NATIONAL RESEARCH UNIVERSITY
HIGHER SCHOOL OF ECONOMICS

Alexander A. Chulok, Dmitry V. Suslov,
Evgeny Ia. Moiseichev

A CONTEMPORARY FRAMEWORK FOR NATIONAL SECURITY RELATED TECHNOLOGICAL RISKS MINIMISATION

BASIC RESEARCH PROGRAM

WORKING PAPERS

SERIES: SCIENCE, TECHNOLOGY AND INNOVATION

WP BRP 34/STI/2015

This Working Paper is an output of a research project implemented within NRU HSE's Annual Thematic Plan for Basic and Applied Research. Any opinions or claims contained in this Working Paper do not necessarily reflect the views of HSE.

Alexander A. Chulok,[1)] Dmitry V. Suslov,[2)] Evgeny IA. Moiseichev[3)]

A CONTEMPORARY FRAMEWORK FOR NATIONAL SECURITY RELATED TECHNOLOGICAL RISKS MINIMISATION[4]

Last several decades have shown a steady broadening of national security issues' spectrum along with an increase in the strictness of international competition driven by advances in high technologies and other factors. National security agenda is nowadays comprised not only of defense issues per se, but also includes economic, social, cultural and other aspects. All this is strongly influenced by the technological trends and the very possession of critical technologies has become a pressing national security issue. Thus, we are witnessing a gradual convergence of national security and technological agendas. Advocating a proactive approach to tackling national security risks of a technological nature, the authors make an attempt to outline the contemporary innovative methodology of assessing, harnessing and counteracting such risks. Their key recommendation lies in the appeal for joining the forces of theorists and practitioners in the field of both national security and science, technology and innovation (STI) policy to overcome the corresponding challenges.

Keywords: national security, economic development, balance of power, science, technology and innovation policy, Russia.

JEL codes: O3

[1] National Research University Higher School of Economics. Institute for Statistical Studies and Economics of Knowledge. International Research and Educational Foresight Centre. Deputy Director. E-mail: achulok@hse.ru

[2] National Research University Higher School of Economics. School of World Economy and International Affairs. Center for Comprehensive European and International Studies. DeputyDirector. E-mail: dsuslov@hse.ru

[3] National Research University Higher School of Economics. Institute for Statistical Studies and Economics of Knowledge. OECD – HSE Partnership Centre. Analyst. E-mail: emoiseichev@hse.ru

[4] This Working Paper is an output of a research project implemented within NRU HSE's Annual Thematic Plan for Basic and Applied Research in 2014. Any opinions or claims contained in this Working Paper do not necessarily reflect the views of HSE.

Introduction

Analysing technologies' effect on national and international security, particular attention is frequently paid to their impact on the country's military and economic strength – and as a result, on the changing balance of power in the world [1–4].

Fully mature technologies are primarily subjected to such analysis for they are the ones that mostly affect the society and its overall security in the short run. But as soon as a technology becomes mature, it becomes less susceptible to change and to external impact – which increases political controversy between those who wish to maintain the status quo, and proponents of more active application of innovations [5].

Such controversy is put on the agenda in the form of challenges and threats associated with the use of the already existing technologies, and potential challenges and threats posed by the emerging technologies. A *sectio aurea* principle should be kept in mind therefore and overestimating potential threats from emerging technologies for instance may negatively affect country's innovation potential [6]. Evidence shows, that this can occasionally result in countries' lagging behind in developing new technologies and their innovative breakthroughs only happen when external challenges outweigh the internal controversy [7].

Correctly assessing emerging challenges posed by advanced technologies requires moving on from analysing their revolutionary effect on the society to studying more complex, not always linear, and chronologically extended technology development trajectories, and their impact on the society [8]. At the same time analysis of challenges and threats which result from inadequate application of existing, and unsatisfactory development of innovative breakthrough technologies, must be integrated into the overall framework for economic, political, and social development.

During the previous decades a trend towards relocation of production facilities to emerging Asian nations became apparent. According to the International Monetary Fund (IMF), the contribution of Asian economies (except Japan) into the global economy in 2014 will amount to 29,6% [9]. It should be noted that in 1820 Asia (except Japan) generated 56,2% of the global GDP [10]. The accelerating industrial revolution in the Western Europe became a key factor of the Asian economies' declining role. In the middle of the 20th century their share declined to 15,5% [10].

