Csaba Krasznay – Péter Bányász – Éva Jakusné Harnos[1]

Geopolitical Context, Ideologies and Motivations

The 21st century global power shift has brought the revival if geopolitics both as a theory of international relations and a framework for analysis. Geopolitics is the study of the struggle for the control of geographical entities for political advantage. On the world stage, states are competing as strategic rivals using their territories and natural resources to a maximum in order to gain control over more. Competition for geopolitical power has material, relational and ideological dimensions. This means that, against the background of the race for material assets, relations, e.g. alliances and institutions are being restructured, and new ideologies are formulated in order to justify the objectives of the rising powers, while discourse about prevalent ideologies is amplified so as to stabilise the current international system established by the leading powers of the post-World War II era. So-called revisionist states have challenged the current status quo in international politics, first of all, China and Russia, and other ambitious rising powers can be seen in each region of the Globe. Fragmentation and re-arrangement impact nearly all components of the geopolitical framework: places, regions, territory and networks. This results in a re-interpretation of territoriality, regionality and identity, the re-conceptualisation of which is facilitated by modern technology, especially digital networks. The latter may also affect societies and disseminate ideologies unnoticed and at incredible speed. Consequently, the population of any country can be directly targeted by any system of beliefs and social or political philosophy, even hostile and subversive, which may lead to the loss of the internal and external sovereignty of a state. The power struggle for establishing a new world order has been extended to cyberspace. The importance of digital technology and the efficiency of digital networks is also proven by a case study of the Ukrainian–Russian war. Apart from the study of the effect of networks, two new factors should be considered: the geographical environment is changing due to climate impact; for instance, the Arctic has been drawn into

[1] Ludovika University of Public Service.

DOI: https://doi.org/10.36250/01236_10

the geopolitical competition; and the role and number of non-state actors is increasing, including NGOs, multinational corporations and high-tech giants.

The geopolitical perspective

Geopolitics in the traditional sense is an academic field studying the practice of states in their efforts to compete for territories and control them.[2] The theory was a justification of a country's regional or worldwide ambitions from the beginning. In the late 19th century, British scholars Alfred Thayer Mahan and Sir Halford Mackinder developed theories on the contest for land and sea power and resources. In parallel, German geopolitics was created by Friedrich Ratzel and Rudolf Kjellen, who claimed that developed states with more sophisticated culture had the right to occupy more territory. Karl Haushofer transformed the idea to extreme ideology under the rule of Hitler, which led to the disgrace of geopolitics and its disappearance from the language of politics after the Second World War for decades. In the United States, theoreticians of geopolitics took a more practice-oriented approach in the first half of the 20th century. For example, Isaiah Bowman, Nicholas Spykman and Alexander P. De Seversky discussed the global role of the U.S. and whether it should conduct an active or an isolationist foreign policy.[3] In Russia, the term and the perspective of geopolitics gained ground only in the 1990s,[4] but in the broad sense of interstate competition and less linked to geographical facts. Despite the criticism levelled at geopolitical theories, the early geopolitics scholars had relevant proposals which were accepted later. When Western strategists lay the foundations for NATO during the Cold War, they relied on Mackinder's 1924 recommendation to establish a Midland Ocean Alliance.[5] In addition, Mackinder's idea that global primacy is the question of who controls Eurasia has survived in Brzezinski's geostrategic views.[6] A comprehensive way of assessing power relations and great power competition is presented in Kissinger's World Order (1997). The major difference between early geopolitics and its contemporary trend is that

2 Flint 2006.
3 Flint 2006; Ashworth 2013.
4 Diec 2019.
5 Flint 2006.
6 Brzezinski 1997.

the former focused on the classification of territories of the Earth and their peoples into hierarchies so as to form a basis for war, alliance, or an empire, while the latter combines geographical and social knowledge so as to justify and interpret events in their overall context. Another important change has occurred in the concept of *geopolitical agent.* An agent is an entity that tries to achieve a specific objective. Nowadays states are not the only agents. Corporations, non-governmental organisations (NGOs) and various groups of people, such as a separatist movement or a group of Green activists can appear as agents. Agents may take a course of action depending on the situation and the structure in which they are embedded. Structures consist of legally enforceable rules and culturally accepted practices, that is, norms. Consequently, according to the current geopolitical perspective, not only geographical and social factors determine what agents do but also the system of international institutions and of international law. These generate expectations and decide what is acceptable. As for the role of states in the international system, agents can be *status quo states,* which want to maintain the current balance of power in the geopolitical space, or *revisionist states,* which have an interest in changing the balance even forcefully.[7] States strive for survival and they make any effort to gain as much power as possible, even aiming at hegemony. However, states cannot be certain about the intention of other states. In an effort to achieve their goals, states form alliances and establish international organisations and institutions.[8] For example, the liberal, multi-lateral institutions and the multi-level governance which we experience were established by the winner powers of the Second World War, including the United Nations Organization, NATO, the European Union, the International Monetary Fund, the World Bank. The international system is dynamic from a geopolitical perspective, that is, alliances and organisations keep transforming and re-drawing the geopolitical map. For instance, the United Kingdom exited from the European Union in 2020; Finland and Sweden have signed an accession bid to join NATO in 2022, and Iran and Argentina have applied to accede to BRICS. A coercive attempt to re-structure the geopolitical space is Russia's aggression against Ukraine and the following war, which will be discussed in a case study below. Since the realist perspective of geopolitics returned to the study of international relations, analyses have investigated the geopolitical aspirations and the underlying ideologies (see below) of revisionist

