Valdai Discussion Club Report

Digitised Realpolitik: Sovereignty, Alliances and Non-Alignment in the 21st Century

Andrei Bezrukov,
Mikhail Mamonov,
Olga Rebro,
Andrei Sushentsov

valdaiclub.com
#valdaiclub

September 2021

ISBN 978-5-907318-48-9

16/1 Tsvetnoy Boulevard St., Moscow, Russia, 127051

About the Authors

Andrei Bezrukov
MGIMO Professor; President of the Technological Sovereignty Exports Association

Mikhail Mamonov
Deputy Minister of Digital Development of the Russian Federation (2018 –2020)

Olga Rebro
Expert at MGIMO Institute for International Studies, Moscow State Institute of International Relations (MGIMO University)

Andrei Sushentsov
Programme Director at the Valdai Discussion Club; Director of the Institute of International Studies, Moscow State Institute of International Relations (MGIMO University)

The authors of the report express their gratitude to the participants of the open discussions, conducted by the Valdai Discussion Club:

- Expert discussion "Competing Technological Platforms in the 21st Century"(22.03.2021).
- Online discussion "The Digital Future of Eurasia: Priorities for Eurasian Integration until 2025" (25.05.2021).
- The Club's session within the framework of the business programme of the St. Petersburg International Economic Forum-2021 "The Right to a Privacy in a World of Big Data" (03.06.2021).

Contents

Introduction

The world is entering a new technology cycle which empowers governments with new tools to advance their interests and creates a space for interaction between states, in which the rules have not yet been determined. At a time where the key military and strategic invention of the previous era – nuclear weapons – remains primarily a deterrent, economic and technological competition has become the main battlefield for offensive actions among the leading players. Digital technologies are gradually filling up the niche which, in the era of bipolarity, was traditionally taken by nuclear weapons as a key strategic tool that was equally important for military leadership, economic growth and global prestige. Using a metaphor, it can be argued that the states that have formed their sovereign technology platforms have become members of a prestigious private club similar to the nuclear club.

In one fell swoop, digitalisation has narrowed the gap in the military-strategic potential of the nation states around the world which previously appeared unbridgeable. Now, comparatively low-cost cybernetic means can be used to inflict albeit not critical but nonetheless significant damage on a rival state. The expanded use of digital technologies in the military has thus shifted the focus in the military-technological competition between states. Another important hallmark of digital technologies is their much broader civilian use, which further blurs the line between economic competition and the arms race.

The ongoing transformations are becoming a factor in strategic planning by states. It is no coincidence that Russia's military doctrine ranks hostile violation of Russia's critical infrastructure by a foreign state second on the list of threats. Many countries have adopted strategic cybersecurity documents, but Russia does not have a separate document of that kind. As leading countries have begun to build their capacity in this area, they are testing new capabilities in practice, which increases the number of cyber incidents happening in an almost unchecked environment.

What will the world order look like in the new technology cycle? What factors will be decisive for determining the power of a country and how will the traditional features of a nation state adapt to new circumstances? Who will set the rules of conduct in the new digital age and how? Today, the world needs to find answers to these questions, since the world system's stability in the decades ahead will depend on those answers.

The agenda for international regulation in a new technology cycle

One of the most important outcomes of digitalisation is the creation of digital replicas of objects and real world processes. The digitised specifications of objects make it possible to speed up data exchange and build relationships that are impossible to build in the real world, to apply new methods of analysis, and to identify patterns as well as, overall, to turn the entire world into a single quantifiable system. The improvement of the global digital replica goes hand-in-hand with ongoing development of technology for storing, transmitting and processing this information, as well as providing interaction channels between the real and virtual worlds, such as sensors, telephones, and biometrics. As digital technologies continue to make their way into everyday life, almost everything is becoming an object of critical information infrastructure. This poses new challenges for the nation states when carrying out their security functions.

First, *infrastructure has become significantly more vulnerable*. It is now possible to cause significant damage with an ordinary smartphone and some expertise in information technology. Digital technologies have not only enriched the toolset of traditional security threat sources, such as armies or terrorist and criminal groups, but have also expanded their number, and almost anyone with enough technical skills can be such a source today.

