Bogdana Sybikowska  
University of Warsaw

THE NEW COLD WAR: CYBER FRONTLINE

DOI: 10.2478/ppsr-2022-0010

Author  
Bogdana Sybikowska is a PhD candidate at the University of Warsaw, specializing in international security and cybersecurity with a specific focus on the Eastern Partnership region and Russia.

ORCID no. 0000-0003-2743-0257  
e-mail: bogdana.sybikowska@gmail.com

Abstract  
The ongoing escalation of animosities between the United States, the Russian Federation and the People’s Republic of China is beginning to resemble the Cold War, which as a historical period might have ended in the twentieth century, but still endures as a state of hostilities between the countries, expressed in the form of an indirect conflict. These countries are actively growing their cyber capabilities that enable indirect and covert operations aimed at their opponents. In cyberspace, the states involved express the hostilities and the aims they try to achieve in the least detectable way. As a result, cyberspace has been securitized. It has been recognized by NATO as a domain of activities. In the United States, the National Cybersecurity Strategy has been published, recognizing cyberspace as an integral part of the economy and defence. A similar document called the Information Security Doctrine was issued in the Russian Federation, which manifests Russia’s aspirations in the field of information technology. The militarization of this area shows that cyberspace is becoming a battlefield in the new cold war. The Russian military invasion of Ukraine is complemented by the activities in the cyberspace. I analyse the new confrontation between the above-mentioned powers, looking for features of the Cold War in it. In particular, I examine the cyber capabilities of the United States, Russia and China. The article claims that the concept of cold war may be applicable to numerous historical eras, including the one that is still in effect now.

Keywords: The United States, Russia, China, cold war, cybersecurity

Introduction  
Historians argue as to the date when the Cold War officially ended. Some point to November 9, 1989 and the fall of the Berlin Wall, while the others suggest the dissolution of the Soviet Union as the official ending of the conflict (Guyatt 2013). The Cold War might have ended in the twentieth century, but a cold war, as a state of hostilities between states, expressed in the form of an indirect conflict, can be applicable to other historical periods, including the one that endures now. This article analyses the current condition of the international affairs, claiming a continuation of a cold war as a state of indirect confrontation between the USA, the People’s Republic of China and the Russian Federation. The militarization of cyberspace that has happened in the 21st century allowed for a conflict between these countries to be extended into the cyber domain. Within that context, cyber activity increases, mirroring the state of confrontation between the United States, Russia and China. These countries have been formulating their cyber strategies for years and it is feasible to portray the cold confrontation based on the cyber strategies and activities that
the countries conduct. This unconventional confrontation resembles the one that took place during the Cold War. I believe that the resemblance can be explained by labeling it with the general term of “cold war” that is applicable to an indirect war between any states in any given period of time.

The main research questions that are answered are:
- Is there a state of a cold war in current global affairs?
- In what ways this cold war is similar to the historical one from the 20th century?
- How is it manifested in a cyberspace?

I verify the following research hypothesis: a cold war as a state is applicable to current international affairs between the United States, the Russian Federation and the People's Republic of China. My goal is to describe the current setting in global affairs from the perspective of elements that were characteristic for the period of the Cold War in the 20th century and apply that description in the cyberspace setting. The factors that indicate a cold war as a condition of hostilities between countries permit the understanding of the techniques and methods that the states are using in the confrontation. For the purpose of this research, I use a comparative method, which allows me to qualitatively look for patterns of similarities and differences, explaining the current state of affairs in the world. The comparable variables that help to determine a state of a cold war are proxy wars, polarity, ideology, disinformation and Mutual Assured Distraction. These are examined through the lens of cyber activities of the aforementioned countries. This comparative research allows me to conclude on the state of a cold war in current international affairs, or a lack thereof. The cold war is examined with a specific focus on cyber domain as a battlefield. Through cybersecurity strategies and activities of countries involved, it is visible what is the level of animosity and the aims the states try to achieve. The literature that explores the topic of cyberspace as the new frontier of geopolitics includes, but is not limited to, Tim Maurer’s *Cyber Mercenaries: The State, Hackers, and Power* and Ben Buchanan’s *The Hacker and the State Cyber Attacks and the New Normal of Geopolitics*.

**The new Cold War: outlook**

In 1989, Francis Fukuyama published an essay, boldly titled *The End of History*, predicting the end of ideological confrontation and the victory of western liberal democracy. According to the scholar the triumph of western liberal democracy marks a finish of mankind’s historical evolution achieved through conflict. Western liberal democracy did not go unchallenged though. Today, a cold war as a term is most famous for the tensions between two World War II allies, the United States and the USSR. However, the unresolved matters from World War II remained. The Russian Federation, as a successor of the USSR, wanted to take its place on the international arena on its own terms. The domestic discussions on Russian foreign policy suggest that Russia maintains the Cold War patterns of thinking. Russian revisionist narratives and global claims imply that, for this country, the Cold War never ended. The Russian Federation is also exercising realpolitik through the United Nations Security Council, where the country holds a permanent seat.

