Valdai Discussion Club Report

Valdai | Discussion Club

International Competition and Leadership in the Digital Environment

Andrei Bezrukov, Mikhail Mamonov,
Maxim Suchkov, Andrei Sushentsov

valdaiclub.com
#valdaiclub

January 2021

The views and opinions expressed in this report are those of the authors and do not represent the views of the Valdai Discussion Club, unless explicitly stated otherwise.

ISBN 978-5-907318-24-3

© The Foundation for Development and Support of the Valdai Discussion Club, 2021

42 Bolshaya Tatarskaya st., Moscow, 115184, Russia

About the Authors

Andrei Bezrukov
Member of the Presidium of the Council for Foreign and Defence Policy;
President of the Technological Sovereignty Exports Association;
Professor at the MGIMO University

Mikhail Mamonov
Director for Support of State Programmes and International Activities
at Russian Post

Maxim Suchkov
Director of the Center for Advanced American Studies at MGIMO University;
Associate Professor of the Department of Applied International Analysis
at MGIMO University; Non-Resident Scholar, Conflict Resolution
and Track II Dialogues Program, Middle East Institute

Andrei Sushentsov
Programme Director of the Valdai Discussion Club;
Director of the Institute for International Studies at MGIMO University

Contents

Introduction

Technology has become one of the most important spheres in the race for power in the 21st century. The two main technology ecosystems – the American and the Chinese – have clearly taken shape by the beginning of the third decade of the new century. A dilemma for Russia in this regard is whether to join one of the existing platforms or develop one of its own. The choice in favour of the first option implies negotiating the conditions for joining. The second option requires a more ambitious strategy that will determine the key parameters of a Russian techno-ecosystem.

The American system is the oldest, the largest and the best developed. It relies on the United States' undisputed technological leadership. A key goal of America's technology strategy is to retain the innovation initiative, prolong its own dominance, and prevent comparable rivals from entering the global marketplace. To this end, America is working on its human resources, creating preferential conditions for its start-up ecosystem development, and using methods of competition that have nothing to do with the economy.

The high market capacity and favourable conditions at home have enabled the United States to bring to the market the largest technology and internet giants whose intellectual property rights are protected by law. An indirect but significant factor in the American techno-economic system is the creation of numerous *common goods*. All this allows American companies to supply trial versions of their own products to the whole world, giving the user access to one of the most advanced technologies without excessive costs. These principles of digital openness and freedom offered by the United States are quite appealing. However, there is little doubt that the moment Americans start questioning their own hegemony in the technological environment, these principles will be immediately revised and insurmountable boundaries and barriers will be built to contain competitors and protect American leadership.

Even domestically, US tech giants' decisions to block and delete more than 70,000 accounts, including President Donald Trump's pages, look like blatant attempts to take away control from the government. Only in this case, the companies played for the political establishment against the unwanted "spoiler" of the system. The team of political, financial and technological globalists is likely to continue to work together in the coming years to oppose the national industrial agenda in America and other countries. At the same time, concerns are voiced in the Democrats' camp that as convenient as the technology offered by corporations is, the growing influence of tech giants is dangerous because "they hold so much economic power" as well as "wield so much control over political communication."[1] The

[1] *How to Save Democracy From Technology* by Francis Fukuyama, Barak Richman, and Ashish Goel. URL: https://www.foreignaffairs.com/articles/united-states/2020-11-24/fukuyama-how-save-democracy-technology

corporations' dominance in the dissemination of information and their ability to politically rally huge audiences is already a threat to democratic governments.

China's techno-economic platform is smaller than the American one; still, its technological leadership claims are just as obvious. Its significant financial and human resources allow the Chinese ecosystem to remain closed to the outside world while administratively reallocating resources to those areas of technology that CPC Politburo deems the most promising. The Chinese were the first in the world to experiment with the autonomy of a number of engines and services, building the Great Firewall of China. Whereas the Americans provide the world with trial versions of their products, the Chinese model's competitiveness relies on the low cost of their offer and co-financing of other states' advanced projects[2]. At the same time, China is playing a waiting game and does not react to US provocations. China rightly views America as a bigger and stronger player in this area. However, the pace of growth in the Chinese technology industry allows Beijing to think it is just a matter of time before it reaches a market position comparable with the United States. It is unlikely the Americans will be able to stop this process. World politics needs more pragmatism now, and heeding that need, an increasing number of America's allies – including in Europe – welcome China's proposals for digital cooperation.[3]

European countries' growing awareness of the importance of digital sovereignty can be potentially interesting for Russia. The key European nations – Germany, France, Italy, the Netherlands – fear dependence on the United States and China. France shows a special concern with developing a national technology platform. The Europeans are afraid of losing their identity in the global technological environment and ultimately finding themselves in a situation where their votes will not be counted[4].

Russia and Europe are united by fears of becoming dependent on leading players and losing their autonomy. At the same time, Russia, like some other European countries, has the competence to establish an independent pole of power in the digital sphere. Russia's arguments about the need to develop a data interoperability standard are more likely to be heard in Europe than in China or the United States. The latter two have a significant amount of data of their own that they are not ready to share with third countries. However, the political differences between Moscow and Europe can become an insurmountable obstacle to a broad collaboration, which is an additional motivator for Russia to build its own technology platform.

[2] Even now, Chinese companies are participating in the development of 5G networks in 45 countries, developing scientific collaborations in 145 countries and implementing city security systems in 71 major cities around the world.

