Valdai Discussion Club Report

Russia and the Competition of Technological Platforms: the Political Economy of the ICT Market

Andrei Terekhov,
Stanislav Tkachenko

valdaiclub.com
#valdaiclub

May 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 978-5-907318-34-2

9 785907 318342

42 Bolshaya Tatarskaya st., Moscow, 115184, Russia

About the Authors

Andrei Terekhov

D.Phil. (Physics and Mathematics), Professor, Head of the Software Engineering Department at the Mathematics and Mechanics Faculty, St Petersburg State University; President, Lanit-Tercom

Stanislav Tkachenko

D.Phil. (Economics), Professor, Director, M.A. Programme “Diplomacy of Russian Federation and Foreign States” at Saint-Petersburg State University; President, ISA POSTCOMM Section

Contents

The Importance of Studying Technological Platforms

There is no accepted definition for the term “technological platform,” because it has been applied to information and communication technologies (ICT) only recently. The experts, politicians and business people who discuss technological platforms understand what one another mean, by and large. But scientific discussions are impossible without a clear definition. In our opinion, the clearest and least controversial definition is the following: a technological platform is the sum total of technological means used to create devices, processes and technologies.

When the topic is highly specialised, the discussion is focused on issues of professional interest for software experts, such as the meaning of “platform,” what kind of technology is implied, and whether it concerns global/universal phenomena or those endemic to national segments.

The COVID-19 pandemic has highlighted the importance of giant IT platforms, such as Amazon, Apple, Facebook, Google and Twitter. In 2020, their power, measured in terms of the number of users, the price of their shares and brands, as well as their ability to influence global and national political processes, peaked. There is consensus that the Big Tech companies have become a threat to democracy even in the most developed countries, but there is yet no consensus on how to respond to this threat.

This survey of technological platforms, and the political and economic effects of their development, is based on the above definition. It implies a specialised approach to technological platforms, depending on the specific features of this forward-looking sector of research, which directly influence the political and socioeconomic aspects of the life of every individual.

Many people see ICT as ephemeral elements used to develop a virtual world through the integration of processes underway in real life. It takes a great deal to ensure that a computer network serves the interests of the state and private business, households and individuals. For example, it is necessary to create a system of specialised universities and scientific schools; to train top-notch software experts; create programming languages and controller software; lay undersea and ground internet cables; launch communication satellites; and coordinate various technical standards. Only sovereign states and their governance systems are able to create the necessary conditions for this today and even in the remote future. The resources of private business are comparable to those of states, but only governments and parliaments have the legal right to regulate the ICT sphere and the authority to control the use of modern technology even despite their owners' resistance.

It is impossible to create a common global ICT network without political will clearly expressed by the main international actors. We must also consider the top-down structure of the community of sovereign states. Until recently, some countries did not have the right to veto global projects, such as the development of the ICT industry on the basis of common standards and the internet combining all the national segments. The attempts to block access to the internet (North Korea and Turkmenistan) or to create high-tech firewalls (China) were laughed down. But these ideas, which looked technologically unviable and economically irrational only recently, gained momentum at the turn of the 2020s. Things that looked impossible are becoming a reality and even the norm.

In this survey we will look for answers to the following questions:

- Is the much discussed diversity of technological platforms an inevitable alternative to an integral digital world?
- Is the catch-up development strategy applicable in the ICT sector?
- Should sovereign states try to build "closed internet systems" within their national boundaries?
- Can public-private partnership accelerate the development of the national technological platform in Russia?

The final stage of the dissolution of the unipolar world is noted for a multitude of political and economic consequences, including the crisis of the liberal international order. Its most interesting aspect is the role of the US hegemony in the modern global economy. According to the hegemonic stability theory created by the realist school of thought, a liberal economy can only exist in a unipolar world controlled by the leader state (hegemon). The acknowledgement that a new multipolar world is inevitably emerging gives rise to the idea that technological wars and the dangers of technological interdependence are not far off. After all, many besides football fans know that the best defence is a pre-emptive strike.

Aware of this threat, citizens turn to the state for protection and safety. The price of the potential victory of the state over the liberal economy will be very high. Its impact will extend beyond a decrease in the effectiveness of the economic solutions traditionally associated with state intervention in the economy. The public and media aspects of this process are no less important. The fact that news can reach the public immediately thanks to the internet, alongside radio and television, is forcing politicians to make decisions and act quickly, often under stressful conditions and with a lack of time to calmly consider solutions. The authorities can always explain tough security measures by the need to protect national interests, but such an explanation is moot when it comes to economic matters, which are the priority when it comes to analysis of the global ICT development processes.