Asia started to reclaim its positions in the 1970s, when productivity growth in developed economies began to slow down. If in 1891-1972 (the period of accelerated development of the second

industrial wave's technologies, such as electric energy, communications, chemistry, etc.) labour productivity in the USA grew by 2,36% a year, in 1972-2013 the relevant figure was only 1,39% [11]. Automated production technologies developed in the 1940s – 1950s didn't have a significant effect on productivity growth during the second half of the 20th century, due to their immaturity [12]. In 1987 Robert Solow, Nobel prize winner for developing economic growth theory, noted that "you can find evidence of computer era anywhere but in productivity statistics" [13].

As early as in the 1960s, American companies started to relocate labour-intensive production to Asian countries, in the subsequent decades followed by more complex production processes such as plate manufacturing and certain R&D operations [14]. But proximity to production processes promotes emergence of new ideas to further develop these processes and products [15]. E.g. in 2009 American production companies' R&D expenditures amounted to 70% of all American R&D costs [16]. Innovations followed the production facilities. If in the 1990s Asia's share in global R&D expenditures (except Japan) was 13,2%, according to the Economist Intelligence Unit's forecast, in 2016 it will reach 33,8% [17].

Relocating production abroad allows to quickly achieve tactical objectives. E.g. companies who've already experienced revenue reduction problems were more willing to move offshore [18]. Still, in the longer term offshoring is not always the most efficient solution: (1) saving on cheap labour has its limits; (2) increased distances between production and R&D facilities negatively affect intellectual property, while (3) the middle class emerging in the developing countries creates new markets [18]. Now companies wish to quickly enter new markets, make personalised products, and quickly react to changing demand on local markets.

These days companies have new requirements to products and their distribution techniques. In the 1960s – 1970s, against the background of the first wave of emerging information technologies (IT), companies automated specific processes of their value creation chains; with the progress of the internet they've merged these processes into integrated systems, and now IT are becoming integral components of products [19]. Traditional product components – hardware and software – are now supplemented with connectivity. Connectivity allows to exchange information between the product and its manufacturer, user, and other systems.

The need to process data quickly forces companies to organise their production and management process in a different way. The "lean production system" is becoming increasingly popular, whose roots lie in Toyota's production system; it allows to increase labour and capital productiv-

ity [20]. Software products reduce complexity of organisation processes and open opportunities for integrating people and robots into production. Closer integration between production of equipment and software allows to reduce complexity of the physical world, and deal with emerging problems "with atoms or bits" [21]. Productivity is increased by optimising product teams' work "bottom-up"[22].

Another source of competitiveness is more efficient use of natural resources. Their production costs are growing, and localisation of production processes coupled with increasing environment pollution are accelerating this trend even further [23]. Companies must reconsider their approaches to optimising their use of natural resources.

Thus three areas connected with technological development were identified (see Attachment A), which will significantly affect national security: (1) development and application of advanced production and organisation technologies; (2) technologies for efficient utilisation of resources; and (3) development of human capital.

For each area, top 10 technologies were selected, to be validated though situational analysis – which will allow to formulate specific political recommendations to minimise threats to Russia's national security connected with insufficiently developed advanced technological structures, including possible "asymmetrical responses".

Technological gap and Russia's national security

The National Security Strategy for the Russian Federation until 2020[24] defines national security as "a state of affairs when individuals, the society, and the country are protected from internal and external threats, which allows to provide constitutional rights, liberties, decent quality and level of life, ensure sovereignty, territorial integrity and sustainable development for the Russian Federation, defence and security of the country". This secure state primarily depends on the country's and society's ability to adapt to external (and partially to internal) challenges, and make use of opportunities these environments provide to protect vital interests of individuals, the society, and the country mentioned in the above definition – i.e. rights and liberties, decent quality and level of life, sovereignty, territorial integrity and sustainable development for Russia, its defence and security.

Thus its ability to adapt to changing external environment and to the challenges and opportunities it creates that ultimately defines any country's national security, including Russia. Of utmost importance here is timely monitoring, analysis, and forecasting of challenges' and opportunities' nature and direction (which rapidly change, especially in recent times), and the country's ability to shape policies oriented towards the current and future – as opposed to the past – challenges. To successfully prepare for the last war guarantees losing the next one. If the government policy is targeting challenges of yesterday, which by now have disappeared or due to various reasons became irrelevant, that at the very least would result in wasting increasingly scarce financial and human resources, and make the country less secure against the current and future threats.