[7] Mearsheimer 2013; Mead 2014.

[8] Walt 1987.

states, especially, China, Russia and Iran.[9] Besides geopolitics, geo-economics has been used to maintain the current balance in contemporary international relations.[10] Whereas geopolitics breaks up the international system into regions, geo-economics may create macro-regions which, despite differences, may help maintain the liberal world order. Nevertheless, this idea has been challenged by China's ambitious New Silk Road Project announced in 2013, later re-named Belt and Road Initiative, which aims at establishing an extensive Eurasian sphere of influence.[11] Formerly, in this section the central role of *place,* more precisely, *space* was mentioned in addition to the key term *agent.* Researchers often distinguish between place (location), locale (local institutions which shape humans' identity) and sense of place (originating from collective identity).[12] However, space is a preferred term these days because of its multi-dimensional character. Key geographical places (features) are easy to identify on a map, for instance, continents, island, peninsulas, seas, oceans, straits, and historical experience suggests which may be fought over. But our perception of place, space and time is dynamic; that is, changes dependent on the circumstances. For instance, new geographical entities may gain significance as a result of the availability of minerals essential to IT industry. Probably, we need to adjust a map when states join or leave an international organisation, or when an ethnic group declares its independence from a state and it is recognised by the international community. Recently, due to climate change, the North Pole has become a territory of strategic importance which Western powers, Russia and China contest for. In consequence, NATO's commitment to safeguarding its security interest in the region has been declared.[13] The inclusion of space and cyberspace among the domains of military operations is also the outcome of our changing perception of *space* and of technological disruptions. The consequence of this change is stated in the strategic concepts of the alliance: Article 5 of the North Atlantic Treaty on collective defence can be invoked if a member is attacked.[14] Cyberspace has been created and maintained by human activity and its control has been crucial for nearly all fields of life, notably, for disseminating strategic narratives,

9 Mead 2014; Bolt–Cross 2018; Diec 2019.
10 Möttölä 2019.
11 Käpylä–Aaltola 2019; Leandro–Duarte 2020.
12 Starr 2013.
13 NATO 2022b.
14 NATO 2022a.

shaping international relations, influencing populations and conducting military operations, just to mention a few examples. Russia regards cyberspace a new domain for power competition referring to it as the *net empire,* which could be exploited for gaining the influence over foreign populations' minds.[15]

Ideologies, propaganda and strategic narratives

The interrelationship between political aspirations and pseudo-scientific theories developed for the justification of the objectives of state or non-state actors is illustrated by ideologies and strategic narratives, that is, types of persuasion. The present political struggle on the international world stage is interpreted as a clash of ideologies by some scholars.[16] Ideology is a set of beliefs, presented as a coherent world view that shapes norms and attitudes in society, leading to behaviour which is desirable for its propagator. It determines what is acceptable, right or wrong in a particular context.[17] Ideology always manifests in political discourse on certain focus topics and concepts, and has a regulatory impact on behaviour. Thus, the prominence of dominant political discourse in international relations is obvious: it sets the agenda, focuses or distracts attention and influences agents in their actions. This explains the importance of the media: the agents who have access to greater publicity will have more efficient strategic communication. The prevalent political discourse always seems obvious to people who are surrounded by it, and discourse which diverts because it represents different ideologies is noticed and identified as an attempt at persuasion. In the international struggle to establish a new world order all states have made propaganda strategies a component of their foreign policies.[18] Although the term "propaganda" has been discredited due to manipulation during the world wars, its definition could still be used as an umbrella term for all types of persuasion: it is "a deliberate, systematic attempt to shape perceptions, manipulate cognitions and direct behaviour to achieve a response that furthers the desired intent of the propagandist".[19] The transfer of ideology often takes the form of strategic narratives in international