We regard this as the main problem in relations between the state and businesses in the sphere of technological platforms. Both parties would like to keep the controlling stake allowing them to dominate this segment of the market. But this rivalry is threatening economic stability and complicating the task of ensuring state security. Therefore, the state authorities and high-tech businesses should coordinate a *modus vivendi* and collaborate in the development of technological platforms by national companies, without trying to infringe on the other party's freedom of operation within the framework of their main mission. The mission of the state is to ensure national security and the mission of businesses is to create effective economic activity.

The first sign of the end of the period of unimpeded growth of the ICT sector was a crisis known as the dot-com bubble, which originated in the equity markets in 1995 and burst on March 10, 2000, when the largest ICT market, the US Nasdaq, which rose five-fold between 1995 and 2000, saw an almost 77 percent drop. The dotcom crash did not destroy the ICT sector, but it became the first example of creative destruction. The term was coined by Austrian-born economist Joseph Schumpeter, who describes it as the "process of industrial mutation that continuously revolutionises the economic structure from within, incessantly destroying the old one, incessantly creating a new one."[1] But the scale of the dotcom crash forced the government agencies and monetary authorities to use hands-on management methods to protect the market players when the ICT industry, still at the development stage and hence still prone to external shocks, could be plunged into a deep and long-term crisis. In this new period of the post-industrial information society, such crises are inevitably followed by other and no less tragic global shocks.

In the early 2000s, businesses and politics moved towards rapprochement in the field of ICT. This actually led to the development of the modern ICT industry, where no clear line can be drawn between its two main elements: private enterprise and public interest.

According to our estimates, the period of domination of the economy over politics in ICT ended in 2001-2004, and the development of digital technologies ceased to be the exclusive mission of businesses. Effectiveness and the priority of pubic goods[2] ceased to be the main reasons for building a global ICT infrastructure, giving way to such notions as "information security," "information rivalry," and "cyberweapons."[3] A new political and

[1] Joseph Schumpeter. Capitalism, Socialism and Democracy. Chapter VII: The Process of Creative Destruction. Moscow, 1995, p. 73.

[2] Public goods are commodities or services that are available to all members of society, regardless of whether each person individually pays for them. Whether the ICT infrastructure is a public good is a moot question, but we believe that it complies with some of the criteria of public goods. In particular, the ICT infrastructure can be described as *non-excludable*, *non-rivalrous* and *indivisible*, if these characteristics are ensured through legal regulation and are coordinated at the interstate level.

[3] Before the Russian-US summit held in Moscow on September 1-2, 1998, the Kremlin proposed discussing a draft joint statement on information security. The Russian draft said that in the obtaining situation the ICT sphere had the potential for humankind's development through a global IT revolution, but there was also a growing danger that new technology could be used to undermine international stability. Washington disregarded the proposal to discuss and sign such a statement. Fyodorov A.V. Informatsionnaya bezopasnost v mirovom politicheskom protsesse [Information security in the global political process]. Moscow, MGIMO University, 2006, p. 187.

economic reality has developed, and we have barely started analysing its characteristics. Experts in many fields of science and practice are aware of the effect of the development of technological platforms in the ICT industry on the security of states and societies. But they don't know exactly how this happens. The stage of limited *ad hoc* interstate cooperation, which began some 15 years ago, has been affected by the superpowers' conflicts in cyberspace.

Global Technology Leaders and Catch-Up Development Model

The catch-up development models are based on the researchers' interest in analysing socioeconomic phenomena and processes and the understanding that successive regimes and economic models are creating an environment that hinders or even precludes the development of lasting models. The goal of the catch-up development theory is to identify the political and economic conditions for reducing the gap between an individual less-advanced country and the regional or global leaders.

The catch-up development theory was proposed by German-American economist Friedrich List. He was born and began his professional career in Germany, which was a conglomerate of two dozen sovereign states, List spent many years in the United States, where he embraced the ideas of the first US Secretary of the Treasury Alexander Hamilton. List was a firm opponent of free trade, which, he believed, was hindering the rise of the national economy and prevented the economic development of states with nascent industries. He believed that only targeted state investment could boost industrial development, because weak banks and penniless citizens cannot invest substantial funds into economic development. The main element of List's catch-up development theory was a tough protectionist policy which, he argued, needed to be applied at the earliest possible stage of modernisation. The goal of the catch-up development model was to become fully independent of the import of high-tech products, which determined the level of economic development and ultimately guaranteed the country's military security.

Since its inception, the catch-up development model was promoted by the school of economic nationalism as an opponent of economic liberalism. The methodological problem, which the liberals have not resolved to this day, is the assessment of the role of the state in economic development. Neo-liberals and Libertarians categorically refuse to regard the state (represented by executive and legislative authorities) as the main or even a politically significant actor in the attainment of the catch-up development goals. The refusal of the market-oriented economists to say which state governance agency could set the line for accelerated development and draft even a somewhat reliable and long-term plan for moving towards that goal was proof of the intellectual weakness of their position. Several successful modernisation examples in the 19th and 20th centuries (united Germany, Japan emerging from centuries-long isolation, and the multinational Russian Empire) show that the state plays the key role in this through its political and economic institutions. Only the state can accomplish this mission.