Russia has a revisionist approach to international order and, as an internationally recognized successor of the Soviet Union, aims to re-establish the position the USSR once
President of the Russian Federation, Vladimir Putin proclaimed a revanchist policy on multiple occasions, making territorial claims to its neighbours by suggesting that sovereign territories of the republics are “gifts” of the Russian people (Altynbayev 2020; “Address by the President of the Russian Federation”, 2022). Similarly to the Cold War times, Russia perceives NATO as a principle threat to its national security (Tsygankov 2018). The alliance’s enlargement and infrastructure deployment near Russian borders are viewed as a threat in the country. The Russian Federation still sees the world in Cold War terms, the war that in its opinion it never lost. The country perceives a current rivalry as an attempt to establish hegemony by the United States and its allies, while Russia plays a role of restoring real balance of power and bringing back the international stability (Weitz 2016). In its current form, the confrontation between Russia and the West has resumed with the rise of the Russian economy at the beginning of 2000s, caused by an increase in global energy prices and the growth in revenues from oil and gas exports. At the same time, Russia’s technological backwardness compared to the West became critical. The country has a strategic disadvantage when compared to the United States, but it is trying to use cyberspace to level the playing field and influence other countries’ agenda. Russia is actively developing cyber capabilities that enable them to compensate for the gap between conventional military and economic capabilities. With the invasion of Ukraine, Russia claimed their disregard of the international law that forbids the use of force as per the Article 2(4) of the United Nations Charter. Russian President Vladimir Putin detests the US and NATO allies by threatening the West with “consequences greater than any you have faced in history” if Western countries decide to interfere in Russia-Ukraine war, claiming its sphere of influence. In June 2022, the Foreign Minister of Russia Sergey Lavrov claimed that the iron curtain between Russia and the West is already descending (InterFax.ru 2022).

The US-China confrontation has been recently on a rise as well. Donald Trump’s presidency marked a period of increasing hostilities between the People’s Republic of China and the United States. President Xi Jinping addressed the possibility of a new cold war in a speech at World Economic Forum conference on January 25, 2021 (Elliott 2021). The economic measures applied by China are mainly tariffs, trade boycotts, trade restrictions, pressure on certain foreign companies and other targeted financial measures. A deep trade connection makes the economies of the two states vulnerable to the use of economic measures for political and economic purposes (Boylan; McBeath; Wang 2021). The United States accuses China of behavior that deviates from the World Trade Organization norms. The country’s government, according to the US, subsidises various industries, steals intellectual property, deliberately undervalues its currency and imposes trade barriers (Boylan; McBeath; Wang 2021, 24). China, in turn, is pushing for the abolition of high trade tariffs on Chinese goods that were introduced by the Trump administration. It also accuses the United States of obstructing the country’s successful tech companies like Huawei (Boylan; McBeath; Wang 2021, 33). The conflict between the two countries, however, goes beyond trade. They disagree on human rights issues and Hong Kong’s national security law (BBC News 2020). The People’s Republic of China is demanding the United States to stop interfering in what China considers to be its internal affairs and vilifying the ruling Communist Party. In the most recent Interim National Security Strategic Guidance from 2021 the United States focused its attention on China, which is characterized as “the only competitor potentially capable of combining its economic, diplomatic, military, and tech-
nological power to mount a sustained challenge to a stable and open international system” (The White House 2021). Robert D. Kaplan (2019) from the Centre for a New American Security believes that the US-China relations are “nothing less than a new cold war: The constant, interminable Chinese computer hacks of American warships’ maintenance records, Pentagon personnel records, and so forth constitute war by other means. This situation will last decades and will only get worse”. However, China did not declare the United States as its official enemy. Its approach is rather patient and restrained. Even amidst the escalated tensions caused by Nancy Pelosi’s visit to Taiwan on August 2, 2022, these tensions have not escalated into a military confrontation. China has been accused of cyber espionage and attacks on corporate and infrastructure computer systems on multiple occasions. The United States blame China on targeted attacks against the U.S. government and defence-related computer systems (BBC News 2018).