Second, larger numbers of digital security space actors imply a variety of motives for their behaviour, which makes it difficult to prevent and predict these threats. Cyberincidents and cyberattacks in the 21st century are not so much episodes of interaction between states as, primarily, a tool used by multitudes of non-state actors. As a number of incidents across a variety of spheres have shown (banking system hacking or an attack on an oil pipeline in the United States, and before that an attack by NotPetya virus), blocking systems for extortion purposes has become a separate transnational crime niche.

Third, migration of social and commercial relationships to the digital space leaves open the question of *what counts as a cyberattack or a cyber incident*. During the 2016 US elections, US security officials pointed to

messages that were spread on social media that concerned the country's most pressing social issues. Having established that Russia was the source of these messages, they accused the Russian government of destabilising US democracy and trying to influence the outcome of the elections. Subsequent studies, however, offered an alternative explanation, having called this exploitation of the hot-button social topics, which guarantee user interest, a social marketing campaign and an attempt to make money on the number of clicks (*clickbait capitalism*).[1] "Influencers" who are able to exert influence on large social groups by way of spreading online messages are tightly implicated in this.

Given these circumstances, *attribution* becomes vital for relations between the states. It is technically very difficult to establish the source of a cyberattack or a cyber incident. But even with the source identified, it is extremely difficult to prove that another country is behind this attack, because an attack could have been made from its territory (or things were staged to make it look like that), but one can never say for sure whether its citizens acted of their own accord or at the direction of the state, and whether these were the citizens of that particular state in the first place. Thus, any accusations on behalf of the affected state can be called unsubstantiated, the responses unfounded and disproportionate, and the conflict itself can quickly spiral out of control.

This challenge can be met by creating an impartial international body – *an independent arbitration tribunal*. This theoretically justified idea runs into problems in practice. As can be seen from the experience of organisations of that kind in other spheres (for example, the Organisation for the Prohibition of Chemical Weapons)[2] there is a threat of politicising the activities of such a body, and it will have limited legitimacy from the very start. Even though the technology behind digital forensics is evolving, it will preclude an impartial examination of the evidence obtained during its use due to the above arguments.

In addition to an increase in the number of participants, *total digitalisation leads to an increase in the amount of available data, among which one should draw a line between personal and large (anonymised) data.*

[1] See, for example, a study by the University of Oxford: The IRA, Social Media and Political Polarization in the United States, 2012-2018.URL: https://int.nyt.com/data/documenthelper/534-oxford-russia-internet-research-agency/c6588b4a7b940c551c38/optimized/full.pdf#page=1

[2] Mate A. Ex-OPCW chief Jose Bustani reads Syria testimony that US, UK blocked at UN. 5.10.2020. URL: https://thegrayzone.com/2020/10/05/ex-opcw-chief-jose-bustani-reads-syria-testimony-that-us-uk-blocked-at-un/

Storing up personal data is an inevitable consequence of the digitalisation of human life. However, despite the fact that this process increases the need for legal regulation of the digital space, concepts like "electronic person," "electronic state," "digital economy," "digital law" or "digital sovereignty" have not been fully worked through and are not well-established.[3] Traditional approaches to the definitions which, one way or another, connect concepts with physical reality (citizens, state borders, and tangible property) become meaningless in the digital environment given the intangible, hence, non-spatial nature of the digital code which is its key component. In this regard, states have taken the path of forcibly tethering the generated information to the physical world. For example, in the United States, Russia and Europe, laws have been adopted that determine the need to store personal data within national jurisdictions on national servers and in national cloud storage.

The ongoing heated debate in the United States regarding the need to update the Communication Decency Act adopted back in 1996 is one of the most vivid examples of such a difference. The act deliberately leaves ambivalent the question of ownership of the information posted online and accountability for its content. Unlike publishers (such as the media), which can edit their publications, obtain rights to them and bear responsibility for their content, or platforms (for example, mobile operators), which cannot deny service and do not obtain rights to transmitted information, but are not responsible for its content, either, the internet companies can do both: moderate the content and bear no responsibility for it, or its safe-keeping, and the like. As a result, the US IT juggernauts had their hands fully untied when it came to determining the rules for the functioning of online space, which made them an independent and highly influential player in a country's domestic political life. This fact was confirmed by the suspension of US President Donald Trump's popular social media accounts in January 2021.