[15] Diec 2019.
[16] Müllerson 2017.
[17] Jowett–O'Donnell 2015.
[18] Jowett–O'Donnell 2015.
[19] Jowett–O'Donnell 2015: 7.

relations. Narratives allocate meaning to past, present or future events and represent perceived interests. Zaffran[20] categorises strategic narratives into three types: system narratives (about international order), identity narratives (agents or actors in the international system) and policy narratives (justifying specific policies or action). In summary, the boundary between ideology and propaganda is narrow: ideology is a seemingly scientifically based system of ideas which is spread by propaganda. The most important communicator of ideas is language and its use in specific situations for political purposes is called political discourse. Propaganda comprises more than political discourse or strategic narratives because it exploits the communicative opportunities lying in language, media, sociological and psychological knowledge. Cyberspace has established new channels for disseminating rival ideologies and designing new techniques for persuasion, which may prove more effective than earlier as a result of multiple variants of disguise (see below). With the appearance of this virtual space, "cyberspace geopolitics" has evolved, with a combination of individual, institutional as well as state actors often involved in adversarial activities in order to gain superiority and occupy cyberspace, similarly to physical space. Contestation in cyberspace manifests in four layers according to Douzet: 1. physical infrastructure; 2. logistical infrastructure; 3. applications and data programmes; and 4. cognitive interactions.[21] Cyber diplomacy and efforts to set norms and legally regulate cyberspace activities have added a fifth layer to cyberspace according to Smith.[22] The layer of cognitive interactions is the location of the competing strategic narratives and influence operations of geopolitical players discussed above. The exploitation of cyberspace for malicious purposes poses a severe security threat because, due to the lack of boundaries, any disguised or covert actor can disrupt a society even in peacetime.

The sections below discuss information operations analysing a case study (cyberspace layer 4, cognitive interactions), then place the security issues of rivalry in cyberspace in geopolitical context (layers 1. physical infrastructure; 2. logistical infrastructure; and 3. applications and data programmes), also exploring the probable motivations of key players. The conclusion summarises the forecast of the UN Group of Governmental Experts on dangers arising from contestation in cyberspace and for cyberspace.

[20] Zaffran 2019.
[21] Douzet 2014: 4–5.
[22] Smith 2023:1225.

Case study: Russo–Ukrainian War

The military operation, launched by Russia on 24 February 2022, surprised the general community, despite the massive information operations that had been conducted by Ukraine and NATO, as well as by Russia, before the start of the war. The United States and its allies, including Ukraine, have regularly accused Russia of preparing to conduct a military attack against Ukraine. Meanwhile, Russia accused Ukraine with a constantly changing narrative, which was often more absurd, attempting to present itself as the victim (systematic genocide of the Russian minority, development of Covid in Ukrainian biological laboratories with U.S. support). The psychological operations that were part of the information operations increased significantly after the beginning of the war on all sides. In the early days of the war, Russia was unable to achieve its assumed goals of gaining aerial and information superiority, which resulted in a lengthened conflict – at the writing of this study, it is unclear when the armed conflict will end,[23] but the ongoing sanctions are pushing Russia towards a significant crisis.[24] The impact of sanctions also poses substantial challenges to European countries, especially regarding energy supply.[25] Among other things, the effects of the war have also drawn attention to the slowdown in the world economy and changes in global supply chains.[26] Presumably, Russia expected marginal reactions from the United States and the European Union following its aggression in 2014,[27] but from a geopolitical perspective, it chose a time for war when the different NATO and EU member state governments, given their domestic political developments, were interested in showing strict unity against Russian aggression and in supporting Ukraine significantly. Just a few examples:

- France had presidential elections during the war, and President Macron's campaign presented him as a strong leader and, in the post-Merkel period, as a visionary politician who would define the future of strong integration of the European Union.

[23] Yarchi 2022.
[24] Smith 2022.
[25] Doukas–Nikas 2022.
[26] Mariotti 2022.
[27] The fact that Finland and Sweden, breaking a decades-old taboo, indicated their desire to join NATO, which was supported by most NATO member states, is also an indication of the Russian side's misjudgement of the situation.

- There will be a mid-term election in the U.S. in the autumn of 2022, and the Biden Administration needs to show strong, competent leadership after the economic crisis caused by Covid-19 and the failed withdrawal from Afghanistan in August 2021.
- Although Poland has historically had severe misgivings about Russia, it has tried to resolve its conflict with the EU Commission on the issue of the rule of law.
- Turkey is heading into a severe recession, but President Erdogan has well recognised the reshaping of the balance of power in the Black Sea, which makes Turkey, and thus himself, an even more unavoidable stakeholder, as he will soon become a key actor in the world's grain supply and Europe's gas supply, in addition to the Syrian refugee crisis.