The tensions between the USSR and the US gave the term “cold war” its current notoriety. The term “Cold War” was first introduced by Bernard Baruch, adviser to US President Harry Truman (Gerber 1982). The Cold War implied an invisible danger, but not yet a large-scale armed conflict. George Orwell (1945), in his article You and the Atom Bomb, defined the Cold War as the relationship between nuclear super-states and the rest of humanity, the epoch “as horribly stable as the slave empires of antiquity.” The power division between those who are capable of conceiving nuclear arsenals and those who are not was impassable, permanently securing a standstill and prolonging “a peace that is no peace” (Orwell 1945). As nuclear weapons made a direct confrontation potentially exceedingly destructive and deadly, thus highly undesirable, a substitute for a direct conflict between superpowers developed. The main feature of the Cold War is the costs of conventional warfare that are too high to conduct it. All actors in the international arena should understand it and behave accordingly. When the costs of an actual direct war increase, states start to reach out to unconventional instruments. Complete annihilation precipitated by nuclear weapon proliferation became probable as soon as nuclear parity was reached by the United States and the USSR. These countries started to avoid an escalation of hostilities through proxy wars. In general, proxy wars became a way of exercising power that was distributed between two power centers. During the Cold War, when there were only two superpowers both in possession of weapon of mass destruction, the only possible model that maintained stability and security in the bipolar world was the balance of power. The two factions not only tried to strategically outplay each other, but they also believed in the global triumph of their socio-economic and political systems, in their ideology. In essence, it was a confrontation of Western capitalism against communism, an ideology that tried to “take over” the world with a communist revolution. Both the United States and the Soviet Union used special techniques to make their ideology more appealing in the eyes of public in the times of warfare. Psychological warfare became an important tool in conducting the Cold War, similar to other conventional military instruments. It involved a dissemination of selected information, threats, psychological pressure and disinformation. Psychological warfare plays a crucial role in conflicts where the use of conventional techniques is limited. This is particularly evident in the case of the Cold War when nuclear weapon proliferation made the costs of a direct confrontation too high. The end of the Second World War demonstrated the full capacity of destruction caused by nuclear weapons, which essentially changed the nature of warfare. The enormous destructive power of nuclear weapons and the possibility of their ultra-fast deployment with a help of
ballistic missiles generated fears of an abrupt, unexpected attack, with the aim of causing a tremendous damage to the opponent, disable the nuclear missile arsenal and the enemy’s armed forces and thereby force them to surrender. The United States and the USSR saw the only way of avoiding this appalling scenario and strengthening their security in guaranteeing a retaliatory strike on such a scale that the opponent considered aggression completely unfeasible. This concept was formalized and defined in a military doctrine, named Mutual Assured Destruction. Summing up, the Cold War in the 20th century was characterized by proxy wars conducted by superpowers via client states; polarity that kept the system stable; ideology that shaped foreign policy; psychological warfare; and the presence of weapons of mass destruction. Later in this research, I use these comparative variables to examine the current state of affairs through the historical perspective. I believe that the cyberspace would be the most suitable setting to display the confrontation.

What makes cyberspace appealing as a theater for animosities between countries involved in a cold war is that it might be difficult to determine who is a threat actor and who is managing it due to a proxy relation between a state-sponsor and operator. Therefore, countries are more willing to express their hostilities in a cyberspace that becomes a battlefield, which is available for all interested actors. Moreover, there is no regulatory scheme for the cyberwarfare, as it is not clear how the Geneva Convention or international humanitarian law applies to it (Khalip 2018). In order to investigate the new cold war through the prism of its manifestations in cyberspace, it is necessary to analyze its nature and characteristics, finding patterns of conflict, exploring the current state of affairs through historical features of a cold war as compared to those experienced currently. I continue with a further analysis of the Cold War through five specific features: proxy wars conducted by superpowers via client states, polarity that keeps the system stable, ideology that shapes foreign policy, psychological warfare and the presence of weapons of mass destruction.

Proxy wars

Throughout the Cold War a great number of small conflicts in different parts of the world flared. Being regional, local, intra- or interstate, the superpowers used those wars to advance their regional or global interests. This type of armed conflicts was defined by the term “proxy wars.” The notion refers to great powers’ hostility expressed via client states rather than being resolved directly between them (Yeisley 2011). Proxy warfare became a way of exercising animosity during the Cold War due to a heightened price of the immediate confrontation between the United States and Soviet Union (Bar-Siman-Tov 1984). Those countries tried to expand the sphere of influence and spread their ideology achieving political goals and security.

Proxy wars again became a way of indirect hostilities. The advantage of cyber warfare in this context is a complexity of determining who is a threat actor, and thus a rising attribution challenge. The impunity with which states operate on a cyber arena, blaming the attacks on non-state actors, allow for covert means of pursuing national interests and expressing hostility in an indirect form (Schmitt; Vihul 2014). Still, based on the aim, intention and scope of the action, some covert cyber operations can be associated with certain states. This is a form of a hybrid warfare that coincides with the definition of proxy as it was perceived during the Cold War. Hybrid warfare is a combination of kinetic or
non-kinetic actions with a use of shadowy actors that is aimed at achieving the goals by creating “exploitable ambiguity” (Cormac, Aldrich 2018, 490). State and non-state actors can be coordinated together, and as a result become blurred into one force (Hoffman 2007, 8). The strategic relation between state-sponsor and non-state actors is a proxy one (Rauta 2019). This relation implies that a state can delegate, orchestrate or sanction non-state actors (Maurer 2017). There is a long tradition of states using non-state actors for the strategic purposes. This tendency is specifically observed in a cyber domain. Since conventional warfare is perceived to be expensive and risky, cyberspace as a battle space is becoming a new way of conducting hostilities. Proxy actors include hacker groups, private companies and organized crime. A state can benefit from the actions of non-state actors that cannot be directly and unquestionably associated with it. Governments rely on private sector as a part of their national security strategy. It is not a classic form of a cold war, neither does it establish the rules for a classic deterrence. Nevertheless, the understanding of how a cold war can be conducted evolves together with technology. The way that proxies are used depend on how a state defines and understands cybersecurity (Maurer 2017, 6).

