Cyberterritory: An Exploration of the Concept

Jori-Pekka Rautava[1] and Mari Ristolainen[2]
[1]University of Oulu, Finland
[2]Finnish Defence Research Agency, Riihimäki, Finland
jrautava@student.oulu.fi
mari.ristolainen@mil.fi

Abstract: What does the future of cyberspace look like? The idealistic notion of cyberspace as a 'free' and 'open' global infrastructure is progressively challenged by projecting territoriality and conveying traditional nation-state models of governance into cyberspace. The aim of this interdisciplinary paper is to examine the process of cyberspace territorialisation and to present a conceptual definition of a theoretical 'cyberterritory' as a bounded sovereign entity that operates under the jurisdiction of a certain nation-state. Firstly, we explain the different views of the cyberspace governance and summarize the latest developments in the UN's efforts to bring order over cyberspace. Secondly, we analyse the different views on 'digital sovereignty' and show how several nations have felt the need to express publicly their views on sovereignty in cyberspace. Thirdly, we discuss the possibility of new techno-economic alliances, because only few (if any) nation-states could have sufficient resources to be 'sovereign' in cyberspace. Finally, we present a conceptual definition of a theoretical 'cyberterritory' that encompasses political, legal and technical aspects. The significance of this paper is in its contribution to the discussion of future cyberspace governance by presenting a definition of a theoretical 'cyberterritory' as an entity of its own - a new nation-state 'digital terrain' of the future.

Keywords: territorialisation of cyberspace, 'cyberterritory', cyberspace governance, digital sovereignty

1. Introduction

Originally, the purpose of the global Internet was to combine geographically isolated intranets into a single network of networks. Ideally, the aim of a global Internet was to erase geographical areas, borders, and state control, and to create a 'global commons' in which data could move and be stored freely across national (geographical) territories (Kahin & Nesson 1997; Goldsmith & Wu 2006). In this so-called 'deterritorialization process' the network of networks developed to be a 'space' outside of the territorial (geographical) space of nation-states. Hence, cyberspace is on one hand an independent and integrated, but also a complex, partly overlapping and confusing combination of public and private services and critical infrastructure that is used by everyone from security authorities to individual citizens.

Despite its idealistic goals, the discussion about cyberspace governance and control has been ongoing since the 1980's (Radu 2019). The main objective has been to find ways to ensure the stability and security of cyberspace. In general, the discussions of the cyberspace governance can be divided into supporters of a 'multistakeholder' and a 'multilateral' governance system. Discussions within the UN (United Nations) have sometimes taken one-step forward and then two steps backwards. Moreover, concepts such as 'fragmentation' and 'balkanization' have been often used when evaluating the future development of the cyberspace (Mueller 2017). Depending on the perspective, the fragmentation of the global cyberspace has been seen as rapid or slower, yet almost inevitable development. Generally, cyberspace fragmentation is divided into three different forms (Drake, Vinton & Kleinwächter 2016). 'Technical fragmentation' is related to the development of the Internet infrastructure that affect the interoperability of devices and the data mobility. 'Governmental fragmentation' encompasses all state actions that restrict or prevent access to the Internet and control the data mobility. 'Commercial fragmentation' involves measures that prevent or impede the use of the Internet and data mobility by various commercial operators (ibid). All the different fragmentation developments serve the interests of different actors. However, it has also been suggested the real aim of the whole fragmentation debate is to subjugate the governance of the Internet under nation-state jurisdiction and to create nation-state power structures in the cyberspace and to supress the global information flows and data movement (Mueller 2017). This development can be called as a 'process of cyberspace territorialisation' (cf. Ristolainen 2021) and the outcome as 'cybered Westphalian age' (Demchak & Dombrowski 2011; Demchak & Dombrowski 2013).

The aim of this interdisciplinary paper is to examine the process of cyberspace territorialisation and to present a conceptual definition of a theoretical 'cyberterritory' as a bounded sovereign entity that operates under the jurisdiction of a certain nation-state. Firstly, we explain the different views of the cyberspace governance and summarize the latest developments in the UN's efforts to bring order over cyberspace. Secondly, we analyse the different views on 'digital sovereignty' and show how several nations have felt the need to express publicly their views on sovereignty in cyberspace. Thirdly, we discuss the possibility of new techno-economic alliances, because only few (if any) nation-states could have sufficient resources to be 'sovereign' in cyberspace. Finally, we present a conceptual definition of a theoretical 'cyberterritory' that encompasses political, legal and technical aspects.

