Russia in the Digital World: International Competition and Leadership

Andrei O. Bezrukov, Mikhail V. Mamonov, Maxim A. Suchkov, Andrei A. Sushentsov

Andrei O. Bezrukov
MGIMO University of International Affairs, Moscow, Russia
Department of Applied International Analysis
Professor

E-mail: a.o.bezrukov@yandex.ru
Address: Room 3036, 76 Vernadsky Prospect, Moscow 119454, Russia

Mikhail V. Mamonov
Russian Post
Director for Support of State Programs and International Activities

E-mail: mamonov2004@gmail.com
Address: Room 4101, 76 Vernadsky Prospect, Moscow 119454, Russia

Maxim A. Suchkov
MGIMO University of International Affairs, Moscow, Russia
Department of Applied International Analysis
Associate Professor;
Center for Advanced American Studies
Director

ORCID: 0000-0003-3551-7256

E-mail: max.suchkov@gmail.com
Address: Room 3036, 76 Vernadsky Prospect, Moscow 119454, Russia

Andrei A. Sushentsov
MGIMO University of International Affairs, Moscow, Russia
Department of Applied International Analysis
Associate Professor;
Institute for International Studies
Director

ORCID 0000-0003-2076-7332

E-mail: asushentsov@gmail.com
Address: Room 3036, 76 Vernadsky Prospect, Moscow 119454, Russia

The reported study was funded by RFBR and EISR, project number 21-011-31278.

This article is an extensively revised version of the paper "International Competition and Leadership in the Digital Environment" originally written for the Valdai International Club: https://valdaiclub.com/a/reports/international-competition-in-the-digital-environment/

DOI: 10.31278/1810-6374-2021-19-2-64-85

Abstract

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 this century. A dilemma for Russia in this regard is whether to join one of the existing ecosystems or develop one of its own. The paper critically examines the impact of contemporary trends in the digital domain on international relations and state policies, weighs up Russia's competitive advantages and the challenges in this domain, and charts a strategy that Moscow should follow in the modern world of digital competition.

Keywords: Russia, U.S., China, technology, digital, trends, ecosystem, sovereignty, great powers.

Technology has become a critical sphere in the race for power in the 21st century. The global digital revolution has triggered just as radical a transformation in the technological and economic order as it did in social relations and lifestyles. These changes inevitably drive international relations. By the beginning of the third decade of the 21st century two main technology ecosystems—the American and the Chinese ones—have clearly taken shape.

The term 'technology ecosystem' may have multiple definitions, but there is clearly a narrow and a broader meanings—both derived from the IT industry in which it is used. In the narrow meaning the tech ecosystem is understood as "a collection of tech solutions that

a company uses to run its business and how these solutions connect with each other" (Campos, 2020). The broader one defines it as "the network of organizations that drives the creation and delivery of information technology products and services" (Iansiti and Richards, 2006). It is in the latter meaning that the term has lately expanded to describe the accumulated technological capabilities of a state and the power it exerts in this domain over other states. Productivity, robustness, and innovation are the three crucial metrics in a technology ecosystem, while consumers, producers, and influencers are the three types of participants in this domain. The companies—and, by extension, the states—that master best ideas, services, and practices across these lines set the tone for the rest. Those who fail to meet the challenge, eventually fall under the influence of the leaders.

The American system is the oldest, the largest and the best developed one. It relies on the United States' undisputed technological leadership in the IT domain. A key goal of America's technology strategy is to retain the innovation initiative, prolong its dominance, prevent the emergence of strong rivals, and hamper their access to the global marketplace. To this end, the U.S. relies on its access to global human resources, creating preferential conditions for its start-up ecosystem development and using "competitive" practices that are often far from being economically just or legally clean.

The high market capacity, favorable economic conditions and hidden subsidies at home have enabled the United States to bring to the market the largest technology and Internet giants whose intellectual property rights are legally well protected. The principles of digital openness and freedom offered by the United States may sound quite appealing. Yet 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, U.S. tech giants' decisions to block and delete more than 70,000 accounts, including President Donald Trump's

pages, demonstrated the power of Big Tech, which can potentially threaten virtual monopoly of the state to control societies. In that case the companies played for the political establishment against the unwanted "spoiler" of the system; in the future, a team of political, financial and technological "globalists" may work together to oppose national interests of other countries. Also, there are concerns that however convenient the technology offered by corporations may be, the growing influence of tech giants is dangerous because "they hold too much economic power" and "wield too much control over political communication" (Fukuyama et al., 2020).

