Role of Techno-Economic Coalitions in Future Cyberspace Governance: 'Backcasting' as a Method for Strategic Foresight

Mari Ristolainen
Finnish Defence Research Agency, Riihimäki, Finland

mari.ristolainen@mil.fi

Abstract: In an increasingly complex threat landscape, many nations struggle with developing and implementing effective cybersecurity policies for cyberspace governance at a national and international level. Balancing between the demands for establishing national sovereignty and strengthening international collaboration in cyberspace have become a problematic assignment. Collaborating with nations supporting extensively dissimilar ideologies and cybersecurity policies is controversial. Yet, it is almost impossible for a single country to achieve 'self-sufficiency' in cyberspace. Thus, in order to remain competitive, protected, and resilient one must either join or strengthen a developing techno-economic coalition with similar national cybersecurity policies and/or ideological framework. Consequently, this paper argues that techno-economic coalitions serve as an emerging issue or trend for strategic foresight in cyberspace governance in the future. This paper discusses the potential formation of techno-economic coalitions and shows how 'backcasting' can be used in strategic foresight. In this paper, 'backcasting' is not used as a method for creating a traditional strategic map to a future goal, but as a framework for determining what should have happened in order for the techno-economic coalitions to emerge in future cyberspace, i.e. for finding issues or trends that should be followed in strategic foresight today. Firstly, cyberspace governance in relation to national cybersecurity policies is contextualised. Secondly, the concept of techno-economic coalition is defined and the potential emerging techno-economic coalitions are explicated. Thirdly, 'backcasting' as a method for strategic foresight is described. Fourthly, the results of a 'backcasting' experiment in a strategic foresight workshop are presented. And finally, the future formation and role of techno-economic coalitions in cyberspace governance and in cyber defence both at a national and international level are discussed. The role of techno-economic coalitions in future cyberspace governance should be understood and considered today when developing strategic plans and implementing national and international cybersecurity policies.

Keywords: National Cybersecurity Policy, Cyberspace Governance, Cyber Defence, Techno-Economic Coalitions, 'Backcasting', Strategic Foresight, Strategic planning

1. Introduction

Many of the security problems in cyberspace can be considered territorial or national (cf. Hare 2010, 214-215; Kovács 2018, 113-114). Contemporary cyber threats are increasingly targeted at national critical infrastructure, economic competitiveness, national security and citizens, both directly and indirectly. Consequently, many nation-states are interested in the safekeeping of their own national cyberspace and their own national systems. The national controllability of cyberspace and the independent defence of various systems add to the sense of cybersecurity (Rautava & Ristolainen 2022, 239-240). However, the cyberspace governance is often not included in national cybersecurity policies. Cyberspace governance requires international and non-territorial cooperation on both policy and technical levels. Therefore, in the increasingly complex threat landscape, many nations struggle with developing and implementing effective cybersecurity policies for cyberspace governance that is leading towards cyberspace territorialisation.

Balancing between the demands for establishing national sovereignty and the strengthening of international collaboration in cyberspace has become a problematic assignment. Moreover, collaborating with nations supporting extensively dissimilar ideologies and cybersecurity policies is controversial. Yet, it is almost impossible for a single country to achieve 'self-sufficiency' in cyberspace. Here 'self-sufficiency' stands for total technical isolation and technical independence over national critical infrastructure, and is to some extent something larger than legal 'sovereignty in cyberspace' (e.g. Liaropoulos 2013, 21-23; Heller 2021, 1498-1499). Thus, in order to remain competitive, protected and resilient one must either join or strengthen developing techno-economic coalitions with similar national cybersecurity policies and/or ideological framework. Consequently, this paper argues that techno-economic coalitions serve as an emerging issue or trend for strategic foresight in the cyberspace governance of the future. This paper discusses the potential formation of techno-economic coalitions and shows how 'backcasting' can be used in strategic foresight. In this paper, 'backcasting' is not used as a method for creating a traditional strategic map to a future goal, but as a method for determining what should have happened in order for the techno-economic coalitions to emerge in future cyberspace, i.e. for finding issues or trends that should be followed in strategic foresight today.