2. Transformation of the cyberspace governance models

The main objective of the discussion about cyberspace governance and control has been to find ways to ensure the stability and security of cyberspace. In general, the discussions of the cyberspace governance can be divided into supporters of a 'multistakeholder' and a 'multilateral' governance model (Glen 2014). However, it is important to notice that the debate is also indirectly influenced by multinational companies (including Google, Alibaba, Yandex) and global civil society networks (including criminal and extremist groups).

Proponents of the state-led governance model aim for regional or national Internet segments of countries or groups of countries and strive for state sovereignty in cyberspace. Sovereign nation-states and their geographical boundaries are to be given priority in the national and global regulation of cyberspace. In this 'multilateral' governance model, driven by Russia and China in particular, cyber-related decision-making would be done by the so-called 'multilateral community', i.e. by the ITU (International Telecommunication Union) (Singh 2009; Glen 2014).

The 'multistakeholder' model, which emphasizes the cyberspace's global, open and interoperable systems, is opposing cyberspace territorialisation. According to the supporters of the 'multistakeholder' model, cyberspace governance should not be dependent on the control of individual state governments. In the 'multistakeholder' model, led predominantly by the US, the cyberspace governance is organized under the 'global community' or the 'stakeholder community', such as ICANN (Internet Corporation for Assigned Names and Numbers). Supporters of the 'multistakeholder' model oppose regional or national Internet segments and seek to preserve the 'freedom and openness' of cyberspace (Strickling & Hill 2017).

Essentially, cyberspace governance models are issues of international law that are being resolved within the UN. Since 1998, within the UNODA (United Nations Office for Disarmament Affairs), Russia has been pushing for a resolution that instead of global transparency a national sovereignty applies in cyberspace (Korzak 2021). No such resolution has been adopted so far, but since 2004, every two years, a Group of Governmental Experts (GGE) has been writing 'consensus reports' on cyberspace governance for the UN General Assembly to approve. These reports have analysed how the international law affects states' actions in cyberspace and tried to find ways to promote compliance with existing cyber standards that are acceptable to all (see, e.g. Ruhl et al 2020).

In 2010, 2013 and 2015, the UN General Assembly confirmed, on the recommendation of the GGE, that international law applies and regulates the activities of nation-states in the cyberspace. At the same time the need to discuss specific features of the cyberspace, such as speed, interdependence, complexity and anonymity, was recognized. The 2015 resolution established voluntary, non-binding standards for responsible state behaviour in cyberspace. However, after the 2015 resolution, the debates stalled. In 2017, the GGE group did not reach consensus and their work was suspended. The application of international law in the cyberspace became a particular problem. In 2018, the UN General Assembly accepted a resolution led by Russia to form a new OEGW (Open-Ended Working Group) to analyse the previous GGE reports in order to identify new standards and to explore to form a new dialogue between different UN institutions (Ruhl et al 2020). However, in 2018, the UN General Assembly also passed a US-led resolution that was in part inconsistent with the Russian-led resolution. The US-led resolution decided to re-establish a new GGE-group to write unanimous reports on state action in cyberspace. Nevertheless, there were significand differences in the composition of the newly established groups. All the UN Member States (193) were invited to join the OEGW-group, while only 20-25 countries have been involved in the GGE-group. The groups were also designed to operate in a different way. The OEGW group will operate until an agreement is reached; the GGE process has a two-year time limit at the time (ibd.).

When the OEGW process started, many individual states felt the need to express their national views on the international law in cyberspace. At this stage, various national openings and new initiatives began to emerge among the proponents of the 'multistakeholder' model. These new openings and initiatives considered in particular state sovereignty in cyberspace. Although the supporters of the original 'multistakeholder' cyberspace governance model still relied on the security deriving from the global system, some, mostly European countries, saw cyber threats more and more in the national framework than at the global level. This 'new thinking' resembled in a way the views of the 'multilateral' model of governance proponents. It seems that the transformation of the cyberspace governance models began when some kind of combination of 'partial multistakeholder' and 'partial multilateral' started to emerge. This development is affected by the fact that cyber threats are targeted at national critical infrastructure, economic competitiveness, national security and citizens, both directly and indirectly. Nowadays, many nation-states are interested in safekeeping of their own national cyberspace and own national systems. The national controllability of cyberspace and the independent defence of various systems add to the sense of cybersecurity. This in turn reflects the original ideas of the proponents of the 'multilateral', i.e. state-led governance model of cyberspace. The efforts of nation-states to resists the influence of multinational corporations, and civil society networks, as well as criminals and terrorists also bring superpowers together and make the state-led governance model an attractive option for many nation-states.