The length of the war surprised most experts, as there was general agreement on Russia's significant military capabilities. In addition to its conventional warfare capabilities, perhaps only Russia's cyber capabilities were – as far as we know today – significantly overestimated. Over the past decades, state-sponsored hackers linked to the Kremlin have been suspected of committing a series of paradigm-shifting cyberattacks that have shaped, guided and framed NATO's strategic thinking on cybersecurity. This includes not only the distributed denial-of-service (DDoS) attacks on Estonia's Critical Infrastructures of government, financial and media services in 2007,[28] but also the interference in the 2016 British Brexit referendum[29] and the American presidential election. Following these events, Russia was always suspected by the Western public to be behind the large-scale cyberattacks, and Russia, whether or not it was involved, used its intensive information operations to reinforce fears of Russian hackers' omnipotence.[30] The Homeland Security and FBI joint report investigating interference in the 2016 U.S. presidential election attributed Russia as the perpetrator.[31] Sophisticated cyberattacks can cause substantial damage because an attack is carried out not only in the physical dimension but also in the cognitive dimension. Following the already mentioned 2007 cyberattack against Estonia, several authors have considered the possibility of outlining scenarios for such complex cyberattacks.

[28] Lesk 2007; Arquilla 2013.
[29] Treisman 2018.
[30] Lanoszka 2019.
[31] Kovács–Krasznay 2017b.

In Hungary, for example, the authors analysed it in terms of Digital Mohács in 2010.[32] They then supplemented it with the impact of the 2016 U.S. presidential election in 2017.[33] The paradigm-shifting events of the Ukrainian–Russian conflict, which was the basis of the case study, inspired the authors to add a new addition, Digital Mohács 3.0, which is being prepared at the time of this writing. As will be seen later, cyberattacks and psychological operations in the cognitive dimension affect each other, not merely complement each other. The events of the recent war period have, in many ways, required us to rethink our perceptions of cybersecurity. Contrary to expectations, Ukraine has surprised us not only in its conventional warfare but also in its high level of cyber capabilities. In the latter, a significant contribution was made by so-called "cyber volunteers". These civilians were outraged by Russian aggression, in which the professional Ukrainian psychological operations also played a considerable part. As citizens of other countries, these hundreds of thousands of civilian volunteers were/are participating in the attack on Russian electronic information systems. Many of them are members of the IT Army, officially created by Ukraine. Volunteers have not only supported Ukraine but also a progressively growing number of pro-Russia groups, typically cybercriminal groups, in the beginning. For many years, Russia has used the Russian cybercriminals in its hybrid operations based on a silent agreement:

- Russian hackers can be active freely, but they cannot attack Russian targets, only foreign ones; and
- if the Russian state interest so requires, they should use their expertise to provide their contribution to Russia's operations in cyberspace

NATO declared at the Warsaw Summit in 2016 that cyberspace is a new field of domain in its strategic thinking.[34] The continuous strategic planning that has been going on since 2007 is necessarily able to reflect on the high-impact events that have occurred, and only on paper is it possible to plan for the capabilities and consequences of cyberspace as a field of domain. The Ukraine–Russia war, however, has rewritten the paper form and has given rise to many new types of threats whose responses we cannot assess today. In the first months of the war, Russia's electronic information systems were subjected to a tremendous amount

[32] Kovács–Krasznay 2010.
[33] Kovács–Krasznay 2017a.
[34] Kovács 2018.

of cyberattacks, with an extraordinary amount of data of various kinds being released, including personal data, financial data, and sensitive and classified data. In addition, large numbers of critical information infrastructures (transport systems, satellites, nuclear facilities, public utilities, etc.) were attacked. In addition to the cyberattacks, as mentioned above, a significant amount of psychological operations was carried out by the participating parties, with different aims. Ukraine, as the attacked party, was in a more favourable position, as it was easier to gain the support of the international public opinion. And this was vital to the war's outcome, as it meant that the European Union and NATO member states were held together, thwarting Russia's supposed expectations. This manifested not only in the acceptance of sanctions but also in substantial arms support, which at the time of writing has evened out the asymmetrical conditions between Ukraine and Russia. The psychological operations of conflict will be discussed in more detail in the chapter of the third volume of *Hybrid Warfare Reference Curriculum* entitled *Social Media: An Instrument of Public Diplomacy and a Weapon of Psychological Operations.* The successful psychological operations that Ukraine carried out led many young people from all over the world to feel the necessity to take a stand against Russian aggression, which led to the emergence of those above mentioned "cyber volunteers". Hundreds of thousands of young people have learned their offensive capabilities to penetrate protected systems without consequences. However, this involves a number of risks, of which one of the most important aspects is the "pacification" of "cyber volunteers" after the war is over. The critical question is how to ensure that they do not end up as cybercriminals, but instead use their skills ethically.[35] At the moment of writing, it is not yet clear when and in what form the war will end. What is certain is that the previous world order has been disrupted, with unforeseeable consequences. In future conflicts, cyber warfare will undoubtedly play an increasing role, with implications for the citizens of participating states and the entire world.