At the same time the nature of challenges is directly connected with development of technologies. Firstly, technological progress creates new tools, formats, and platforms for international competition; note that as S&T progress accelerates, the areas of more intense competition also change more rapidly, and countries frequently turn out to be unprepared for that. Technological development (evolutionary and abrupt alike) is the main driver of external environment's changes – adapting to which, and transforming which according to the country's interests, are the main goals of national security policy.

Therefore having various technological gaps with other nations dooms the country to lose in relevant competitive areas, and hinders its adaptation to the changing environment – thus making it insecure to new risks and threats. Particularly dramatic consequences arise if the country "oversleeps" not just emergence of a specific new competitive area, but a new round of S&T revolution, emergence of a new technology structure. An example is the collapse of the USSR which relatively successfully competed with the West in the arms race, but had hopelessly lagged behind in cybernetics and ICT.

Secondly, technological development in itself increases countries' "muscle" potential, being the main driver of changing the balance of forces in the world; thus it creates risks to countries whose international positions deteriorate as a result of this process. Radical changes in the global balance of forces frequently result from emergence of certain "breakthrough" technologies, which for a certain period of time remain available only to a single country, or to a limited group of nations. Examples include emergence in the 15th century of long-term meat storage technology which made possible long sea voyages; emergence of steam ships in the 19th century; emergence of nuclear weapons in the middle of the 20th century, and high-precision conventional weapons in the late 20th century; shale oil and gas production technologies in the early 21st centu-

ry; etc. Despite frequent protestations to the contrary, the "zero sum game" law still applies to international relations, and relative strengthening of some countries (due to technological progress) leads to relative weakening of others.

At the same time the interconnection between technologies and national security risks is non-linear, and frequently controversial. New technologies may both strengthen and weaken countries – including the ones where such technologies have been developed. There are numerous examples when new technologies change people's behavioural models, extend their opportunities and skills, and increase the requirements people make to the government - which is not always able to meet them (not by a long shot). This results in a crisis of confidence in the government and in the so-called "loyalty deficit", occasionally leading to a political crisis. The country's (and its institutions') ability to adapt plays a crucial role here – the ability to change quickly enough and produce the social benefits the society begins to require as a result of the technological progress.

Thirdly, there's a group of technologies which themselves significantly affect specific segments of national security. These are the technologies heads of the RF national security agencies should pay the most attention to. Particular risks to national security emerge if the country starts lagging behind in developing these technologies. Such gaps sharply reduce its potential in the areas which will define its international positions, and increase the country's vulnerability to external environment. Meanwhile the competition get new opportunities to weaken the country even further.

Relevant examples again are plentiful. The USSR's lagging behind in ICT and cybernetics – which were among the highest-growth sectors of the global economy in the 1980s and 1990s – determined the overall crisis and then the downfall of the centrally planned economy, the socialist economies' increasing gap with the West, and as a consequence, the collapse of the country. Many energy exporting countries' (including Russia) lagging behind in high-technology energy generation (such as development of slate, shale, and hard-to-reach fields, "green" energy, etc.) simultaneously creates risks of reduced production of Russian energy resources, and shrinking of markets for Russian energy exports, with increased competition in the global energy sector. This in turn poses a challenge to stability of Russian energy exports, and potentially can lead to a significant reduction of the country's revenues. The gap between Russia and other countries in agriculture increases its dependency on imports of more competitive agricultural products – thus undermining the nation's food security and generally making it more vulnerable to external chal-

lenges. An example of such dependency is the situation which has emerged on the domestic Russian food market, and in Russia's relations with Eurasian integration partners after Moscow limited imports of various agricultural products from Western countries.

Accordingly, the following seems to be quite important to achieving national security: a) identifying technologies and technology groups most relevant to national security (in this case Russia's); b) out of them, identifying areas where Russia lags behind the leaders; c) identifying related risks and threats; and d) identifying steps to be taken to overcome the risks (see Annex 1).