On the other hand, the case of the EU, where the General Data Protection Regulation has been in effect since 2018, is quite telling. Under this regulation, the rights related to the generated information (right to be forgotten, security, data confidentiality) belong to users who are EU citizens, and companies

[3] See, for example: Sarkisyan T. Integratsionny "plan GOELRO" dlia XXI veka (GOELRO integration plan for the 21st century) // Rossiya v globalnoi politike (Russia in global politics). Mar 9,2021. URL: https://globalaffairs.ru/articles/czifrovoj-suverenitet-eaes/ or monograph Transformatsia prava v tsifrovuyu epokhu (Transformation of law in the digital age) // Izdatelstvo Altaiskogo gosudarstvennogo universiteta (Altai State University Publishing House). 2020, pp. 103-110. URL: https://www.asu.ru/files/documents/00023452.pdf

that process such information are in charge of implementation. However, this approach is extremely restrictive in nature and severely limits the ability to collect and store data to the detriment of improving mechanisms for handling big data.

In turn, big data sharing is an even less studied issue at a time when it matters much more for intelligence communities and economic agents than personal data. Focused work with massive data sets can help form a picture of the epidemiological situation in a particular region, economic development, the demographic situation and social stability and predict the way the identified trends will unfold. Using the exceptionally strong computing power of modern computers, multiple scenarios for future developments, as well as the likelihood and conditionality of their occurrence, can be simulated on the digital twin. This, in turn, makes it possible not only to observe the situation or a process in question, but also to influence them as needed. Access to this kind of information makes it possible to find out almost everything about a nation state and is a colossal resource and a challenge for national security. The rules for exchanging the arrays of this kind of information have not yet been drafted, and the nation states have yet to create corresponding mechanisms.

The correlation of personal and big data is a separate aspect that needs clarification. Collecting user data (the "digital footprint") which was provided knowingly or not, companies or state authorities use it as a single big data set for purposes that are not always known to the user, which constitutes a violation of their rights. Anonymising big data is an effective solution to this situation, but, in this case, the regulators are confronted with the need to develop mechanisms for verifying the fact of anonymisation. The case of Estonia, where data anonymisation is replaced with mandatory deanonymisation of the instance of using personal data, is interesting in this regard. Access to the citizens' digital data is open to competent agencies and companies, but each case of accessing this data is recorded and, if needed, it is possible to establish who used the personal information and for what purpose.[4] This system guarantees transparency and self-regulation of the country's digital environment: fully aware of the fact that they can check at any time how their data was used, the people are more amenable to provide it, while companies and government agencies are more cautious about using it. As a result, the level of trust between the

[4] Jaan Priisalu & Rain Ottis, Personal control of privacy and data: Estonian experience. URL: https://link.springer.com/article/10.1007/s12553-017-0195-1

three carriers of sovereignty in the digital space improves, and this system thus helps store more information rather than limit the volume of collected data (which is what the EU regulations are aimed at with a limit, among other things, on the personal data storage time).

Alongside security-related aspects, the problem of digital activities' economic regulation is becoming increasingly important. For example, many digital transnational giants do not have a legal office in Russia, use our citizens' economic resources and national infrastructure, but do not pay taxes on revenue generated in Russia. Leading social media, email services and search engines use access to user data regardless of their geographic location to attract advertisers. The efforts to develop common principles for taxation of digital giants have been underway since 2013 within the OECD and the G20, and the EU is striving to come up with common principles for regulating this sphere.

The identical nature of the emerging digital problems and challenges pushes states to start a dialogue. In this regard, digital issues are bringing the countries around the world closer rather than dividing them.

