Dóra Molnár[1]

Great Power Cyber Diplomacy - China on the International Cyber Platform Accompanied by the United States and Russia

DOI 10.17047/Hadtud.2022. 32.E.227

The world's great powers are also at the forefront of guaranteeing their cyber security, in which, in general, cyber diplomacy is playing an increasingly important role. The study briefly outlines the cyber-diplomatic steps taken by the world's three leading powers, and as part of this, differing views and steps on international cyber regulation.
Keywords: cyber diplomacy, China, Russia, United States

Nagyhatalmi kiberdiplomácia - Kína a nemzetközi kiberplatformon, az Egyesült Államok és Oroszország kíséretében

A világ nagyhatalmai élen járnak kiberbiztonságuk garantálásában is, amelyben – általánosságban elmondható, hogy – egyre jelentősebb szerepet tölt be a kiberdiplomácia. A tanulmány röviden ismerteti a világ három vezető hatalmának kiberdiplomáciai lépéseit, s ennek részeként a nemzetközi kiberszabályozással kapcsolatos eltérő álláspontokat és lépéseket.
Kulcsszavak: kiberdiplomácia, Kína, Oroszország, Egyesült Államok

The dominant powers in the world play a key role in shaping all areas of security, and this is no different for cybersecurity. For there is no cyber diplomacy in and of itself, just as there is no cyberspace in and of itself. At present, however, there is no comprehensive international convention that sets out the rules of state behavior in cyberspace and regulates issues related to the use of cyberspace. While an international cyber convention would undoubtedly be a huge diplomatic success, the question arises: is it even necessary? A group of experts believe that this will not be due to the new and emerging challenges posed by the rapid technological change and the difficulties in monitoring compliance with the Convention. Instead, informal cooperation and strategic deterrence are seen as the way forward. Another group of experts, on the other hand, insist on the need for an international convention and cite 20th-century arms control agreements as a successful example. An international cyber regime would provide an opportunity for states to discuss key issues and could contribute to effective cyber deterrence.

There are a number of arguments against the cyber regime (NABEEL 2018). One is that it is impossible to incorporate monitoring and enforcement mechanisms due to the properties of cyber weapons. The reason for this is that control should begin at the time of the development

1 Assistant professor at the International Security Policy Department, National University of Public Service, Budapest, Hungary. Address: 2 Ludovika square, Budapest, H-1083, e-mail: molnar.dora@uni-nke.hu; https://orcid.org/ ORCID: 0000-0002-1476-5253

of weapons, and not the use of weapons themselves should be controlled.[2] Other counter-arguments are the length of the negotiation period, the lack of adaptability to rapid technological change, and the premature conclusion of such an agreement. Conventions are usually concluded after the technologies have been used. Moreover, only truly committed states would become parties to such an agreement, and even for them, participation would be a kind of coercion.

It is conceivable that the international cyber regime could also be built along looser regulatory structures. In this case, confidence-building measures can play a central role, as evidenced by the decades-long practice of the Organization of Security and Cooperation in Europe (hereinafter OSCE) and Association of Southeast Asian Nations (hereinafter ASEAN)[3]. Beginning in 2009, the United States has become the leading state on the OSCE's cyber agenda since the Obama administration announced its new international cyber policy. The foundations for the organization's cyber activities and strategic cyber security dialogue were laid at a joint meeting of the Security Cooperation Forum and the Permanent Council in June 2010. Already at that time, the United States proposed to discuss the standards of state behavior and then, a year later, to shape confidence-building measures. In parallel, the United States and Russia negotiated an initial set of cyber confidence-building measures (ZIOLKOWSKI 2013), which were agreed in 2013. The essential elements of the agreement are as follows (*Joint Statement by the Presidents …* 2013):

- establishing communication channels and information sharing agreements between CERTs to protect critical information systems;
- allowing the use of a direct communication channel between countries' nuclear risk reduction centers (between the US State Department in Washington and the Russian Department of Defense in Moscow);
- establishing a direct secure telephone link between the US Cyber Security Coordinator and the Deputy Secretary-General of the Russian Security Council, and setting up a bilateral working group on the dangers of info communications technology within a month.

