Cyberspace Geography and Cyber Terrain: Challenges in Producing a Universal map of Cyberspace

Alexander Grandin
Finnish Defence Research Agency, Riihimäki, Finland

alexander.grandin@mil.fi

Abstract: Much in the same way that cyber has become the fifth military domain, cyberspace has also brought forth the research area of Cyberspace Geography. The challenge of producing a universal map of cyberspace however still exists. Cybersecurity specialists, military personnel and researchers still begin with a blank sheet on which the wanted elements of cyberspace are arranged before solving their actual problem. The abundance of elements in cyberspace requires a careful selection of factors to include in one's map, depending on how it will be used. However, a complex and ever-changing environment such as cyberspace could make use of a generally acknowledged starting point, facilitating this work. In previous research cyberspace has been described as a combination of the physical world, the social world and the information world. The multidisciplinary research in Cyberspace Geography has developed models for mapping and displaying cyberspace. This is often done by creating topological maps, much like the map of the New York subway system. Military cybersecurity researchers have through the concept of Cyber Terrain presented similar models of cyberspace for military operations. Research has also been produced on the techniques and methods for mapping cyberspace as well as the different presentations of the mapped information. Graph theory has for instance been used as a mathematical model of cyberspace. It is nonetheless unclear if there is some degree of universality in the elements that the different research presents. Which are e.g. the similar features between the cyberspace maps that are used for military operations, that describe the cyber environment of a country or between the elements used for modelling a cybersecurity system? This paper aims to present a solution to this challenge by systematically reviewing the research on Cyberspace Geography and Cyber Terrain using thematic analysis. The different elements of the maps of cyberspace are reviewed. The research will answer if a universal map, that can be used as a starting point for solving multiple challenges in cyberspace, can at present be prepared.

Keywords: Cyber Defence, Cyber Terrain, Cyberspace Geography, Cyber Territory, Cyberspace Mapping

1. Introduction to Cyber Terrain and Cyberspace Geography

According to Google Scholar[1], Cyberspace Geography has yearly appeared in publications since 1993 and Cyber Terrain since 1998. Interestingly, Cyberspace Geography experienced a small renaissance around the year 2019, with nearly as many search hits as under its previous highlight around 2000. This seems to be a result of for instance Chinese scholars using the term frequently since 2017. The term has not found an especially large audience, since only about 196 search hits appear altogether on Google Scholar compared to Cyber Terrain that produces 520 search hits.

Cyber Terrain however was more widely used after 2009, with most search hits between 2017 and 2018, as can be seen in figure 1. If Cyberspace Geography was at least in the beginning associated with geographers, Cyber Terrain research seem to be associated with the term cyberwar, cyberoperations and, at least in part, with military planning in western countries.

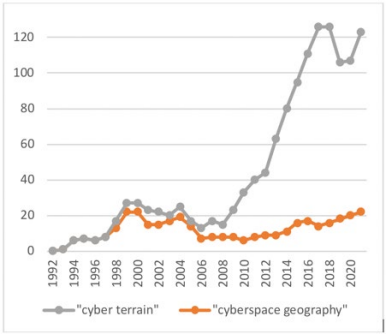

Figure 1: Search hits on Google Scholar, showing "cyber terrain" in gray and "cyberspace geography" in orange since 1992

[1] *The limitations of using Google Scholar were identified, but were outweighed by the possibility to gain an international and interdisciplinary approach to the chosen search terminology. For instance, EBSCO does not provide some of the Chinese research on cyberspace geography, that has been published on Springer. The point of view was thus chosen to be as broad as possible, even though it might have lacked in depth.*

Mills (2012) describes in his article the evolution of the traditional warfare concept of key terrain, derived from Carl von Clausewitz, to the concept of key cyber terrain. Mills argues that key cyber terrain has traditional components as well as contemporary nodes. For instance, a data centre has a physical dimension as well as a distinct cyber dimension. Key cyber terrain is a combination of traditional concepts of warfare adopted to cybersecurity, in the same manner that cyberspace geography is a bridge between traditional geography and cyberspace. The question is if these two traditional ways of looking at the physical realm also portray cyberspace in the same manner, and if that could form the basis for a multidiscipline map for cyberspace.