Russia actively uses proxy actors in a cyber domain as part of its strategy in a current cold war. It is also a hub for cyber criminals (Maurer 2018). The government disregards their malicious activity as long as they target victims from states considered as enemies. These are actors that have a proxy relationship with their state-sponsors, a relation that is typically distinguishing for a cold war. There are multiple threat groups acting on behalf of Russian government. One of the most known Russian-nexus threat actors that is associated with espionage and intelligence, generally targeting governments of “unfriendly” countries is Turla, also known as Venomous Bear. Its main targets are North Atlantic Treaty Organization (NATO) and its members. For the first time it has been attributed to operations against the Pentagon in 2008. It develops a unique malware and infrastructure and uses new tactics, techniques and procedures (TTPs), specifically targeting research, military and diplomatic data. Turla used a proprietary Crutch toolset in espionage attack against undisclosed European government organization (Insikt Group 2020).

Polarity

The distribution of power in the world is inevitably uneven, and therefore it is necessary to single out “centres of power” where power resources are accumulated. Polarity is a power distribution concept in the international system that can help explain the nature and features that characterize it in any given point of time. Based on the power configuration, three types of systems can be identified: unipolarity, bipolarity and multipolarity with four or more centres of power (Deutsch; Singer 1964). The power in those systems can be assigned and apportioned in different ways. During the Cold War, when there were only two superpowers, both in possession of weapon of mass destruction, the only possible model that maintained stability and security in the bipolar world was the balance of power (Deutsch; Singer 1964, 406). According to Morgenthau (1978) the principle and mechanism of balance of power is the main form of limiting this struggle.

Following the collapse of the USSR, the distribution of power in the world has changed. In 1990, Charles Krauthammer (2017) in his article in Foreign Affairs proposed a concept

---

1 For instance, Hezbollah was used during the Cold War by Iran and Syria as a tool to reduce Western influence (Machnikowski 2020).
of a unipolar international system, underlining the unchallenged position of the United States. After the Cold War the United States was left with a huge military-industrial complex and managed to become a dominant global superpower. Its hegemony was also claimed by the American administration and is visible in the country’s foreign policy, with the United States being informally referred to as the world’s policeman, specifically in the context of its activity in Middle East (Davis 2016). The structure of international society in the view of American scholars had to remain unipolar for a long time, being the most beneficial for security and peace (Wohlforth 1999). The perception of American primacy was challenged by Russia and other BRICS countries, as well as the European Union that are in favor of a multipolar structure of the world (European Commission 2010).

Multipolarity, a model of power distribution, is only achieved when there are more than two states that have more or less equal military, political, economic and cultural influence. It is still a power structure formed by states that have it, the number of which can vary from one to many. A multipolar structure is not necessarily cooperative in its nature; it can also generate conflicts. Moreover, contrary to the assumptions that constitute balance of power theory, the multipolar system can be very unstable with diffused dangers and obscure interests (Waltz 1964). To put it differently, multipolarity can lead both to stability and instability, expressed in conflicts. Deterrence is much more difficult to achieve in a multipolar world, with a number of actors that have diverse interests.

The United States is a leader in internet inclusivity. The country virtually developed the internet and, if putting it in sports terms, it has home-field advantage. Companies such as Facebook, Microsoft Google, Apple and Cisco that originated in the US, dominate the international market. Their software is widely used all over the world. Key submarine cables connecting the world are positioned in the United States or its allies (Buchanan 2020, 18). It was the first country to spread the digital revolution. The US military have been exposed to computers and cyber technology before their counterparts in other countries. The internet was securitized in the United States before it was in any other country. The first ever digital weapon, a malware that was able to physically affect the target, was created allegedly in the United States with the help of Israel (Der Spiegel, 2013). The virus, named Stuxnet, was a sophisticated digital weapon that aimed not to abruptly attack and destroy, but rather carefully annihilate the attacked country’s belief in its own abilities. Shaping is the strategy that the United States uses the most, undermining confidence and modeling the situation in a desired way.

The surveillance program PRISM, under the auspices of the United States National Security Agency (NSA) that was revealed by the NSA contractor Edward Snowden, is another proof of the US far-reaching intelligence efforts. This mechanism of acquiring information from American technology companies serves as one of the main sources of intelligence. Initially, the program was just an arrangement between Microsoft and the government, but it significantly expanded over the years to eight providers, such as Google, Apple, Facebook, YouTube, Yahoo, Skype, Paltalk and others. The NSA is able to use the program to conduct intelligence operations starting with a selection of an IP address or an email of the target. There are two possible types of collection: surveillance and stored communications (Buchanan 2020, 29). As a result, all online activities of the target become available to the operator. It is also possible to transfer the data that compa-

---

2 Acronym for five emerging economies: Brazil, Russia, India, China, and South Africa.
ny has on target to the government, making all previous activities from the past available to the operator, including messages, photos and videos. Data, allegedly, is not collected without a warrant. Nevertheless, the United States are able to take advantage of what is called a passive collection. Data flowing through the United States or to the United States through the telecommunication cables and hubs located in the country is fairly accessible to the government of the United States. The United States can collect data within its “transit authority”.