Regarding the range of steps to be taken within the OSCE framework, each state has come up with different proposals. Germany distinguished two major groups of confidence-building measures: transparency and stability measures. While the former included risk mitigation and information exchange (in terms of applicable international law, organizational structures, strategies and partners), the latter included joint cyber exercises and the establishment of crisis communication channels and CERTs (*Cyber Security: Confidence and Security-Building Measures (CSBMs)).*

2 For all this, Eilstrup-Sangiovanni uses the terms exante and ex-post. See EILSTRUP-SANGIOVANNI, 2018: 399

3 In the case of ASEAN, the issue is being discussed in the framework of the ASEAN Regional Forum.

Russia has made a broader list. According to the Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space published in 2011, it is the task of the armed forces to define the scope of confidence-building measures for the military use of the information space, and in 2012 a further document detailed the range of measures. These include the harmonization of national rules, the development of an internationally agreed system of information security terminology, and the establishment of an organizational framework for international cooperation between police forces (FEDOSOV 2012).

All these are serious efforts on the part of the international community, but it must not be forgotten that an international cyber regime can only be successful if the widest possible range of states are involved. The involvement of the leading states in cyber security is essential, but there are still serious battles between the Western world and China-led emerging states over the most fundamental issues of the regime. Suffice it to say that in November 2018, more than 50 states (accompanied by 130 private companies and 90 scientific bodies) signed the International Cyber Security Pact on the need to establish rules for cyber warfare, but the United States, China, Russia, North Korea, Israel, Iran, Australia and Saudi Arabia, as well as Huawei and ZTE were not among the signatories (*UK and 50 nations sign cyber security pact.)* The aim of this study is to illustrate what cyber-diplomatic maneuvers mean in practice for each country. The study analyzes the main cyber diplomatic steps of the three leading cyber world powers, China, the United States and Russia.

China and cyber diplomacy: another success story?

It is no exaggeration to say that China has also taken the lead in diplomacy. This is indicated by the size of the diplomatic network, which is also a measure of the degree of global influence. By 2019, China had 276 diplomatic posts worldwide, ahead of even the leading United States, which has "only" 273 branches (BLEY 2019). This could also be a turning point in great power competition, because China is certainly ready to use its global power *in realit*. According to some opinions, China is no longer just a cyber superpower, but has grown into a *cyber superpower* in the last few years (SEGAL 2018). All this cannot be a coincidence when we look at the words of the Chinese President in 2016: without cyber security, there is no national security, and without informatization, there is no modernization (*Xi Jinping gives speech…*).

The basis for diplomatic action is the new Cyber Security Strategy Paper issued in March 2017 titled as International Strategy of Cooperation on Cyberspace. In its name, the strategy suggests that China envisages resolving cyber conflicts primarily through cooperation and the use of peaceful means - and that cyber diplomacy has a key role to play in this.

The strategy states that the future of cyberspace is in the hands of all countries, and although the digital divide between countries and regions is widening, the international community is to work together as a whole in a spirit of mutual respect and understanding to ensure the sovereignty of the Internet world. And here we come to the key concept, the concept

of *sovereignty*. Sovereignty appears in the document as one of the four principles (alongside peace, shared governance, and shared benefits), and in this context, the importance of Internet sovereignty permeates the strategy as a whole — not surprisingly. The strategy also defines the concept of Internet sovereignty (or cyber sovereignty): states are to respect each other's right to choose the path of cyber development, the model of cyber regulation and the Internet policy, and ensure that they can equally participate in the governance of international cyberspace. No state may break into cyber hegemony, interfere in the internal affairs of another state, or support cyber activities that undermine the national security of another state. The issue of sovereignty is also one of the strategic goals, in the first place as "guaranteeing sovereignty and security". The country envisages achieving this strategic goal primarily through the use of peaceful means, and aims to prevent cyberspace from becoming a new battleground. At the same time, China will continue to develop its defense cyber capabilities and give the military an important role in cyberspace missions. It also plans to create a stand-alone cyber force.

Among the strategic goals, I would like to highlight the creation of the second named system of international rules, as well as the issue of fair internet governance, which is the third. With regard to the former, China advocates the establishment of a universally agreed system of international rules and codes of conduct within the United Nations, which sets the framework for states' behavior in cyberspace. In the context of the latter, the strategy states that there is a need for a "multilateral, democratic and transparent" global Internet governance based on the principles of equal participation and co-decision. The multilateral indicator deserves emphasis, as it represents one of the main differences with the Western powers, which want to implement a multi-stakeholder model of Internet governance.