The term Cyberspace Geography has in recent years been connected to the term Cyberspace Surveying and Mapping (CSM) by researchers like Xu (2019) and Kou, Ni & Du (2022). Xu (2019) also connects the concepts of network mapping, cyberspace mapping and cyberspace cartography to the subject and treats these as identical. The concept of the "ternary world" has also been proposed at least as early as 2011 by Xu & Li. This concept of a world consisting of the physical world, the social-human world and the information world is further developed by Lü, Yuan & Yu (2021). The division into three spatialities or levels is conceptually quite near the US Joint Chiefs of Staff (2018) definition of the three layers of cyberspace, which are the physical network layer, the logical network layer and the cyber-persona layer.

Ferreira & Vale (2021) describes how cyberspace has been explored by geographers, and notes that the research has most notably used the terms "geographies of internet", "cyber geography", "geography of cyberspace" and "virtual geography". The recent revival of Cyberspace Geography, especially in China, seems to be well described by Kou, Ni & Du (2022), stating "*Studying cyberspace surveying and mapping technology and comprehensively mastering cyberspace characteristics and resource distribution have very important theoretical significance and practical value for ensuring national security.”*.

2. Previous research and realization

The systematic literature review was conducted using the keywords "Cyberspace Geography" and "Cyber Terrain" to find relevant research on the subjects. The primary source of information was Google Scholar. Articles and documents dating from 2002 were collected, which resulted in 10 sources on cyberspace geography and 24 on cyber terrain. The sources were thematically analysed in order to define how cyberspace was constructed by the authors. 5 sources on cyber terrain were deemed irrelevant and 8 sources did not provide information that defined what constitutes cyber terrain. On cyberspace geography, one source proved irrelevant and 3 sources did not provide required information. This left 17 sources for the thematic analysis. The sources were primarily research articles or conference papers, but also reports and theses (6 sources) and government publications (2 sources). The thematic analysis was done by listing the definitions and viewpoints on the subject and comparing these to find reoccurring elements and themes. Some, albeit few, of the analysed articles dealt directly with the task of defining (key) cyber terrain.

The concept of "key cyber terrain" has previously been assessed by Huntley (2016). Huntley (2016) notes that "*The concept of "key terrain" applied in cyberspace is necessarily metaphorical.*" and continues by stating that this simple fact is rarely noted. He reviews 11 studies or doctrinal publications, primarily by the U.S. Department of Defence or by actors tied to them. He concludes that key cyber terrain is primarily linked to the US Department of Defence (DoD) definitions of cyberspace and (physical) key terrain, and thus also to the physical aspects of cyberspace, such as hardware and infrastructure. He continues by noting that there seems to be a practical need to try to take advantage of existing military planning concepts, such as key terrain, and translate these into cyberspace, even though this might result in loosing valuable virtual aspects of cyberspace, such as cyber-persona and virtual spaces. Huntley also identifies that in the studies he examined, the concept of key cyber terrain varies on different operational levels, and concludes by questioning the usefulness of the concept and even the possibility to define the terrain in a useful way.

Martin Dodge and Rob Kitchin (2001) published the first book devoted to cyberspace geography, *Mapping Cyberspace*. The book provides an analysis of cyberspace from a geographer's point of view, but draws on research in e.g. cartography, sociology and information visualisation. The book and the research around cyberspace geography seem to be especially supported by the discussion around the year 2000 if geography was becoming obsolete, as ICT's eliminates the time and distance between spaces and places.

Boos (2017 pages 13-38) discussed in his book the term cyberspace by reviewing academic literature on human geography, sociology and cultural anthropology. The review is however strictly defined, and only focus on concepts of on- and offline life. He however states that since the virtual world of cyberspace is connected to the real world, there must also be different cyberspaces for different connections between the on- and offline world.

These also change over time as the topologies of information change. He also cites research that point out that cyberspace is mainly virtual and socio-cultural. This points out the difference between the reality of how cyberspace is conceived by users (mainly as a virtual social construction) and the cybersecurity community, that focus on how it is constructed, which highlights the physical and logical foundation of cyberspace.