The world is advancing towards regulated freedom that the people gained through digitalisation. Previously, the choice of a digital platform was determined by its user friendliness, whereas now the choice is more likely to depend on national security reasons, which can make many services illegal. This is justified from the point of view of the state; however, individuals have understandable concerns about losing control over their personal data and seeing their choice of technological devices and solutions contract. In part, this is inevitable and, over time, society will be compelled to recognise the new reality: metal detectors that appeared at the airports in the early 21st century do not bother anyone today. However, unlike passengers at an airport, it is difficult to channel digital data flows into one corridor, and excessive restrictions will provoke the creation of ways to circumvent regulation and the development of virtual private networks (VPN), as well as encryption tools available to the general population (PGP or end-to-end encryption systems in instant messengers, to name a few) and darknet. The nation states are faced with the dilemma of striking a balance between *protecting sovereignty and ensuring security*, on the one hand, and *protecting individual rights and ensuring the availability of information*, on the other. At the same time, in the absence of a more effective solution to the need to increase control over the internet space, nation states

are resorting to the already described proven method which is to create physical restrictions on access to the network's national segment. At the same time, the internet itself retains its primary importance for the technological, economic and social evolution of humankind, while remaining global.

In an attempt to resolve this dialectical contradiction, the world of the future may find itself in a situation where *digital space will become a conversation between sovereign national "internets"* based on their fundamental compatibility. This format will allow the nation states to overcome the problem of ensuring security in the digital space with the least damage to the convenience of the users, who will not see major changes in practical terms. An alternative path – disintegration of the planet's communication unity – will lead to a spiral of crisis with no chance of getting out.

The "struggle of standards" is another hallmark of the new stage of development where nation states or individual corporations (which, in some aspects, have become equal to nation states) are trying to secure the universal status of individual solutions and standards, which will predetermine the contours of the world's technological image going forward: the proprietors of these standards will thus get a head start.

The importance of this struggle is underestimated in Russia while it is already underway, for example, for the use of a depletable radio frequency resource. If you do not standardise the rules for working with it, the border countries may have serious problems, since the use of the portions of the radio frequency spectrum by the military department of one nation state makes it impossible for other states to use the same portions of the spectrum for civilian needs. Without ensuring coordination and compatibility of national systems, these discrepancies may become a problem down the road, in particular, for developing cross-border traffic of unmanned vehicles from Russia to the EU.

Failure to work out a single standard will lead to the emergence of technological barriers that hamper economic development within integration associations. So, not all EAEU counties use encryption standards that are acceptable to the Russian Federation from the point of view of ensuring the security of the national segment of the integrated information system. The absence of this universal standard hinders the legally important electronic paper flow between our countries, which could accelerate business processes in the EAEU by orders of magnitude.

Bloc-based confrontation between digital powers

As we wrote earlier, rivalry between the great powers has led to a world that is divided into *competing technical and economic blocs* which function on the basis of different technological platforms.[5] These blocs exist in the form of nation states or formal or informal country associations with an array of natural and human resources, their own economic model, financial system, developmental philosophy and technology to ensure the critical infrastructure's sovereignty and security. A *technology platform* is an array of technological means that are used as a basis to create other arrangements, processes and technologies.

Technological ecosystems have become a confrontation tool used by major global players. The countries that do not have the necessary set of competencies and national ICT technology have to join the existing technical and economic blocs. Digital colonisation can be considered the ultimate form of a nation state's technological dependence.

Earlier, metropolises viewed colonies as a source of natural resources, but modern "digital colonies" will become a source of big data that will become the new oil. Big data only comes into its own when it can be handled properly. The states that do not have this capability do not consider big data a valuable resource and are therefore ready to exchange it for attractive offers coming from advanced countries that allow them to leap from notional feudalism to the digital era, skipping the stage of industrialisation (5G without 2G, the use of drones in areas that do not even have roads, the transition from manual labour to computers, skipping the assembly line phase). After states have switched to the standards adopted by advanced companies, they become objects of digital and economic activity.