[3] The Hungarian government is actively inviting Chinese manufacturers to set up 5G networks in Budapest. In Germany, the discussion about China's participation in the development of national 5G networks reached the level of the president and chancellor.

[4] This is the motive behind the French President Emmanuel Macron's initiative to launch 25 French technology "unicorns" by 2025.

Global Trends in the Development of the Digital Environment

The global digital revolution has triggered a radical transformation not only in technological and economic order but also in social relations and the very philosophy of human life. These changes have been fully reflected in international relations. The current world situation is similar (although at a fundamentally new level) to the time when nuclear weapons were invented and space exploration began, with technological changes substantially affecting the international conduct of states. It is already possible to identify a number of trends, emerging as a result of the new technology, which will determine the further evolution of the system of international relations.

Rapid progress of science and technology has created the prerequisites for reducing socio-economic inequality at national and global levels. However, at the same time it has increased the vulnerability and suspicion of society in the face of new challenges and threats (or the old ones in a new guise). New channels and means of communication have greatly enhanced the world's information links. But at the same time, they have facilitated the atomisation of states that want to protect these channels against foreign interference. The explosive growth of technology and the means of using it continue to blur the line between the virtual and the real world and between fact and invention. This leads to uncertainly and anarchy in international relations.

This uncertainty is being further aggravated by the growing gap between the dynamics of the development and introduction of innovations and the speed with which these changes are reflected in regulations. The phenomena that are not covered by international law are becoming a challenge to the classical system of international relations. Thus, the absence of codified agreements on limiting the use of artificial intelligence, supercomputers or cloud computing in the military sphere drags the countries possessing this technology into a vicious circle of a continuous arms race that diverts their resources and attention from developing these innovations for civilian use. Moreover, in the new conditions it is the internet that is becoming the main source of new threats. That said, the world governments do not have a common approach to defining the notion of "sovereignty in cyberspace." They are not yet drafting international agreements similar to the treaties on outer space, the Antarctic or air space sovereignty.

The universal character of the digital transformation is attracting the attention of the increasing number of international organisations, both

directly relevant (ITU) and not (UNESCO, UNCTAD, PACE). This is eroding the international digital agenda and multiplying mutually exclusive approaches to its issues. The absence of a common clear-cut framework of categories and concepts in this area is aggravating differences and disputes[5].

The fight for the universal recognition of technical standards created by states or major corporations is unfolding in the more technologically advanced international government and non-government venues. The most successful government and corporate lobbyists gain a substantial market advantage if their standards are codified: the entire world begins to use their products and they gain an opportunity to exert major influence on the further development of the chosen technology. This fight for standards also has far-reaching international political consequences. Considering the continued rapid digital penetration of social life, the countries supplying digital technology are strongly anchoring their customer states to themselves and getting them to use certain standards and solutions, thereby making them more dependent on their exports – by analogy with arms or energy exports.

The situation faced by the EAEU countries in implementing their digital integration is a graphic illustration of how serious this threat is. The development of the unified electronic exchange system has been substantially complicated by the fact that different EAEU countries use various cryptographic standards not all of which are considered safe. The lack of coordination at the time of their introduction, albeit for objective reasons, created a technical barrier to the development of integration processes with long-term political and economic consequences.

Global digitisation has greatly enhanced the international legal standing of non-government participants in international relations. The initially technical Internet Corporation for Assigned Names and Numbers, created with the participation of the US Government to regulate the use of domain names, IP addresses and the functioning of the global network, has become a leading institution of "internet governance" where the states do not play the main role[6].

Transnational giants – Google, Facebook, Microsoft, Huawei, TikTok, Alibaba, YouTube – are already addressing national and foreign governments as equals. They cannot be ignored as a national security factor. On the one hand,

[5] The UN polemics over the terms of "information security" and "cyber security" are indicative in this respect.

[6] In 2016, this corporation withdrew from the contract with the US Government but many countries are mistrustful of the political neutrality of this NGO that determines "the rules of the game" in the cyber world. Regardless of whether there are grounds for these suspicions or not, this is an important precedent whereby a non-government player regulates a critical national security area.

the information accumulated by such ecosystems and their advanced solutions are of enormous interest to the competent agencies. On the other hand, their ability as information resources to broadcast various information messages, directly or indirectly – through controlled replies to search queries – to a giant audience, is becoming a factor of national political life. The said ability of such corporations entitles them to "the right to vote" in the international arena and at the same time makes them subject to strict national regulation. The understandable striving of states to control their information activities and receive access to their data leads to the erosion of liberal values – freedom of speech and secrecy of correspondence and private life – and raises the issue of their applicability in the digital era.

Fair taxation of corporations, especially when their services operate in a foreign jurisdiction, is a separate issue in the standoff between corporations and states.[7] It is important to prevent the double taxation of these platforms in order to avoid a deterioration in the position of consumers and the products and services they receive.

It is probably the first time that ordinary citizens have gained the ability to directly influence international relations on today's scale. The social media, messengers and online television have practically won the competition with the traditional media. They have turned all owners of smartphones into potential journalists and given them the opportunity to instantly make their own "news" for millions of people. At first sight, this manifestation of freedom to speak out and be heard seems commendable but it is overshadowed by the lack of any requirement to verify facts in order for us to have confidence in them in the "post-truth" era. At best, the unintentional bias or craving for attention of an amateur reporter who is not restricted by professional ethics or the policy of a publication, or at worst, the dissemination of obvious disinformation could have destructive consequences for society and the state.