3. Results from the thematic analysis

The analysis shows that cyber terrain remains difficult to define. Guion & Reith (2017) and Price et al. (2017) describe how key cyber terrain can be evaluated by subject matter experts. The lack of definitions in cyberspace has been discussed by Applegate, Carpenter & West (2017), identifying research that extensively list key cyber terrain, thus confusing it with the elements of cyberspace. They point out that previous efforts have three main flaws. First, they state that instead of *what* cyber terrain consists of, the research should focus on how *key* terrain can be identified. Secondly, the concept is not linked closely enough to military planning and thirdly, that critical assets and cyber key terrain are confused with each other. Cyber terrain and key cyber terrain are in multiple studies (e.g. Bodeau, Graubart & Heinbockel (2013), Raymond et al. (2014) and Jabbour & Muccio (2011)) described using the US Joint Chiefs of Staff publication 2-01.3 (JP 2) (2009) definition, which is "*Any locality, or area, the seizure or retention of which affords a marked advantage to either combatant*".

Price et al. (2017), Applegate, Carpenter & West (2017) and Franz (2012) makes the distinction between cyber terrain on the tactical, operational and strategic levels. It is unsurprising that cyber terrain should be redefined at different levels – a module of a software may be critical for a system, that in turn is critical for a network etc. Another emblematic feature of cyber terrain is the temporal linkage to a specific (military) mission, as presented by Bertoli & Raio (2018) and Franz (2012). Several researchers, as Guion & Reith (2017), Price et al. (2017) and Jackson (2016) highlight the role of subject matter experts in defining key cyber terrain, but offer little advice on how this should be done.

Key cyber terrain is e.g. by Williams (2014) exemplified by a system (e.g. the Ballistic Missile Defence System (BMDS)). Bertoli & Raio (2018) describe the difficulty of distinguishing between cyber terrain and cyberspace in their article, and find that cyber terrain usually equals the features that build up cyberspace. They however note, that compared to the physical world, where terrain is defined, cyber terrain is not defined as a finite subset of the cyberspace domain, but comprise of all features of the cyberspace domain. They also argue that the concept of key terrain is difficult to translate to cyberspace. They mention that if the physical representation of a system such as BMDS does not constitute key terrain, then how could the virtual part of the system be key cyber terrain

Jakobson (2011) defines cyber terrain by a structure consisting of the hardware, software and service sub-terrains. The hardware sub-terrain is constructed of connected network infrastructure and devices, including information such as location and connectivity for these. The software sub-terrain consists of e.g. operating system and applications. The software components could have additional information such as vendor, release and known vulnerabilities. The service sub-terrain consists of the services and their intra-dependencies, including databases, e-mail, universal time, etc. The definition that Jakobson presents evades to shine light on what the difference between cyber terrain and cyberspace is, as his definition is similar to that of cyberspace. He however does not identify cyber persona as a factor of cyber terrain.

Mills (2012) define key cyber terrain primarily as consisting of physical objects, such as data centres, undersea information cables and internet service providers (ISP:s) but also mention BIOS (Basic Input-Output System), cyber workforce, supply chains, international standards bodies and innovation. He states that the Clausewitzean key terrain concept holds for cyber key terrain, because of its physical manifestations. He mentions "*geographic duplicity of data stores*" but still pinpoint data centres as key cyber terrain. Interestingly, he highlights the importance of cyber workforce, international standards bodies and innovations. Innovations, workforce and international standards bodies hardly change the outcome of any specific mission or operation in cyberspace. Mills seem to highlight important features and assets on a strategic level, that may impact the bigger picture of a nation-state's capabilities in cyberspace. Franz (2012) presents similar examples of key cyber terrain as Mills (2012) and names optic cables, satellite communications, subnets, databases with usernames and passwords and technicians in his work.