United States

A separate technological bloc has already formed in the United States. The digital agenda is becoming an increasingly important matter in US domestic politics. The 2020 US presidential election clearly showed the role of online platforms in shaping the information space and, accordingly, influencing the voters' preferences. At the same time, the platforms remain private companies

[5] A. Bezrukov, M. Mamonov, M. Suchkov, A. Sushentsov. Suverenitet i "tsifra" (Sovereignty and "digital") // Rossiya v globalnoi politike (Russia in global politics). Mar 1, 2021.URL: https://globalaffairs.ru/articles/suverenitet-i-czifra/

and follow the logic of maximising profit. For example, accusations against *Facebook* in the summer of 2020 of declining to moderate the statements made by right-wing groups have led to a boycott of this social media by advertisers, which cost the company $7.2 billion in lost revenue and an 8.3 percent drop in share prices.[6] Shortly after, Facebook CEO Mark Zuckerberg said he "committed to reviewing our [company's] policies ahead of the 2020 elections," and "Facebook will take extra precautions to help everyone stay safe, stay informed…" during this stressful period in the country's life.[7] Talking about direct coordination between the Democratic Party and the internet giants would be a stretch, but the liberal values they share create an environment where publication of a non-consensual point of view is taken as inciting social hatred, and is thus subject to moderation, since it threatens national security.

Even though in their fight against populism, the internet platforms have found themselves on the same side of the barricades with the political establishment, Washington understands the need to limit their omnipotence. On June 11, 2021, five bills containing actions to prevent monopolisation of the digital space were submitted to Congress ending a 16-month congressional probe.

Despite the purported principle of a free and open digital space, the United States is moving to the concept of *digital Realpolitik* in its foreign policy. Washington will operate based on, above all, its own interests and maintain allied relations with the countries that see the rise of China and Russia's actions as a challenge. Demonising Beijing and Moscow, whether on the basis of ideology (democracy vs. autocracy) or economy (undermining "fair" market competition) will come as an important tool in an effort to rally countries around the United States. Two trends will underlie these allied relations: *politicisation* (the US approaches must be shared and its leadership recognised) and *pragmatism*.

China

However, the United States is gradually losing the potential to maintain hegemonic stability. China is claiming a bloc of its own as well. Beijing is creating its own platforms and is investing heavily in artificial intelligence, quantum computing, and semiconductors. Increasingly, it declares its leadership in areas such as the cluster of brain sciences, genomics, biotechnology, and deep space.

[6] Datoo S. Mark Zuckerberg Loses $7 Billion as Companies Drop Facebook Ads // Bloomberg. 27.06.2020.URL: https://www.bloomberg.com/news/articles/2020-06-27/mark-zuckerberg-loses-7-billion-as-companies-drop-facebook-ads

[7] Zuckerberg M. // Facebook. 27.06.2020. URL: https://www.facebook.com/zuck/posts/10112048980882521

In cyberspace, China is seeking to "open up" and "close" at the same time. While promoting the idea of the *sovereign internet*, Beijing simultaneously declares the concept of a community of shared destiny in cyberspace and comes up with initiatives for international cooperation (establishing a Digital Economy Association, creating the Digital G20, and launching bilateral digital dialogues).[8]

The United States and China's primacy today is undeniable. As noted in a 2019 report by the United Nations Conference on Trade and Development (UNCTAD), these two countries collectively account for 75 percent of all blockchain patents, 50 percent of global IoT project spending, over 75 percent of the global cloud market and 90 percent of the market capitalisation of the 70 largest digital platforms, as well as 40 percent of the information and communications sector of the global economy. At the same time, the growth rates of digital economic sectors significantly exceed the GDP growth rates.[9]

Among other things, over the past four years there has been a separation of the once symbiotic economies of the United States and China, which merged into a concept of Chimerica back in the mid-2000s. This is particularly obvious in technology, where dependence on material supplies, the exchange of intellectual property and even the electronic component supply chain vulnerability are perceived as a threat to national security. Given the atmosphere of mutual mistrust, the likelihood of striking compromises in the regulation of the digital sphere is waning, which could lead to the formation of *bipolar competitive platforms* and the Information Cold War. Acting as "digital colonialists," Washington and Beijing will vie to bring as many states as possible onto their platforms.