Firstly, cyberspace governance in relation to national cybersecurity policies is contextualised. Secondly, the concept of techno-economic coalition is defined and the potential emerging techno-economic coalitions are explicated. Thirdly, 'backcasting' as a method for strategic foresight is described. Fourthly, the results of a 'backcasting' experiment of a strategic foresight workshop are presented. And finally, the future formation and role of techno-economic coalitions in cyberspace governance and in cyber defence are discussed. This paper claims that the role of techno-economic coalitions in future cyberspace governance should be understood and considered when developing strategic plans and implementing national cybersecurity policies at present.

This paper is exploratory and belongs to the field of strategic foresight that allows more a creative envisioning of potential futures than maybe more traditional academic papers do. Hence, the developments and scenarios presented may to some seem speculative, but it is crucial to develop sustainable methods and frameworks and to preserve the forward-looking mindset, especially within security organisations (cf. Habegger 2022).

2. Cyberspace governance and national cybersecurity policies heading towards 'cyberterritories'

In previous studies (Ristolainen 2021; Rautava & Ristolainen 2022), it has been estimated that cyberspace governance and national cybersecurity policies are progressively heading towards a formation of a so-called 'cyberterritory', i.e. cyberspace is increasingly considered something similar to territorial waters, airspace and/or land area, i.e. the physical areas over which a sovereign state has jurisdiction over. 'Cyberterritory' can be defined as "an entity of networks and technical infrastructure containing services and the data processed in them that are controlled by a sovereign nation-state" (Ristolainen 2021; Rautava & Ristolainen 2022, 243). This development is seen in the change of cyberspace governance models and national cybersecurity policies that aim for particular state 'sovereignty'[1] in cyberspace (ibid.). Essentially, cyberspace governance models are issues of international law that are being resolved within the UN. Nevertheless, the discussions within the UN show that sovereignty and national controllability of cyberspace are emerging within many nations (ibid.). However, sovereignty in legal terms differs, to some extent, from technical 'self-sufficiency' in cyberspace, i.e. a total technical isolation and technical independence over national critical infrastructure.

Therefore, only a few (if any) nation-states could have necessary resources to be truly 'self-sufficient' in cyberspace. Those who could have the resources (e.g. the United States), don't have the need or desire to be 'self-sufficient' in cyberspace. The nation-states that want to be 'self-sufficient' in cyberspace – wish to gain the same position as the United States (or to deny it) – in a political, a technological, a software infrastructure and a standardization level. The aims can be limited to the control of one's own 'cyberterritory' or to the wider control of global information flows. For these countries the closing of 'the national segment of the Internet'[2] (as, for instance, Russia is planning to) and 'self-sufficiency' is reachable and could work in the time of crisis (Kukkola 2020; Kukkola 2021).

When assessing potential future developments, it seems possible that cyberspace governance and national cybersecurity policies are heading increasingly towards 'cyberterritories' that will eventually lead to a formation of new techno-economic coalitions. In order to remain competitive, protected and resilient national 'cyberterritories' must either join or strengthen developing techno-economic coalitions with other nation states sharing similar cybersecurity policies and/or ideological framework.

3. Techno-economic coalitions

'Techno-economic coalition' is an emerging concept (cf. MGIMO 2019; Ristolainen 2021; Rautava & Ristolainen 2022) that can be defined as: "a coalition formed by separate cyberterritories that develop new coalitional level services, which are based on technologies innovated on coalition level, and thus, promote and benefit the

[1] Cyberspace is associated with very different conceptions of sovereignty - often referred as 'digital sovereignty' (Pohle & Thiel, 2020). However, by 'digital sovereignty' is referred frequently to national regulation of data mobility, i.e. 'data sovereignty' (Braud et al. 2021). In one context, 'digital sovereignty' refers to much broader 'information sovereignty' (see, e.g. Yefremov 2017), and in another context, 'digital sovereignty' denotes a 'national segment of the Internet' that can be disconnected from the global network (see, e.g. Kukkola 2020). Thus, there is no single conception of what sovereignty in cyberspace means, although the same concept 'digital sovereignty' is used (more, see, e.g. Rautava & Ristolainen 2022).