Cyberspace, the new domain

One of the most interesting sites of geopolitical struggle is cyberspace. While traditional physical dimensions such as the oceans, the poles and outer space have been the scene of intense competition between great powers throughout

[35] Feledy–Virág 2022.

history, digital technologies and the networks they create have only emerged lately and radically transformed our world in the last 30 years. Moreover, unlike physical space, which is mostly shaped by nature, cyberspace is a virtual space created entirely by humanity, and more specifically by the United States of America, which would not exist without the help of excellent scientists and U.S. government funding. Moreover, in cyberspace, it is not easy to identify the classical resources that could justify the special attention that this intangible space receives in the world political arena. The particular importance of cyberspace must be sought in the social and economic development of the 21st century. Computers began to proliferate in the 1980s, the Internet in the 1990s. At that time, the Internet was primarily a playground for a few million Western scientists and engineers. Today there are nearly 5 billion internet users globally. Although the importance of computers was clear from the beginning, with their use spreading steadily in both government and business, few people imagined that the digital space would one day become a dominant issue in world politics after the fall of communist regimes and the dawn of the global expansion of Pax Americana. However, U.S. government policy at the time foresaw the internet as a tool for global dominance. One of the early, but perhaps most important strategies of Bill Clinton's first presidency was *The National Information Infrastructure: Agenda for Action (NII).* It includes the following objective: "The benefits of the NII for the nation are immense. An advanced information infrastructure will enable U.S. firms to compete and win in the global economy, generating good jobs for the American people and economic growth for the nation. As importantly, the NII can transform the lives of the American people – ameliorating the constraints of geography, disability, and economic status – giving all Americans a fair opportunity to go as far as their talents and ambitions will take them. […] Information is one of the nation's most critical economic resources, for service industries as well as manufacturing, for economic as well as national security. By one estimate, two thirds of U.S. workers are in information-related jobs, and the rest are in industries that rely heavily on information. In an era of global markets and global competition, the technologies to create, manipulate, manage and use information are of strategic importance for the United States. Those technologies will help U.S. businesses remain competitive and create challenging, high paying jobs. They also will fuel economic growth which, in turn, will generate a steadily-increasing standard of living for all

Americans."[36] These ideas foreshadowed the need for the powers competing with the U.S. to be able to offer an alternative in the field of information technology and to develop their own capabilities. At the time of the Agenda's publication, Japan appeared to be the most competitive country in this area, but by the 2020s, China is clearly the country that is the main challenger to the U.S. in the technological field. For a country that was economically insignificant in the early 1990s, China's emergence as a second power, a clear competitor to the U.S., is extraordinary. Paradoxically, the global opening of the Pax Americana has helped a lot. Chinese students turned up en masse at the best universities in the U.S., while U.S. manufacturers opened manufacturing plants in China in the hope of cheap labour. Ostensibly, it was all about the U.S. economic advantage, as the brain drain strengthened the U.S. knowledge economy, while the resulting products could be made as cheaply as possible in Asia. In the 2000s, however, Chinese engineers and scientists began to return home and put their knowledge to work in Chinese universities and companies. Intellectual property that was brought to China in the course of manufacturing was treated rather loosely by the locals, who copied Western solutions to the point of industrial espionage. No wonder that by the 2010s, the intellectual capital and manufacturing capacities to create digital products and services had been created.[37] The 12th Five-Year Plan, adopted in 2012, explicitly supports the strengthening of manufacturing capabilities in emerging technologies, and the 13th Five-Year Plan in 2017 puts a strong emphasis on the diffusion of technologies such as mobile technology, cloud computing or the Internet of Things. The China 2025 strategy makes it clear that China's goal is to become the strongest "cyber power".[38] However, it is questionable whether this can be achieved. The U.S. already recognised the Chinese threat in the technological field during the Obama presidency and has tried to push back against it with tough sanctions during the Trump presidency (from the ban on 5G technologies, to the blocking of some Chinese mobile phone manufacturers from U.S. software, to the attempted acquisition of one of the most popular Chinese-owned social networks). Under President Biden, this trend is deliberately continuing, with China as the primary strategic adversary for the U.S., and he is doing everything he can to maintain U.S. global position and

[36] The White House 1993: 3.
[37] Zhang–Zhou 2015.
[38] Godement et al. 2018: 2.