At the same time, a different trend is illustrated by the removal of Donald Trump's Twitter account. Throughout his four-year presidency, Twitter was an important resource of his power and the main instrument used to fight against his political opponents. Trump used it to create his information agenda, dictate his political will, appoint his associates and dismiss with shame his former soul mates. For millions of his supporters, Twitter became a mouthpiece

[7] How to calculate and collect taxes from such a platform as Booking.com, that merely brings together the demand and the supply and provides guarantees of payment but has no property except for its digital infrastructure? Meanwhile, the subjects of "the physical world" – hotel owners and customers pay taxes on transactions with it.

of discontent with Washington. The elites didn't understand him but at least heard what he said. Therefore, some people were amused by the President's tweets, whereas others were scared by them and still others annoyed.

As a symbol, the removal of Trump's account – even after he backpedalled and urged his supporters towards peaceful protest – was a much more demonstrative and sudden termination of his presidential position two weeks before the expiry of his term than it would have been through court or impeachment. Even more important is the fact that this "elimination" mission was performed not by Congress, the military or the Supreme Court but by the head of Twitter, a technology company.

Most probably, on the one hand, this case will result in third countries demanding "digital sovereignty" from American technical giants, and on the other hand, will strengthen their intention to protect themselves against the domination of their own and foreign technology companies by imposing tougher legal regulations on their activities at home. In the longer term, this could harden the world's political fragmentation.

Further development of cognitive technology, primarily, *deepfake*[8], provides the wrongdoers with unlimited opportunities to create toxic content that may already be listed in the category of weapons of mass destruction, given its force of impact[9].

Thus, growing freedom of society and the consolidation of instruments of its realisation is paradoxically accompanied by the strengthening of the state's police might and this is becoming a new norm of everyday life. The second trend is becoming stronger also for objective reasons: the striving of states to ensure the security of their citizens, in part, by limiting their access to the Darknet and other uncontrollable elements of the network can hardly be described as the dictatorial whim of governments. The extent of the de-anonymisation of users on the internet will continue to grow.

The absence of arbitration institutions recognised by all players, the lack of investigation of cyber accidents and cybercrime, and the so far underdeveloped instruments of digital forensics are making it practically impossible to reliably determine the guilty party. In turn, this is increasing the level of mistrust and strife between countries. The development of new technology, primarily the Internet of Things and autonomous intellectual systems allows the wrongdoers

[8] Method of faking an image, which is based on artificial intelligence.

[9] A person is not even needed to make an authentic-looking fake – a neural network can create simulacra itself and provide them with authentic biographies and probably make clips of any content with them in the near future.

to hack the security system of a critical infrastructure facility and trigger a catastrophe or obtain sensitive information with a fairly powerful home computer or even a smartphone. In these conditions, a technically talented teenager rather than a subversive or terrorist can act as a hacker.

The attempt of countries to protect themselves against such penetration has a number of consequences. First of all, the states are striving to limit the vulnerability of the network by encouraging import substitution and deep localisation – it is easier to trust one's own controlled hardware producer or software developer. This leads to the disintegration of international production chains and a certain erosion of the principles of the international division of labour. In conditions where everyone capable starts producing its own critical hardware and software (servers, operating systems, anti-virus software and security systems), economic specialisation is losing its appeal. In addition, the need to appoint authorised operators and limited competition in the market are inevitably slowing down the development of technology thus putting states on the horns of a dilemma between progress and security. As with many other aspects of the global digital economy, this one reveals the discrepancy between information exchange as a global phenomenon and the physical infrastructure that is located on a particular territory and, hence, is under a certain sovereignty.

This discrepancy is becoming abundantly obvious in data storage and processing or the transfer of information via internet channels. Historically, there is a serious imbalance between the geographical distribution of the base infrastructure and the national affiliation of the main internet players. Over 60 percent of the total number of domains are governed by American players (Verisign, Afilias); more than half of the content delivery networks belong to US companies (Amazon, Akamai, CloudFlare), and all main first level providers are US residents; ten out of 13 DNS servers are also located in the United States. It is no surprise that this "internet geography" and the United States' willingness to take extreme measures[10] in implementing its unilateral sanctions is compelling the states that are not direct US allies to create an alternative protected contour of "national, sovereign internet" and the number of such states is growing. However, according to experts, satellite internet might oust cable internet by the middle of this century, and in the new round the fight will move to outer space or the upper layers of the atmosphere[11] – but its nature,

[10] Thus, there are periodic conversations about an opportunity to disconnect Russia from the SWIFT rapid payments system. Given that Russia is among the 20 most active users of this system, this risk cannot be considered very high but it is not negligible, either.

[11] Hurst N. *Why Satellite Internet Is the New Space Race* // PC, 2018. URL: https://www.pcmag.com/news/why-satellite-internet-is-the-new-space-race

that is, the reluctance of states to leave their key infrastructure outside the zone of their sovereign control, will remain the same.

The striving of an increasing number of states for sovereign control is also reflected in their attitude to the storage of the personal records of their citizens. For all the nuances, the European GDPR, and the so-called Russian Yarovaya package emphasise the need for all internet market operators to store personal details on the servers located within the national jurisdiction. There is aggressive opposition to this approach, primarily from the Anglo-Saxon members of the Five Eyes (FVEY) intelligence alliance – the US, Britain, Canada, New Zealand and Australia. They claim that this measure is excessive and limits rights and freedoms. Considering the afore-mentioned imbalances in the internet space, the position of the US and its allies is understandable. However, with the development of the digitisation of the human personality and opportunities for its digital identification and transfer of all of its personal data to the cloud storage, the price of an error in protecting this information is spiralling. If the security of the data storage is violated, the threat is not limited to attackers taking over a person's identity but could result in the total erasure of the individual's identity. Such a digital death would make it impossible for the victim of the attack to implement their fundamental social rights. This is exactly why the increasingly strict national data storage requirements are becoming a dominant demand of our era.