The authorities must maintain dialogue with the business elite, the scientific community and civil society organisations. This dialogue only complements the other activities of the sovereign state, its political leaders and the heads of government, the parliament and the regions. Our analysis of the political economy of the ICT industry showed that the development of globally competitive technological platforms by an individual state is a special case of the catch-up development model.[4]

The term "information and communication technology" was first used in research published in the *Harvard Business Review* in December 1958.[5] US leadership in this sphere remained indisputable and unchallengeable until the end of the 20th century. But the rapid rise of the Chinese and Indian economies and the development of high-tech sectors in Russia created an environment where US domination could be contested. The national technological platforms of the United States, China and Russia are now competing for domination. Moscow shares the main principles of China's cybersecurity policy of regulating the internet.

[4] Tkachenko S. The Political Economy of Russian Information & Communication Technologies // PONARS Eurasia Policy Memo No 533. URL: http://www.ponarseurasia.org/sites/default/files/policy-memos-pdf/Pepm533_Tkachenko_June2018.pdf

[5] Leavitt H. J., Whisler Th. L. Management in the 1980s. // Harvard Business Review, 1958. URL: https://hbr.org/1958/11/management-in-the-1980s

Since the 1980s, when China adopted the catch-up development model, it has become the world's largest economy (by GDP) and the second largest pole of the global political and economic system equal to the United States by the majority of indicators. Cyberspace and the high-tech sector are their battleground for global domination. The rivalry of these two global powers, as well as several other poles of the multipolar world, including India, the EU and Russia, is taking place according to rules that differ from those of the previous century. A conflict is developing in a world of global supply chains and international cooperation regulated by the WTO and several regional agreements. The US-China confrontation could create a situation where the potential economic decoupling[6] of China and the United States could become a reality of two hostile national technological platforms.

Why is the state's excessive interference in ICT development unwelcome and only acceptable as an exception for a challenging period, to be abandoned at the first opportunity?

Anthropologists Allen Johnson and Timothy Earle have applied a seemingly jocular principle of least effort as a motor of evolution and social change. According to this principle, any society resists innovation and refuses to change as long as possible.[7] This notion, which contradicts our views on rational behaviour, is based on the analysis of situations showing that the average elites dislike innovation. Stagnation and conservatism prevail in the country as long as the elites have the necessary resources and can relatively painlessly contain the striving of the larger part of society for change. The creation of a globally competitive technological platform is an innovation challenge which not every elite can accept.

Those who study technological platforms can make use of the much discussed biological principle of excessive diversity. It is now possible to study extremely long processes only in biology, because the history of technology is too short for such analysis. There were numerous crisis situations in the evolution of biological species, when previously useless, ancillary and surplus features turned out to be vital for survival and progress to a new stage

[6] For political economists, decoupling is the gradual decrease in the US-China economic interdependence, which developed between 1980 and 2010. The US-China technological, investment and financial decoupling will inevitably sour bilateral relations and increase the probability of a large-scale conflict between them.

[7] Johnson, Allen W., Earle, Timothy. The Evolution of Human Societies: From Foraging Group to Agrarian State. Moscow, Gaidar Institute Publishers, 2017.

of evelopment. In other words, in a situation where it is impossible to predict the exact nature of the next crisis, the existence of various properties that go beyond the minimum requirements increases the probability of success in dealing with problems that arise. During calm periods, diversity is excessive because its maintenance requires additional reserves. On the other hand, excessive specialisation makes a biological or social system inflexible, which can lead to a crisis or even collapse.

This analogy is also applicable to engineering. IT experts are well aware that a system with absolutely no surplus is totally unreliable, because the break-down of any component will result in system outage. On the other hand, it has been proved that a highly reliable system can be composed from unreliable components, thanks to excessive diversity, of course.

The task of the state is to determine the required level of diversity in the development of a national technological platform, so that Russian industry and the Russian economy as a whole will be ready to deal with the largest possible number of shocks in the non-lineal development of the world. The state represented by the authorities is unable to create such diversity, which can only develop in a free and competitive market environment.

Yet another much discussed and highly controversial principle is the optimal fragmentation principle, according to which excessive competition in a social or biological system is dangerous because it can lead to chaos, whereas insufficient competition is dangerous as well, because it promotes inflexibility and dampens the striving for change. Therefore, one more unconventional task for the state, on which the future of the country and its citizens depends, is to outline an optimal area somewhere between the two extremes. Experts point out that the optimal number of participants in a competition, when rules are coordinated and observed and there are incentives for competition stimulating development, is between three and six. When there are only two competitors, they tend to drift towards frontal confrontation, which can result in the suppression or even elimination of one of the parties involved. When there are more than six competitors, they cannot reliably monitor what the other parties in this "game" are doing, eventually losing focus in the ensuing chaos.[8]

[8] This principle has been formulated by two American scientists, independently of each other: sociologist Randall Collins and biogeographer Jared Diamond. The most famous follower of the principle is the founder of Microsoft Bill Gates, who believes that the use of this principle helps create and effectively manage the most complex systems.