In the summer of 2021, both the OEGW and GGE groups came to some conclusions (United Nations 2021a). It was decided to continue the OEGW for another five years, and the group reached a final statement which was accepted both the US and Russia (United Nations 2021b). Similarly, the GGE experts approved their final report that was also confirmed by the UN General Assembly in the summer of 2021. However, the GGE final report is, in fact, a reduplicate of the 2015 report (United Nations 2021c).

In both OEGW and GGE final statements sovereignty in cyberspace is considered only as a general principle that could not lead to legal consequences in the cyberspace. Nor was the role of UN extended in the cyberspace governance. Nevertheless, the supporters of the state-led cyber governance model extended the process to the entire UN level (e.g. OEGW process), created a certain dissimilarity among the original supporters of the 'multistakeholder' model and gained the opportunity to influence more countries' views on the future of the cyberspace governance. This can be seen as an effort by the proponents of the 'multilateral' model to increase the legitimacy of their model of governing the cyberspace, which seems to be a planned normative line of effort (Kukkola, Ristolainen & Nikkarila 2017).

3. Sovereignty in cyberspace

The recent change in the governance models of cyberspace reflects a change in how different nations see sovereignty in cyberspace and how they desire to use similar international laws that direct the relations between states in the physical geographical environment also in cyberspace. However, this poses certain problems because the so-called 'national cyberspace' does not necessarily follow the physical borders of a nation-state and there is no internationally unified understanding of what sovereignty means in cyberspace.

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. Efremov 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.

As noted earlier, several nations have felt the need to express publicly their views on sovereignty in cyberspace after the two conflicting UN resolutions in 2018. Many European countries have expressed the view that the principle of State sovereignty applies in cyberspace. For instance, Tallinn Manual (2017) states that "a State enjoys sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations."[1] Cyber infrastructure is defined as "Cyber infrastructure: The communications, storage, and computing devices upon which information systems are built and operate" (ibid.). According to this definition, the state would have a jurisdiction of all information and communication technology (ICT) and the persons operating it located in its territory, which sounds rather totalitarian.

[1] This statement refers to the 2015 GGE report; see United Nations 2021c.

According to Tallinn Manual (2017), sovereign authority includes 'cyber infrastructure' within the physical geographical state territory, where, however, the ownership of 'cyber infrastructure' is divided between public administration, business, organizations and individuals both nationally and internationally. Moreover, it is not clear whether the sovereign authority includes strategic data and services in global cloud services that are not physically located within the physical territory of the state. On the other hand, a physical territory tied definition is problematic in a situation where the physical territory of the state contains 'cyber infrastructure' owned by a foreign state and 'persons involved in cyber activities' that are foreign citizens. Likewise, satellites, electromagnetic spectrum or marine cables not located on the physical territory of the state that are critical to functioning of the 'cyber infrastructure' of different countries. It could be possible that one country defines these as its sovereign authority, which can lead to uncomfortable situations and expose the physical territory owner to hybrid influencing. Sovereignty in cyberspace requires a definition of 'cyber borders' that has not been done by so far.

The definition of a cyberterritory should be as broad as possible. If the definition is too strict, it is easy to argue that the only way to implement a cyberterritory is totalitarian ownership of the infrastructure. A cyberterritory should be implemented in a way that technical solutions allow having control over the infrastructure without taking over the infrastructure from companies owning it. The owner should be able to achieve three goals to define borders of a cyberterritory: 1. Delimitation and demarcation; 2. Protection; 3. Control (Kukkola & Ristolainen 2018).