In the next few years, national states will be faced with two important issues.

The first issue is their ability to guarantee the viability of their critical information infrastructures in conditions of a cyberwar and the growth of network piracy. Cyberattacks or system-wide failures in networks may switch off whole industries and cities for a long time, with unpredictable consequences for the affected countries and their populations. However, there is not yet a full understanding of the topicality and magnitude of such threats.

The second issue is how well the governments understand the principles and methods of ensuring the security of personal data and how they will regulate the turnover of depersonalised big data. If another state obtains such data, it will be able to create an authentic picture of the economic and industrial development of the state in question, its agricultural vulnerabilities, its epidemiological situation and consumption patterns and adjust its own political, military or economic strategy accordingly. Obviously, the accelerated development of national legislation regulating the processing of national big data and the start of interstate talks on this issue will take place in the not so remote future.

States and the Digital World of the Future: Duopoly or Oligopoly?

Today, it is impossible to conceive of a situation where a state in the major league of international politics doesn't have an established development strategy to guide it through the global digital environment, resources, and its own ideas and products in this area. *The very notion of a great power in the 21st century implies the availability of own technological platforms and ideally the formation of a technoeconomic bloc*. This bloc must necessarily control a significant share of the global market, operate its own currency zone and an emission centre, pursue its own development model, and have access to a set of resources, technologies and scientific competencies that allow it to act independently, at least in the key areas such as defence and critical infrastructure.

Any attempt by such a bloc to rule out the possibility of its competitors influencing its critical infrastructure will inevitably lead to politicising technology and technology wars. As a cross-cutting tool for the entire modern economic and sociopolitical space, digital technologies have become the main battlefield in a new war.[12] Cyberattacks against critical digital infrastructure can be no less destructive than the attacks with the use of nuclear or biological weapons.[13]

There's a threat of digital inequality and digital colonialism caused by the dominance of a number of developed countries in digital technologies and the emergence of global monopolies that will control the network infrastructure and data flows. *Digital technological sovereignty has become a rerequisite for political sovereignty and national independence*.

The restructuring of the principles underlying international economic relations and the entire global geoeconomics model creates new opportunities for the leading technoeconomic blocs, which are a variety of digital neo-colonialists of modern times. The gap – this time digital – between global

[12] Maxim Suchkov, Sim Tack *The Future of War*. The Valdai Club Report. URL: https://valdaiclub.com/a/reports/the-future-of-war/

[13] Andrew Futter *Why We Must Prohibit Cyberattacks on Nuclear Systems: The Case for Pre-Emptive US-Russian Arms Control*." Valdai Paper No. 95. URL: https://valdaiclub.com/a/valdai-papers/why-we-must-prohibit-cyberattacks-on-nuclear/

providers of digital technologies and the recipient countries, which are gradually falling under increasing dependence on technologically advanced states, continues to widen.

At this stage, the digital neo-colonialist countries provide exclusively favourable terms to the countries that are objects of their economic conquest so that they can create the infrastructure that they need in order to access the digital future. That way, they instantly make them part of their own solutions ranging from payment systems to data storage systems and electronic paperwork. Most importantly, they obtain unlimited and almost free access to big data, thus getting effective tools to control their digital colonies in addition to enjoying a direct economic effect and an extra advantage in developing their own AI tools and neural networks[14].

Digital colonialism will continue to expand, and a revival of the UN Trusteeship Council – this time with new digital functions and powers – cannot be ruled out. Clearly, the canonical borders of the countries of the first, second and third world have already undergone major changes and will continue to change. Former third world countries now have an opportunity to make a proverbial leap "from feudalism to socialism, bypassing the stage of capitalism," that is to create an advanced new-generation infrastructure without the need to maintain the old infrastructure, which is non-existent.

In this regard, one can foresee a digital leap by richer Middle Eastern and African states to a place where they have meaningful roles in the digital arena. Finally, international financial and labour relations are also changing with digital assets moving to more comfortable jurisdictions with even greater ease than financial ones, and leave almost no traces of making such a transition. The emergence of crypto currencies deprives the monopoly states of yet another sovereign right: the note-issuing privilege. The concepts of brain drain and labour migration are also changing. National "digital proletarians" no longer need to relocate abroad. All they need to do is stay home and work for a foreign corporation forfeiting their intellectual property. Alternatively, talented hipsters can move to a country with a better climate while continuing to work for their respective national economy.

At the same time, digital technologies, which underlie the daily life and the information space of each person, are beginning to exert an increasingly noticeable influence on the human psyche and decision-making practices. Individuals are not only becoming enslaved by digital platforms operated by global monopolies, but are actually put in a situation where their entire life is tethered to devices such as a mobile phone, a tablet, or a smartwatch. Under the guise of providing convenience, they restrict individual choices in

[14] The global market of big data will reach $230 billion by 2025.

decision-making and manipulate behaviour, including by pushing a person to follow a certain route. In this unequal relationship, under the threat of being excluded from the social environment, digital monopolies expropriate and uncontrollably exploit personal data and even creative content.