Raymond et al. (2014) defines cyber terrain through the definition of cyberspace developed by Raymond et al. (2013). By their definition, cyber terrain consists of "*the systems, devices, protocols, data, software, processes, cyber personas, and other networked entities that comprise, supervise, and control cyberspace*." They define key cyber terrain similarly to JP 2. By this definition, all of cyberspace can at some point be defined as key terrain, depending on the mission and situation. A very similar description of cyber terrain is offered by Lemay, Knight

& Fernandez (2014). They use direct analogies to the physical terrain in their article and define cyber terrain as based on "*material and logical infrastructure*". In the same way they define key terrain as that which is of essence for the task at hand, but offer little definition of cyber terrain in general.

Phister (2010) also defines cyber terrain through an analogy to physical terrain. He states that cyber terrain "*…is primarily hardware (i.e., switches, routers) and software (i.e., operating systems, protocols)"*. He also presents the analogy of cyber paths, which he describes as communication links connecting the various entities. He however does not highlight cyber persona or actors in cyberspace in his definition.

Moore (2004) provides seven categories through which a network environment can be described. These are (1) network classification (which networks are used in the operation), (2) architecture types (VPN:s, ethernet, wireless networks etc.), (3) software applications, (4) operating systems, (5) existing vulnerabilities, (6) types of information (stored or processed in the identified networks) and (7) the network activity baseline.

Since the publication of the earlier mentioned report by Huntley (2016), a new version of the US Joint Chiefs of Staff publication 3-12 *Cyberspace Operations* (JP 3-12) was released (2018) which broadens the definition of key cyber terrain so that it expands into the virtual realm of cyberspace, stating "*An additional characteristic of terrain in cyberspace is that these localities have a virtual component, identified in the logical network layer or even the cyber-persona layer*". La Pierre (2020) further broadens the definition by including elements of the Electromagnetic Spectrum (EMS) and needed power sources. He also deepens the definition of the cyber persona layer, naming the focus of this layer as "*virtual actors and how they relate to real individuals or organisations, as well as how they interact with each another, and with the network."*, citing the Danish doctrine for military cyberspace operations (2019) and Craig Jones (2015).

Youn et al. (2021) operationalize the three-layer definition of cyberspace into elements. The physical network layer includes the geographical location for network devices as well as hardware, software and infrastructure. Critical information storage locations are also included. The logical network layer is the virtual space of cyberspace. They expand the social and cyber-persona elements into the logical layer, by naming websites of influence and social platforms as elements of it. The cyber-persona layer includes IP-addresses and personal information about users. They also include organizational elements and structures in this layer.

The US JP 3-12 publication defines cyberspace (2018) as consisting of three layers, which are the physical network layer, the logical network layer and the cyber-persona layer. The physical network layer consists of "*the IT devices and infrastructure in the physical domains that provide storage, transport, and processing of information within cyberspace, to include data repositories and the connections that transfer data between network components*." This includes the geographic location of devices, such as hardware and infrastructure. The logical network layer consists of the connected elements that are "*abstracted from the physical network*". They highlight that the elements of this level can "*can only be engaged with a cyberspace capability*". They thus conclude that information stored in the logical network cannot be affected by physical means, as previous studies suggest, due to the virtual nature of storage. This is naturally not always the case, as data or information can be stored in a single facility, but can be deemed a logical starting point. The cyber-persona layer is constructed by virtual identities that are derived from the logical network plane, such as e-mail addresses and IT user accounts. Their definition of cyberspace is "*A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."*. This definition was according to Phister (2010) presented as early as 2008.

Different definitions of cyberspace are abundant. For instance, Gao et al. (2019) citing Boos (2017), defined cyberspace as consisting of five levels, which are the geographical layer, the physical network layer, the logical network layer, the cyber-persona layer and the persona layer. These layers consist according to Gao et al. (2019) of geospatial support elements, IT equipment, infrastructure, data, applications and network processes, user accounts and physical users. A similar definition was presented by Franz (2012), naming them the geographic layer, physical infrastructure, the information layer, cyber identity and people.