The authors of this report believe that in the long term no government will be able to imitate a competitive environment or plan the development of a national technological platform, taking into account the multitude of internal and external factors that could influence its progress. The market can do much better, while states will have the opportunity to make use of the individual achievements of the national ICT industry to ensure state security.

The projects undertaken by some researchers, notably Kaifeng Yang and James Melitski, have shown that the executive and legislative authorities developing a state ICT policy and infrastructure come across problems that effectively prevent reliable long-term planning.[9] Any government's top priorities, surpassing the task of creating a national technological platform in the early 21st century, are internal/external security; election cycles and the election factor; contradictions between the declared economic and social policy goals, which require constant manoeuvring; the conflict of interests between organisations and individuals involved in the IT sector; resistance to innovation typical for the majority of people; plus legal problems arising during the transition to digital technologies. The situation started to improve relatively recently. The involvement of governments in the countries that were lagging behind in the development of technological platforms only became systematic after the world's largest economies joined the process.

The global economy, where the ICT industry has become the main growth driver, has proved the effectiveness of privatisation. It involves the deregulation of some segments of the national economy and can also create conditions for partnership among business structures, for example, through the establishment of self-regulating organisations or professional associations such as the Information & Computer Technologies Industry Association (APKIT) or the association of software developing companies RUSSOFT.

However, in a situation when political threats outstrip a state's economic possibilities, the authorities have a right to come forward to mitigate the negative effects of external shocks. This is the situation Russia is in now. In light of the economic sanctions orchestrated by Washington

[9] Yang K., Melitski J. Competing and Complementary Values in Information Technology Strategic Planning // Public Performance & Management Review. Vol. 30. No 3. March, 2007. PP. 426-427; Holley L.M., Dufnet D., & Reed, B.J. Got SISP? Strategic Information systems planning in U.S. state governments. Public Performance & Management Review. Vol. 27. No 4. June, 2002. PP. 398-412.

to ndermine and ultimately destroy Russia's economy, the government had to take emergency economic measures to repel this new kind of aggression and to defend the country during an economic war. Support for Russian software companies and other elements of the national ICT ecosystem, plus the transfer of the production of hardware and software components to Russia are an effective response to the hostile actions.

At this difficult time, the government can hardly be required to maintain a competitive economic environment. However, businesses can put forth a no less important demand: the government must ensure a transparent and effective functioning of all institutions of the national economy, including independent courts, it must combat corruption and cleanse the bodies of power of inefficient executives and practitioners.

The Russian ICT Sector and the National Technological Platform

The Russian ICT sector only started developing 30 years ago, after the dissolution of the Soviet Union. Thirty years is not long enough to say that we know everything about the sector, its laws of development and its global influence. But it would be safe to say that the Russian ICT sector does exist. It has not only survived in a rapidly changing and sometimes very aggressive political and economic situation, but it is also becoming the mainstay of the national economy and can take its rightful place in the global economy of the 21st century (table 1).

Russia has always been and will always be a great power influencing global developments and the international lineup of forces, maintaining law and order and preventing the threat of anarchy in international relations. The Russian economy, which is now in a transition period, will eventually become one of the world's top five economies. But it will be impossible to attain this goal without boosting ICT development.

TABLE 1. OVERALL FIGURES FOR THE RUSSIAN SOFTWARE SECTOR (AS OF DECEMBER 31, 2020)

Russian stable software companies	at least 4,000
Companies with export receipts	at least 2,500

Software engineers	persons
Software engineers working in Russia (in all industries (including IT departments)	> 580,000
Software engineers working in the Russian software development industry (overall), including:	> 180,000
- in overseas development centres	> 10,000
- in Russia	≈170,000
Software engineers in service companies (working for foreign clients)	≈90,000 (40,000)
Software engineers in product companies	≈70,000
Software engineers in Russian R&D centres owned by foreign companies	≈8,000

Source: RUSSOFT Association URL: https://russoft.org/russoft-analytics

A study of ICT regulation in the world's top 10 market economies conducted by Kaifeng Yang and James Melitski shows that governments make deliberate strategic choices among two pairs of essentially political goals.[10]

The first, the internal/external orientation presupposes a choice between *internal economic development* and *integration into the global economy*. In fact, this search for internal/external drivers of long-term economic growth began 400 years ago. It often turned out to be a false choice, because you need a strong national industry to be able to integrate into the global economy. Therefore, the stage of internal accumulation should be followed by a period

[10] Yang K., Melitski J. *Competing and Complementary Values in Information Technology Strategic Planning. Observations from Ten States* // Public Performance & Management Review. Vol. 30. No 3. March, 2007. P. 426-427.

of opening up the national economy and subsequent product expansion by the young national industry into external markets.