The widespread adoption of digital technologies, including the digitalisation of industry and government bodies, as well as the introduction of 5G networks, forms the imperative for ensuring the security and robustness of the entire critical digital infrastructure. Without overcoming this challenge, digitalisation may become an exercise in building a house on the sand.

To remove "barricades" and "minefields" on the path to digital economy, the state must guarantee individual and corporate safety and easy-to-understand legal relations in the digital environment. This is particularly true of owning and using personal and depersonalised data and generated content.

Data ownership and price are just a fraction of the digital world problems that needs a speedy solution. No less urgent is the need to resolve the differences between the requirements for national or local data storage and global transparency of technological and corporate processes, where engine data from an aircraft operated by an airline of one country flying over another country are processed in real-time in a third country.

As technoeconomic blocs take shape, digital competition becomes a war of platforms and standards.[15] At the same time, a number of countries and regional associations that do not have control over a large part of the global digital market or dominant platforms, such as India, Brazil, Japan, Russia and the EU, will be compelled to look for common ways to preserve independence and competitiveness, including by way of creating common platforms based on open architecture and open source.

Russia on the Digital Agenda: Opportunities and Limitations

Russia is one of the few countries that have the technology and human competencies required to build its own technology ecosystem. The strong engineering and mathematical school that Russia received as legacy from the Soviet Union remains a source of high-skilled workers who are a key resource

[15] Its current examples include confrontation between US and Chinese tech giants Huawei and CISCO, Alibaba and Amazon, Facebook and WeChat.

behind digital progress. Russia possesses most of the attributes of a sovereign technology platform. A national search engine has been developed and continues to improve. Russian social media, such as VKontakte and Odnoklassniki, are still more popular than Facebook and Instagram not only in Russia, but in the majority of CIS countries as well. Russia is developing its own cloud technology and designing processors. Digital solutions offered by Russian companies – primarily, cognitive and self-learning systems, cyber security solutions, secure electronic paperwork and platforms for providing public services – enjoy significant export potential. Launched two years ago, the Digital Economy national programme will provide 97 percent of national households and all social infrastructure facilities (schools, hospitals and police stations) with high-speed broadband internet access by 2024. This will drastically improve the environment for businesses, telemedicine and distance learning, and help Russia bridge the digital gap. Russia is already among top 10 countries in terms of the number of internet users, and the Gosuslugi website with its 2 trillion annual transactions is the most popular government services website worldwide.

The digital economy's share in the country's GDP is on the rise. For all the vagueness of the term itself, it now amounts to about 4-5 percent of GDP, but continues to grow rapidly at a rate comparable to that of international digital leaders. In addition, Russia has an impressive satellite and radio frequency resource, which is key to the successful development of next-generation networks.

It would be wrong to underestimate the challenges that Russia faces in its digital development. Some of them are just a digital consequence of analogous problems and threats. Others have a fundamentally different nature of their own. In particular, Western sanctions not only restrict, among other things, access to international technology, but also increase the risks of preserving dependence on this technology to unacceptable levels. Siemens's refusal to supply turbines to Crimea jeopardised plans to provide the peninsula with heating. If we extrapolate this incident on the digital realm, a similar refusal by SAP, Oracle, CISCO or Microsoft to provide updates for their solutions operating in Russia could cause disruption – even collapse – of critical systems, including public administration and banking sector.

These and other trends in the international politics that have been unfolding in the past few years have made the task of introducing reliable protection for its own critical digital infrastructure a top priority for Russia. Whether we achieve this goal or not depends on effective phased transition from imported software and hardware systems and on creating an effective nationwide command chain from the regulator to the executor.

The government decision to create registers of domestic software and radio electronic equipment is designed to mitigate such risks. Without being part of these registers, companies cannot count on supplying their solutions to Russian state corporations and government bodies. These measures have a long-term positive effect on Russia as a sovereign technological power.

Coming up with information security countermeasures is a challenge given a conceptual ambiguity where two close but different information flow-related areas are not clearly delineated. Both the security of signals in the physical network carrying information and malicious ideological content are defined in Russia using the term "information security". Meanwhile, Russia's competitors in digital leadership define signal security and network security as "cyber security." [16] Countering threats in these two areas calls for different sets of competencies. Even though Russia has a fairly good understanding of how to deal with cyber threats, extra efforts are needed to conceptualise and promote its information content strategy.

Accusing Moscow of cyber intervention in other states' domestic affairs was used as a pretext to increase sanctions pressure and certainly tarnished Russia's international reputation. Moreover, this campaign had implications for a number of large Russian enterprises and firms. They faced problems and discrimination on some Western countries' markets. The risk that these accusations will be used by the United States and its allies as excuse for delivering "retaliation cyber strikes" or even "preventive cyber strikes" against Russia is perhaps even more significant than reputational or even economic implications.

In the information space, Russia's vulnerabilities are quite clear due to the dominance of US monopolies – Google and Facebook – in the domestic segment. These monopolies exploit Russian data for free and are increasingly trying to influence the information field and the political situation in Russia's domestic politics, including through manipulation of content and restricting Russian users' access to information and means of communication. Other non-Western countries face similar challenges. It makes sense to establish closer dialogue with them on the principles of digital era legal regulations, especially in terms of data ownership rights, data storage and access rules, joint fight against online piracy, and general rules of online conduct for governments and businesses. Keeping pace with the technologies and practices, especially in areas that are important for society such as cybercrime and digital finance, is the biggest challenge for the Russian legislators in the digital sphere.