China's techno-economic platform is smaller than the American one, but its technological leadership claims are just as obvious. China's significant financial and human resources allow its digital ecosystem to feed on huge resources allocated to the technology areas that the CPC Politburo deems most promising. The Chinese were the first in the world to create an autonomous area of the Internet, building the Great Firewall of China (Griffiths, 2019). Whereas the Americans provide the world with trial versions of their products, the Chinese's competitiveness relies on the low cost of their products and co-financing of other states' advanced projects (Berkley and Letzing, 2019).

At the same time, China is playing a waiting game and does not react to U.S. provocations. China rightly views America as a bigger and stronger player in this area (Danilin, 2020). However, the pace with which the Chinese technology industry is growing allows Beijing to think it is just a matter of time before it reaches a market position comparable with that of the United States. It is unlikely that the Americans will be able to stop this trend. 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 (Chivot and Jorge-Ricart, 2020).

A dilemma for Russia in this regard is whether to join one of the existing ecosystems or develop one of its own. The choice in favor of the first option implies negotiating the conditions for joining. The second option requires a more ambitious strategy that will determine key parameters of a Russian tech ecosystem.

Russia is one of the few countries that have the technology and human competencies required to build its own technology ecosystem. However, the challenges on this path are many. Moreover, they are profoundly systemic and for now seem to overwhelm the resources. Yet the imperative to architect such an ecosystem is of paramount importance for two principal reasons.

First, genuine digital technological sovereignty has become a prerequisite for political sovereignty and national independence. If a state equates its existence to its sovereignty, directing all state efforts to the creation of its own tech ecosystem is a must.

Second, staying a relevant actor in the international affairs in the 21st century implies having one's own technological platforms. If, however, a state strives for a great power status, it has to form its own tech ecosystem. If Russia wants to continue to play a key role in global affairs, including in the security field, and be a co-designer of the new world order, it has no viable alternative.

In the 21st century Russia's best chance for building its domestic economy and its global influence is to position itself as a leader of the global digital "non-alignment movement"—a group of countries from Europe, Asia, Africa and Latin America which feel uneasy about the extent to which American and Chinese Big Tech may compromise their sovereignty and security, and also seek access to high-quality digital products and services.

MEASURING THE IMPACT OF TECHNOLOGY ON INTERNATIONAL RELATIONS

The influence of science and technology on international relations has always been in the focus of scholars and practitioners. This interest would usually rise at times of key technological breakthroughs, such as the invention of nuclear weapons or space exploration. In the 1960s, the Soviet-American race for space and nuclear arms established a direct link between the "superpower status" and "science capability" (Fox, 1968, p. 1).

A decade earlier, Karl Deutsch, a renowned American sociologist, detailed what he then called "modern myths" of the way technology

impacts international affairs, which sounds extremely topical today. In particular, he challenged three important propositions of that time which he believed would determine further evolution of the system of international relations. First, he confuted the argument that technology makes governments omnipotent, and that it thus removes "previous limitations on the powers of dictatorship." Second, Deutsch questioned the idea that technological change "shifts power from the many to the few." Finally, he debated whether modern technology, when applied to war, "only favors attack as opposed to defense" (Deutsch, 1959, p. 669).

Deutsch's critical look at the problem produced a valuable input into the field. He warned against five overestimations that states tend to make in their assessment of their adversaries: 1) overestimation of one's own scientific and technological prowess and underestimation of that of others; 2) overestimation of the immediate military significance of single technical innovations, which often makes elites conceive of the possibility of winning "lightning wars with the help of miracle weapons"; 3) overestimation of the power of surprise in nuclear warfare; 4) overestimation of small military elites and of a "limited nuclear war"; 5) overestimation of the capabilities of dictatorship and of highly centralized political power (Deutsch, 1959). All these arguments remain central to the modern-day study of the state behavior in the digital era.