The second, the effectiveness/efficiency orientation is a choice between *building an effective economy,* where the interests of all stakeholders are taken into account whenever possible and where none of them develops by suppressing the others, and *developing an economic model that brings immediate results*, a model that ignores or has little regard for the strategic consequences of the executive and legislative authorities' current activities.

Theoretically, this choice looks artificial, because an effective economy is a strategic goal for any country and government. But since the time factor is often more important in politics than in the economy, officials, motivated by short-term electoral interests, often take measures that look attractive but are far from the best.

A survey of the OECD countries' macroeconomic policies shows that their governments almost always make the choice in favour of internal development and an economic development model that promises immediate budgetary and operating revenues. The decision-making process is influenced by numerous and not always predictable factors. They include internal political changes, the electoral policy (the need to implement one's ideas during one electoral cycle, disregarding longer-term objectives), and the difficulty of choosing national development priorities within the framework of multiparty ruling coalitions. In this environment, politicians and officials tend to put business interests, including the interests of high-tech businesses, on the back burner.

But in practice, the processes that are crucial for the global political and economic system are developing more positively for the ICT sector. The private business is compensating for the authorities' short-term tactical activities with investment decisions, which initiate long-term trends and are used to implement large-scale projects, disregarding the "government factor" or regarding it as an unavoidable but surmountable obstacle. An analysis of the global ICT industry has confirmed the importance of the above mentioned trends for Russia. The one and only conclusion is the huge importance of public-private partnership as an institutionalised dialogue between the authorities and businesses. They should act as equal and mutually supportive allies in the development of the national high-tech industry.

According to Alexander Galitsky, an international venture investor and a recognised expert on the global ICT sector, "public-private partnerships are considered to be one of the most effective forms of launching innovative processes in the world."[11] The centuries-long history of relations between the state and the market shows that governments are ineffective merchants. It would be wrong to entrust officials with building a national technological platform or with marketing software products created within the framework of this activity. Considering the current level of ICT development, society should set a new goal for the authorities: to develop a market infrastructure, including legislation, law enforcement, education and other components. Private venture capital investors have a two-pronged task: **first of all**, to choose the most promising innovation companies and start-ups with a high survival rate, and **secondly**, to reduce the risk of failure and loss of investment as much as possible. If both parties do this, the state will have the intellectual resources and the financial capability to build a national technological platform while giving the initiative to the national ICT companies.

This is where there is the potential for the interests of the state and businesses to meet. *Businesses* should make economic decisions on the basis of as much information as possible to enable rational targeting. The rate of rationality (awareness) during managerial decision-making will be higher if businesses are assured of the stability of the institutional structure of the economy. *The state* should minimise the risk of businesses making wrong decisions that could lead to financial loss and failure. The priority task of the authorities during the building of a national technological platform should be the following: to provide organisational and consultative assistance to venture financing companies and to ensure that macroeconomic indicators are maintained at the level necessary for creating the most favourable environment for innovative development.

In other words, a deal between the state and businesses during the creation of a national ICT platform could include an exchange of the government's political support at the initial stage of innovative projects for the experience of private businesses in the implementation of high-tech projects, an active involvement of businesses during all stages of project implementation, and readiness to invest major private funds as soon as it becomes clear that the project has survived and holds out good business prospects (table 2).

[11] Galitsky A. Public-Private Partnerships – Fostering Innovations in Russia // Baltic Rim Economies. Issue 2. April 29, 2014. P. 39.

TABLE 2. RATING OF RUSSIAN REGIONS IN TERMS OF SOFTWARE DEVELOPMENT (2020)

Capital cities A	
1 (1)	Moscow
2 (2)	St Petersburg

Moscow and St Petersburg together account for some 50 percent of total software development

Leaders B	
3 (3)	Novosibirsk Region
4 (4)	Nizhny Novgorod Region
5 (5)	Tatarstan

Contenders C	
6 (7)	Rostov Region
7 (6)	Sverdlovsk Region
8 (13)	Samara Region
9 (9)	Voronezh Region
10 (10)	Tomsk Region
11 (12)	Chelyabinsk Region
12 (11)	Perm Territory
13 (14)	Krasnodar Territory
14 (18)	Omsk Region
15 (22)	Saratov Region
16 (8)	Moscow Region

Genesis 1 D	
17 (20)	Udmurt Republic
18 (17)	Tula Region
19 (15)	Ulyanovsk Region
20 (16)	Yaroslavl Region
21 (24)	Kaliningrad Region
22 (31)	Mari El Republic
23 (23)	Krasnoyarsk Territory
24 (28)	Vologda Region
25 (37)	Sakha (Yakutia) Republic
26 (21)	Volgograd Region
27 (27)	Tyumen Region
28 (25)	Irkutsk Region
29 (26)	Penza Region
30 (34)	Ivanovo Region