Russia's place in the new technological cycle

Amid the formation of two major economic and technological centres, all third countries are faced with a choice between maintaining sovereignty and the prospect of lagging behind technologically and economically, on the one hand, or giving up a portion of their sovereignty in exchange for

[8] A. Belova, President Tsentra Kitaya i globalizatsii Van Huiyao rasskazal o razvitii tsifrovoy ekonomiki Kitaya (President of the Centre for China and Globalization Wang Huiyao speaks about the development of China's digital economy) // Rossiyskaya gazeta. Dec. 25, 2020.URL: https://rg.ru/2020/12/25/sovetnik-gossoveta-knr-van-huejiao-rasskazal-o-razvitii-cifrovoj-ekonomiki-kitaia.html

[9] Digital Economy Report 2019 // United Nations. 2019. P. xvi. URL: https://unctad.org/system/files/official-document/der2019_en.pdf

economic promise, on the other. In and of itself, transferring a portion of sovereignty is not a matter of survival for any state. Abandoning their independence in the military sphere did not prevent Japan and Germany from becoming influential players in the international arena. By the same token, in the digital sphere, Singapore, South Korea and Israel failed to form a sovereign technological platform, but have not lost their leadership in developing high-tech products.

The willingness to abandon certain elements of sovereignty is closely related to the strategic culture of a particular state. In Russia, with its historical experience of confrontation with other states, a stable and well-founded conviction has developed that transferring even a few elements of sovereignty can undermine the country's survival. Therefore, it cannot afford not to have a national platform of its own, and ensuring technological security is one of the most important goals of Russian domestic and foreign policy.

Today, Russia has every attribute of a sovereign technological platform which relies on a mathematical school inherited from the Soviet Union. It has its own search engine which enjoys leading positions in certain regions of the world, its own social media and a number of competitive solutions (artificial intelligence, smart city, e-government, cybersecurity – many Russian companies are internationally recognised, such as Kaspersky, whose activities in North America were once an object of the political struggle).[10]

Russia's focus on creating independent national solutions to ensure infrastructure sustainability appears more than justified. Everyone remembers when, under the sanctions, *Siemens* said it was not ready to transport turbines to Crimea, which jeopardised the Crimean residents' lives and safety. Using Russian-made equipment entirely based on borrowed solutions created by foreign countries involves great risks. A situation like the one mentioned above, but in the sphere of cybersecurity or e-government, would not allow the state to effectively perform its sovereign functions to ensure the security and rights of its citizens.

The presence of such risks prompts the search for national answers to global digital solutions. Two registers have been created with the support of the Ministry of Digital Industry and the Ministry of Industry and Trade, namely, national software and national radio-electronic equipment. If there are comparable domestic analogues in them, Russian authorities and state-owned companies must choose solutions from the lists featuring in the registers.

[10] Sukharevskaya A. Vlasti SSHA vveli postoyanny zapret na goszakupki produktsii "Laboratorii Kasperskogo" (The US authorities introduce a permanent ban on government purchases of Kaspersky Lab products) // Vedomosti. Sep. 16, 2019. URL:https://www.vedomosti.ru/technology/articles/2019/09/16/811360-zapret

In the process of creating its own competitive solutions and for the purpose of systematic technological development, Russia needs to find a balance between ensuring competition on this sensitive market and protecting its interests. To begin with, it is necessary to create a new mechanism for innovation-driven activities within the framework of the *state defence order* so as to ensure the systematic development of domestic technologies. In the digital sphere, disconnects between the needs of society and the needs of the state can be avoided. As international practice shows, technologies are first developed in the defence industry and then become civilian property.

In the digital world, the bonds between governments and technology leaders will grow stronger. In the United States, CEOs of such companies visit various authorities up to 200 times a year. On the one hand, the state cannot ensure technological sovereignty in limited volumes without relying on technical and economic agents (private or public-private business). On the other hand, these companies have no less clout in the digital sphere than the state and talk to it as an equal, so a dialogue is the only thing that is possible here, since any attempt by the state to impose its rules will have limited success. In addition, they contribute to the development of critical elements in the interest of technical progress (AI and platform solutions, as well as solutions in telemedicine and distance learning) and make it possible to resolve a large number of socioeconomic problems at a relatively low cost, which appears to be quite attractive to the state.