Another American scholar, Charles Weiss, designed a more practically applicable toolkit for the study of the technological impact on international affairs. Weiss identifies six basic patterns by which advances in science and technology have an influence on international relations: 1) as a juggernaut or escaped genie with rapid and wide-ranging ramifications for the international system; 2) as a game-changer and a conveyer of advantage and disadvantage to different actors in the international system; 3) as a source of risks, issues and problems that must be addressed and managed by the international community; 4) as key dimensions or enablers of international macro phenomena; 5) as instruments of foreign policy or sources of technical information for the management of an ongoing international regime; 6) as the subject of projects and institutions whose planning, design, implementation

and management provide grist for the mill of international relations and diplomacy (Weiss, 2015, p. 413).

Taken together, Weiss argues, these patterns set a broad analytical framework that helps distinguish the many roles of science and technology in the international arena and identify areas for further studies. Most importantly, although these patterns are analytically distinct, they are not mutually exclusive. A technological advance may have impacts that fall into more than one pattern. Simultaneously, the impact of a particular technology may display different patterns at different times. For instance, the issues it presents may begin as a new crisis and evolve into an obstinate problem needing adequate management.

As the most dramatic examples of some of the patterns Weiss discusses milestones in the development of means of warfare. From nuclear arms to drones to information technology to social media he shows how new capabilities have "conferred substantial advantage on those who can manage them effectively." He makes a strong case for how they have affected the balance of power between numerous groups on multiple levels: between the civil and the military within a single country, between democratic and authoritarian nation-states, between stronger and weaker powers in war, between buyers and sellers in commerce, between governments and non-state actors, and between hierarchical organizations and networks in a wide variety of contexts. As a result, this led to a counter-reaction from those "whose relative power has been affected by the change in technology, and to an effort to restore the previous relative power or competitive relationship (Weiss, 2013, p. 416).

The present study adopts a similar methodological approach. It is also based on the participant observation method which dwells on the many years of practical work of some of the co-authors in the fields of technology and policy-making. It first outlines key international trends in how technological advances impact politics and policies and then dwells on implications of these trends for nation-states. Furthermore, it provides a detailed assessment of where Russia stands in the digital environment and what it should do to stay relevant in the ongoing transformation of the international system.

GLOBAL TRENDS IN THE DEVELOPMENT OF THE DIGITAL ENVIRONMENT

Swift advances of science and technology have created the prerequisites for reducing socio-economic inequality at national and global levels. At the same time, they have increased the vulnerability of societies 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. Yet they have also facilitated the atomization of states that seek to protect these channels against foreign interference. The continuing blurring of lines between the virtual and the real world and between facts and fakes leads to greater anarchy in international relations.

The uncertainty is 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 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.

The universal character of the digital transformation is attracting the attention of the increasing number of international organizations. 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 (Danilin, 2019, pp. 124-28).

The fight for 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. As the entire world adopts their products, they gain an opportunity to exert major influence on the further development of the chosen technology. This fight for standards enables the countries that supply digital technology

to anchor their customer states to themselves and make them use certain standards and solutions. This makes the latter more dependent on these products and, by extension, on their suppliers as is the case with arms or energy exports.

Global digitization has greatly enhanced the international legal standing of non-state actors. The initially technical Internet Corporation for Assigned Names and Numbers, created, in part, by the U.S. 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." The political neutrality of this and other relevant NGOs are dubious. But even if these doubts are groundless, the very precedent whereby a non-government player regulates a critical national security area is important.

The so-called Big Tech—giant IT companies—are already addressing national and foreign governments as equals and can no longer be ignored as a national security factor. On the one hand, the information they accumulate and their advanced solutions are of enormous interest to the security services. On the other hand, their ability to broadcast various information messages, directly or indirectly, to a giant audience, is becoming a principal political factor.

The termination of then-President Trump's Twitter account, together with those of thousands of his supporters, was a wake-up call for many reasons. On the one hand, this case might result in third countries demanding "digital sovereignty" from American IT giants. On the other hand, it may 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. That states strive to control their information activities and receive access to their data is understandable but leads to the erosion of liberal values—freedom of speech, secrecy of correspondence and privacy—and raises the issue of their applicability in the digital era. In the longer term, this will most likely harden the world's political fragmentation.