China's foreign policy has three main goals: to reduce the threat that the Internet and the flow of information can pose to internal stability and the legitimacy of the system; to shape cyberspace in a way that increases the country's political, military and economic influence; and to offset U.S. dominance while increasing China's room for maneuver (SEGAL 2017). The country's cyber-diplomatic steps also fit into this target system. Under the presidency of China Xi Jingping, he changed his previous reactive and defensive cyber policy and decided to use active cyber diplomacy to build his cyber diplomacy channels in a very short time, which he uses very effectively to achieve his goals. Cyber security can simultaneously provide Beijing with countering the threat of terrorism, guaranteeing regional influence and building bilateral relations with important partner countries such as the United States. In 2014, China hosted the first World Internet Conference in Wuzhen. At that time, the President of China sent only a welcome message to the event attendee. A year later, Xi Jinping personally attended the conference and gave a speech, signaling the increased importance of cyber security issues for China. In addition to the issue of Internet sovereignty, the Chinese President's speech focused on the issue of global Internet governance, including the promotion of multilateralism. It was no small diplomatic gesture that Russian President Medvedev immediately responded to the Chinese president's words in his conference speech and assured him of his support

(BANDURSKI 2015). Incidentally, the two countries enjoyed considerable success on the day before the conference, when, thanks to their successful lobbying activities, the term multilateral has been included in the text of UN General Assembly Resolution A/RES/70/125.

Chinese cyber-diplomacy is rooted in the recognition of the principle of non-interference in internal affairs and the principle of equal participation, the importance of capacity-building and development assistance, as well as support for the United Nations and other international institutions. The result of all this is the issue of cyber sovereignty or internet sovereignty, which has been a central issue since the beginnings of cyber diplomacy. China sees the world of the Internet as a double-edged sword: as an essential element in ensuring economic development and governance, but at the same time a threat to internal stability and the legitimacy of the system. The country intends to provide answers primarily through in-country censorship (see the Great Firewall), but also emphasizes the importance of international cooperation.

China's cyber-diplomatic efforts have for many years highlighted the fight against the unequal distribution of Internet resources and, in this context, the need for strong U.S. control over IANA[4] and the reform of ICANN. 10 of the world's 13 root servers are located in the United States, and IANA was also created as a result of a contract between ICANN and the U.S. Department of Commerce (SWAINE 2013). Therefore, it is not surprising that China supports the implementation of multilateral Internet governance in order to break US dominance.

Cyber issues are also gaining ground in China's *bilateral and regional relations*. Beijing is using cybersecurity to strengthen its regional position on the one hand, and to secure its leading position among regional and developing countries on the other. It has a *privileged bilateral relationship with the United States*, but the relationship between the two great powers has been quite volatile on cyber issues. The strengthening of bilateral relations was initially forced by the United States, but the dialogue was mostly limited to economic issues - in part due to the fact that Chinese diplomats came from the State Department staff and lacked cyber expertise. The United States sounded louder and louder, and in June 2013, when the leaders of the two countries met in California, Obama warned the Chinese president that cyber espionage would seriously damage their bilateral relations. Shortly afterwards, the Snowden case erupted and the United States indicted five Chinese hackers – that was followed as China's response by freezing bilateral talks. During this period, two major research institutes on both sides produced annual reports on the current state of cybersecurity (CSIS in the US and CICIR in China).[5]. Relations were consolidated only after the charges against Chinese hackers were dropped. In September 2015, President Xi arrived on an official visit to Washington, where as a result of the two-day talks; the two great powers signed a bilateral agreement of epoch-making

4 Internet Assigned Numbers Authority
5 CSIS – Center for Strategic and International Studies; CICIR – China Institute of Contemporary International Relations

significance, which also specifically addresses cyber security issues. The signing of the convention was also an important step because it also served as a model for shaping cyber relations in the United Kingdom, Germany and other Western states.

The bilateral agreement (*Fact sheet* …) signed on September 25, 2015 stipulates that requests for information or requests for assistance shall be answered in a timely manner if they relate to malicious cyber. The parties are required to cooperate in the detection of cybercrime and the collection of electronic evidence, and to provide up-to-date information on the status and outcome of the investigation. They also undertake that no government shall engage in or support cyberspace activities for theft of intellectual property. Both sides support the establishment of rules of conduct for states in cyberspace, an issue that will be examined more closely by an expert group to be set up. Finally, a special cooperation mechanism will be set up to discuss cybercrime issues, with a group called the "High Level Joint Dialogue" meeting twice a year to consult (RENARD 2015).