The changing nature of security

The nature of challenges and threats to Russia's security was lately undergoing through fundamental transformation – which in turn was a result of radical transformation of international competition. Firstly, the competition – between everybody with everybody else – is becoming significantly tougher. It's not just competition between "old" Western and "new" non-Western centres of gravity, but also between the great powers – members of the same group. The sharp aggravation of relations between Russia and the West in 2014, which have already deteriorated into a systemic confrontation (especially with the USA) makes this competition particularly severe, and raises the sides' stakes (especially for Russia).

Secondly, and most importantly, the spheres where competition becomes particularly tough and crucial for the international situation and security, are also changing. From the military sphere competition now flows into the economic, humanitarian, and information spheres.

The military sphere and the need to maintain the defence potential of course remain important. Military power is still the main factor which ultimately ensures countries' survival. However, due to such factors as nuclear weapons (which minimise the probability of war between the great powers), and political awakening of people (which reduces the ability to control other countries and peoples through use of military force, or achieve sustainable political results using it), military power ceased to be the factor which primarily determines countries' position on the international arena, their political influence, and stability against external challenges.

The rate and the quality of economic growth, the ability to present an attractive image and lead in information rivalry, countries' stability in the most survival-wise important areas (such as food, energy), and the quality of human capital are increasingly becoming the determining factors of that kind. Therefore they predominantly define countries' security, and gaps in this areas

create – and will continue to create in the foreseeable future – the biggest threats and challenges to Russia's security. That's where the toughest competition is taking place.

A vivid illustration of the role economic growth and its quality play in achieving security is the major shift in the balance of forces which took place in the early 21st century: the rise of non-Western centres of power and the relative weakening of the West – ultimately of economic, not military nature. The USA's lead in the military area – far ahead of all other centres of military force – became the biggest at the end of George Bush Jr.'s presidency – and that was also the period when overall, the country was at its weakest since the end of the "cold war". It was no chance that the Obama administration and the most influential American experts alike saw recovery of dynamic economic growth as the key to restoring the USA's international positions and strengthening its security. Richard Haass, president of the Council on Foreign Relations, speaking about the main threats to the USA's national security, didn't mention Russia, China, or Iran, nor international terrorism and proliferation of weapons of mass destruction – but America's foreign debt and budget deficit. Obama's National Security Strategy 2010 was largely devoted to internal issues – economic improvement, correcting economic misbalances, and, most importantly, improving the quality of American education and health care systems as the key factors affecting the quality of human capital. The document clearly stresses the idea that reviving American innovation, inventiveness, and dynamism would make the biggest contribution to achieving the USA's security and leadership in the 21st century – as opposed to military expenditures, wars, or military presence.

At the same time the USA and the West still dominate in the information and media sphere. Their ability to create and present an attractive image is one of the main factors of their international influence in the world, which is now much more polycentric than it used to be. This potential allows the USA and the West to set the global political agenda, to establish rules and the mood in the media favourable for them, artificially increasing the potential of certain players (including themselves) while presenting others weaker than they are, and to pursue their political and economic interests through information campaigns and warfare – by setting appropriate agendas for the world's mass media. An example of the latter is the political crisis and the coup d'état in Ukraine in 2014, which was largely caused by targeted media campaign to support "Euromaidan" and discredit and blackmail the then Ukrainian authorities.

Another example of countries' vulnerability to media campaigns and to narratives thrust upon people by international mass media – and of how that vulnerability may turn out to be fatal to

national security – are the events of the "Arab spring". The regimes in Tunisia, Egypt, Yemen, Libya, and Syria were simply not able to counter the information warfare which has mobilised their populations for mass protest and riots. Note that mass protests have recently become an almost universal phenomenon, common to developing countries (and among those, both the weak ones, and the new emerging centres of power) and developed nations alike.

A good illustration of the toughest competition's shifting from the military to the economic, information, and humanitarian areas is the pressure the West is currently applying to Russia because of the Ukrainian crisis, and the nature of the unilateral sanctions imposed against it. These are not of military nature. The actual scale of measures the USA and NATO have taken in response to the RF's actions towards Ukraine, was minuscule. The main blow was dealt in the economic and information spheres. The economic and financial sanctions imposed by the West against Russia in 2014, as well as other (even more painful) steps, such as accelerated reduction of oil prices, are such that they cannot force Russia to change its foreign policy in the short term, but they're quite efficient in weakening the RF in the medium and long term – pushing it out of the global competition and in an even longer term, creating in Russia preconditions for a profound internal political crisis, and even breakdown of the country.