[2] The national segment of the Internet can be defined as "a portion of the Internet infrastructure and services which resides on a state's territory and under sovereign jurisdiction" (Kukkola 2020, viii).

economy of the coalition". Techno-economic coalitions could solve the problem of ideological division. Collaborating with nations supporting similar ideologies and cybersecurity policies would be straightforward.

The role of data is central in the differentiation of techno-economic coalitions. Techno-economic coalitions would share certain values and ideology and distinguish themselves from other coalitions by different attitudes towards (personal) data usage and protection. Where other coalitions would, for instance, use data freely for commercial purposes, others for political and/or religious control, there other coalitions would protect (personal) data profoundly. Data would stay within the techno-economic coalition and be protected (confidentiality, integrity, and availability) by the techno-economic coalition. Data security requirements could vary widely between different techno-economic coalitions. The growing role of data is something that should be taken into consideration already in contemporary strategic planning (e.g. choosing cloud services for national sensitive data).

Potential techno-economic coalitions could emerge around the 'Anglosphere' led by the United States; around China; around Russia; around the European Union; around Islamic countries; around criminal and anarchical groups, and (possibly) around a so-called 'wild card' country or commercial consortium (cf. original listing (1-4) MGIMO 2019; additions (5-7) author). In the following, the most reasonable techno-economic coalitions are categorised[3] in more detail.

3.1 America first and others will follow

The 'Anglosphere' techno-economic coalition would be led by the United States. It would be formed around the USA, Canada, United Kingdom, Australia and New Zealand that are economically tightly integrated and their alliance could also be attractive to countries such as Mexico (MGIMO 2019). This coalition would use its privileged position and geographical location in the world to create the best conditions for itself. This techno-economic coalition would use data freely for commercial purposes and the person would be a product of the business both legally and technically.

3.2 Digital silk road

Similarly, China would be expanding its coalition with neighbouring countries and the Middle East and Africa – tying them to China's economy and infrastructure. The Chinese model would be based on absolute self-sufficiency and it would have access to enormous markets that are largely closed to their competitors' technology and user data. Digital silk road techno-economic coalition could, for instance, export services for network surveillance and social scoring. Data would be controlled by the state and used for commercial purposes.

3.3 Digital Soviet Union

Obviously, Russia wishes to remain an independent global actor and this would be possible only as part of some kind of techno-economic coalition. Russia's coalition would be dependent on the domestic market and public investments. Russia's rational partners would be the members of the Eurasian Union, i.e. the individual states of the former Soviet Union and members of the Collective Security Treaty Organisation (Belarus, Azerbaijan, Kazakhstan, Uzbekistan, Tajikistan and Moldova). The Digital Soviet Union techno-economic coalition would rely on the nostalgia of past ideology and empire-building and use state owned data for ideological control.

3.4 European data, technology and infrastructure idealists

The EU's Digital Strategy of 2020 states that the EU must strengthen its digital sovereignty and set standards instead of lagging behind others (Shaping Europe's Digital Future 2020). EU's idealistic coalition would focus on data protection, technology and infrastructure. The aim would be to strengthen Europe's technological capacity, independence and confidence, and to improve Europe's position in global competition. Data would be owned by the person and data protection and privacy requirements would be extremely high. Still, the future of the EU's techno-economic coalition seems rather uncertain – at the most – idealistic.

[3] This categorisation and the descriptions were enhanced in the research workshop organized by the Finnish Defence Research Agency (FDRA) in 2022.

3.5 Halal Internet

Islamic countries could form a so-called 'Halal Internet' based on shared religious values. This techno-economic coalition would protect the Islamic values from the influence of 'Western culture' and provide digital 'halal', i.e. 'permissible' services, that is, for instance, localized email services and search engines that promote and protect their religious values. Data would be owed by the state and used for controlling what is permitted and forbidden. The success and appeal of this techno-economic coalition could be based on selling religious content filtering and 'permissible services' also for other religions than Islam.