In the post-agreement period, cyber-espionage activities between the two countries have been reduced to a lower level, but re-growth is not ruled out - and this could make cyber security a top priority in US-China bilateral relations. However, the probability of this is low, but at the same time there are fundamental issues in which the positions of the two great powers differ radically. These include the question of the militarization of cyberspace, the question of the applicability of international law to cyber warfare, and the assessment of the legitimate extent and purpose of cyber espionage. However, this tension inevitably carries the risk of a potentially more serious conflict. To prevent such a conflict, the logic and purpose of arms control could also be applied to cyberspace relations - despite the fact that arms control mechanisms during the Cold War applied to the nuclear arsenal and were fundamentally different[6] from cyberspace conditions (LEVITE-JINGHUA 2019). However, if the one-way and unilateral diplomatic moves of the Trump administration or the future US leadership continue into the future, further tensions are expected in the relationship between the two countries.[7]

Bilateral relations must also include *Sino-Russian relations*. In May 2015, the two countries signed 32 bilateral agreements - including a cooperation agreement on international information security (ROTH 2015). In it, they commit themselves not to launch hacker attacks against each other and condemn attempts to destabilize domestic politics over the internet. The latter is one of the elements of the agreement that can be considered new compared to the agreements already concluded under the auspices of the Shanghai Cooperation Organization. Another step forward is the naming of specific measures, such as setting up contact points or running joint scientific cyber projects.

---

6 Cyber capabilities are dual-use and mostly invisible, the main actors in cyberspace are private sector entities (as opposed to nuclear powers as states), control of cyberspace commitments is essentially impossible, and cyber weapons are well placed to achieve localized and transient effects.

7 For more details, see DOLLAR-BADER 2019

Among bilateral relations the partnership established with the *European Union* in 2012 should also be mentioned. The EU-China Cyber Group also meets regularly as part of the annual EU-China Summit, which has essentially become a forum for expressing the Union's concerns about China's cyber security policy and discussions on Internet governance (PAWLAK 2015). The working group held its seventh meeting in China on January 13, 2020, where the expansion of practical cooperation and the deepening of the bilateral comprehensive strategic partnership were assessed as significant achievements (*The 7th China-EU Cyber Taskforce…*). Among the European states, China also discusses cyber issues with the United Kingdom on an annual basis in the framework of the bilateral partnership, focusing mainly on cybercrime issues.

At the heart of China's diplomatic agenda will certainly remain the issue of cyber sovereignty and will improve its position in cyberspace through economic means. Already, one of the special, yet highly developed areas of Chinese cyber-diplomacy is *trade and investment policy*, which it uses as economic and indirect policy tools. By opening up new markets around the world, it is gaining new supporters for Chinese foreign policy and, at the same time, for China's cyber policy and the adoption of cyber norms. However, investment cannot always be directly converted into political influence; it often appears in an indirect form. An example of direct influence is Huawei's entry into the African market. In 2005, Huawei opened a school in the Nigerian capital, and five years later it was already operating in 50 African countries, serving 300 million African users. Another good example is the One Belt, One Road (OBOR) initiative. It is made up of two elements: one is the Silk Road economic belt, which connects China to the Persian Gulf, the Mediterranean and the Indian Ocean, and the other, the 21st Century Maritime Silk Road, which connects the region's waterways. In connection with this, there are also plans to build an "information silk road", which originally meant laying cross-border optical cables and other communication networks.[8] The planned fiber optic cable, which connects China with 48 African countries, is 200,000 km long and the planned cost of deployment is $ 173 billion (*Chinese Firm Hopes*…). However, the plan was completed in November 2019 and will not only lay a lot of cabling, but will also include network devices and software, as well as smart ports to support future management structures (*China's Digital Silk Road…)*.

The evolution of Chinese cyber politics and diplomacy in the coming period will be determined by two external factors. One is the processes taking place in the United States. If the country focuses primarily on its internal problems, it will be an opportunity for China to play a greater role in creating rules in cyberspace. The other is the evolution of the cybersecurity environment, which is becoming increasingly dangerous based on current trends and there are fears of a "militarization of cyberspace".[9] However, the ancient Chinese principle of deliberate

8 The cornerstones of the plan were fixed in 2016 and its implementation was planned for 2018, but the actual development is yet to come..
9 ibid. p.2

progress is unlikely to be abandoned by China, and diplomacy on cyberspace will remain the mainstay of its prudent political-economic moves.

Russia and cyber diplomacy

Russia's cyber potential is one of the largest and most technologically advanced in the world, alongside that of the United States and China. In recent years, however, the country has used these capabilities on several occasions with offensive intent - as has been the case with Estonia or Georgia, but even against the United States. Russia is using cyber conflict as a coercive tool, as part of a great strategy against the enemy to achieve its desired goals. However, these actions cross the borders of the post-Soviet region only in the rarest of cases - the question is why? The answer lies in the fact that Russia's national interests and goals also focus primarily on the post-Soviet region, and the global stage is only secondary to this - and this is no different for cyberspace.