Raymond et al. (2013) defines cyberspace as consisting of five planes, which are the supervisory plane, the cyber persona plane, the logical plane, the physical plane and the geographic plane. The geographic plane consists of physical resource locations, such as infrastructure (including power etc.). The physical plane includes hardware and its details (serial number and attached devices) as well as communication protocols, and the other aspects of the ISO Open System Interconnection (OSI) models' layer 1. The other layers of the OSI model belongs to the logical plane. Users virtual identities lie above the logical plane and forms the cyber persona plane. The authors

have interestingly added a supervisory plane, that other models don't identify as an own plane. This plane consists of the persons and systems "*that provide the command and control necessary to start, stop, or redirect cyber weapons*". Jackson (2016) use the same cyberspace definition but uses it to define key cyber terrain. He however does not present the features in greater detail.

Ferreira & Vale (2021) approach cyberspace from a geographic point of view. They suggest, as does Boos (2017), that the notion of one cyberspace should shift to multiple cyberspatialities undergoing digital transformation. They present a flora of concepts that portray cyberspace such as the geographies of internet, cyber geography, geography of cyberspace and virtual geography. The authors also cite Graham (2013) and present the notion that cyberspace is a geographical metaphor, such as Huntley (2016) described cyber terrain. They also contend that cyberspace is influenced by the Cyber Divide, as does Boos (2016), by which different assemblages of data, people, devices, infrastructure and space creates, according to the authors, different cyberspatialities for different users.

Grant (2014) approach cyberspace from a combined military-geographical starting point. He presents a layered ontology meant to support military command & control processes. He includes the geographical layer, the physical layer, the information layer, the cognitive layer and the socio-organizational layer in his ontology. The geographical layer consists of physical locations and the paths between these. The physical layer consists of the physical objects of interest (e.g. devices and humans) and the links between these, such as cables and wireless transmission links. These have one or several locations on the geographical layer. Devices and links usually have a physical and virtual location. The information layer presents data and information, including the software processing it. The cognitive layer presents knowledge stored and relayed by humans. Knowledge and information may have a location based on the person possessing knowledge or the media containing the information. The authors separate knowledge into beliefs and operators. The socio-organizational layer presents the relationships between persons belonging to a group. Groups using ICT systems may have a physical and a virtual location.

Lü, Yuan & Yu (2021) further develops the concept of a ternary world. This concept divides the world into the physical, socio-human and the information world. The physical world are the traditional, physical domains of land, sea, air and space and the socio-human world the social relationships and civilizations that humans form. The information world links these to each other. The surveying and mapping of the information world has according to the authors not been developed. They propose that seven geographical elements and seven social-human elements should be used to form information geography.

Xu et al. (2019) use what they call the generally accepted three-domain model of cyberspace, consisting of the physical, logical and cognitive level. These levels include nodes and edges. The nodes and edges and entities are presented in table 1 below. Relationships and attributes are connected to the entities to form a description of cyberspace using graphs.

Table 1: Cyberspace features divided into three layers according to Xu et al.

	Physical Level	Logical Level	Cognitive Level
Nodes	network equipment, countries, cities	IP address, network applications, network services	identity, e-mail address, ID number
Edges	connection relationships between nodes	logical connections such as VPN, switching, peer-to-peer applications	interactions between nodes
Entities	devices and resources that form the network infrastructure	application services	media and people using physical level entities to participate on logical level services

Kou, Ni & Du (2022) approach cyberspace by defining targets for CSM. They classify targets into physical and virtual assets, with the goal to "*obtain comprehensive and complete information of various elements in cyberspace.*". The physical assets include firewalls and computers etc. but also intelligent wear and Internet of Things (IoT) devices. Of these assets, information, location and topological relationships are collected. Virtual assets are according to the authors mainly virtual human information, such as photos, e-mail and social media information. Zhao, Luo & Liu (2016) use the same division of physical and virtual assets when listing tools for CSM. They also include organizational structures and avatars as part of the virtual assets. According to them, the main objective of CSM of physical assets is defining a geographical location and of virtual assets to map social space.

4. Conclusions

The challenge of defining cyber terrain, cyberspace and the possible differences between them, remains. As emphasized by cyberspace geographers, cyberspace is heterogenic and changes constantly. The layers of cyberspace seem to have different inertia, and the geographic information usually changes more slowly than the virtual information. It is remarkable how little the temporal aspect of cyberspace, and how time affects the different levels or planes, is covered in research. The research on cyber terrain identifies the effect of time as part of its operational focus, but no clear description of these effects were found. The temporal dimension of cyberspace would require more research.