The absence of arbitration institutions recognized by all players, the lack of investigation into 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 allows the wrongdoers 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 sometimes even a smartphone.

NATION-STATES IN THE DIGITAL WORLD OF THE FUTURE

The attempts of states to protect themselves against foreign digital interferences have a number of consequences. First, the states seek to limit vulnerabilities of their networks by encouraging import substitution and deep localization. After all, governments have more confidence in national hardware producers or software developers than they do in foreign ones. When national companies are prioritized for the production of their own critical hardware and software, economic specialization is losing its appeal. This leads to the disintegration of international production chains and further erosion of the international division of labor.

In addition, the need to appoint authorized operators and limited competition in the market slow down the development of technology, thus making states choose between progress and security. Like with many other aspects of the global digital economy, this one reveals a discrepancy between information exchange as a global phenomenon and the physical infrastructure that is located on a particular territory and, hence, is under some sovereignty.

A discrepancy in data storage and processing or the transfer of information via Internet channels is even more obvious. 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% of all domains are governed by American players (Verisign, Afilias); more than half of the content delivery networks belong to U.S. companies (Amazon, Akamai, Cloudflare), and all main first-level providers are U.S. residents; ten out of 13 DNS servers are also located in the United States (CISCO, 2020).

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

The first one is their ability to guarantee the viability of their critical information infrastructures under threat of cyberwar and 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.

The second one 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 depersonalized 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.

Today, a state that seeks to be part of the major league of international politics must have an established strategy to guide it through the global digital environment, as well as resources and its own ideas and products in this area. This state or a bloc of states must control a significant share of the global market, operate its own currency zone and currency issuing procedures, 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 defense and critical infrastructure.

Meanwhile, the looming challenge of digital inequality and "digital colonialism" already stems from the dominance of a handful of developed countries in digital technologies. The emergence of global monopolies will ensure their control over the network infrastructure and data flows.

For now, the "digital neo-colonialists" provide favorable terms to their "customer states" so that they can create the infrastructure they need in order to access the digital future. That way, they instantly make them part of their own solutions for payment systems, 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.

At the same time, digital technologies, which underlie the daily life and the information space of each person, are beginning to exert a noticeable influence on the human psyche and decision-making practices. Individuals are not only becoming enslaved by digital platforms operated by global monopolies, but they are actually put in a situation where their entire life is tethered to devices (Andreula and Sprothen, 2019, pp. 9-28). Under the guise of providing convenience, they restrict individual choices in decision-making and manipulate behavior. In this unequal relationship, threatening to exclude others from the social environment, digital monopolies expropriate and uncontrollably exploit personal data and even creative content.

As techno-economic blocs take shape, digital competition becomes a war of platforms and standards (Tse and Esposito, 2017, pp. 39). At the same time, some 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, are likely to 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 AND 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. Its strong engineering and mathematical school—legacy of the Soviet Union—remains a source of high-skilled workers who are a key resource behind digital progress: the national search engine Yandex, its own social media, such as VKontakte and Odnoklassniki, that are more popular in some respects than Facebook and Instagram in Russia as well as in the majority of post-Soviet countries (Brand Analytics, 2020).

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—possess a significant export potential. Launched two years ago, the Digital Economy national program will provide 97% of national households and all social infrastructure facilities (schools, hospitals, and police stations) with high-speed broadband Internet access by 2024. This must drastically improve the environment for businesses, telemedicine and distance learning, and help Russia bridge the digital gap. Russia is already among the top ten countries by the number of Internet users, and the Gosuslugi website with its two 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. It now amounts to about 4-5% of GDP, but it 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 the key to the successful development of next-generation networks.

Yet the challenges that Russia faces in its digital development are tremendous. Some of them are merely 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 at unacceptable levels. (Probably the opposite is true regarding the sanctions impact on this dependence.)

These and other trends in 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 this goal could be achieved depends on an effective phased transition from imported software and hardware systems and on the creation of an effective nationwide command chain from the regulator to the executor.

The government's decision to create registers of domestic software and radio electronic equipment is designed to mitigate these risks. Unregistered companies cannot count on supplying their solutions to

Russian state-controlled corporations and government agencies. These measures have a long-term positive effect on Russia as a sovereign technological power.