Examining cyber interactions (BRANDON –MANESS 2014), it is striking that Russia is by far the last, while the United States and China are towering high. It follows that Russia underestimates the importance of cyber diplomacy and does not seek to resolve cyberspace conflicts through the tools of diplomacy, but rather through the use of cyber (offensive) capabilities.[10] The reason for this should be sought in the "executive circle". While in the West, many institutions of civil society are the custodians of soft power, in the case of Russia it is the exclusive right of state bodies controlled by the state-controlled media. It is therefore not surprising that cyber-diplomatic tools are not in the first place among Russia's repository of foreign policy tools (McNABB 2016).

However, this was not always the case. In the early 2000s, Russia was still actively involved in multilateral and regional cyber consultations, but as these efforts did not produce the desired results, diplomatic actions were increasingly replaced by offensive cyber actions. Russia sees its cyber power as an integral part of the Great Strategy and intends to use it to achieve its political goals - in line with the Clausewitz idea: war is the continuation of politics by other means (WIRTZ 2015).

As for the initial period, Russia's diplomatic moves were aimed at preventing conflicts and cyber arms competition between states. A sign of this was the adoption of the UN General Assembly Resolution A/RES/53/70 in 1999 on the initiative of Russia. Even then, Russian Foreign Minister Igor Ivanov drew the attention of states to the danger of the militarization of cyberspace, stressing also the possible harmful effects of cyber weapons (DAM- OWENS 2009). However, all this had not yet been fully understood by the states at the time (partly because the number of Internet users was still low, at around 250,000 - at the time). However,

10 In contrast, the United States, which would have had the opportunity to deploy its advanced cyber capabilities during the conflict in Iraq, Afghanistan, or even Libya, has not done so..

Russian diplomatic efforts continued and took shape in 2009 in the UN General Assembly resolution A/RES/64/211 entitled the Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures. However, as the decision was not legally binding, its practical implementation was not achieved.

Russia continued to seek diplomatic solutions within the UN system and welcomed the establishment of the UN Group of Governmental Experts in 2004. By this time, however, the purpose of Russian cyber-diplomacy had changed, and regulation had become a priority rather than prevention. This is because so far many countries (including Russia) have been actively developing their cyber capabilities. However, the first results had to wait until 2014, when the report of the UN GGE stated that international law - and in particular the UN Charter - was also applicable in cyberspace (*UN General Assembly Resolution A/68/98*). Government work continued thereafter, and the group's 2015 report already laid the groundwork for a government code of cyber conduct, but processes stalled thereafter.

At the same time, Russia forced the need for a code through its *regional relations*. In 2011, on behalf of the Shanghai Cooperation Organization, it submitted a proposal to the UN with three other countries, and in 2011 also drafted the International Convention on Information Security.[11] Both documents emphasize the principles of state sovereignty and territorial integrity in relation to cyberspace. The Russian will was also enforced in the Organization for Collective Security Treaty and among the BRICS states by adopting resolutions and setting up working groups.

Finally, Russian diplomacy has also sought to achieve the regulation of cyberspace through *bilateral partnerships*. In the world, the first bilateral cyber agreement between Russia and the United States was concluded in 2013. However, the success is not clear because the convention was limited to the technical issues of cooperation. It noted the need for information exchange between national CERTs and the creation of a cyber hotline. There was hope in the Russians that a wider Russian-American agreement could be signed, but the Ukrainian conflict stalled the negotiation process, and then in 2017, when Russia repeatedly tried to draw up a convention on dangerous military activities, the American party withdrew the day before signing – presumably due to developments revealed in the Russian intervention in the 2016 presidential election (POPESCU-SECRIERU 2018). In addition to the first cyber agreement, Russia has already concluded similar agreements with several countries, such as China, India, South Africa, Belarus or Cuba, and plans to conclude further agreements with France, Germany, Israel, Japan and South Korea.

Russia already enshrined the need for international regulation of cyberspace in its cyber strategy 20 years ago and, together with China and other CSTO member states, it still insists on

11 The fact that the power of the Internet became apparent to all states in the light of the events of the Arab Spring, and Russia wanted to avoid manipulating the Russian political system from outside, may have played a role in the creation of the documents.

the applicability of cyber codes of conduct and sovereignty and non-interference in internal affairs in cyberspace. Unlike the West, led by the United States, which has opposed it in the past, it has recently shown a growing willingness to recognize the need for rules. The divide between the two camps is also having a very negative effect on Russian-American and Russian-European relations, with the result that the chances of global agreement are diminishing - even if the UN Secretary-General himself is in favor of establishing a set of rules (*US Chief Calls for…*).