The United States’ home-field advantage and monopoly on technological developments in cyberspace from which the country used to benefit is being undermined. China advanced in developing hardware via tech companies such as Huawei. The country even holds a hardware-based leadership position when it comes to 5G wireless network (Allison; Schmidt 2022). In 2019, Chinese telecommunication company Huawei – that is allegedly beholden to the Chinese government – was placed on a “blacklist” composed by the US Department of Commerce that forbids American companies to supply Huawei with goods and services without an authorization from the government (Segev; Doron 2019). Companies like Google, Vodafone and Panasonic stopped their cooperation with Huawei. The reason for such actions of the US administration at the time were security concerns that Huawei can be used by the Chinese government for cyber-espionage. According to Chinese Cyber intelligence law of 2017 companies operating in China should hand over information and technologies to Chinese authorities if required (Segev; Doron 2019). Huawei could provide an access to Chinese government to its inner workings, which is controversial due to the fact that the company is involved in the build-out of 5G infrastructure. The infrastructure implies that there will be a lot of data both in core and periphery, and therefore countries should be confident that the information and network would not be exploited for cyber-espionage purposes. In a Pentagon report of April 2019, these charges were explained in more detail: “Evidence of backdoors or security vulnerabilities have been discovered in a variety of devices globally. Many of these seem to be related to requirements from the Chinese intelligence community pressuring companies to exfiltrate information about domestic users” (Segev; Doron 2019). Moreover, Huawei has been accused of a theft of intellectual property on multiple occasions.

The United States is urging its allies to ban Chinese involvement in 5G infrastructure construction, and it seems a digital Iron Curtain is rising. The Chinese government is actively mobilizing resources to rapidly deploy the technology nationwide and become a global leader in 5G. The development of 2G, 3G and 4G wireless connection was led by the United States, Japan and Europe. China fell behind in the industry and lost an opportunity to compete. However, the country realized it had to act quickly to overtake the leadership. The strategy Made in China 2025 identified specific goals for companies to become more innovative and cutting-edge in such a crucial emerging industry as 5G (Ahang 2019). All wireless carriers belong to state and thus, the government can accelerate the progress of 5G development. Withal, there are certain concerns that rise from this fact as well. The success of Huawei in building 5G infrastructure may be too appealing for China to take advantage of passive collection. Passive collection is fundamentally about collecting information from telecommunication cables and hubs. A 5G infrastructure built by Chinese vendor may serve as collection points where the intelligence flows by (Buchanan 2020, 21).
**Ideology**

The Cold War is traditionally described as being a clash of ideologies. In essence, it was a confrontation of Western capitalism and communism that tried to “take over” the world with a communist revolution. According to John L. Gaddis, “Both the United States and the Soviet Union had been born in revolution. Both embraced ideologies with global aspirations: what worked at home, their leaders assumed, would also do so for the rest of the world” (Gaddis 2005). According to Gaddis (2005, 84), the Cold War was not a simple geopolitical confrontation between superpowers possessing nuclear weapons, but a rivalry between two different approaches to organizing a society.

Despite all factors that contribute to determining the state of a cold war in the world, the existing hostilities cannot be explained in the terms of ideology as we know it from the Cold War. The twentieth century ideological battle between communism and capitalism ended with the dissolution of the USSR. Although there are still communist countries that aim at building and achieving socialism or communism, the possibility of Marxist world revolution is unlikely. According to Francis Fukuyama (1989, 3–18), the demise of communism led to a victory of Western liberal democracy that is the only viable ideological model. From the perspective of time, the evidence suggests that ideological contest remains, but it takes a different form. The fall of communism has given the rise to a range of other ideological forces (Heywood 2017). Political ideologies, such as ethnic nationalism, religious fundamentalism, right-wing populism and others, are growing in different parts of the world. Moreover, liberalism is becoming more differentiated than it used to be in the twentieth century. According to Michael Freeden (2003, 6), ideological boundaries are shifting, and it is much more difficult to capture the changing framework of political belief system. The scholar believes that there is a need to find a holistic dominant convention that would serve as a cluster for all existing ideologies. Globalism could be this underlying conceptual network due to its uniqueness, context-bound explanatory character for political issues and structural sophistication. While globalism is an ideology, globalization, thus, is a set of social processes that constitute its core. In order to point out ideological differences between the United States, Russia and China, their perceptions of globalization are examined further. Globalization is characterized by the compression of time and space as a result of political, economic and cultural transformations, as well as technological progress (Agsnew 2001, 133). It displaces conventional ideology in a form that existed during the Cold War. Globalism is a universal paradigm. There is a division, though, in how countries look at it and how they perceive it.