Accusing Russia of cyber interference in other states' domestic affairs has been widely used as a pretext for increasing sanctions pressure and has certainly tarnished Russia's international reputation. Moreover, this campaign has had implications for a number of large Russian enterprises and firms that frequently face problems and discrimination on some Western countries' markets. The risk that these accusations will be used by the United States and its allies as an excuse for delivering "retaliation cyber strikes" or even "preventive cyber strikes" against Russia is perhaps much more significant than reputational or even economic implications. Meanwhile, over the past twenty years, Russia has worked towards establishing international norms of responsible behavior in cyberspace at the UN and other international organizations. China follows in the footsteps of the Russian position, which is different from that of the United States and its allies (Gady and Austin, 2010).

In the information space, Russia's vulnerabilities are quite clear due to the dominance of U.S. 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, including by manipulating content and restricting Russian users' access to information and means of communication. Other non-Western countries face similar challenges. It makes sense for Moscow to establish closer dialogue with them on the principles of digital legal regulations (above all, 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.

The low competitiveness of Russian companies and the government compared to global corporations in attracting the best

talent is yet another problem at hand. Brain drain may not occur formally as Russian talents continue to reside in Russia, but it makes their intellectual added value available to foreign companies. Considering 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 do little to influence the technical standards and regulations that support 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 by internationally recognized standards and protocols that ignore Russian interests.

RUSSIA'S LEADERSHIP IN THE DIGITAL ENVIRONMENT: A WAY FORWARD

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. There is a niche for Russia to exploit as a leader of ***"digital non-alignment" movement*** for countries that seek to avoid the tech dictate of "digital neo-colonialists."

One of the biggest challenges for Russia is the implementation of the EAEU digital integration program within the Eurasian Economic Union. Conditions must be created for the member states' government agencies and businesses to exchange important legal 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 that lean towards the EAEU and the states with which the EAEU has or plans to sign free trade agreements—Vietnam, Iran, Egypt, Singapore, and Serbia. Digital integration in this case can and must proceed ahead of physical integration.

Another important instrument could be a special program, possibly implemented jointly with the Eurasian Development Bank, to introduce 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 employing available political mechanisms for this purpose. Making use of the positive potential of Russia's ties with India, Indonesia, Brazil, and other leading economies of the future should be a priority policy track.

A digital dialogue with the EU is another important avenue for cooperation.

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, Russia needs closer coordination with Europe on the use of the radio frequency spectrum, which is currently hindered by the existing contradictions with EU border countries. Russia and the EU will need to coordinate a single standard for next generation networks and 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 harmonized for the convenience of businesses. Moreover, Russia and the EU would like to impose fair taxes on foreign digital giants, primarily American ones. 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.

Collaboration with the EU is important, if only because the Russian and European integration blocs are being squeezed by the two big "data behemoths"—self-sufficient American and Chinese information platforms.

Fourth, just like the Russians, some Europeans are afraid of losing their identity in the global technological environment and ultimately find themselves in a situation where their voice will not count (Dillet, 2019). The EU, despite being one of the most important generators

of data, one of the biggest global economic regions, having a large population, and having high-tech and medium tech industries globally, commands significantly less power in setting global technological trends and exercising technological sovereignty than the U.S. and China (Muniz, 2019). Yet its potential and pursuit of technological sovereignty make it an appealing partner for Russia in a number of important aspects as far as digital sovereignty is concerned.

For now, however, it is the political differences between Moscow and Europe that so far have appeared to be an insurmountable obstacle to broad collaboration, which is an additional motivator for Russia to build its own technology platforms.

Relations with the leading digital powers—the United States and China—are also of critical importance.

Russia should continue to coordinate ***its positions with China*** on international platforms when it comes to Internet governance and data safety. The two countries have similar approaches, although Russia's position is more liberal and does not imply building its own version of the Great Firewall of China. But there are two delicate issues that Moscow should not shy away from discussing with Beijing.

The first one 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 by the EAEU Digital Agenda 2025.