The United States as a cyber-diplomatic giant

The section on U.S. cyber diplomacy is shorter than the sections on the first two countries. This is due, on the one hand, to the fact that I have already touched on a number of issues related to US cyber policy in connection with the previous two states, and on the other hand, US cyber diplomacy has such a broad theoretical background and practice. Therefore, in this study, I summarize only the most important stages of the American cyber-diplomatic process, which was officially launched in 2009.

The cornerstone of U.S. cyber diplomacy was the adoption of the country's *International Strategy for Cyberspace* in May 2011. With the release of the strategy, the United States has put the issue of cyber diplomacy on a solid footing and has also set up its organizational structure. The document itself defines the concept of cyber diplomacy: it covers a wide range of American interests in cyberspace - this includes not only cybersecurity and internet freedom, but also internet governance and the military use of the internet, innovation and economic growth. The Office of the Coordinator for Cyber Issues has been set up in the Ministry of Foreign Affairs, with Christopher Painter as its first (and last) head. The office may have served as evidence of U.S. primacy in cyberspace (as it usually does in global force). It was the first such organization in the world, which has ever since been followed as a model by the foreign affairs apparatus of other countries. Cyber diplomacy has become a critical component of U.S. foreign and national security policy. During its six and a half years of operation, the Office has established a number of bilateral and multilateral partnerships and has negotiated formally or informally worldwide on a wide range of cyber issues (PAINTER 2019). Several expert proposals revealed the need for further cyber-diplomatic construction, but the Trump administration had a different view on the future of the issue, and Secretary of State Tillerson decided to close the Office (and relocate staff to the Department's Economic and Business Affairs Office). This created a huge gap that was to be filled by creating a new cyber strategy ordered by a presidential decree (*Presidential Executive Order…)* in May 2017, but its failure has led to further uncertainties among diplomatic corps. The transformations of the American cyber-diplomatic organization are, in fact, the result of a struggle between internal organizational and power interest groups as, in the second half of 2010, a serious struggle began within the US state administration over which interests, sectors and aspects to become decisive. And similarly, the bill was rejected because it did not actually succeed in resolving the

differences between the opposing interest groups in it. The bipartisan consensus proposal for a law on cyber diplomacy was presented to the House of Representatives in September 2017. However, although introduced on January 24, 2019, and passed by the House Committee on Foreign Affairs in March, the bill has yet to receive a vote neither at the House nor at the Senate. According to the bill, the country intends to contribute to an open, interoperable, reliable, unrestricted and secure Internet governed by a multi-stakeholder model. The United States, therefore, continues to persevere in rejecting the multilateral approach, by which confronting developing world led by China and Russia. The strategy exacerbated all this by naming countries and groups that pose a threat in cyberspace: Russia first, followed by China, Iran and North Korea, terrorist and criminal groups. At the same time, the document highlights the importance of bilateral relations and names the bilateral agreements concluded between 2014 and 2018.[12] To correct the anomaly in the organizational space, the Office of International Cyberspace Policy will be set up as a new central cyberspace, headed by a cyber ambassador appointed by the President.

As for the sequel, it was so certain that it would not be enough to devise a new strategy and set up a new office to answer the confrontations and dilemmas facing the country in cyberspace, but the elaboration of detailed questions was still pending. If the United States is to succeed in this area as well, open confrontation with both China and Russia shall be avoided at all costs; a policy consistent with these states shall be pursued and communicated to allies and other states in the world. The solution for the United States could be to persuade the states of Europe, Africa, South America, and Central, South, Southeast Asia to choose some of the leading states in their region - thus offsetting Chinese and Russian dominance (CHAPMAN 2019).

Final remarks

There are several indicators to compare the cyber security situation of the state. Of these, I highlight the Global Cybersecurity Index, listed by the United Nations International Telecommunication Union, which compares states along five indicators. The fifth indicator is cooperation, in which, among other things, bilateral and multilateral cooperation frameworks and membership in international organizations are the yardstick. Based on the overall rating of the index, the United States ranks 2nd, Russia 26th and China 27th in the world rankings (*Global Cybersecurity Index 2018…)*. It can be seen that the United States is clearly one of the three countries studied, which is indeed a cyber-diplomatic superpower. In the case of China, the relative lag reflected in the indicator is due to the fact that the country has only begun to engage in active cyber diplomacy in recent years, and the effects of the initial steps are not yet reflected in the index figures. In the case of Russia, the result is not surprising, as the Russians

12 Countries include China, Japan, the United Kingdom, France, Israel, South Korea and Australia, among others.

do not necessarily want to use their diversified network of contacts in the field of cyber security. At the same time, in the case of all countries, it can be said that the co-operation indicator can be said to be low, therefore it is expected that the field of cyber diplomacy will start to develop greatly in the future.