[16] The United States has officially proclaimed the Defend Forward CyberStrategy, made its cyber troops a separate branch of the armed forces and created a separate agency to protect its critical digital infrastructure

The low competitiveness of Russian companies and government with regard to global corporations when it comes to attracting the best talent is yet another problem at hand. The brain drain may not occur formally as Russian talents continue to reside in Russia, but make their intellectual added value available to foreign companies. Taking into account the incomparable economic potentials of Russian and transnational businesses, this problem can be resolved only as part of an administrative or conceptual (but, in any case, state-sponsored) approach.

Also, Russia and Russian companies hardly do anything on international platforms to introduce technical standards and regulations which would promote Russian products. This is partly due to Russia's lack of a doctrine outlining its international priorities in this area similarly to the National Security Strategy or the Foreign Policy Concept. Over time, this may lead to technological isolation or actually force Moscow to work with internationally recognised standards and protocols in the development of which Russia did not participate.

Roadmap for Russia's Leadership in the Digital Environment

Russia's digital agenda must reflect the country's standing as a leading power in the global system and an exporter of security and stability. Russia must become the leader of "digital non-alignment" for countries that would like to avoid the technological dictate of digital neocolonialists.

The development of the digital sector in the Russian economy, including electronics and information technology, must be complemented with its expansion into the global markets. Only in this event will Russia be able to recoup investments in breakthrough technologies, take over the main technological platforms of the next-generation economy and create large competitive businesses.

A country with 11 time zones, Russia continues to play the role of a safe link between Europe and Asia even though distances are shrinking dramatically in today's globalised world. This is also true for the global energy infrastructure needed to maintain the extremely energy-intensive digital economy of the future, and the network of quantum communication

for safe data transmission. The cold climate of Russia's northern regions and cheap energy are competitive advantages when it comes to the placement of large data storage and processing centres.

One of the biggest challenges for Russia is the implementation of the EAEU digital integration programme (EAEU Digital Agenda). Conditions must be created very quickly for the member states' government agencies and businesses to exchange legally important documents via the EAEU Integrated Information System (EAEU IIS). This will accelerate cargo transit across the EAEU territory, enhance the economic impact of the process and improve the quality of EAEU integration.

In addition, Russia as the main stakeholder in this process must promote the interoperability of the EAEU IIS with the information systems of the CIS countries which have leanings towards the EAEU and the states with which the EAEU has or plans to sign free trade agreements.[17] Digital integration in this case can and must proceed ahead of physical integration. Another important instrument could be a special programme, possibly implemented jointly with Eurasian Development Bank, of introducing national e-government standards in interested partner countries.

The goal of expanding Russia's economic and digital space cannot be achieved without strategic allies in the digital world, which calls for using available political mechanisms for this purpose. We should make use of the positive potential of our ties with India, Indonesia, Brazil and other leading economies of the future.

It is no less important to develop a digital dialogue with the EU. **First**, seamless digital transport corridors for business will only be effective if we ensure the interoperability of the EAEU IIS with the European and Chinese information systems. **Second**, we need closer coordination with Europe on the use of the radio frequency spectrum, which is currently hindered by the existing contradictions with EU border countries. It is especially important to settle this issue considering that cargo will soon be transported between states by automated vehicles. Russia and the EU will need to coordinate a single standard for next generation networks and will require a single frequency band to be allocated to them. **Third**, Russia and the EU have put in place similar requirements, at least when it comes to principles, for personal data storage and transmission. But they must be harmonised for the convenience of businesses.

[17] Vietnam, Iran, Egypt, Singapore and Serbia.

Moreover, Russia and the EU would like to impose fair taxes on foreign digital giants, primarily American ones. Consensus-building on such taxation principles would promote the efficiency of Russia and the EU on the related multilateral platforms. It would also be reasonable in the medium term to create a joint cross-border pool of big data, which should be tagged in a standard mode and made available, including on a commercial basis, to third parties, primarily American and Chinese companies.[18]

Collaboration with the EU is important, if only because the Russian and European integration blocs are being squeezed by the self-sufficient American and Chinese information platforms, both of which are "big data monsters". Russia and the EU, which are relatively small entities when it comes to population size and volume of data generation, must join forces to become new centres of gravity.

The common rules and operating principles of national data management systems, which should clearly stipulate who can or cannot have access to the data concerned and under what circumstances, will reliably protect the national security of Russia and the EU. The big data array of individual states or groups of states clearly has huge intelligence, political, economic and military value, and hence protecting it is a key national security priority. But there is a more immediate political argument in favour of Russia-EU digital cooperation. The continuing deterioration of bilateral relations has removed the really important subjects from the bilateral agenda. The objectives of boosting the digital economy and joining forces against shared digital threats, which we have in common, can become fundamentally new spheres for confrontation-free interaction.

Relations with the leading digital powers – the United States and China – are a special concern for Russia. Unlike the European and Eurasian tracks, there is little probability of joint economic projects with the US and China. Nevertheless, Russia should continue developing digital ties with Washington and Beijing in the current political situation, though based on different systems of logic.

Russia should continue to coordinate its positions with China on international platforms when it comes to internet governance and data safety. We have similar approaches, although Russia's position is more liberal and does not provide for the creation of an analogue of the Great Firewall of China.

[18] Common data tagging would allow big data to be regarded as a single array. This would increase the value of big data, and facilitate the use of this "new crude oil" to promote national AI support programmes and self-learning software, enhancing their competitiveness.