break China's emergence as a (cyber)power. However, there are a number of points in the relationship between the two superpowers that will leave open the question of dominance over cyberspace in the coming decades.[39] Perhaps the most important question is how the post-World War II world politics based on multilateral relations and international organisations will be transformed. Russia's military aggression against Ukraine and the annexation of sovereign Ukrainian territories by a member of the UN Security Council clearly shakes up the international order, upsets the status quo and could reinforce China's intentions to shape an international order that is fit for the 21st century, including a national shift in global (U.S.-dominated) cyberspace, helping to create a 'splinternet' of national networks. Another important issue is China's intentions in relation to Russia and Taiwan. Russia's belligerent aggression is punished by the Western world with heavy technological sanctions, so if Russia wants to keep its economy in the 21st century, it has only China to rely on. In cyberspace, Russia has been fighting U.S. dominance for decades and exploiting the leverage of technology to achieve its own ends, but its belligerence will cut it off from these opportunities for a longer period of time, both diplomatically and technically. However, it has typically moved with China in cyber diplomacy, so it is likely that intentions will not change, but will be articulated by China in the future, primarily in its own interests. Thus, Russia will in all likelihood lose its position as a cyber power and become dependent on China. The case of Taiwan is particularly important for cyberspace because it currently produces roughly two-thirds of the world's chips and although there are serious aspirations to bring some of this manufacturing capacity back to the U.S., this is only conceivable at least in a decade. Therefore, if China interferes in Taiwan's trade, either by blockade or direct military strike, it will certainly have a longer-term impact on the digital economy in the U.S. and the world as a whole, given that the production and supply of basic cyberspace infrastructure such as computers, mobile devices and networking solutions will be at stake. Apart from these three powers, there are no other actors who have a meaningful say in the shaping of cyberspace. Some regional powers, such as the European Union, are actively trying to shape the rules of cyberspace, but there is a clear sense of an East–West confrontation, led by the U.S. on one side and China and Russia on the other.

[39] Hass–Blanchette 2022.

Conclusion

This can be clearly traced within the UN, where since the early 2000s, the so-called Group of Governmental Experts (GGE) has been working on international relations in cyberspace, with a focus on the West. But in 2019, on Russia's initiative, a parallel group, the Open Ended Working Group (OEWG), was created to deal with essentially the same issues as the GGE, but with an emphasis on the East. And while of course digital transformation due to Covid-19 and the Russian–Ukrainian war are in the process of completely rewriting the balance of power in cyberspace, it is worth reviewing what the GGE 2021 report identified as the major threats along which the power relations in cyberspace will evolve over the next decade:

- "While ICTs and an increasingly digitalized and connected world provide immense opportunities for societies across the globe, the Group reaffirms that the serious ICT threats identified in previous reports persist. Incidents involving the malicious use of ICTs by States and non-State actors have increased in scope, scale, severity and sophistication. While ICT threats manifest themselves differently across regions, their effects can also be global.
- The Group underlines the assessments of the 2015 report that a number of States are developing ICT capabilities for military purposes; and that the use of ICTs in future conflicts between States is becoming more likely.
- Malicious ICT activity by persistent threat actors, including States and other actors, can pose a significant risk to international security and stability, economic and social development, as well as the safety and well-being of individuals.
- In addition, States and other actors are actively using more complex and sophisticated ICT capabilities for political and other purposes. Furthermore, the Group notes a worrying increase in States' malicious use of ICT-enabled covert information campaigns to influence the processes, systems and overall stability of another State. These uses undermine trust, are potentially escalatory and can threaten international peace and security. They may also pose direct and indirect harm to individuals.
- Harmful ICT activity against critical infrastructure that provides services domestically, regionally or globally, which was discussed in earlier GGE reports, has become increasingly serious. Of specific concern is malicious

ICT activity affecting critical information infrastructure, infrastructure providing essential services to the public, the technical infrastructure essential to the general availability or integrity of the Internet and health sector entities. The Covid-19 pandemic has demonstrated the risks and consequences of malicious ICT activities that seek to exploit vulnerabilities in times when our societies are under enormous strain.