After the end of the Cold War, many people in different regions in the world have accepted core tenets of globalism. Thus, they incorporated large parts of the normative framework that proposed the idea of markets deregulation, the liberalization of trade, privatization, neoliberal values and, after 9/11, the approval of the global War on Terror under the leadership of the United States. Globalization has received a large support in non-Western countries (Steger 2005). However, the views of how its processes should be handled greatly differ there. During the Cold War the world was divided into Western and Eastern blocs. The observable division during this era is a division in the views how globalization should be approached. Globalization is not ideologically neutral. It goes in parallel with neoliberalism (Heywood 2017, 156). This fact makes globalization West-
ern-led. Countries like Russia, China, Iran, and others accuse the Western globalization for an unbalanced distribution of wealth and unjust international system.

During a meeting of a Moscow-based discussion forum Valdai in 2016, Russian speakers indicated that Russia and China-led globalization would have been better visioned with better outcomes for the world than the Western-led globalization that according to them is failing (Weitz 2016). According to Richard Weitz (2016), a senior fellow and director of the Centre for Political-Military Analysis at Hudson institute Russia perceives globalization as Western-led, neoliberal and “universally destructive economically, culturally and politically and responsible for sparking a worldwide revolt”. Moreover, the concept of international law is considered to be born in the West rather than in the East. The majority of international institutions are situated in the West, and because of that reason international law is often accused of being bereft of universal character. There is an obvious division in regards to the concept of human rights and human rights values. The principle of universality of the concept has been questioned by the governments, specifically those of South-East Asia (Davidson 2001). The values are perceived to be a product of Western political thought that promote individualism.

The existing division between East and West can be also observed by how permanent members of the UN Security Council vote on important matters for peace and security in the world. Veto-holding countries, such as the United States, Great Britain, France, People's Republic of China, and the Russian Federation can block virtually any resolution by resorting to their right of veto. As a matter of fact, the Union of Soviet Socialist Republics (USSR) cast the first veto on the February 16, 1946 on a draft resolution regarding the withdrawal of foreign troops from Lebanon and Syria (The Security Council Report 2020), and since then the veto has been used 281 times (UN Documents). The major split between Western veto-holding superpowers and Eastern ones has led to an undeniable inability of Security Council to address many international conflicts.

The division is being projected onto cyberspace that becomes a new and primary battle space of the ideological confrontation. According to Alexander Klimburg, Director of Cyber Policy at the Hague Centre for Strategic Studies, countries are split into two groups. The first group advocates for free internet, the unconstrained information movement that is transnational, and not limited by national borders or culture. They try to defend this freedom by appealing to international cooperation. While the second one, led by China and Russia, insists on cyber-sovereignty, meaning ultimate governmental control over the informational flow. To pursue this strategy China hires more people for its cyber department than for its armed forces (Klimburg 2018, 332). The second group of combatants use offensive techniques to advance national interests. They perceive internet and cyberspace as a weapon. As a result, the increase in cybersecurity concerns leads to more governmental control. Communication is being pre-emptively restricted due to many instances of bad content found online or spread of terrorism planning. Klimburg believes that their ultimate goal is “a reconceptualization of the entire Western-defined global order,” an intention that is openly expressed by the governments of these countries (Klimburg 2018, 145). The scholar assumes that there is possibility of internet being the tool that reinforces the historical East-West division that is an embodiment of a cold war.
Psychological warfare

Psychological warfare is a term that describes the activity aimed at destroying the enemy’s spirit and will to fight, influencing opinion of allies or neutral nations with the use of all available communication tools, and using propaganda to accomplish national goals (Padover 1951). Disinformation and propaganda campaigns, widely used during the Cold War, remain an effective weapon when it comes to indirect confrontation. During the Cold War, people received information mainly through newspapers, television and radio. The information was easier to control if one knew the source where it was coming from. It was rather difficult for people to have a complete and objective picture of what was happening in the world. Everything has changed today. In order to access any available information from a diverse range of sources one just needs an internet connection (Rid 2020). This variety of sources and an effortlessness with which information can be accessed could create a delusion of its reliability. The intentional dissemination of false information poses a tremendous challenge to a national security. Information warfare is even more effective in a cyber domain that allows for a fluent information flow and can be handled with relatively low costs.

Russia has a leading position in the information warfare. The state takes an approach of undermining opponent’s and shaping a public perception in a way that benefits national interests of Russia. The country promotes its national policy objectives using different concepts and methodology. Reflexive control is a Russian concept aimed at influencing enemy’s decision-making process by feeding the opponent with deceptive information to create confusion or incline the enemy to make desired decisions. Timothy Thomas (2004, 237), a senior US military analyst, defines reflexive control as “means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action”. In fact, the actor creates a distorted picture of the world by spreading disinformation, leaking selected information at a specifically chosen moment and embed a different posture of someone (Kowalewski 2017). The concept has its name from “reflex”, which is controlled by the actor and this way it is possible to shape the opponent’s behaviour. The descriptions of reflexive control were present in Russian military journals already in early 2010s (Vasara 2020).