Genesis 2 E	
1 (30)	Altai Territory
2 (19)	Bashkortostan Republic
3 (32)	Belgorod Region
4 (–)	Bryansk Region
5 (33)	Kaluga Region
6 (38)	Karelia Republic
7 (–)	Kemerovo Region
8 (35)	Primorye Territory
9 (36)	Ryazan Region
10 (29)	Tver Region
11 (–)	Khabarovsk Territory

Source: RUSSOFT Association URL: https://russoft.org/russoft-analytics

One of the biggest problems is that the government, if it acts single-handedly, could make a wrong decision due to a misunderstanding of ICT processes or because of a lack of the information needed for making a rational decision. Margaret Thatcher believed that in many cases the government did not solve problems but only complicated them. Therefore, the main external conditions for the creation of a successful national ICT platform in Russia are as follows: set the right distance between the authorities and businesses, use negotiations as the basis of their relationship, and ensure the crossflow of personnel between them.

The Russian government is implementing innovation support projects primarily on the basis of the experience of the most economically advanced countries of the Global North: the United States and Western Europe. It has adopted laws to incentivise innovation and has created, launched and even reformed development institutions (VEB, Rusnano and the Russian Venture Company), special economic zones (e.g., Alabuga in Tatarstan), business incubators and technology parks. However, Alexander Galitsky believes that reliance on foreign experience has encouraged expectations of quick results, the absence of which makes society and politicians nervous. And second, the adjustment of the legislation and law enforcement practice in the field of innovations is taking place too slowly to meet current requirements, which is opening the door to corruption and the preservation of superfluous procedures/practices in relations between businesses and the authorities.[12]

It has transpired recently that ICT development can have large-scale political consequences such as changes in the structure of state power and an increase in the government agencies' capability to implement their constitutional function of maintaining state power. The expert community has split into two large groups: those who see ICT, including a national technological platform, as an *exogenous factor* capable of influencing (or not influencing, depending on a multitude of factors) the relative power of states in the global system. Their opponents believe that ICT and the national technological platform are the *embodiment of*

[12] Galitsky A. Public-private partnerships – fostering innovations in Russia // Baltic Rim Economies. Issue 2. April 29, 2014. P. 39.

state power and factors that can form/change the political and economic nature of a sovereign state.[13]

In our opinion, the above two views (the neutrality of the ICT versus its political and economic omnipotence) are wrong because they are single-valued. The ICT is definitely not neutral towards state power, and it cannot be disregarded in the ranking of countries. On the other hand, the ICT is a universal tool, which it took humankind centuries to create and which can be used now instead of the weapons and hardware of the past ages.

Political analysts are forcing us to choose between the above two positions. We believe that it would be best to take a position which our foreign colleagues describe as the *middle ground*. The priority issues that must be addressed at discussions on the "power of the internet" as a factor of state power are *cybersecurity*, *international laws regulating the internet* and *network neutrality*. Politicians, the military and the intelligence community are making use of ICT resources to deal with both the traditional and new tasks facing the authorities. But whatever the authorities' attitude to the ICT, including the standards of internet freedom, they have to formulate their position on the above three issues.

It is true that the internet is just a technology and, as such, cannot incorporate such standards and values as democracy, freedom or human rights. Its ability to exert a decisive influence on interstate conflicts can be quite real in some cases and imaginary in others. This is why John Mearsheimer, a recognised authority on the modern theory of international relations, wrote in his book, The Tragedy of Great Power Politics: "… non-material factors sometimes provide one combatant with a decisive advantage over the other… Although material resources alone do not decide the outcome of wars, there is no question that the odds of success are substantially affected by the balance of resources."[14] It is alarming that

[13] The ambivalence of high technology as a factor of state power has been aptly described by former US President Barack Obama: "It's the great irony of our Information Age -- the very technologies that empower us to create and to build also empower those who would disrupt and destroy." President Barack Obama, Remarks by the President on Securing Our Nation's Cyber Infrastructure. Office of the Press Secretary. Washington, D.C., the White House. May 29, 2009. URL: https://obamawhitehouse.archives.gov/realitycheck/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure

[14] Mearsheimer J. The Tragedy of Great Power Politics. New York: W.W.Norton & Company, 2001. P. 58.

the subject of non-material factors of national security is taking too long to emerge on the agenda of the Russian authorities. The parliament and officials are reluctant to involve ICT professionals and experts in their discussions on this subject.

Russia's idea to use BRICS to build an "independent internet" on a special technological platform that would be free from the control of the regulatory bodies of the US or any other global economic leaders looks dangerous. However, this idea was recently discussed at a forum on a new form of internet governance and protection within the framework of individual countries' sovereignty.