First, delimitation means that the place of borders is decided between nation-states through negotiations. With demarcation is meant that the cyberterritory owner must be able to set strict boundaries for when the network traffic enters a cyberterritory. Demarcation is based on delimitation agreements that set the agreed boundaries (Kukkola & Ristolainen 2018). We argue that for the definition of a cyberterritory, it is not necessary to define how the demarcation is done. Second, protection means that the owner must be able to protect the cyberterritory for which it has set boundaries (ibid.). There is some entity that has the responsibility to arrange the measures for protection. The entity responsible of the protection is also responsible of the control of traffic across the border. Finally, control means that the owner must have control over the cyberterritory (ibid.). We argue that the control and protection are strictly tied together. Without control, it is not possible to efficiently protect the area and without protection, it is naive to say that one would for sure have control over the area.

4. Techno-Economic alliances in future cyberspace

When assessing potential future developments, it seems possible that the state-led model of cyberspace governance could gain more supporters. This can lead to a formation of new techno-economic alliances, because only few (if any) nation-states could have sufficient resources to be 'sovereign' in cyberspace. Techno-economic alliances could be based on competing technical platforms and national solutions (MGIMO 2019). Techno-economic alliances could develop new technologies at national (or alliance) level and build services based on national (alliance) technology. Many countries are striving for self-sufficiency and 'digital sovereignty'. However, in order to remain competitive, they must either join or strengthen emerging techno-economic alliances.

Potential techno-economic alliances could be formed around the 'Anglosphere' led by the US, around China, around Russia and around EU (ibid.) US, Canada, Great Britain, Australia and New Zealand are economically tightly integrated and their alliance could also be attractive to countries such as Mexico. This alliance would use its privileged position in the world to create the best conditions for itself. Similarly, China is expanding its alliance with neighbouring countries tying them to China's economy and infrastructure. The Chinese model is based on the absolute self-sufficiency and it would have access to enormous markets that are largely closed to competitors' technology and user data. Russia wishes to remain an independent global actor and this would be possible only as part of some kind of techno-economic alliance. Russia's alliance 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 (Belarus, Azerbaijan, Kazakhstan, Uzbekistan, Tajikistan, and Moldova) (ibid.). The EU's Digital Strategy of 2020 states that the EU must strengthen its digital sovereignty and set standards instead of lagging behind others. EU's alliance would focus on data protection, technology and infrastructure (Shaping Europe’s digital future 2020). The aim would be to strengthen Europe's technological capacity, independence and confidence, and to improve Europe's position in the global competition. However, the future of an EU's techno-economic alliance seems rather uncertain. Furthermore, the role of South-America and Africa in techno-economic alliances remains ambiguous. Both continents will be under heavy influence of several alliances in the future.

The border between techno-economic alliances is technological. However, the delimitation process is still between nation-states and ratified by the UN. It can be argued that cyber borders run in the competition between competing critical infrastructure technology platforms controlled by governments at the national or at the alliance level. Due to national security, it will be impossible to allow third parties access to independent critical infrastructure. Alliances would require a desire to use the classical principles of international law in the cyberspace, i.e. all the similar law that govern state relations in the physical geographical environment (cf. state-led 'multilateral' cyberspace governance model). Therefore, techno-economic alliances are also military and political alliances and have strategic importance (Kukkola 2021).

5. Definition of a theoretical 'cyberterritory'

Based on the above presented developments and discussions, it can be estimated that territoriality and traditional nation-state models of governance are conveyed more and more into future cyberspace. Nevertheless, territorialisation of cyberspace is relatively new phenomenon, i.e. it requires a comprehensive conceptualization. In the spring of 2021, a research workshop for military and civilian experts was held at the Finnish Defence Research Agency (FDRA), where the aim was to find a conceptual definition of a theoretical 'cyberterritory' that encompasses political, legal and technical aspects (FDRA 2021).

In the research workshop was formed a preliminary definition of a cyberterritory as *"an entity of networks and technical infrastructure containing services which is controlled by a sovereign nation-state".* Next, we elaborate the definition by first defining what entity or who can own a cyberterritory. Big multinational corporations might have bigger and more complex networks than those of small nation-states. The corporations also have independent control over their networks. For example, Google has its datacentres all around the globe spanning its networks to almost every part of the globe (Safenames Ltd, 2017). Large corporation networks could be dealt as cyberterritories in this sense but there is one major piece missing. Big corporations do have control only over the infrastructure in their own premises, but when the connections leave from the premise, they move to infrastructure which is controlled by someone else, usually in many different nation-states. This infrastructure cannot be controlled by the companies, which introduces a critical difference between nation-states and corporations. Moreover, as the Russian and Chinese examples show, companies can be forced to open their networks and to control their networks in the way nation-states want. Therefore, nation-states can have at least some control over the infrastructure through legislation in their territory even when the infrastructure belongs to some company.