3.6 Where there is light, there must be shadow

The 'shadow' techno-economic coalition would be loosely formed by criminal and anarchic groups. Criminal and anarchic groups could join their forces into a single techno-economic coalition that could try to operate in-between the other techno-economic coalitions and to maintain a 'black-market' for services. The success of this techno-economic coalition would be based on operating outside of any rules and/or laws.

3.7 Wild card

The formation of the 'wild card' techno-economic coalition would happen unexpectedly, perhaps even shockingly. The 'wild card' techno-economic coalition formed by a country or commercial consortium could be a coalition formed around a country of 'sudden success'. The success could be based on, for instance, a discovery of a new raw material (commodity) or a disruptive technological breakthrough.

In the distant future, all the aforementioned techno-economic coalitions could be based on competing national or coalitional technical standards and solutions. Furthermore, techno-economic coalitions could develop new technologies at a national or coalitional level and build services based on national and/or coalitional technology. Nevertheless, the factual occurrence of techno-economic coalitions remains to be seen. Strategic foresight could provide frameworks to analyse the processes that could cause the techno-economic coalitions to emerge factually.

4. 'Backcasting' and strategic foresight

Strategic foresight aims to explore different plausible futures that could arise, and to foresee the opportunities and challenges the future developments could present (Habegger 2022; Kuosa 2012). In this paper, the aim is to find a systematic and structured framework for the estimation of the emergence of techno-economic coalitions. 'Backcasting' is similar to reverse-engineering that works backwards to reconstruct a selected machine or software. Simply, 'backcasting' is a process starting from a 'proposed future' and looking back to contemporary moment to identify the most strategic steps or actions necessary for achieving that specified future (Quist 2016, 125).

In this paper, 'backcasting' is not used as a method for creating a traditional strategic map to a future goal, but as a method for determining what should have happened in order for the techno-economic coalitions to emerge in future cyberspace. In this case, 'backcasting' starts by defining an event that will occur in the future (the emergence of techno-economic coalitions) and then asking the question 'how did this event come to be…?'. The task is then to develop a scenario (or series of events) that explain how the 'proposed future' might actually come about. And finally, the results can be used for finding issues or trends that should be followed in strategic foresight today.

A 'backcasting' experiment offers a way to get a group to envision a 'proposed future' and then to determine together what must happen in order for the 'proposed future' to become reality. Nevertheless, it needs to be highlighted that the results of one particular 'backcasting' experiment serve only as an example of the issues or trends that should be followed in strategic foresight today. Every 'backcasting' experiment produces different results that depend on the people taking part in the experiment. Therefore, 'backcasting' events should be regularly repeated with a different set of experts in order to increase validity.

5. 'Backcasting' experiment as an example

In the spring of 2022, a 'backcasting' experiment for military and civilian experts was held at the Finnish Defence Research Agency (FDRA), where the aim was to test 'backcasting' for strategic foresight. The main task of the FDRA 'backcasting' experiment was to determine which events and changes lead to the appearance of techno-

economic coalitions, i.e. to explain how the 'proposed future' might actually come about. The 'backcasting' experiment started by defining the 'proposed future'. Secondly, the key factors and pathways (keywords) were defined. Thirdly, the identified key factors and pathways were developed into sentences and series of events. Finally, the sentences were summarised into a complicated scenario that was tested from a strategic foresight point of view, i.e. the scenario was used for finding issues or trends that should be followed in strategic foresight today.

The 'proposed future' was defined as a situation where technically delimited 'cyberterritories' have occurred in cyberspace. 'Cyberterritory' refers to an area in cyberspace over which a sovereign state has jurisdiction, i.e. 'cyberterritories' have similar power structures to nation states. Global information flows are controlled at a national level. Many countries are pursuing self-sufficiency and digital sovereignty, but in order to remain competitive they need to either join and/or strengthen the techno-economic coalition. Techno-economic coalitions begin to emerge and they develop new technologies at a national and coalitional level and build services for the coalition based on national/coalitional technologies. Techno-economic coalitions gradually begin to challenge military alliances.

