

> *"The ability to continuously deliver the intended outcome despite adverse cyber events".*

The researchers Björck et al. (2015) consider cyber resilience at six different levels: 1) technical; 2) functional; 3) organisational; 4) regional; 5) national; and 6) supranational. For cyber resilience to be effective and efficient, it needs to be addressed holistically and on several levels and in parallel. We aim to use these levels as a framework when evaluating the cyber resilience of structurally and technologically different networks.

It is evident that the resilience is constructed differently in open network based systems when compared to closed national networks. In the closed national networks, resilience may be constructed by controlling and restricting information flows therein. The sought-after resilience can be achieved by controlling and protecting the information infrastructure nationally and by controlling core routers nationally. In the open network, the critical infrastructure is controlled and protected by applying other means, the infrastructure may be decentralised and it may controlled by standards and audits. Modelling the critical infrastructure of a closed national network has just begun (Nikkarila et al. 2018). In open networks, it is not generally possible or even desired to monitor and control the information flows nationally. The service providers both in the critical infrastructure and routing are private companies.

Two-sided[4] wargame on cyber resilience

In the two-sided wargaming, there are two or more opposing teams of players that execute cyber operations on a map or board based playing surface regulated by a set of game controllers (White Cell). The control team does not assist or advise the competing teams in any way. The control team ensure that the actions taken are consistent and determine the outcomes of actions. The competing teams deploy and manoeuvre counters on the map or board in an attempt to achieve their objectives.

In this research, we propose using the format of a table top exercise (TTX[5]) to extract the desired information of the resilience of closed national networks. In practice, the goal

[4] "Number of Sides: The number of sides in a game is determined by the nature of the conflict and the nature of the opposition being gamed and the number of independent entities who can make decisions and take independent action that influence the direction of the game. Games can have 1 side, 1 ½ sides, 2 sides or more. The number of sides does not always equal the number of cells." (Simpson 2017).

[5] Simulation wargames depicting an armed conflict.

- A table-top exercise is a discussion-based wargame where players sit at tables and interact with one another to address the key issues of the wargame. While not specifically structured as a turn based of the table top exercise for participants is to gain a greater understanding of commonalities and differences in approach and capabilities in dealing with cyber resilience of a closed national network. The gameplay is represented on a physical map or board by using counters that represent personnel, equipment, assets and actions. The table top exercise is to use the matrix gaming methodology, which relies on the use of structured argumentation. Actions are proposed and argued for by the player teams in turn and a game controller determines outcomes based on the strength of supporting and opposing arguments. A stochastic method (rolling of dice) can be used to reflect the chance involved in actions if desired. The matrix gaming methodology is limited only by players' imaginations.

Framing the two-sided cyber wargame on cyber resilience

The idea of the wargame (experiment) is to reveal the new properties that a closed national network brings when securing individual systems. It is likely that the establishment of a closed national network causes effects, e.g. situation awareness, and one object of the experiment is to unveil these effects as well. Essentially, we propose experimenting the changed circumstances with different new technologies, strategies or tactics, as well as procedures (TTPs) compared to more traditional ones. This approach is used for development of TTPs not yet connected with any real cyber operation.

At the technical and tactical level, we are considering the two paradigms:

1. open source software, open architectures, industry best practices (hardening of operating systems, configuring of open security products), solid commercial third party products, the ability to fix open source components; and
2. Security by obscurity, tight restrictive rulesets, strict firewalling and segmenting from the outside internet, "Running national Internet as a company intranet"

Notably, we shall consider how these differ when considering national cyber defence at the strategic and operational levels.

We propose setting up a cyber wargame that uses at least one red team against at least two blue teams. In addition, there could be different evaluator teams and an umpire

game, facilitators will often cause players to consider issues in a particular order, to determine the relationship between specific decisions or actions (Simpson 2017).