Russia's key goal in technological diplomacy is to protect its sovereignty and avoid dependence on Chinese or US technological platforms. This can be achieved through a more resource-intensive formation of its own technological platform within the EAEU or the implementation of joint technological projects with the EU (which, however, is rather difficult amid the political polarisation of the West), or coming up with an alternative approach to international cooperation unlike the one promoted by the United States or China.

Russia's creation of its own technological platform within the EAEU relies on a solid foundation. A fairly extensive regulatory and financial environment is now available that makes it possible to implement the digital agenda. Originally, this agenda was perceived through the lens of information and communication technology and as a standalone area of integration, but now there's awareness of the need to develop digital tools and to promote integration across all areas of the association's activities, including transport, education, healthcare, and greater mobility of labour resources.

Innovative financing tools created by the Digital Initiatives Fund of the Eurasian Development Bank came as a major incentive for the development of joint digital projects. They were instrumental in developing job search services for citizens of the participating countries throughout the territory of the integrated association. Amid the COVID-19 pandemic, seamless transmission of data on test and vaccination results has been established, and projects on navigation seals for cargo tracking are being developed.

But in order to create a single technical and economic platform in the EAEU, a number of barriers will need to be removed. The relatively belated understanding of the total significance of globalisation has led to each country choosing a separate path for the development of information technologies and the introduction of their own standards and regulations, including legal ones, for handling data. In particular, Armenia and Kyrgyzstan are using encryption standards that Russia believes are inadequately secured. Kazakhstan is not ready to transfer information about its economic agents to the shared system, as it believes that this system is sensitive. Instead, it prefers to store the data in the national circuit. Obstacles to creating a single platform also include differences in understanding the level of threat posed by the use of borrowed technology by the EAEU member states and a lack of political will.

Russia can take a different path and become the leader of the *digital non-alignment* movement, which will bring together the countries that are unwilling to join either existing digital platform, US or Chinese. Just like Russia, many countries value their sovereignty highly, but lack the resources to ensure their digital independence. Russia's leadership in this group can be ensured through the proposed open source solutions, the use of which Moscow is consistently promoting. As part of this approach, in addition to the technology that they acquire, the states also receive its source code and, accordingly, the ability to introduce changes to it. The supplier does not have access to the data accumulated as a result of such changes, which eliminates the risk of "digital colonialism" and non-invasive external control.

The commitment to open source can be of critical importance for the future digital world's variables. Unlike the proposals advanced by individual companies, open source solutions allow the end user to make changes to the source code of the programme, modify the programme or change cybersecurity parameters. This makes it possible to avoid the risks involved in using equipment or solutions with "undocumented capabilities," which allow their owners to covertly monitor users or collect their data. Another

risk that is mitigated when using open source is the proprietary solution owners' remote influence on the performance and correct functioning of their hardware and software, or the owners' refusal to make such means available to the state under the pretext of sanctions or changes in export policies.

Russia is confidently claiming leadership in open source. This year and next year, Russia's Ministry of Digital Development plans to initiate a full-blown programme of events dedicated to open source, and the open source theme itself is key to the election campaign of the Russian candidate for the position of Secretary-General of the International Telecommunication Union which is the leading international platform for global harmonisation of approaches and standards in the field of digital development and administration.

The temptation to form a digital non-alignment movement is strong. The propensity for nationalising key digital tools can be seen not only in global players, but also in regional powers and just strong states. The stronger appeal of open solutions as compared with proprietary ones is recognised by leaders of the developer and programmer community, which boosts the moral authority of the state that comes up with such an initiative in the international arena. Perhaps, the idea of a digital non-alignment and its promotion in the international community will become a significant factor in mobilising Russia's leadership potential in the 21st century world.

ValdaiClub

ValdaiClub

ValdaiClub

valdai@valdaiclub.com

Council on Foreign and Defense Policy

RIAC
Russian International Affairs Council

MGIMO UNIVERSITY

HIGHER SCHOOL OF ECONOMICS
NATIONAL RESEARCH UNIVERSITY