BIBLIOGRAPHY

BANDURSKI, David (2015): *China's cyber-diplomacy*. December 21, 2015, Available at http://chinamediaproject.org/2015/12/21/chinas-cyber-diplomacy/ (Downloaded on April 9, 2020)

BLEY, Bonnie (2019): *The New Geography of Global Diplomacy. China Advances as the United States Retreats.* November 27, 2019, Available at https://www.foreignaffairs.com/articles/china/2019-11-27/new-geography-global-diplomacy (Downloaded on April 8, 2020)

BRANDON, Valeriano – MANESS, Ryan C. 2014. "The Dynamics of Cyber Conflict between Rival Antagonists, 2001–2011." *Journal of Peace Research* 51 (3): 347–360., Available at https://www.researchgate.net/publication/256046745_The_Dynamics_of_Cyber_Conflict_between_Rival_Antagonists_2001-2011 (Downloaded on April 10, 2020)

CHAPMAN, Justin (2019): *Threats and Opportunities of Cyber Diplomacy at PolicyWest.* December 24, 2019, Available at https://www.pacificcouncil.org/newsroom/threats-and-opportunities-cyber-diplomacy-policywest (Downloaded on April 13, 2020)

China's Digital Silk Road (DSR): The new frontier in the Digital Arms Race. February 19, 2020, Available at: https://www.silkroadbriefing.com/news/2020/02/19/chinas-digital-silk-road-dsr-new-frontier-digital-arms-race/ (Downloaded on April 20, 2020)

Chinese Firm Hopes to Wire Continent with Same Strategy that Boosted Internet Access Across China. *Global, Times*,March 13, 2017, Available at: http://www.globaltimes.cn/content/1037500.shtml (Downloaded on April 8, 2020)

Cyber security: confidence and security-building measures (CSBMs)., Federal Foreign Office website. Available at http://www.auswaertiges-amt.de/EN/Aussenpolitik/Friedenspolitik/Abruestung_/KonvRueKontrolle/VN-Konventionelle-Abruestung-Ruestungskontrolle_node.html (Downloaded on April 10, 2020)

DAM, Kenneth, W. – OWENS, William (2009): *Technology, Policy, Law and Ethics Regarding U.S. Acquizition and Use of Cyberattack Capabilities*. Committee on Offensive Information Warfare, National Research Council, 2009. p.328. Available at https://lawfare.s3-us-west-2.amazonaws.com/staging/s3fs-public/uploads/2013/01/NRC-Report.pdf (Downloaded on April 15, 2020)

DOLLAR, David, HASS, Ryan, BADER, Jeffrey A. (2019*): Assessing U.S.-China relations 2 years into the Trump presidency.* January 15, 2019, Available at https://www.brookings.edu/blog/order-from-chaos/2019/01/15/assessing-u-s-china-relations-2-years-into-the-trump-presidency/ (Downloaded on April 8, 2020)

EILSTRUP-SANGIOVANNI, Mette (2018): Why the World Needs an Internationa Cyberwar Convention. *Philosophy&Technology* 30, no. 3 (2018): 399

Fact sheet: President Xi Jinping's State Visit to the United States. The White House, Office of the Press Secretary, September 25, 2015, Available at https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states (Downloaded on April 8, 2020)

FEDOSOV, Sergey (2012): *Statement by the Russian participant at the UNIDIR Cyber Security Conference 'What does a Stable Cyber Environment Look Like?*, UNIDIR, Geneva, November 8-9, 2012, Available at http://www.unidir.ch/files/conferences/pdfs/pdf-conf1922.pdf; (Downloaded on April 10, 2020)

Global Cybersecurity Index 2018. UN ITU, Geneva, 2019., Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf (Downloaded on April 20, 2020)

International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World. May 2011, Available at https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf (Downloaded on April 13, 2020)

International Strategy of Cooperation on Cyberspace. Ministry of Foreigh Affairs of the People's Republic of China, March 1, 2017, Available at https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1442390.shtml (Downloaded on April 8, 2020)

LEVITE, Ariel (Eli), JINGHUA, Lyu (2019): *Chinese-American Relations in Cyberspace: Toward Collaboration or Confrontation.* January 24, 2019, Available at https://carnegieendowment.org/2019/01/24/chinese-american-relations-in-cyberspace-toward-collaboration-or-confrontation-pub-78213 (Downloaded on April 8, 2020)

McNABB, David E. (2016): Vladimis Putin and Russia's Imperial Revival. *CRC Press*, 2016. p.65.