Security and Defence Quarterly
ISSN 2300-8741 eISSN 2544-994X
2019 June Volume 24 Number 2
https://doi.org/10.35467/sdq/103346

(a so-called White team). One of the blue teams relies on the open network infrastructure and the other on the closed network infrastructure. The red team represents an outside threat and attacks (influences) both of the blue teams simultaneously. In the game, we propose that the blue teams compete on the level of their network's cyber resilience against one red team, i.e. their "ability to continuously deliver the intended outcome despite adverse cyber events" is evaluated. The tools used by the red team are equivalent to a certain extent that enhances the comparability and validity of the exercise. Nevertheless, during the exercise, the red team improves its attack methods depending on their mission success. Results are compared in order to find out the differences in the cyber resilience of studied network infrastructures.

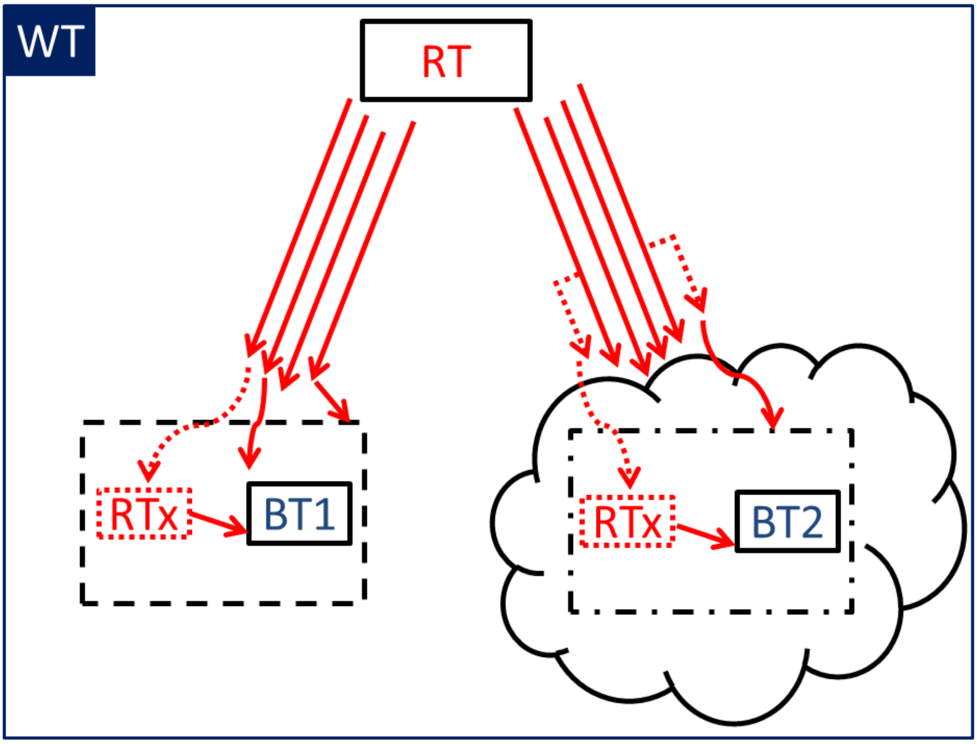

Fig. 2: A schematic outline of the two-sided cyber wargame. The open network is shown on the left. Blue team 1 (BT1) relies on the open network infrastructure (box on dashed line). The closed national network is shown on the right. Blue team 2 (BT2) relies on technologically different network infrastructure (box on dashed-dotted line). Red team (RT) is actively attacking both blue teams and possibly operating inside both networks (RTx). The red arrows represent attack-methods and their variations. Attacks can be targeted both against the infrastructure or the specific blue team systems. The control team (or White team, WT) holds all the knowledge of the game and obtains all occasions therein. Therefore, WT is visualised as a solid line consisting of everything in the game.

The scope of this paper is not to present an exclusive formalism of the suggested wargame. Instead, our aim is show the need for the mentioned wargame and to present exemplary guidelines for its design process. We propose forming representative use cases that may be applied when deriving the actual scenarios of the wargame. For example, one use case could be the usage of a cloud services provider for a company's (or an authority's) internal and external needs. In practice, this could include email and calendar services, shared disks, intranet, and extranet, just as an example. The notional company could operate on international markets either exporting or importing significant amounts of goods (or services), or the qualitative value of the goods is vital for the country in question. The services could also be immaterial like programming. Another use case could be how the closing of the national networks affects citizens' internet services when operating in homeland and or abroad. One could also form a use case where the core services, such as resolving the DNS-address of a foreign website from inside the closed national network, are tested. Additionally, one could also test how standard email services of the closed national networks operate inwards and outwards or how end-to-end encryption is affected by the closing process.