The definitions of cyber terrain and cyberspace agree on including physical devices, geographic location and the logical layer, but seems to differ on virtual representations. Though tree layers are often used to describe cyberspace, five layers is frequently used as well. The trend in cyber terrain research seems to be towards including cyber persona and other virtual aspects of cyberspace. Most researchers agree on presenting information and data to some extent, but for instance socio-organizational information or cyber persona information divides the research. The research on cyberspace geography, especially the research linked to the concept of the ternary world, seems to highlight cyber persona and socio-organizational aspects. Some expand cyber terrain into the electromagnetic spectrum or human knowledge spheres, without widespread support. It however seems clear that since cyberspace is a human construction, the definitions of it change depending on the portrayed need.

There seems to be a need to use the traditional military definitions and processes created to handle conflict in the Cartesian space also in cyberspace. This might seem practical for the military establishment, but some researchers question if valuable aspects of cyberspace are neglected this way. Especially the metaphor of cyber terrain is questioned – is there a clear need to define this analogy to physical terrain, or would it be more beneficial to use the concept of *key* cyber terrain as a metaphor for what in cyberspace is useful for the mission at hand. There is however call for a clear definition of which elements can be integrated into key cyber terrain and which cannot. It seems easier to define what cyberspace is, and more difficult to define what it at least is not. The tacit knowledge of subject matter experts seems to be essential as long as definitions and processes are developed.

Further research is needed to identify the tools and techniques for mapping cyberspace. Some previous research has been identified, and there are multiple identified tools available. It is not clear if all aspects and levels of cyberspace can efficiently be mapped. Furthermore, the collected information should be stored in an efficient way and presented when needed. These considerations would also benefit from further research.

References

Applegate, S. D.;Carpenter, C. L.;& West, D. C. (2017). Searching for digital hilltops, A Doctrinal Approach to Identifying Key Terrain in Cyberspace. *Joint Force Quarterly 84.1*, 18-23.

Bertoli, G.;& Raio, S. (2018). The elusive nature of cyber terrain. *Journal of Cyber Security and Information Systems*, 40-47.

Bodeau, D.;Graubart, R.;& Heinbockel, W. (2013). *Mapping the Cyber Terrain; Enabling Cyber Defensibility Claims and Hypotheses to Be Stated and Evaluated with Greater Rigor and Utility .* Bedford, MA: the MITRE corporation.

Boos, T. (2017). Geographies of Cyberspace: Internet, Community, Space, and Place. In *Inhabiting Cyberspace and Emerging Cyberplaces. Geographies of Media* (ss. 13-38). Palgrave Macmillan.

Dodge, M.;& Kitchin, R. (2003). *Mapping Cyberpsace.* London: Routledge.

Ferreira, D.;& Vale, M. (2021). From cyberspace to cyberspatialities? *Fennia 199(1)*, 113-117.

Franz III, G. J. (August 2012). *Effective Synchronization and Integration of Effects Through Cyberspace for the Joint Warfighter.* Baltimore: presentation at AFCEA TechNetLand Forces-East Conference in Baltimore, MD: Armed Forces Communications and Electronics Association.

Gao, C.;Guo, Q.;Jiang, D.;Wang, Z.;Fang, C.;& Hao, M. (2019). Theoretical basis and technical methods of cyberspace geography. *Journal of Geographical Sciences, volume 29*, 1949-1964.

Grant, T. (2014). On the Military Geography of Cyberspace. *Proceedings, 9th International Conference on Cyber Warfare & Security (ICCWS 2014)* (ss. 66-76). Purdue University, West Lafayette, IN, US: ICCWS.

Guion, J.;& Reith, M. (2017). Cyber terrain mission mapping: Tools and methodologies. *2017 International Conference on Cyber Conflict (CyCon U.S.)* (ss. 105-111). Washington D.C.: IEEE.

Huntley, W. L. (2016). *Cyber Key Terrain: A Conceptual Assessment.* U.S. Naval Postgraduate School.