On September 26, 2017, the Russian Security Council instructed the Ministry of Digital Development, Communications and Mass Media and the Foreign Ministry to propose a discussion at the BRICS platform on the idea of an independent system of parallel root servers of the Domain Name System (DNS).[15] The system should be independent of US-dominated international structures such as ICANN, IANA[16] and VeriSign[17]. The main goal of that initiative is to ensure that the requests of users from BRICS countries are processed in the event of global internet malfunctions or, even more important, if an attempt is made to block the BRICS users' access to the internet. Security is the main component of the Russian initiative. The Russian Security Council has advanced that initiative because of concerns that the internet could be used by Russia's adversaries, namely the US and NATO members, to launch offensive cyber operations. However, the initiative has not been supported at the international level.

[15] Sovet bezopasnosti poruchil sozdat "nezavisimy internet" dlya stran BRICS [The Security Council orders the creation of an "independent internet" for BRICS countries.] // RBC News Agency, 2017. URL: https://www.rbc.ru/technology_and_media/28/11/2017/5a1c1db99a794783ba546aca

[16] The Internet Assigned Numbers Authority (IANA) is a standards organisation that oversees global IP address allocation and root zone management in the Domain Name System (DNS), registers Multipurpose Internet Mail Extensions (MIME), and other internet Protocol-related symbols. Currently it is a function of Public Technical Identifiers, an affiliate of ICANN.

[17] Verisign is a US-based global leader in the field of domain name registries and internet security. It supports the operation of the most important domains and ensures the cyber protection of websites and companies around the world. Verisign is responsible for the operational validity and stability of .com and .net domains, plus the management and protection of the DNS infrastructure for over 144.3 million domain names. The company's technological platform handles some 135 billion operations a day to ensure reliable and secure operation of the internet around the world.

In our opinion, these concerns are substantiated, but the proposed mechanism for repelling them is excessive. In this particular case, the medicine could be more dangerous than the disease. The Domain Name System (DNS) is a distributed directory service (data storage system) that is crucial for the operation of the internet, because it contains all the domain names and related IP addresses. The DNS is a hierarchical system based on 13 root servers that provide access to information about all top-level domains, including country code top-level ones *(.ru, .it)* and generic TLDs *(.com, .net)*. An absolute majority of root servers are located in the United States, and the remaining ones are in Western Europe and Japan. Several other countries, including Russia, have "mirrors" whose function is to provide on-site service to requests from local users rather than through the DNS server located across the globe. However, these "mirrors" duplicate the information of the root servers and do not contain original information.

Regarding Russia's security, it is worth remembering that the agencies responsible for the operation of DNS root servers include such bodies of US executive authority as the Department of Defence and the National Aeronautics and Space Administration (NASA). The international community cannot influence their activities in any way or expect the US executive authorities' decisions regarding other states to be transparent.

Is the idea of an independent BRICS system of DNS root servers an acceptable method of ensuring national security? Of course, the answer depends on the proposed structure's objective and its implementation. Creating new DNS root servers to gain independence from foreign partners would be futile within the current global internet architecture, because information would still come from one source, the IANA. In other words, the idea of building a BRICS system of root servers independent from international (US) administrators is nothing other than a call for the creation of a parallel internet space as an alternative to the existing network and not connected with it in any way.

This is the essence of the problem. What if Russia is using the threat of a parallel internet to create an effective and competitive national technological platform and, as a result, to have relative advantages in potential talks with the

United States on a favourable international legal framework for the internet? In this case, the real objective of this initiative should be proclaimed as the creation of a new architecture of international security based on the realities of the Fourth Industrial Revolution.

If this is true, we can only wish Russian diplomacy every success. But we would like to add that it will be a tough battle with few chances of success. Like Russia, the United States has never changed its policy under pressure from other states, especially if pressured publicly. Resisting pressure from foreign countries and protecting the internal political system from external influence is the sovereign right of any state, a right which only a small group of really sovereign states/great powers, including the United States and Russia, are using. A decision to terminate the arduous dialogue with the United States and its allies and to resort to ultimatums on cybersecurity and uninterrupted operation of the internet has not been made yet. It should be thoroughly discussed by the expert community. It is very difficult to develop trust-based relations between great powers in the field of cybersecurity, but we do not see any alternative to this. The Cold War left a valuable legacy in the form of the practice of trust-based dialogue on security issues, during which Moscow and Washington have exchanged information and coordinated mechanisms that have helped them avoid a catastrophic conflict. We are convinced that now is the time to launch a dialogue on cybersecurity. Perhaps this is already underway, but the public is unaware of it.

The idea of rallying the BRICS countries to create conditions for *global technological leadership* by 2035, set out in the National Technology Initiative,[18] is questionable. The possibility of using BRICS to create a multipolar world, which has been promoted by Russia until recently, looks unfeasible now.[19] On the other hand, BRICS could be an ideal format for creating technological alliances to boost the development of high-tech

[18] The idea of the National Technology Initiative (NTI) was put forth by Vladimir Putin in his Address to the Federal Assembly delivered on December 4, 2014. The NTI is a long-term interagency programme of public-private partnership aimed at promoting the development of new promising markets on the basis of high-tech solutions, which will determine the evolution of the Russian and global economies in 10-15 years.