Cyberterritory must be tied to an actual nation-state and its jurisdiction (FDRA 2021). Nation-states have their borders and embassies are part of the nation-state for which they belong. Similarly, all the infrastructure should belong to a cyberterritory which is controlled by a sovereign nation-state. The nation-state controlling cyberterritory has undisputed and sovereign control over the infrastructure in the region of their cyberterritory. Yet, the 'international cyberspace' outside of national cyberterritories evokes questions: Does all infrastructure belong to some nation-state or is there parts of international cyberspace which do not belong to anyone particularly i.e., nobody has sovereign control over the part of the cyberspace? This is strictly related to cyberterritory spreading outside of the borders of the nation-state controlling a cyberterritory. Embassy can have direct connection to the original cyberterritory for example via VPN (Virtual Private Network), but the infrastructure which the VPN uses to create the connection is not (completely) controlled by the owner of the cyberterritory (FDRA 2021).

Moreover, in the FDRA research workshop, a series of questions, concerning data in a cyberterritory was raised: Is it possible to have cyberterritory without data? Alternatively, is the data what makes some entity of infrastructure a cyberterritory? Thus, we must consider the importance of data in the context of a cyberterritory. We produce more data every day than ever before. There are huge amounts of data moving around in networks and that data is used to sell people things, to gather information of behaviour of individuals, to make business decisions and many more. Our whole world is run by data. Data is something that is saved and moved in a cyberterritory and between cyberterritories (FDRA 2021). Data is also something that can be stolen from a cyberterritory. If data can be stolen from a cyberterritory, then is a part of a cyberterritory stolen also? A cyberterritory inevitably contains massive amounts of data. Data in a cyberterritory always belongs to someone.

For a cyberterritory to be a place where citizens want to belong the nation-state cannot own all data in a cyberterritory. In a cyberterritory, the data belongs to entities who have produced it or have legal right to own it. Because the owner of a cyberterritory cannot own all the data in a cyberterritory and the data in a cyberterritory can be stolen, we argue the definition of data is not necessary for the definition of a cyberterritory. This does not mean that data would not be a crucial part of a cyberterritory. Without data a cyberterritory is not very useful and thus data is integral part of the actual implementation of a cyberterritory even if it is not a part of the definition.

6. Discussion: 'Cyberterritory' - a new nation-state 'digital terrain' of the future?

The purpose of a cyberterritory is to provide more control for the owner of the cyberterritory. Owner of the cyberterritory would be able to control the data flowing to and from the cyberterritory. This of course raises a problem if the controller of the cyberterritory is so-called totalitarian or authoritarian nation. A totalitarian nation in this context is a nation that prohibits the existence of opposition parties and treats dissidents as criminals. It is safe to assume that those totalitarian nation-states will find ways to oppress the people if they want to even without a cyberterritory. The purpose of controlling data flow is strictly related to security. If a conflict escalates, the variety of tools used to influence the enemy is wide. The cyberspace is inevitably one medium for different tools for impacting the enemy. Thus, controlling the cyberspace would benefit the defender since they would be able to create asymmetric situation towards the attacker (Kukkola 2020; Kukkola 2021).

A cyberterritory should allow citizens to maintain their privacy. A cyberterritory should also provide a possibility to block harmful content. It is up to the owner of a cyberterritory to decide what is considered harmful. A cyberterritory should provide tools to redirect traffic to 'border crossing points'. The great firewall of China (GFW) should not be considered as a 'border fence' of a cyberterritory because firewall does not provide sufficiently fine-grained control. The existing GFW can either block or allow traffic. A cyberterritory should be able to simultaneously block and allow content from the same source, something that firewall is not able to do. E.g., Russia used BGP (Border Gateway Protocol) and geoblocking when defending its 'cyberterritory' in the war against Ukraine in spring 2022 that allows more effective control over network flow than a firewall such as GFW (Goodin 2022).