Jabbour, K.;& Muccio, S. (2011). The Science of Mission Assurance. *Journal of Strategic Security, Volume IV Issue 2* , 61-74.

Jackson, N. (2016). *The Cyber War: Maintaining and Controlling the "Key Cyber Terrain" of the Cyberspace Domain .* Maxwell Air Force Base, Alabama: Air Command and Staff College, Air University.

Jakobson, G. (2011). Mission Cyber Security Situation Assessment Using Impact Dependency Graphs. *14th International Conference on Information Fusion* (ss. 1-8). Chicago, IL, US: IEEE.

Joint Chiefs of Staff. (2009). *Joint publication 2-01.3, Joint Intelligence Preparationof the Operational Environment.* Washington DC: Joint Chiefs of Staff.

Joint Chiefs of Staff. (2018). *Joint publication 3-12, Cyberspace Operations.* Washington DC: Joint Chiefs of Staff.

Kou, W.;Ni, L.;& Du, J. (2022). Research on Technical System for Cyberspace Surveying and Mapping. *Advances in Artificial Intelligence and Security. ICAIS 2022. Communications in Computer and Information Science, vol 1587.* (ss. 566-574). Springer.

La Pierre, H. (2020). *Intelligence Preparation Of The Operating Environment: Building Towards A Better Understanding Of Cyber Operations.* Toronto, Canada: Canadian Forces College, Collège des Forces Canadiennes.

Lemay, A.;Knght, S.;& Fernandez, J. (2014). Intelligence Preparation of the Cyber Environment (IPCE): Finding the High Ground in Cyberspace. *Journal of Information Warfare, Vol. 13, No. 3*, 46-56.

Lü, G.;Yuan, L.;& Yu, Z. (2021). Information geography: A new fulcrum of geographic ternary world. *Science China Earth Sciences, 65(2)*, 383-386.

Mills, J. R. (2012). The Key Terrain of Cyber. *Georgetown Journal of International Affairs,* , 99-107.

Moore, C. J. (2004). *Preparing the Virtual Battlefield for War: A Cyber Threat "Survival Kit" for Commanders.* Newport, RI, USA: Naval War College.

Phiter, P. W. (2010). Cyberspace: the Ultimate Complex Adaptive System. *the International C2 Journal vol. 4 num 2*, 1-30.

Price, P.;Leyba, N. A.;Gondree, M.;Staples, Z.;& Parker, T. (2017). Asset Criticality in Mission Reconfigurable Cyber Systems and its Contribution to. *Proceedings of the 50th Hawaii International Conference on System Sciences.* Hawaii.

Raymond, D.;Conti, G.;Cross, T.;& Fanelli, R. (2013). A Control Measure Framework to Limit Collateral Damage and Propagation of Cyber Weapons. *2013 5th International Conference on Cyber Conflict (CYCON 2013)* (ss. 1-16). Tallinn, Estonia: IEEE.

Raymond, D.;Conti, G.;Cross, T.;& Nowatkowski, M. (2014). Key Terrain in Cyberspace: Seeking the High Ground. *6th International Conference on Cyber Conflict (CyCon 2014)* (ss. 287-300). Tallinn: IEEE.

Williams, B. T. (2014). The Joint Force Commander's Guide to Cyberspace Operations. *Joint Force Quarterly 73*, 12-15.

Xu, R.;Zhang, Z.;Rao, Z.;Chen, J.;Li, M.;Liu, F.;& Pan, S. (2019). Cyberspace Surveying and Mapping: Hierarchical Model and Resource Formalization. *IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (ss. 68-72). IEEE.

Xu, Z.;& Li, G. (2011). Computing for the masses: Virtual extension. *Communications of the ACM*, 129-137.

Youn, J.;Oh, H.;Kang, J.;& Shin, D. (2011). Research on Cyber IPB Visualization Method based on BGP Archive Data for Cyber Situation Awareness. *KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS VOL. 15, NO. 2*, 749-766.

Zhao, F.;Luo, X.;& Liu, F. (2016). Research on cyberspace surveying and mapping technology. *Chinese Journal of Network and Information Security 9.2* , 1-11.