- New and emerging technologies are expanding development opportunities. Yet, their ever-evolving properties and characteristics also expand the attack surface, creating new vectors and vulnerabilities that can be exploited for malicious ICT activity. Ensuring that vulnerabilities in operational technology and in the interconnected computing devices, platforms, machines or objects that constitute the Internet of Things are not exploited for malicious purposes has become a serious challenge.
- Capacities to secure information systems continue to differ worldwide, as do the capacities to develop resilience, protect critical information infrastructure, identify threats and respond to them in a timely manner. These differences in capacities and resources, as well as disparities in national law, regulation and practices related to the use of ICTs, and unequal awareness of and access to existing regional and global cooperative measures available to mitigate, investigate or recover from such incidents, increase vulnerabilities and risk for all States.
- The Group reaffirms that the use of ICTs for terrorist purposes, beyond recruitment, financing, training and incitement, including for terrorist attacks against ICTs or ICT-dependent infrastructure, is an increasing possibility that, if left unaddressed, may threaten international peace and security.
- The Group also reaffirms that the diversity of malicious non-State actors, including criminal groups and terrorists, their differing motives, the speed at which malicious ICT actions can occur and the difficulty of attributing the source of an ICT incident all increase risk."[40]

[40] United Nations General Assembly 2021: 7.

Questions

1. What is the difference between classical and modern geopolitical theories?
2. Why is our perception of time, place and space changing?
3. How are ideology and strategic narrative connected?
4. What may be the geopolitical implications of the Russia–Ukraine war?
5. Why has cyberspace become the new location for geopolitical struggle?

References

Arquilla, John (2013): Twenty Years of Cyberwar. *Journal of Military Ethics,* 12(1), 80–87. Online: https://doi.org/10.1080/15027570.2013.782632

Ashworth, Lucian M. (2013): Mapping a New World: Geography and the Interwar Study of International Relations. *International Studies Quarterly,* 57(1), 138–149. Online: https://doi.org/10.1111/isqu.12060

Bolt, Paul J. – Cross, Sharyl N. (2018): *China, Russia, and Twenty-first Century Global Geopolitics.* Oxford: Oxford University Press. Online: https://doi.org/10.1093/oso/9780198719519.001.0001

Brzezinski, Zbigniew (1997): *The Grand Chessboard. American Primacy and its Geostrategic Imperatives.* New York: Basic Books.

Diec, Joachim (2019): Major Trends in Russian Geopolitics after 1991. *Politeja,* 5(62), 141–160. Online: https://doi.org/10.12797/Politeja.16.2019.62.08

Doukas, Haris – Nikas, Alexandros (2022): Europe's Energy Crisis – Climate Community Must Speak Up. *Nature,* 608(7923), 472–472. Online: https://doi.org/10.1038/d41586-022-02199-5

Douzet, Frédérick (2014): Understanding Cyberspace with Geopolitics. *Hérodote,* (152–153), 3–21. Online: www.cairn-int.info/article-E_HER_152_0003–understanding-cyberspace-with-geopolitic.htm

Feledy, Botond – Virág, Csaba (2022): An Assessment of Cyber Volunteer Groups in Interstate Conflicts and Their Impact on Public Policies. *Scientia et Securitas,* 3(1), 12–18. Online: https://doi.org/10.1556/112.2022.00091

Flint, Colin (2006): *Introduction to Geopolitics.* London – New York: Routledge. Online: https://doi.org/10.4324/9780203503768

Godement, François – Stanzel, Angela – Przychodniak, Marcin – Drinhausen, Katja – Knight, Adam – Kania, Elsa B. (2018): *The China Dream Goes Digital: Technology in the Age of Xi.* European Council on Foreign Relations. Online: https://ecfr.eu/publication/the_china_dream_digital_technology_in_the_age_of_xi/

Hass, Ryan – Blanchette, Jude (2022): *Central Questions in U.S.–China Relations amid Global Turbulence.* Center for Strategic and International Studies. Online: www.csis.org/analysis/central-questions-us-china-relations-amid-global-turbulence

Jowett, Garth S. – O'Donnell, Victoria J. (2015): *Propaganda and Persuasion.* Los Angeles: SAGE.

Käpylä, Juha – Aaltola, Mika (2019): Critical Infrastructure in Geostrategic Competition: Comparing the US and Chinese Silk Road Projects. In Wigell, Mikael – Scholvin, Sören – Aaltola, Mika (eds.): *Geo-economics and Power Politics in the 21st Century. The Revival of Economic Statecraft.* London – New York: Routledge, 43–60. Online: https://doi.org/10.4324/9781351172288-4

Kissinger, Henry (2014): *World Order.* New York: Penguin Press.

Kovács, László (2018): Cyber Security Policy and Strategy in the European Union and NATO. *Land Forces Academy Review,* 23(1), 16–24. Online: https://doi.org/10.2478/raft-2018-0002

Kovács, László – Krasznay, Csaba (2010): A digital Mohács, egy kibertámadási forgatókönyv Magyarország ellen. *Nemzet és Biztonság,* 3(1), 44–56.

Kovács, László – Krasznay, Csaba (2017a): Digitális Mohács 2.0: Kibertámadások és kibervédelem a szakértők szerint. *Nemzet és Biztonság,* 10(1), 3–16.