Journalist Adrian Chen (2015) published in the New York Times an investigation on Russia’s information capabilities and its “army of trolls” from the Internet Research Agency in St. Petersburg. The shadowy organization is responsible for hoaxes and false information spread on the internet. Its goal is to post pro-Kremlin propaganda on social media “in order to create the illusion of a massive army of supporters”. The employees of the Internet Research Agency, referred to as trolls, are using proxy services to hide their real I. P. addresses. Russian trolls use a deception technique by creating an impression of real people posting their opinions on social networks. The issues raised concern Russian opponents, enemies and opposition in the country. According to Chen (2015), the main target of troll farms is “the utility of the Internet as a democratic space”. Russian disinformation campaigns are weapon that the country uses in its offensive approach to international order, and are a part of a cyber warfare.

China completely controls the flow of information within its country, having established a sophisticated system of firewalls. The country introduced a cybersecurity law,
according to which the government can request any information on demand from telecommunication companies. These factors raise security concerns that Chinese 5G infrastructures can be used to the advantage of cyber-espionage and intellectual theft. The country is successfully implementing the Golden Shield project (the unofficial name is the Great Chinese Firewall), within the framework for which a complex system for filtering Internet content has been created in the PRC. A sophisticated system of firewalls has been imposed on Chinese Internet traffic, which restricts access to external sources that the government considers “problematic.” Chinese Great Firewall Internet blocks sources and services of such giants as Google and Facebook.

**Mutual Assured Destruction**

Nuclear weapons still pose a threat and also restrict other countries from going to war as a method of resolving international disputes. Nuclear powers virtually define international security. Moreover, a possibility of a combination of nuclear forces and cyber technology raises a new security challenge. Potentially non-attributable cyber-attacks and conventional ones carried out together or separately present a challenge for defence planning strategies. The costs of direct war are increasing and are higher than they used to be during the Cold War with new technologies developing, and entirely new theaters opened for operations, which is a cyberspace. If the threshold for making a decision on the use of nuclear weapons is high enough, cyber weapons are already being used today and are causing more and more damage.

Cyberization has modified the way of thinking about the means of addressing international security issues in general. Cybersecurity is now a real concern in military planning. Cyberspace has been recognized by NATO as a domain of operations reaffirming its importance for security (North Atlantic Treaty Organization 2020). An analogy can be made with nuclear weapons that emerged at the dawn of the Cold War and was a serious challenge to take into account in strategic planning. The US National Cyber strategy recognized cyberspace being an integral component of economy and defence (The White House 2018). The internet, the development of which was funded by the US Development of Defense, has been securitized and its weaponization pose a strategic challenge (Featherly 2021). The United States, the first nation to use a nuclear bomb, was first in weaponizing the internet as well. According to Peter Pattara (2021), the “cyber Hiroshima” was a Stuxnet malware designed to destroy uranium enrichment facilities of Iran in 2009 (Pattara 2021). Stuxnet was not a regular virus. It managed to escape the digital realm and caused real physical damage. This instance is considered the first deployment of a digital weapon (Alvarez 2015). The event marked a redefinition of Mutual Assured Destruction. Stuxnet demonstrated that cyberattacks may inflict physical harm similar to that caused by conventional weaponry. The main distinction between airborne attack and cyberspace strikes is the fact that cyberattacks are more accessible, allowing numerous countries, as well as non-state actors, to develop top-notch cyberattack capabilities. Offensive cyber weapons can cause mass destruction and mass casualties, defined as more than one thousand deaths or injuries if unconstrained and can be considered as weapon of mass destruction similarly to nuclear weapons (Hatch 2018). Among the examples of cyber weapon triggering mass casualties, indicated by the Department of Defense Law of Armed Conflicts,
are a nuclear plant meltdown, disruption of air traffic control, and releasing dams over a populated area.

The range of destructive capability of cyber weapons go from small- to large-scaled that can cause tremendous disruption. A threat actor can exploit and take advantage of a vulnerable software gaining an access to protected resources or disrupting services of a host. Potential damage can include blinding air defence networks, military communication networks disruption, blackouts and power outages. In April 2022, Unit 74455 of Russia’s military intelligence agency conducted an attack targeting Ukrainian high-voltage substations. The malware imposed by Russia interacts directly with substation devices and controls the flow of power. It was an attempted physical blackout that was very much real (Greenberg 2022).

Historically, the first cyber weapons to be used were various types of distributed denial-of-service (DDoS) attacks. This kind of an intrusion uses multiple remotely controlled botnets, created or repurchased, that flood a network with internet traffic that it cannot accommodate making it inoperable. The purpose of such an attack is to block internet users from accessing certain network resources. DDoS attacks are often aimed at websites, banking services, network management systems for energy or transport and others. After government agencies began to deal with DDoS attacks, they started to create botnets, placing malicious codes on government websites and, thus, infecting a large number of machines (Security Centre 2020). It gradually became clear that incidents occurring in a digital realm can damage objects in the real world. Moreover, it is not necessary for the target to be connected to the Internet to be damaged as a result of the attack.