It is noted that the idea of a cyberterritory is, in some extent, first proposed through the supporters of 'multilateral' governance model. Some of those initial supporters are rather authoritarian nation-states. Therefore, it is obvious that cyberterritory could be used for terror, surveillance, and oppression of citizens. Nevertheless, some of the original supporters of the 'multistakeholder' governance model have also started to move towards the idea of controlling nation-state networks. Sovereignty in cyberspace has had negative connotation because -states like China, Iran and Russia have been supporting the nation-state-controlled Internet (Litvinenko 2021).

It is clear that controlling the cyberspace in a cyberterritory enables authoritarian control. However, the control in cyberspace also enables securing the network from external and internal threats. Companies already have security operation centres (SOC), which monitor what happens in the internal networks of a company. Similarly, SOCs could be established in the context of a cyberterritory to monitor traffic in nation-state wide networks to find anomalies and malicious activities. For example, some telecommunication operators already have SOCs to monitor their networks (Elisa 2021; Telia 2021; AT&T 2022), these could be chained together in nation-state SOC that would get information from different telecommunication providers and then gather the information together in one place to monitor the nation-state status in networks. Sovereignty comes from the ability to decide what happens on the area controlled by sovereign nation-state. Thus, digital sovereignty demands the ability to have control in the networks of a nation-state.

The benefits of a cyberterritory when implemented by non-totalitarian nations are greater than the possibility of misuse; the nation-states who want to control their citizens will find the ways to do it anyway. Through a cyberterritory it would be possible to better protect citizens and companies in a cyberterritory from cybercrimes and other malicious actors. In case of crisis, it is easier to manage the internal affairs when the amount of data from outside can be reduced. For example, misinformation campaigns can be shut down before they even start to reduce the damage produced by misinformed people. In normal situation the non-totalitarian cyberterritory has not any difference from the current state of networks. However, in case of conflict or escalation the nation-state could better control their digital territory by controlling the traffic in a cyberterritory (cf. Kukkola 2021). Thus, in the non-totalitarian cyberterritory the benefit of control and surveillance would fully emerge only when the political situation is something else than normal. The legislation should be updated according to technical aspects of a cyberterritory to reduce the risk of unwanted surveillance towards citizens.

The core responsibilities of a nation-state are derived from the universal declaration of human rights that serves as cornerstone for law making in many nation-states. The core responsibilities for nation-state towards its citizens are to protect the peace of a society, to protect right to life and liberty for everyone and to provide equal justice for everyone regardless of their socio-economic status (United Nations 1948). To achieve these responsibilities in cyberspace the nation-state should have visibility to nation-state-level networks in its cyberterritory.

The idea of a cyberterritory has evolved through 2010s and the evolution will continue through 2020s (United Nations 2021a). It makes sense to define and produce a technical framework that can be agreed upon by many countries. The framework should be something that approved by both supporters of ‘multistakeholder’ and 'multilateral' governance models. When creating the framework together, it is possible to preserve the open nature of Internet and give the possibility of territorialisation. Creating the framework together also could prevent the birth of techno-economic alliances, which could prevent conflicts and competition in cyberspace. Cyberterritory can be implemented in such manner that regular user knows no difference in user experience when compared to the current situation. Through mutual interests of nation-states, it is possible to create safer implementation for a cyberterritory since there are more observers during the development. In this process, a theoretical 'cyberterritory' as an entity of its own can turn into a new nation-state 'digital terrain' of the future.

References

AT&T (2022) Security operations Center, [online], https://cybersecurity.att.com/solutions/security-operations-center, [Accessed January 13 2022].

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.

Demchak, C., & Dombrowski, P. (2011) “Rise of a Cybered Westphalian Age”, *Strategic Studies Quarterly*, Vol 5, No. 1, pp 32-61.

Demchak, C., & Dombrowski, P. (2013) “Cyber Westphalia: Asserting State Prerogatives in Cyberspace”, *Georgetown Journal of International Affairs,* International Engagement on Cyber III: State Building on a New Frontier, pp 29-38.

Drake, W. J., Vinton, C. G., & Kleinwächter, W. (2016) ”Internet Fragmentation: An Overview”, *World Economic Forum*, Davos, [online] https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Over-view_2016.pdf, [Accessed October 12 2021].