At the same time the recent events showed that Russia remains most vulnerable in the economic and financial areas. It has already suffered significant economic losses (and there's more to come), and has almost immediately lost the information war with the West – having allowed it to create in the global media space an image of an "unhinged" revisionist imperial power – a kind of a big rogue country. The Ukrainian crisis clearly demonstrated that the main threats to Russia's security are concentrated not in the military area – far from it, but in the economic and information spheres.

An important factor of any country's national security in today's world is the relatively new information security element of cybersecurity – protection of information and data, securing automated production and technological processes' management and control systems. Cyber-attacks and cyber warfare – when foreign states or other players obtain unauthorised access to databases, information, and control systems, for the purposes of stealing or getting control of them - are becoming increasingly important threats to security of most countries in the world, especially industrially developed ones which possess advanced infrastructures and powerful, technologically advanced armed forces, including Russia. Such actions may result in a technological disaster, use of various kinds of weapons including

nuclear ones, in a collapse or paralysis of certain sectors of the economy or industries, malfunctioning of crucial infrastructures or production facilities.

Taking into account individuals', societies', and states' high vulnerability to such cyberattacks, and the fact that these attacks (performed by countries, unofficial players, and individuals) are becoming increasingly common in international relations, putting in place a security system against them becomes one of the highest priorities of the national security policy. And there's an obvious connection between this area and technology, first of all ICT.

But ultimately, the most important factor which ensures national security in the new competitive international environment is the quality of human capital. High-quality human capital allows to: a) create "breakthrough" technologies capable of taking over and extending markets, to find new sources of growth and thus ensure competitiveness; b) promote diversification of the economy by discovering new grounds for growth and development, thus providing economic stability (which is particularly relevant in the sanctions situation); c) make the society less vulnerable to effects of radical destructive ideas and factors (political and religious radicalism, populism, etc.); d) ensure overall adaptability of the society, economy, and public institutions to changing external environment. In today's world, development and stability of civil society (which is yet another direct function of human capital) are much more important to national security than the government's ability to control societal processes.

Components of Russia' national security

According to the changes in the nature of security threats described above, five areas can be identified which most significantly affect Russia's security, the situation in which in turn is defined by Russia's technological development or lack thereof.

Rate and quality of Russia's economic growth

This area includes the following components:

- Economic growth rate. Today, leadership and influence in the world, countries' ability to present an attractive growth model directly depend on their economic growth

rate. High growth rate also enables countries to accumulate financial reserves, solve socio-economic problems, implement important infrastructural projects.

- Quality of economic growth. No less important are becoming the factors determining the economic growth. If high growth rate is achieved by extensive exploitation of resources (be it natural or labour ones), despite the short-term attractiveness, in a longer term such growth model cannot support sustainable economic growth – and therefore, economic security. A much stronger effect provides growth achieved by increasing productivity, by application of innovations, creation of new sectors of the economy and new markets, production of innovative products capable of conquering and holding the markets, and by being a leader in developing new technological structures. This is the model which mostly depends on technological development.
- Diversification of the economy. An economy which has a number of sectors and thus doesn't depend on the situation in any particular one, is much more sustainable. Economic diversification is also closely connected with technological progress.
- Availability of all relevant production inputs (natural, human, and financial resources, developed R&D system, access to external markets and a high-capacity domestic market, transport infrastructure).

Thus the rate and quality of economic growth directly depend on development and application of advanced production and organisation technologies, on Russia's leading or, on the contrary, lagging behind the world leaders in developing technologies which are now, and will continue to be in the short to medium term, the most important ones for achieving high quantitative and qualitative parameters of economic growth.

Energy security

According to the Russian Energy Strategy Until 2030 approved on 13 November, 2009,[25] energy security is defined as "a state of affairs when the country, its citizens, the society, the state, and the economy are protected from threats to reliable fuel and energy supply". The document also describes the main energy security parameters: sufficient supply of resources, economic availability of resources, environmental and technological admissibility of their exploitation. Each of these parameters is directly relevant to technological development, and to Russia's lagging behind the world leaders in certain technological areas important for the parameters.