Kovács, László – Krasznay, Csaba (2017b): „Mert övék a hatalom": Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során. *Nemzet és Biztonság*, 10(3), 3–15.

Lanoszka, Alexander (2019): Disinformation in International Politics. *European Journal of International Security,* 4(2), 227–248. Online: https://doi.org/10.1017/eis.2019.6

Leandro, Francisco José B. S. – Duarte, Paulo Afonso B. eds. (2020): *The Belt and Road Initiative. An Old Archetype of a New Development Model.* Singapore: Palgrave Macmillan. Online: https://doi.org/10.1007/978-981-15-2564-3

Lesk, Michael (2007): The New Front Line: Estonia under Cyberassault. *IEEE Security and Privacy Magazine,* 5(4), 76–79. Online: https://doi.org/10.1109/MSP.2007.98

Mariotti, Sergio (2022): A Warning from the Russian–Ukrainian War: Avoiding a Future that Rhymes with the Past. *Journal of Industrial and Business Economics,* 49, 761–782. Online: https://doi.org/10.1007/s40812-022-00219-z

Mead, Walter R. (2014): The Return of Geopolitics: The Revenge of the Revisionist Powers. *Foreign Affairs,* 93(3), 69–79.

Mearsheimer, John J. (2013): Structural Realism. In Dunne, Tim – Kurki, Milja – Smith, Steve (eds.): *International Relations Theories. Discipline and Diversity.* Oxford: Oxford University Press. Online: https://doi.org/10.1093/hepl/9780198814443.003.0003

Möttölä, Kari (2019): US Grand Strategy in Flux. Geo-Economics, Geopolitics, and the Liberal International Order. In Wigell, Mikael – Scholvin, Sören – Aaltola, Mika (eds.): *Geo-economics and Power Politics in the 21st Century. The Revival of Economic Statecraft.* London – New York: Routledge, 89–98. Online: https://doi.org/10.4324/9781351172288-7

Müllerson, Rein (2017): *Dawn of a New Order. Geopolitics and the Clash of Ideologies.* London – New York: I. B. Tauris. Online: https://doi.org/10.5040/9781350986022

NATO (2022a): *NATO 2022 Strategic Concept.* Online: www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

NATO (2022b): *Joint press conference with NATO Secretary General Jens Stoltenberg and the Prime Minister of Canada, Justin Trudeau.* Online: www.nato.int/cps/en/natohq/opinions_206908.htm?selectedLocale=en

Smith, Elliot (2022): Russia Faces "Economic Oblivion" Despite Claims of Short-Term Resilience, Economists Say. *CNBC,* 2 August 2022. Online: www.cnbc.com/2022/08/02/russia-faces-economic-oblivion-despite-short-term-resilience.html

Smith, Hanna (2023) The Geopolitics of Cyberspace and the European Union's Changing Identity. *Journal of European Integration,* 45(8), 1219–1234. Online: https://doi.org/10.1080/07036337.2023.2277329

Starr, Harvey (2013): On Geopolitics: Spaces and Places. *International Studies Quarterly,* 57(3), 433–439. Online: https://doi.org/10.1111/isqu.12090

Stoltenberg, Jens (2022): *NATO Is Stepping Up in the High North to Keep Our People Safe.* Online: www.nato.int/cps/en/natohq/opinions_206894.htm?selectedLocale=en

The White House (1993): *The National Information Infrastructure: Agenda for Action.* Online: https://clintonwhitehouse6.archives.gov/1993/09/1993-09-15-the-national-information-infrastructure-agenda-for-action.html

Treisman, Daniel ed. (2018): *The New Autocracy. Information, Politics, and Policy in Putin's Russia.* Washington, D.C.: Brookings Institution Press.

United Nations General Assembly (2021): *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security.* New York: United Nations General Assembly.

Walt, Stephen M. (1987): *The Origins of Alliances.* Ithaca: Cornell University Press.

Yarchi, Moran (2022): The Image War as a Significant Fighting Arena – Evidence from the Ukrainian Battle over Perceptions during the 2022 Russian Invasion. *Studies in Conflict and Terrorism,* 1–13. Online: https://doi.org/10.1080/1057610X.2022.2066525

Zaffran, Raphaël (2019): Strategic Narrative and Security. In Taylor, Bryan C. – Bean, Hamilton (eds.): *The Handbook of Communication and Security.* New York: Routledge, 354–367. Online: https://doi.org/10.4324/9781351180962-21

Zhang, Ying Ying – Zhou, Yu (2015): *The Source of Innovation in China. Highly Innovative Systems.* Houndmills: Palgrave Macmillan. Online: https://doi.org/10.1057/9781137335067