It is worth considering how the red team operates in practice, as the systems are different and the goal is to extract results that are idealistically commensurate. We acknowledge that the results are not necessary commensurate and consequently, the comparison of the two networks is not straightforward. It is also important to value the costs related to the amendments of the closed (and open) network that an actor encounters when it has to fix the vulnerabilities discovered from their proprietary techniques.

Planning and executing the wargame

In the planning phase, the aim is to form a representative picture of the technical structure of a closed national network. The formation of the technical framework structure of previously unknown or significantly different networks requires a substantial amount of research and expertise. Ideally, a multinational group of experts is formed to resolve how the technical functionality of a closed network differs from the functionality of the open network. Furthermore, the most important infrastructure assets (e.g. internet core routing techniques)[6] of the studied networks need to be defined, for example in the form of use cases. These assets contribute to the technical framework that forms the 'game board' and influences the rules of the wargame.

In the following step of the planning phase, the rules of the wargame are defined. These rules include, for instance, what kinds of systems are to be protected by B1 and B2; at which level of cyber resilience these systems are located; what kinds of outcomes the determined systems need to deliver. To quantitatively compare the cyber resilience of different networks, measures of effectiveness (MoEs) need to be defined and the scoring principles need to be included in the rules.

For the wargame to be playable and beneficial, there needs to be certain rules of engagement. The rules of engagement both enable and restrict the RT actions in an appropriate manner. For instance, in a traditional technic level cyber wargame, an initial compromise is guaranteed at the beginning to ensure the playability of the game. In the proposed wargame, it has to be decided whether the initial access is guaranteed or if the game is to be played by applying alternative means. The objectives and means of the RT are defined and phased. Phasing enables profounder analysis of the cyber resilience of the different networks. (What factors do we want to compare in the two networks?)

The overall purpose of the wargame is to unveil the differences in the cyber resilience of a closed national network and the open network. Consequently, all other elements (e.g. RT attacks, BT systems and their operating principles) are standardised, if and when possible and relevant. The authors realise that to construct this wargame on a technical level is extremely challenging. Therefore, we propose to apply table top wargaming at the beginning. The table top wargame workflow could be, for example, as described in the following. A question set has to be formed i.e. the specific questions we want to answer with wargaming. Also, the MoEs, assumptions, abstractions, and rough scenario settings need to be formed. In the proposed case, BT1, BT2 networks have to be defined as well the networks which they are encapsulated in. In the following phase, the wargame rules need to be defined.

Since we are comparing two alternatives, it is vital for the success of the study to ensure commensurability or, if the results are not commensurate by nature, to recognise their non-commensurability. The technical and structural differences between BT1 and BT2

[6] E.g. ENISA's Threat landscape and good practise guide for Internet Infrastructure

networks need to be described in sufficient detail by subject matter experts (SMEs), especially those factors that are expected to influence the MoEs.

- A rule of thumb: things that are to be compared, are to be conducted in detail, the rest with less detail.

At the same time, one has to consider the RT's capabilities and possibilities for action.

All assumptions, abstractions, MoE and other background information need to be documented (a version-controlled living document).

Conclusions

In this article, we have reviewed several potential analytical frameworks and as an intermediate conclusion, we propose setting up a table top cyber wargame that tries to find resilience differences of closed national networks when compared to open networks. The proposed cyber wargame brings more authentic, yet simulated, information of the operational properties of structurally and technologically different networks. It is important to note that the designing, constructing and executing of the proposed wargame requires a substantial amount of expertise from technical up to strategic levels. Consequently, the authors suggest that a multinational team is formed to respond to the challenge. This paper serves as an intermediate step in the continuation of more detailed research that is necessary to understand how the formation of closed national networks affects cyberspace. The authors acknowledge that the work is at the beginning and the situation is constantly changing. However, this research improves the situation awareness and gives potential directions to direct resources.