It would make sense to add to these parameters retaining the existing and entering new markets for Russian fuel and energy products; adopting such a management regime for energy markets which would best reflect Russian interests; and energy efficiency. Adding these seems to be important considering the role the fuel and energy sector is playing in the Russian economy and in the structure of the federal budget revenues. Losing some of the energy export markets, or accepting an unfavourable model of Russia's energy relations with partners, would create major risks for the country's economic stability and development. In turn, energy efficiency directly affects survival, sustainability, and competitiveness of the fuel and energy sector, especially in the medium to long term; ability to increase supply of energy resources through their more efficient production and usage; and increase exports through more efficient use of energy inside the country. According to the strategy, the unrealised potential for energy saving through organisational and technological measures amounts up to 40% of the total internal Russian energy consumption.

Ability to implement these parameters also directly depends on the Russian fuel and energy sector's technological development. The latter affects such factors as ability to maintain production volume when old mineral deposits are exhausted; efficient exploitation of mineral reserves; competitiveness of Russian energy products given the overall increase of competition on the global energy markets; reliability of supply by the Russian fuel and energy companies; Russia's ability to build relevant infrastructure; energy efficiency; etc.

The Russian Energy Strategy highlights the following main problems with the country's energy security: high wear rate of the fuel and energy sector's capital assets (in electric power industry and gas industry it's almost 60%, in the oil refinery industry – 80%); low investments in development of the fuel and energy industries (during the last five years the investments in this sector amounted to about 60% of the level indicated in the Russian Energy Strategy Until 2020); overdependence of the Russian economy and energy industry on natural gas, whose share in the internal consumption of energy resources is about 53%; *the fuel and energy sector's production capacity doesn't match the global S&T level, including environmental standards*; insufficient development of energy infrastructure in the Eastern Siberia and Far East. Note that the document stresses the gap between the Russian fuel and energy sector and the global S&T development level as one of the biggest challenges and problems.

Food security

By its very nature, availability of food is a key national security factor. Chronic shortage of food in the USSR in the 1970s – 1980s played the primary role in the crisis of the socialist development model, losing the competition with the capitalist world, the union's demise and collapse. The population took the USSR breakdown quite lightly not because it was against the idea of the union state within the 1991 borders, but because it (the breakdown) was perceived as a natural "by-product" of moving on to market economy – which people expected to be able to "fill the shelves in shops".

The Russian Federation's Food Security Doctrine of 30 January, 2010[26] defines food security as "a state of affairs in the country and in the economy when the Russian Federation's food independence is assured; physical and economic availability of food products matching the requirements of the Russian Federation laws on technical regulation is guaranteed to each citizen, in the amounts no less than reasonably required for active and healthy lifestyle". The document clearly states that food security is one of the most important national security aspects, a major element of the country's demographic and social policy, and a factor of maintaining national sovereignty.

The Doctrine indicates that to ensure its food security, Russia must maintain the following threshold shares for domestically produced agricultural, fishery, and food products in the total turnover on the relevant domestic markets: grain at least 95%; sugar at least 80%; vegetable oil at least 80%; meat and meat products (in meat equivalents) at least 85%; milk and dairy products (in milk equivalents) at least 90%; fishery products at least 80%; potatoes at least 95%; white salt at least 85%.

Food security directly depends on technological development. The Doctrine clearly states that one group of risks to Russia's food security is "technological risks caused by lagging behind developed countries in terms of technological level of the Russian production capacity; different requirements to food safety, and to a system for monitoring and controlling compliance with them".

Information security

The current understanding of information security includes two major aspects. The first is ability to set the media agenda, to present images and dominate in global media, to successfully wage information warfare and counter information campaigns by the opposition. The second is cybersecurity: ability to protect information and data (ranging from individuals' personal bank cards to

national-level information constituting state secrets), and security of automated production and technological processes' management and control systems at crucial infrastructures.

Both these components are becoming extremely relevant and important for national security as a whole. The information sphere is becoming a major area of countries' competition with each other; information campaigns and warfare are turning into efficient tools for internal destabilisation and even destruction of countries (like in the case of Syria), and weakening them internationally (the media campaign against Russia which began even before the coup d'état in Ukraine). And cyber-attacks today are a much more reliable way to bleed and disarm countries than "classic" military action.