But there are two delicate issues Russia should start discussing with Beijing without any self-consciousness.

The first is China's technological infiltration of the EAEU states within the framework of the Digital Silk Road doctrine. Just as in the case of Eurasian integration in general, Chinese business and government activities should be aligned and coordinated with the events stipulated under the EAEU Digital Agenda 2025.

Second, we should create rules of behaviour for Chinese companies on the Russian market of highly skilled labour and start-ups. Huawei is conducting a large-scale campaign to purchase Russian technology companies and attract Russian professionals to its R&D divisions. Huawei offers above market salaries to lure professionals from Russian companies. This is a logical process for a market economy based on the freedom of choice, but we must discuss compensation for the national economy with our Chinese partners. China would have never allowed the companies of third countries to act in this manner in its own market. The requirements for foreign digital companies working in Russia must include broader cooperation with universities, the localisation of not only R&D but also production, as well as the creation of joint products rather than the cannibalisation of start-ups' products.

It is even more important to develop political interaction with the United States despite our adversarial relationship. First of all, we should coordinate confidence-building measures in cyberspace, restrictions on the military use of digital technologies, and rapprochement in the field of internet governance. Russia and the United States could initiate talks on the creation of new verification instruments for new military technologies. We also need to agree on the terms: when speaking about "Russian hackers," the Americans most often provide examples of social engineering.[19] We must do our best to restore pragmatism to our bilateral relations, even though Washington does not appear to have any interest in this now. This does not amount to giving the United States a vote of confidence. Rather, we should consider each move by Washington not as a priori hostile, but in a balanced manner and in terms of its possible outcomes.

Russia must have a coordinated and clearly articulated and structured agenda for working in multilateral associations, such as the International

[19] Unlike the hackers who gain illegal access to information or disrupt the operation of a system, the internet users who post their information or videos on social media do not infringe on information security. Asking difficult but legitimate questions on which American society is divided is not necessarily an "effort to sow discord" and definitely cannot be defined as "spreading disinformation."

Telecommunication Union (ITU), the Digital G20 and OECD. Instead of wasting time promoting exclusively Russian approaches and waging diplomatic battles with our partners, it would be reasonable to admit, at least inwardly, the existence of two groups of "digital truths."

First, the location of DNS servers and internet mainlines is not one of Russia's strong points. Russia is not a top-level provider. When it comes to formulating the digital agenda, Russia is not the second pole of the system but a large regional power. Some digital corporations have reached a scale where they can talk with states as equals.

Second, the world is not leaning towards digital bipolarity as strongly as it may seem, which is especially obvious in the sphere of cyberspace regulation. Despite the declared principle of the free movement of information, the majority of states try to localise data storage, in one form or another. All countries pursue authoritarian policies when it comes to digital regulation. Indeed, some spheres must be strictly regulated even in the more democratic countries. On the other hand, it would be irrational to completely reject the concept of multistakeholderism in making decisions on the governance and further development of novel technologies. Regulators must maintain dialogue with the owners of technology, most of which are businesses. By becoming aware of these realities, Russia will be able to act as a mediator focused on compromise in multilateral associations.

Russia can also represent the interests of states that strive for digital sovereignty and don't want to become part of the Chinese or American digital empire but do not have sufficient identity for this. Our activity in both spheres could increase our opportunities for realising our leadership potential and becoming a "gravitational nucleus." This would allow us to promote Russian candidates for leading positions at multilateral associations such as the ITU.

Another major step towards reforming Russian activities at international organisations should be a more careful choice of delegation members, who should be more multifaceted. At this moment, Russian diplomats are not sufficiently aware of the technical aspects of issues on the agenda, while technical specialists have inadequate negotiation skills. A special role should be assigned to the lobbyists of our businesses, which are the end beneficiaries of most of the decisions made. This digital realism would shift Russia's focus from responding to provocations and foreign policy ballyhoo to the practical matter of ensuring our digital interests in the world.

The admission that we have lost the initiative and cannot seriously influence the 5G agenda should encourage Russia to focus on preparing proposals concerning 7G (or 6G?) standards and to step up efforts to prevent our isolation when it comes to the allocation of radio frequencies for next generation communications. Russia's views in this sphere do not coincide with those of the majority of other countries. The distinctive feature of the legal regulation of the digital sphere is that new laws will be written by those who write codes. In other words, the technical content will largely determine the legal framework. This is why Russian specialists must redouble their efforts to create standards and protocols for forward-looking technology.

The most important technological markets of the future include the market of platforms for sovereign critical infrastructure, in particular, cybersecurity, communications, energy, transport, finance and urban economy management systems, as well as biological and food security. In the context of increasing tensions and uncertainty worldwide, states have to pay more attention to national security and national control of their critical infrastructure.

The market of sovereign critical infrastructure, where contracts signed for decades ahead are worth trillions of dollars, is similar to the global arms market. Decisions on technological partnership are taken at the sovereign level based on the friend-foe principle, sales contracts are signed for entire systems rather than components, and implementation entails a high level of trust and localised production of some of the technologies as an element of long-term political influence.

Just as in the case of the arms market, Russia has a niche on the market of sovereign critical infrastructure, which is estimated at between 20 and 30 percent of the global market.[20] An important factor is that Russia positions itself as a leader on the security systems market and has engineering schools capable of creating complex systems.