In order to find the key factors and pathways, an adapted model of the PESTEL analysis was used as a supporting research tool. PESTEL is a framework for analysing trends, developments and phenomena in the political, economic, social, technological, environmental and legal environments (cf. Marmol 2015). The experiment applied a PESTEL-M framework to assess political, economic, social, technological, environmental, legal and military factors that could have led to the proposed future. The participants of the 'backcasting' experiment were asked to describe cumulative factors and pathways under each PESTEL-M category that they regarded as necessary for the potential realisation of the 'proposed future'.

In the first phase, the following basic key factors and pathways (keywords) were defined by the participants of the experiment (Table1).

Table 1: 'Backcasting' experiment (PESTEL-M): 1st Phase: basic key factors and pathways (keywords)

Political	– a global confrontation continues – federalism – federal development – the right to privacy – the monitoring of people – the regulation of data usage
Economic	– successful digital currency – global tax agreement – decentralized production – platform economy – remote work
Social	– anonymity (you can be whoever) – inequality – isolation
Technology	– encryption technology changes – fusion energy – data processing and storage – metaverse
Environment	– climate refugees – the reduction of living space – diseases
Legal	– the first virtual person legalised – new types of crimes, e.g. 'cyber homicide' – cyberweapons are legally regulated
Military	– fighting cyber war becomes possible – wars without human casualties – asymmetry – cyber deterrence

In the following phase, the identified basic key factors and pathways were reduced and developed into more complex sentences and series of events that could have led to the formation of techno-economic coalitions (Table 2).

Table 2: 'Backcasting' experiment (PESTEL-M): 2nd Phase: sentences and series of events

Political Development	– Europe (and/or Islamic nations) form a federal state. – A scandal related to data-breach etc. leads to the break-up (disintegration) of the UN. – The need to control personal data grows extensively. – Politicians use the political situation to promote different techno-economic coalitions. – Different techno-economic coalitions use the political atmosphere to distinguish themselves in relation to how individuals can use their personal data and to control how the personal data is collected, stored and used.
Economic Development	– Some form of 'big' digital currency will actually succeed and retain its value (e.g. Digital Dollar, Digital Euro etc.). – Tax unification, i.e. a tax treaty that breaks traditional physical borders between nation states.
Social Development	– It is possible to work remotely globally throughout your career. – Digital isolation is increasing and digital hermits, i.e. persons that exist only in the digital world, are ordinary. – The value of work changes significantly.
Technology Development	– Contemporary encryption technology collapses suddenly (e.g. someone develops a material etc. that causes this) and it leads to the scandal that causes the UN to break-up. – Fusion energy is concretely in sight, i.e. the first devices are already being built. – The processing and storage of large amounts of data evolves, i.e. there are agreements about data storage. – Data becomes available to everybody.
Environmental Development	– A natural disaster causes a large country to become almost uninhabitable and the situation is solved within a techno-economic coalition. – The viable area on earth shrinks.
Legal Development	– The legal definition of 'person' is changed. – The birth of the first fully virtual person is legally possible. – A person other than a legal person can commit a crime. – New types of crimes, e.g. 'cyber homicide', emerge. – Cyber warfare (or a cyber operation that caused significant damage) is tried in court.
Military Development	– To fight cyber warfare becomes possible, i.e. cyber operations cause comparable harm to kinetic operations (cf. legal factors). – Critical infrastructure is defended by military forces. – Wars can be fought without human casualties. – Cyberweapons are legally regulated (cf. legal factors). – Cyber asymmetry and deterrence are reachable with military allies.