[19] Tkachenko S. L., Coyle W. BRICS and a New Model of Hegemonic Stability // Vestnik of St Petersburg University. International Relations, 2020, vol. 13, Issue 3, pp. 294-309.

industries and to protect the five countries' technological sovereignty from the attempts to marginalise it, which are being made by the major Global North companies with support from their governments. The technological standards of the five BRICS countries and the states that could objectively be ranked in this category (Turkey, Argentina and Saudi Arabia) are relatively similar. But their economic structures differ. China is focused on mass production and India specialises in services and ICT, while Russia is the largest raw materials supplier with unique military technologies.[20] These three leaders of the BRICS group must not miss the opportunity to develop relations of cooperation and mutual interdependence in the sphere of technology. Diplomatic efforts to build a multipolar world could provide a political umbrella for such interaction.

Conclusions

First of all, the creation of a successful ICT platform in Russia depends on complex 3D software, which can only be created with a wide range of tools designed by Russian software engineers, including image and text editors, translators from high-level algorithmic languages, debugging solutions and profilers. Modern computers run on operating systems (OS), which perform basic tasks such as process, memory and file management, as well as ensuring security. The tools, OS and the computers where these are used are known as technological platforms. The creation of a national technological platform should begin with building a solid foundation; no daydreaming is acceptable in this sphere.

Second, all of the above systems are obviously vulnerable in this age of information war. The functioning of OS or translators can be suspended or blocked, by chance or deliberately at an external signal, which will be difficult to detect. It will not necessarily be a code-behind, rather it might be a combination of harmless codes or even the absence of signals during particular intervals. Unfortunately, there have been a great many examples of

[20] Dau-Schmidt K. G. *Labour Law 2.0; the Impact of New Information Technology on the Employment Relationship and the Relevance of the NLRA* // Emory Law Journal. Vol. 64. P. 1597.

this in the past decades. Therefore, the desire to create one's own, fully national OS and translators is not a challenge to the rational logic of an effective market, but a forced step prompted by national security considerations. The current task is not for Russia or the allied EAEU and CSTO countries to create an "independent internet," which will be an extremely expensive undertaking with no certainty about its effectiveness. But the Russian federal authorities can set the task of creating a narrow segment that would not be connected to the global internet even via a single cable. This segment could be used for state/military purposes and would be extremely useful in the event of emergencies. Russian scientists are able to carry out this task quickly on the basis of their experience and available national production capacities.

Third, numerous attempts have already been made in Russia to create national technological platforms, but no breakthrough solutions have been found. The opponents of the idea of a national technological platform usually argue that it took the West decades and hundreds of billions of dollars to create such platforms, and so Russia should not even attempt to do the same. But it is not necessary to accomplish all tasks at once. Instead, the authorities and the ICT business should pinpoint the areas where Russia's security interests could be affected most painfully before attaining the goals they formulate within the framework of public-private partnerships. As the Chinese saying goes, a journey of a thousand miles begins with a single step.

Fourth, it is necessary for state corporations, as the country's largest software customers, to allow the marketing of the much-needed domestically-created software.

Fifth, there must be public recognition of the achievements of the system programmers, who will be working on the creation of a national platform. Many Russian-made software applications are being used in the country, but very few people know who created them and how. This form of publicity is extremely important for young software engineers.

In other words, we need a national technological platform to protect the country's information security and ensure our technological independence from the Western suppliers of platforms. But there is no simple solution, because in the next few years the national leadership will be focused on ensuring state security and on solving the problems that will arise in the process of catch-up development without destroying the national market economy.

We would like to point out in conclusion that there is no uniquely Russian ICT that is not connected to global technologies. A national ICT development strategy must ensure the protection of state security and use certain restrictions to protect Russian market players during the development stage. At the same time, we must improve the mechanisms for promoting Russian companies on international markets and enhancing their global competitiveness.

The Russian executive authorities have the right, which is sealed in legislation and supported by national traditions, to prevent any security threats in the sphere of ICT. If the concerned agencies expose any cyber threats, the Russian ICT sector must have the resources for defence and response. However, these actions should only serve as the backdrop to the stage where the Russian ICT sector is operating and progressing. This stage is the global competitive market.

ValdaiClub

ValdaiClub

ValdaiClub

valdai@valdaiclub.com

Viribus unitis

Council on Foreign and Defense Policy

RIAC

Russian International
Affairs Council

MGIMO
UNIVERSITY

HIGHER SCHOOL OF ECONOMICS

NATIONAL RESEARCH
UNIVERSITY