The second one is that the rules of behavior for Chinese companies on the Russian market of highly skilled labor and start-ups should be outlined. Huawei is conducting a large-scale campaign to purchase Russian technology companies and attract Russian professionals into its R&D divisions with lucrative salaries. This is a logical practice for a market economy based on the freedom of choice, but this does not mean that compensation for the national economy should not be negotiated with Chinese partners. In fact, requirements for any foreign digital company working in Russia must include broader cooperation with universities, the localization of both R&D and production, and the creation of joint products rather than the "cannibalization" of start-ups.

Despite the adversarial state of ***relations with the U.S.,*** engaging with Washington in the digital domain is equally important. First, Russia and the U.S. should elaborate on confidence-building measures in cyberspace, negotiate restrictions on the military use of digital technologies, and give a chance to cooperation in the field of Internet governance. Talks on the creation of new verification instruments for new military technologies may also be a venue for cooperation. All these initiatives should not be seen as giving the U.S. a vote of confidence. Rather, when interpreting any move that Washington makes in this sphere as a priori hostile and reacting to it, Moscow should be carefully assessing it in terms of possible outcomes.

Russia must have a coordinated and clearly articulated agenda for working in multilateral associations, such as the International Telecommunication Union (ITU), the Digital G20, and the OECD. Instead of wasting time promoting exclusively "Russian approaches" and waging diplomatic battles, it would be reasonable to admit, at least inwardly, the existence of two groups of "digital truths."

Firstly, the location of DNS servers and Internet mainlines is not one of Russia's strong points. When it comes to formulating the digital agenda, Russia is not the second pole of the system but at best a large regional power.

Secondly, the world is not yet 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 localize data storage. All countries pursue authoritarian policies when it comes to digital regulation. Indeed, some spheres are strictly regulated even in the countries that call themselves "democratic." On the other hand, it would be irrational to completely reject the concept of "multi-stakeholderism" 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.

While admitting that Russia has lost the chance to influence the 5G agenda, Moscow should focus on preparing proposals concerning 7G standards and step up efforts to prevent national isolation when it comes to the allocation of radio frequencies for next-generation communications. Russia's views on 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. That is why Russian specialists must redouble their efforts to create standards and protocols for a forward-looking technology.

The most important technological markets of the future include the market of platforms for sovereign critical infrastructure, specifically in cybersecurity, communications, energy, transport, finance and urban economy management, as well as in biological and food security. In view 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, with billion-dollar contracts signed for decades ahead, is similar to the global arms market. Decisions on technological partnership are taken at the sovereign level based on the "friend or foe" principle, sales contracts are signed for entire systems rather than components, and implementation entails a high level of trust and localized production of some of the technologies as an element of long-term political influence.

This market could become the most promising export sphere for Russia. Russia's recognized unique competencies in the creation of complicated systems make the country one of the leading potential suppliers. The independent hardware and software environment, which is being created in Russia, is another competitive advantage. Theoretically, the ongoing "Cold War" between Washington and Beijing offers Moscow an opportunity to expand into the markets of Greater Eurasia, the Middle East, Latin America, and Africa, which will try to reduce their technological and political dependence on the warring parties.

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.

* * *

Big data as the "new oil" of the digital era needs to have a clear owner and an understandable value for the individual, business, and government. The removal of the social media accounts of then U.S. President Donald Trump and his supporters, as well as the more recent de-platforming of the social app Parler clearly show the ways how powerful tech giants could eliminate economic and political rivals.

The export of technologies and competencies that protect sovereign critical infrastructure to countries wishing to ensure their independence and defense 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 path.

Moscow should consider mechanisms for 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 on the national information environment.

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, and insufficient financial capabilities to work on large and long-term projects.

For Russia, the minimal task is to preserve the sovereignty of decision-making in the main areas of its national security; the maximal task is to create its own competitive technological ecosystem, become the leader of a techno-economic bloc and a key participant in the development of new rules of the game in this sphere.

References

Andreula, N. and Sprothen, V., 2019. *Flow Generation: A Survival Guide for Our Unpredictable Lives.* Smith Lakes: Daimonriver Press.

Berkley, A. and Letzing, J., 2019. Tracing the Global Rise of China's Tech Giants. *World Economic Forum* [online]. Available at: <www.weforum.org/agenda/2019/06/tracing-the-global-rise-of-chinas-tech-giants/> [Accessed 7 June 2019].