And finally, the sentences were summarised into a complicated scenario that demonstrates the driving forces for techno-economic coalitions. The developed scenario and trends that should be followed in strategic foresight today are as follows:

"Unexpected scandals and/or environmental catastrophes are rather difficult to foresee but obviously to be followed when they occur. Some kind of global data breach affecting almost everybody, but especially the world leaders and decision-makers, is likely to happen sooner than later. In the worst-case scenario, this kind of data-breach would be related to the UN or another global actor. The focus in strategic foresight could be on geopolitical challenges and political transitions of different geographic areas that are potential in forming a techno-economic coalition, i.e. according to the results of this backcasting experiment, it is productive to follow the development of countries heading toward a more federally structured government system.

Successful digital currency could be a result of (or benefit from) federally structured government system, i.e. it is important to follow research or prototypes or deployments of digital national currencies. Development of a successful digital currency could also advance the global tax agreement. Global taxing would make it possible to work remotely globally throughout your career, i.e. the different tax proposals and global tax policies should be followed. Nevertheless, the described development could have rather negative side-effects, such as, digital isolation and digital hermits, i.e. the social factors to be followed could be how the meaning and value of work are changing and how the major transformations in the global labour market are fulfilled.

Legislation and law-making processes always play catch-up with technological development. Therefore, legal issues are often outdated for strategic foresight. Nevertheless, the precedents related to the legal definition of a person, new types of cyber crimes and cyber warfare are important to follow. For instance, discussions of the relationship between natural and artificial persons are ongoing and how the law recognises a virtual person needs to be solved in the future.

Legislation and technological development are deeply related to the utilisation of military capacities. When it is possible to fight a cyber war without human casualties, the targets are in the operating systems of the critical

infrastructure. Therefore, cyber defence in the future could be based on the different values and technical standards and solutions developed nationally and/or at the techno-economic coalition level. Different solutions and technologies would create cyber asymmetry and deterrence between techno-economic coalitions."

This modest 'backcasting' experiment shows that the listed keywords, paths, trends, developments and phenomena may seem at first disconnected and trivial. However, together they form drivers of change that may eventually affect the development of techno-economic coalitions in considerable ways. This experiment demonstrates that 'backcasting' offers a usable framework for strategic foresight.

6. Discussion: Role of techno-economic coalitions in cyberspace governance and in cyber defence

The change in cyberspace governance models reflects a change in how nation-states consider cyber threats more in the national framework than at the global level. This development is affected by the fact that cyber threats are targeted, both directly and indirectly, at national critical infrastructure, economic competitiveness, national security and citizens. Nowadays, many nation-states are interested in the safekeeping of their own national cyberspace and their own national systems. The national controllability of cyberspace and the independent defence of various systems add to the sense of cybersecurity.

Increasingly, the sovereignty and 'self-sufficiency' in cyberspace are seen as an answer to security threats. The desire to use similar international laws, which direct the relations between states in the physical geographical environment, in cyberspace is growing. Eventually, this leads to the formation of 'cyberterritories' that could restrict (or control) everything from data movement and storage to political and/or religious control. Nevertheless, it is almost impossible for a single country to achieve 'self-sufficiency' in cyberspace. In order to remain competitive and protected, one must either join or strengthen emerging techno-economic coalitions.

This paper argued that the role of techno-economic coalitions in the future cyberspace governance should be understood and considered when developing strategic plans and implementing national cybersecurity policies at present. This paper examined what it would take for techno-economic coalitions to factually emerge in the future. 'Backcasting' was implemented to explore concrete changes and actions that are necessary for the techno-economic coalitions to develop. The results of the backcasting were placed into a scenario to find issues or trends that should be followed in strategic foresight today. According to the 'backcasting' experiment the trends are, for instance, the expansion of federally structured government systems, digital national currencies, changes in global and remote labour market, the development of global taxing and different legal precedents related to cyberspace.

Divergent techno-economic coalitions would significantly influence and complicate the international cyber law development and application in practice. Nevertheless, techno-economic coalitions would require a desire to use the classical principles of international law in cyberspace, i.e. all the similar laws that govern state relations in the physical geographical environment. Therefore, techno-economic coalitions are also military and political alliances and have strategic importance. Thus, also cyber defence in the future would be based on the different values and technical standards and solutions of future techno-economic coalitions. Consequently, the role of traditional military alliances in future cyber domain would diminish substantially, which should be considered when doing strategic planning.