Acknowledgement: The authors wish to thank Capt Juha Kukkola (Finnish National Defence University) for his valuable comments and opinions during the writing process of this article.

https://doi.org/10.35467/sdq/103346

References

Anteroinen, J., 2012. Integration of existing military capability models into the comprehensive capability meta-model. *IEEE International Systems Conference (SysCon) 2012.*

Björck, F., Henkel, M., Stirna, J., and Zdravkovic, J., 2015. Cyber Resilience – Fundaments for a Definition. In Á.Rocha, A.M. Correia, S. Costanzo, and L.P. Reis (eds.), *New Contributions in Information Systems and Technologies*, pp. 311-316.

Choucri, N., 2012. *Cyberpolitics in International Relations*. MIT Press, Cambridge.

Kantyshev, P., and Golits'na, A. 2016. Runet budet polnost'iu obosoblen k 2020 godu. *Vedomosti,* 13 May.

Klimburg, A., 2012. National Cyber Security Framework Manual, *NATO CCD COE Publication,* Tallinn.

Koivisto, J. and Tuukkanen, T., 2017. Comprehensive capability meta model tested by a cognitive radio. *Military Communications Conference (MILCOM),* IEEE.

Kuehl, D., 2009. From Cyberspace to Cyberpower: Defining the Problem. In F. Kramer, S. Stuart, and L. Wentz (eds), *Cyberpower and National Security*, Washington, D.C., National Defense University Press.

Kukkola, J., 2018. The Russian Segment of Internet as a Resilent Battlefield. *ISMS Annual Conference 2018 "Military Sciences and Future Security Challenges" (ISMS),* Warsaw, Poland.

Kukkola, J., Nikkarila, J-P and Ristolainen, M., 2017a, Shaping Cyberspace – A predictive analysis of adversarial cyber capabilities. *IST-145 specialists' Meeting Predictive Analytics and Analysis in the Cyber Domain,* Sibiu, Romania.

Kukkola, J, Ristolainen, M. and Nikkarila, J-P, 2017b. Game Changer: Structural Transformation of Cyberspace Riihimäki: Finnish Defence Research Agency. [online]. Available: http://puolustusvoimat.fi/web/tutkimus/tutkimuslaitoksen-julkaisut [Accessed 14 May 2018].

Nikkarila, J-P, Åkesson, B., Kuikka, V., and Hämäläinen, J., 2018. Modelling Closed National Networks – Effects in Cyber Operation Capabilities. *17th European Conference on Cyber Warfare and Security (ECCWS),* Oslo, Norway.

Nye, J., 2010. Cyber Power. *Belfer Center for Science and International affairs*. Cambridge MA.

Simpson, W. L., 2017. A Compendium of Wargaming Terms. [online]. Available: https://www.movesinstitute.org/wp-content/uploads/2017/09/WargamingTerms.pdf [Accessed 08 Oct 2018].

Authors:

Heikki Lantto, Maj
Finnish National Defence University, Helsinki, Finland
Simo Huopio, M.Sc.(Tech)
Finnish Defence Research Agency, Riihimäki, Finland

Security and Defence Quarterly
ISSN 2300-8741 eISSN 2544-994X
2019 June Volume 24 Number 2
https://doi.org/10.35467/sdq/103346

Bernt Åkesson, LCdr (Eng), D.Sc.(Tech)
Finnish Defence Research Agency, Riihimäki, Finland
Juha-Pekka Nikkarila, SrLt (Eng) Ph.D
Finnish Defence Research Agency, Riihimäki, Finland
Marko Suojanen, M.Sc.(Tech.)
Finnish Defence Research Agency, Riihimäki, Finland
Mari Ristolainen, Ph.D
Finnish Defence Research Agency, Riihimäki, Finland
Topi Tuukkanen, Cdr (GS)
Finnish Defence Research Agency, Riihimäki, Finland