Brand Analytics, 2020. Sotsialnye seti v Rossii: tsifry i trendy [Social Media in Russia: Figures and Trends]. *Brand Analytics* [online]. Available at: <vc.ru/social/182436-socialnye-seti-v-rossii-cifry-i-trendy> [Accessed 30 November 2020].

Campos, L., 2020. *Building a Technology Ecosystem: What You Need to Know.* [online]. Available at: <blog.hubspot.com/website/technology-ecosystem> [Accessed 28 March 2021].

CISCO, 2020. Cisco Annual Internet Report (2018–2023) White Paper. *CISCO* [online]. Available at: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html [Accessed 5 October 2020].

Chivot, E. and Jorge-Ricart, R., 2020. The EU's Approach to 5G and the Reshaping of Transatlantic Relations. *European Leadership Network* [online]. Available at: https://www.europeanleadershipnetwork.org/commentary/the-eus-approach-to-5g-and-the-reshaping-of-transatlantic-relations/ [Accessed 20 September 2020].

Danilin, I.V., 2019. Evolutsiya mezhdunarodnogo nauchno-tehnicheskogo sotrudnichestva: globalnye trendy i rossiyskaya politika [The Evolution of International Scientific-Technological Cooperation: Global Trends and Russian Policy]. *Innovatsii*, 12 (254), pp. 124-134.

Danilin, I.V., 2020. Amerikano-kitaiskaya tehnologicheskaya voina: riski i vozmozhnosti dlya KNR i globalnogo tehnologicheskogo sektora [U.S.-China Technological Tag of War: Risks and Opportunities for the PRC and Global Technology Industry]. *Sravnitelnaya politika,*11(4), pp. 160-176.

Deutsch, K., 1959. The Impact of Science and Technology on International Politics. *Quantity and Quality,* 88(4), pp. 669-685.

Dillet, R., 2019. The Year of the French Unicorns. *Extra Crunch*, 27 December, [online]. Available at: https://techcrunch.com/2019/12/27/the-year-of-the-french-unicorns/ [Accessed 30 January 2021].

Fukuyama F., Richman B., and Goel, A., 2021. How to Save Democracy from Technology. *Foreign Affairs,* 100(1). Available at: https://www.foreignaffairs.com/articles/united-states/2020-11-24/fukuyama-how-save-democracy-technology [Accessed 30 January 2021].

Fox, W., 1968. Science, Technology and International Politics. *International Studies Quarterly,* 12(1), pp. 1-15.

Gady, F-S. and Austin, G., 2010. Russia, the United States, and Cyber Diplomacy: Opening the Doors. *East-West Institute* [online]. Available at: https://www.files.ethz.ch/isn/121211/USRussiaCyber_WEB.pdf [Accessed 27 January 2021].

Griffiths, J., 2019. *The Great Firewall of China: How to Build and Control an Alternative Version of the Internet.* London: Zed Books.

Hout, Th. and Pankaj, Gt., 2010. China vs the World: Whose Technology Is It? *Harvard Business Review.* Available at: https://hbr.org/2010/12/china-vs-the-world-whose-technology-is-it [Accessed 18 December 2020].

Iansiti, M. and Richards, G., 2006. Information Technology Ecosystem Health and Performance. *Harvard Business School Working Papers.* Available at: https://hbswk.hbs.edu/item/information-technology-ecosystem-health-and-performance [Accessed 29 March 2021].

Mayer, M. et al., 2014. The Global Politics of Science and Technology: An Introduction. In: Mayer M (et al.), ed., *The Global Politics of Science and Technology - Vol. 1, 1st ed.* Berlin/London: Springer, pp. 1-35.

Muniz, M., 2019. The Coming Technological Cold War. [online]. *Project Syndicate.* Available at: https://www.project-syndicate.org/commentary/us-china-technology-cold-war-by-manuel-muniz-2019-04?barrier=accesspaylog [Accessed 29 March 2021].

Tse, T. and Esposito, M., 2017. *Understanding How the Future Unfolds: Using DRIVE to Harness the Power of Today's Megatrends.* Austin: Lioncrest Publishing.

Weiss, Ch., 2015. How Do Science and Technology Influence International Affairs? *Minerva*, 53(4), pp. 411-430.