Elisa (2021) “Elisa's Cyber Security Services”, [online], https://yrityksille.elisa.fi/en/cyber-security, [Accessed January 12 2022].

FDRA (2021) Finnish Defence Research Agency: *Research workshop for military and civilian experts on cyberterritory*, 29.-31.3.2021.

Glen, C. M. (2014) “Internet Governance: Territorializing Cyberspace?”, *Politics & Policy*, Vol 42, No. 5, pp 635-657.

Goldsmith, J., & Wu, T. (2007) *Who Controls the Internet? Illusions of a Borderless World*, Oxford University Press, New York.

Goodin D., "After Ukraine recruits and 'IT Army', dozens of Russian sites go dark", [online], https://arstechnica.com/information-technology/2022/02/after-ukraine-recruits-an-it-army-dozens-of-russian-sites-go-dark/, [Accessed March 18, 2022].

Kahin, B., & Nesson, C. (1997) *Borders in Cyberspace: Information Policy and the Global Information Infrastructure*, The MIT Press, Cambridge, Massachusetts and London, England.

Korzak, E. (2021) “Russia's Cyber Policy Efforts in the United Nations”, *Tallinn Paper No. 11*, CCDCOE.

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.

Kukkola, J., & Ristolainen, M. (2018) ”Projected Territoriality: A Case Study of the Infrastructure of Russian Digital Borders”, *Journal of Infromation Warfare*, Vol 17, No. 2, pp 83-100.

Kukkola, J., Ristolainen, M., & Nikkarila, J.-P. (2017) *Game Changer: Structural transformation of cyberspace*, Finnish Defence Research Agency, Riihimäki.

Litvinenko, A. (2021) “Re-Defining Borders Online: Russia's Strategic Narrative on Internet Sovereignty”, *Media and Communication*, Vol 9, No. 4, pp 5-15.

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 October 11 2021].

Mueller, M. (2017) *Will The Internet Fragment? Sovereignty, Globalization and Cyberspace*, Polity Press, Cambridge.

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

Radu, R. (2019) *Negotiating Internet Governance*, Oxford University Press, Oxford.

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 December 17 2021].

Ruhl, C., Hollis, D., Hoffman, W., & Maurer, T. (2020) ”Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads”, *Working Paper.* Carnegie Endowment for International Peace, [online], https://carnegieendowment.org/files/Cyberspace_and_Geopolitics.pdf, [Accessed December 15 2021].

Safenames Ltd. (2017) “Google Data Center FAQ”, [online], https://www.datacenterknowledge.com/archives-/2017/03/16/google-data-center-faq-part-2, [Accessed January 12 2022].

Scott, K. (2021) “Connected, Continual Conflict: Towards a Cybernetic Model of Warfare”, *ECCWS 2021 20th European Conference on Cyber Warfare and Security*, pp. 375-381.

Shaping Europe’s digital future (2020) “Shaping Europe's digital future”, *Publications Office of the European Union*, [online], https://ec.europa.eu/info/sites/default/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf, [Accessed December 15 2021].

Singh, J. (2009) “Multilateral Approaches to Deliberating Internet Governance”, *Policy & Internet*, Vol 1, No. 1, pp 91-111.

Strickling, L. E., & Hill, J. (2017) “Multi-stakeholder internet governance: success and opportunities”, *Journal of Cyber Policy*, Vol 2, No. 3, pp 296-317.

Tallinn Manual 2.0. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge University Press, Cambridge.

Telia (2021) Cyber Security, [online], https://www.telia.fi/business/one-large/security?intcmp=b2b-en-large-grid-cyber-security, [Accessed January 12 2022].

United Nations (1948) “The Universal Declaration of Human Rights”, [online], https://www.un.org/en/about-us/universal-declaration-of-human-rights, [Accessed January 12 2022]

United Nations (2021a) “Developments in the field of information and telecommunications in the context of international security”, [online], https://www.un.org/disarmament/ict-security/, [Accessed December 17 2021]

United Nations (2021b) “Open-ended Working Group”, [online], https://www.un.org/disarmament/open-ended-working-group/, [Accessed December 17 2021]

United Nations (2021c) “Group of Governmental Experts”, [online], https://www.un.org/disarmament/group-of-governmental-experts/, [Accessed December 17 2021].

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