A special class of a threat actor is an advanced persistent threat (APT). These programs are created by professionals sponsored by a nation state. As a rule, these are targeted attacks, and the motivation of intruders is often political. Operators implementing this type of attack use the full range of capabilities that exist at the moment. These include technologies of computer intrusion, interception of telephone conversations, analysis of information from satellites and others. If required, attackers can get an access to any means available on Internet, including the development of any complex software products. Threat actors are focused on a certain specifically defined tasks, rather than looking for opportunities for financial or other benefits. Therefore, it is possible to assume that attackers are controlled externally (Lord 2018). The destructiveness of cyber attacks raises the costs of war and thus states prefer not to engage directly into a confrontation, but rather use other actors to pursue their strategic goals. This leads to a deterrence or a cold form of confrontation between potentially conflicting nations.

Recently, China developed a new technology under the name Great Cannon, an extension of the Great Firewall, that distributes denial of service attacks targeting services that allow to bypass the Great Firewall, transforming it into an offensive instrument. In 2015 GitHub, the United States-based software company, became a victim of the DDoS attack initiated by China. The firm hosted two projects related to anti-censorship organization GreatFire.org from China, that enabled users from PRC to access GreatFire’s website and the New York Times in Chinese (Griffiths 2019). Traffic was clustered and servers crashed. The malicious JavaScript codes were inserted into search engines. It was a new powerful tool of offensive censorship that aimed targets not only within China, but as well overseas.
Conclusion

A concept of a cold war is evolving, but its core remains unchangeable: it is a state of indirect, unconventional confrontation between states on the ground of ideological difference of views, with a weapon that rises the costs of war making the direct conflict too damaging. A cold war, characterized by proxy wars conducted by superpowers via client states, polarity that keeps the system stable, ideology that shapes foreign policy, psychological warfare and the presence of weapons of mass destruction, can be a term applicable to an international system at any given period of time. Overall, based on the analysis, I came to the conclusion that the palpable tensions between the United States, Russia and China can be identified as a cold war. The current cold war somewhat differs from the one in the 21st century. Although, it is worth noting that along with technological progress and new processes in international environment, the concept will develop and be adapted accordingly. Cyberspace is a front line where, considering a nature of the confrontation, states are expressing their hostilities using different strategies, such as shaping and signalling. Intelligence gathering, damaging and destructive cyber-attacks, hybrid wars with a use of non-state actors, disinformation and propaganda are the key elements characteristic for the cold cyberwar. By applying comparative method, I have found certain similarities between the current activities of the USA, China and Russia in the cyberspace and the times of the Cold War from the 21st century. A doctrine of Mutual Assured Destruction, known from the Cold War, has evolved and is once again relevant with cyber weapons playing the same role in deterrence and military planning, as does a nuclear weapon. Moreover, those two types of weaponry can be combined that can cause additional damage and raises the costs of war exponentially. Proxy wars developed into a new form, which is a hybrid warfare that is conducted with a help of non-state actors in a cyber realm. As a result, a new tendency can be observed, which is the rising attribution challenge when it is difficult to determine who is responsible for the attack. Other cold war elements include disinformation and propaganda, techniques widely used during the Cold War. They remain being an effective weapon that evolved together with technological progress. There are new aspects of a cold war too, as a form of indirect confrontation, that did not exist during the Cold War. Today the structure of international system is gradually evolving from hegemony to multipolarity with regional powers aspiring to become global. The United States and its NATO allies are challenged by the Russian Federation and People's Republic of China. This confrontation is no longer based on communism-capitalism ideological battle though. On the contrary, there is a new common ideology, which is globalism and globalization at its core. Rivals are divided on the ground of the views on how globalization processes should be conducted, and who should lead those. The main limitation of a conducted research is the attribution problem. The adversaries that act on behalf of a state are not officially claimed by it. In many cases the actions in a cyber domain that are happening now can be traced back to the source in a couple of years. However, this is what makes cyber weapons the perfect weapons under the conditions of a cold war. The depth and breadth of the extent to which states are using them is not easy to define due to a covert character of these operations. Cyber operations are almost never side on side encounters. Russia tries to destabilize and undermine the democracy in the United States, China aims at dominating the new technology that potentially can give a lot of intelligence advantages, the United States benefit from their position as an innovator. All these
tactics compose a strategy that countries pursue in this new cold war that we experience today. Cyberspace, non-intuitive, untraceable, and unpredictable is an ideal environment for it. Countries act indirectly, avoid escalation and focus on deterrence, which is much more problematic due to accessibility of the cyber arsenal. Analogously to a traditional warfare, a cyberattack can range from small-scaled combats to all-encompassing battles. Considering the fact that modern society is extremely reliant on internet and other digital communication technologies, every gadget can become a weapon in a cyber war and the most digitalized societies can be the most vulnerable to this type of a warfare. Hence, it is extremely important to consider cyber threats in military planning. Cyberspace became a new existential dimension and requires a lot of analysis. It is crucial to understand how the countries perceive international system and what techniques and methods they use in order to be able to strategically build the defense. A way of dealing with instability and uncertainty in a current condition of international system described in the research as well as potential consequences for the US security would be a field for future research.

References


29