The market of critical sovereign infrastructure could become the most promising export sphere for Russia. Russia's recognised unique competencies in the creation of complicated systems make the country one of the leading potential suppliers alongside the United States and, partially, China. The independent hardware and software environment, which is being created in Russia, is another competitive advantage. Theoretically, the ongoing "cold war" between the United States and China offers Russian an opportunity to expand into the markets of Greater Eurasia, the Middle East, Latin America and Africa,

[20] It includes countries with which Russia maintains privileged political relations and which intend to retain control of their digital sovereignty.

which will try to reduce their technological and political dependence on the warring parties.

By establishing itself as a security exporter in Eurasia, Russia could also act as the guarantor of its partners' technological sovereignty. A trillion-dollar market of potential partners and unique competencies could be used to formulate a strategy of high-tech exports for years ahead.[21] Russia would be able to protect its own security, build up its international influence and also try its hand at priority technological development.

However, it is impossible to penetrate the market of sovereign critical infrastructure without creating breakthrough integrated platform solutions. Likewise, the implementation of this strategy is impossible without solid ties with technological partners and Russian educational and technological footholds in other countries.[22]

Conclusions

With the virtualisation of all aspects of social life, the information landscape is being militarised. The digital environment has no interstate borders or generally accepted rules of conduct; governments and various organisations under their control take advantage of this situation and distribute biased content and misinformation to promote their own interests and values. Technologies such as *deepfake,* which shape virtual reality, leave users with almost no way of separating lies from reality and are capable of provoking religious and ethnic conflicts with impunity, of wrecking families and destroying the reputations of politicians and innocent people.

[21] Our prospective export products could be:
1) critical infrastructure (CI) protection systems and technologies;
2) hardware/software solutions for cybersecurity;
3) Smart City systems, including energy management;
4) logistics and transportation management solutions;
5) information systems for the financial sector and digital currencies; and
6) environmental monitoring and crisis response technologies and equipment.

[22] In general, the strategy of exporting critical infrastructure platforms implies (1) the creation of consortiums capable of offering integrated platform solutions, (2) support for companies that are capable of becoming technological, financial and project integrators, and (3) the creation of continuous presence capability for the leading Russian high-tech companies and universities.
This strategy also calls for establishing project headquarters to coordinate the efforts of private companies and government agencies to penetrate foreign digital markets, and a global technological information and promotion system, which will update potential clients on the advantages of Russian technologies in conditions of harsh and often unfair competition.

The regulation of the entire global internet network will inevitably be put on the agenda in the coming years. Internet governance is already being divided into digital "enclaves" under the pressure of technological confrontation, mainly between the United States and China, as well as ideological and political fighting. The basic value of the internet as a global, equal and democratic environment (*web neutrality*) is also being undermined by attempts – in particular those promoted by the United States – to make the quality and speed of network traffic dependent on the client's wallet. The inclusive nature of the internet is becoming key to reducing the digital divide, and along with it, a guarantee of global economic growth and social development.

Big data as the "new oil" of the digital era needs to have a clear owner and understandable value for the individual, business and government. Only if a person, a citizen is in the centre of digital services, will there be a balance of human rights, national priorities and business interests, and only then will it be possible to regulate the currently uncontrolled global digital monopolies for the benefit of society as a whole. The removal of the social media accounts of US President Donald Trump and his supporters, as well as the more recent *deplatforming* of the social app Parler, particularly popular among the Republicans, clearly delineate the ways in which the powerful tech giants could eliminate economic and political rivals if these tech giants chose to operate outside the United States. If they can relatively easily and effectively deal with their ideological opponents in the United States, why cannot this practice be made extraterritorial? Moreover, there have already been precedents.

For Russia, the minimum task is to preserve the sovereignty of decision-making when it comes to the main areas of national security. The maximum task is to create our own competitive technological ecosystem, become the leader of a technoeconomic bloc and a key participant in the development of new rules of the game in this sphere. In this sense, gaining economic sovereignty is a simpler task than gaining information sovereignty. But the latter seems vital for the survival of states in the future.

The export of technologies and competencies that protect sovereign critical infrastructure to countries wishing to ensure their independence and defence capability can and should become one of Russia's most important political and foreign-economic priorities. This will generate a significant financial inflow and ensure international influence. The powers that claim leadership in this area have already embarked on this trajectory.

The implementation of Russia's strategy for the export of critical infrastructure technologies is constrained by Russian high-tech companies' lack of experience in creating integrated platform solutions, their weak presence in the markets of potential partners, as well as insufficient financial capabilities to work on large and long-term projects.

As the civilisational and ideological confrontation intensifies, and cases of subversive information activity become more frequent, more and more countries become aware of the need for a more careful monitoring of harmful and subversive content on the internet. In the United States, where an information war is now unfolding between hostile political forces – as the 2020 presidential campaign has shown – digital monopolies resort to outright censorship and manipulation to help their ideological supporters.

Russia should consider some mechanisms for the effective shaping of the information landscape that would allow the country to lead in terms of the relevance and quality of content and thereby limit foreign influence in the national information environment.

The challenge of the new age is the audience's short attention span – a brief video or post on social media beats a comprehensive news story or analytical report; the variety of multimedia experiences scatters a person's attention, and change occurs so fast that life turns into a race against time. The conservative and traditionally unhurried sphere of interstate communication is compelled to change and run fast to be able to at least stay in the same place. Those countries that will be able to revise their cumbersome foreign policy mechanisms faster than others stand every chance of taking a leading position in this fast-paced *brave new 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