Acknowledgement

I wish to acknowledge the expertise of all the participants of the 'backcasting' experiment and colleagues at the Finnish Defence Research Agency (FDRA) whose observant comments enhanced this paper significantly.

References

Braud, A., Fromentoux, G., Radier, B., & Le Grand, O. (2021) "The Road to European Digital Sovereignity with Gaia-X and IDSA", *IEEE Network*, Vol 35, No. 2, pp 4-5.

Habegger, B. (2022) Securing the Future: The Use of Strategic Foresight in the Security Sector. *Strategic Security Analysis*. Geneva Centre for Security Policy (GCSP), January 2022, Issue 23.

Hare, F. (2010) The Cyber Threat to National Security: Why Can't We Agree? *Conference on Cyber Conflict Proceedings 2010*, C. Czosseck and K. Pollins (eds.), CCD COE Publications, 2010, Tallinn, Estonia, 211-225.

Heller, K.J. (2021): In Defence of Pure Sovereignty in Cyberspace. *International Law Studies*, Vol. 97, pp. 1432-1499.

Kovács, L. (2018) National Cybersecurity as the Cornerstone of National Security, *Land Forces Academy Review*, Vol. XXIII, No 2(90), 113-120.

Kukkola, J. (2020) *Digital Soviet Union: The Russian national segment of the Internet as a closed national network shaped by strategic cultural ideas*, National Defence University, Helsinki.

Kukkola, J. (2021) *Rakenteellisen kyberasymmetrian strategiset vaikutukset: Venäjän kansallinen internetsegmentti sotilasstrategisena ilmiönä*, Finnish Defence Research Agency, Riihimäki.

Kuosa, T. (2012) *The Evolution of Strategic Foresight: Navigating Public Policy Making*. Routledge, London & New York.

Liaropoulos, A. (2013) Exercising State Sovereignty in Cyberspace: An International Cyber-Order Under Construction? *Journal of Information Warfare*, Vol 12, No. 2, pp. 19-26.

Marmol, T. (2015) *PESTLE Analysis: Understand and Plan for Your Business Environment*. 50Minutes.

MGIMO (2019) "Mezhdunarodnye ugrozy 2020: Kazhdyi za sebia", *Laboratoriia analiza mezhdunarodnykh protsessov MGIMO MID Rossii*, [online], https://mgimo.ru/upload/iblock/2ac/int-threats-2020.pdf, [Accessed December 19 2022].

Pohle, J., & Thiel, T. (2020) Digital Soverignty, *Internet Policy Review*, Vol 9, No. 4, pp 1-19.

Quist, J. (2016) Backcasting. *Foresight in Organizations: Methods and Tools*, P. van der Duin (ed), Routledge, London & New York, 125-144.

Rautava, J-P., & Ristolainen, M. (2022) Cyberterritory: An Exploration of the Concept, *Proceedings of the 21st European Conference on Cyber Warfare and Security (ECCWS)*, Thaddeus Eze, Nabeel Khan & Cyril Onwubiko (eds.), Chester, Academic Conferences International Limited, 239-246.

Ristolainen, M. (2021) "Softaa kyberrajalle! Katsaus kybertilan valtioalueellistamisprosessiin meillä ja maailmalla", *Tutkimuskatsaus 1/2021*, Puolustusvoimien tutkimuslaitos, [online], https://puolustusvoimat.fi/web/tutkimus/tutkimuslaitoksen-julkaisut#tutkimuskatsaukset, [Accessed January 18 2023].

Shaping Europe's digital future (2020) Luxembourg: Publications Office of the European Union [online], https://ec.europa.eu/info/sites/default/files/communica-tion-shaping-europes-digital-future-feb2020_en_4.pdf, [Accessed January 18 2023].

Yefremov, A. (2017) "Formirovanie kontseptsii informatsionnogo suvereniteta gosudarstva", *Zhurnal Vysshei ekonomiki*, No. 1, pp 201-215.