NABEEL, Fahrad (2018): International Cyber Regime: A Comparative Analysis of the US-China-Russia Approaches. *Strategem* Vol. 1, No. 2, December 2018. 8-27. Available at https://www.academia.edu/38296708/International_Cyber_Regime_A_Comparative_Analysis_of_the_US-China-Russia_Approaches (Downloaded on April 8, 2020)

PAINTER, Christopher (2018): The rise of the internet and cyber technologies constitutes one of the central foriegn policy issues of the 21st century. *The Foreign Service*

Journal, June 2018, Available at https://www.afsa.org/diplomacy-cyberspace (Downloaded on April 13, 2020)

PAWLAK, Patryk (2015): Cyber Diplomacy: EU Dialogue with Third Countries. European Parliament Think Tank, June 29, 2015, Available at https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/564374/EPRS_BRI(2015)564374_EN.pdf (Downloaded on April 8, 2020)

POPESCU, Nicu – SECRIERU, Stanislav (eds): Hacks, leaks and disruptions. Russian cyber strategy. *Chaillot Papers* No. 148., October 2018, European Union Institute for Security Studies Available at https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf (Downloaded on April 20, 2020)

Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. May 11, 2017, Available at https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/ (Downloaded on April 13, 2020)

RENARD, Thomas (2015): *US-China cybersecurity agreement: a good case of cyber diplomacy*. October 1, 2015, Available at http://www.egmontinstitute.be/us-china-cybersecurity-agreement-a-good-case-of-cyber-diplomacy/ (Downloaded on April 8, 2020)

ROTH, Andrew (2015): *Russia and China Sign Cooperation Pacts*. The New York Times May 8, 2015, Available at https://www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html?_r=0 (Downloaded on April 8, 2020)

SEGAL, Adam (2017): Chinese Cyber Diplomacy in a New Era of Uncertainty. A Hoover Institute essay. *Aegis Paper Series* No. 1703. p.1. Available at https://www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf (Downloaded on April 7, 2020)

SEGAL, Adam (2018): *Year in Review: Chinese Cyber Sovereignity in Action.* January 8, 2018, Available at https://www.cfr.org/blog/year-review-chinese-cyber-sovereignty-action (Downloaded on April 8, 2020)

SWAINE, Michael D.: Chinese View on Cybersecurity in Foreign Relations. *China Leadership Monitor*, 2013. No. 42. p.5. Available at https://carnegieendowment.org/email/South_Asia/img/CLM42MSnew.pdf (Downloaded on April 7, 2020)

The 7th China-EU Cyber Taskforce was Held in Beijing. January 13, 2020, Available at https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/jkxw_665234/t1731937.shtml (Downloaded on April 8, 2020)

The White House, *Joint Statement by the Presidents of the United States of America and the Russian Federation on a New Field of Cooperation in Confidence Building* (17 June

2013) Available at http://www.whitehouse.gov/the-pressoffice/2013/06/17/joint-statement-on-a-new-field-of-cooperation-in-confidence-building (Downloaded on April 10, 2020)

UK and 50 nations sign cyber security pact. November 13, 2018, Available at https://www.itproportal.com/news/uk-and-50-nations-sign-cyber-security-pact/ (Downloaded on April 16, 2020)

UN General Assembly, Resolution A/68/98., „Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.", June 24, 2013, Available at https://www.un.org/ga/search/view_doc.asp?symbol=A/68/98 (Downloaded on April 6, 2020)

US Chief Calls for Regulatory Scheme for Cyberwarfare. (2018) *Radio Free Europe/Radio Liberty*, February 19, 2018, Available at https://www.rferl.org/a/un-guterres-calls-for-cyberwarfare-rules/29049069.html (Downloaded on April 6, 2020)

WIRTZ, James J.: Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy. In GEERS, Keneth: *Cyber War in Perspective: Russian Agression Against Ukraine*. NATO CCD COE Publications, Tallinn, 2015. p.32. Available at https://ccdcoe.org/uploads/2018/10/Ch03_CyberWarinPerspective_Wirtz.pdf (Downloaded on April 20, 2020)

Xi Jinping gives speech at Cybersecurity and Informatization World Conference. April 19, 2016, Available at https://chinacopyrightandmedia.wordpress.com/2016/04/19/xi-jinping-gives-speech-at-cybersecurity-and-informatization-work-conference/ (Downloaded on April 8, 2020)

ZIOLKOWSKI, Katharina (ed) (2013): *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, NATO CCDCOE Publication, Tallinn, 2013. p.519.