According to the Russian Information Security Doctrine approved on 9 September, 2000, information security is broadly defined as "the state of affairs when the country's national interests in the information sphere, which are determined by the sum of balanced interests of individuals, the society, and the state, are protected"[27]. The interests of the state in this sphere are defined as "creating conditions for harmonious development of Russian information infrastructure, for exercising human and civil constitutional rights and liberties concerning accessing and using information, in order to ensure stability of Russia's constitutional system, sovereignty, and territorial integrity, its political, economic, and social stability, unconditionally ensure the rule of law, law and order, and promote mutually beneficial international cooperation".

According to this document, Russian national interests in the information security area include, among other things, "information support of the Russian Federation's national policy, to provide to Russian and international public reliable information about the Russian Federation's national policy"; "development of advanced information technologies and the Russian information industry, including informatisation and telecommunication technologies"; and "protection of information resources from unauthorised access; ensuring security of information and telecommunication systems". Accordingly, among threats to Russia's information security were mentioned disabling Russian state media's activities aimed at informing Russian and international public about Russian policy and its assessment of international events; their low efficiency due to various reasons; and unauthorised access to Russian information and communication networks and databases. Securing these interests and minimising these threats directly involves technologies, primarily ICT.

Various cybersecurity-related issues are described in more detail in the document entitled "The main aspects of the national policy on security of automated production and technological processes' management and control systems for crucial infrastructures in the Russian Federation", approved on 3 February, 2012. Security of crucial information infrastructures is defined as "the overall state of crucial information infrastructure components, under which subjecting it to computer attacks does not result in heavy adverse consequences". And practically any way to increase this security has a completely technological nature; these include development of Russian ICTs, and minimising (as far as possible) dependence on foreign technologies.

Quality of human capital

Quality of human capital is a fundamental factor which ultimately determines countries' national security and their place in the international system. It includes several components, the most important being the population's health (which in turn is determined by environmental risks and level of the healthcare system), and education, which affects not just the population's skill level but their morals, civil conscience, legal culture, and other factors vitally important to the country's security and wealth. Thus factors which most profoundly affect the quality of human capital as the foundation of national security, include: the development level and the efficiency of the healthcare system; ability to minimise environmental risks to people's health; and the education level.

All three these areas are directly connected with technological progress, and each of them poses risks in case the RF lags behind the world leaders in developing critical technologies. Thus quality of healthcare is directly affected by technological development, and a gap in this sphere not only creates additional risks to the population's health – due to inability to treat certain diseases – but also increases the country's dependency on importing foreign-made drugs and equipment, which, if the international situation deteriorates and such supplies are terminated, may put to risk stable operation of the healthcare system. The country's ability to minimise environmental risks to people's health also is directly determined by the level of technologies required to minimise harmful emissions, manage industrial waste, make production and transport systems more environmentally friendly.

Finally, the level and quality of education are also closely interconnected with technological development. On one hand, certain technologies, first of all ICT, create new opportunities for education (distant learning, increased access to literature, etc.). On the other hand, the country's abil-

ity to develop, apply, or accept certain advanced or cutting-edge technologies, including the ones which significantly affect its national security, depend on the level of education, and the country's potential to train professionals capable of maintaining these technologies. In case there's no such abilities and potential, acquiring technologies may weaken rather than strengthen the security of such a country – because it will become completely dependent on other nations for technologies critical to its security.

Conclusions and discussion

Currently, all countries, including Russia, are faced with brand new global challenges related to fundamental changes in production processes, transformation of socio-economic processes, cultural values and the redistribution of profit in global value chains. New technologies and their corresponding markets are constantly emerging and evolving. At the same time the scope of national security issues has broadened significantly and now also includes economic, social, cultural, moral, ethical, ecological and other issues. These drive the adaptation of states to the changing global economic and political environment.

On one hand, technologies determine to an extent the emergence of new centers of power. On the other hand, technology issues begin to penetrate the political agenda as states try to tackle national security risks related to technological development. Thus, science, technology and innovation (STI) and national security agenda converge progressively which was discovered in the study.

In order to find practical and theoretically grounded solutions to technology related risks to national security one would need to bring together both policy-makers and scholars in the corresponding areas.

In reality it is not about treating technologies as a hostile element and trying to get rid of their impact. Quite the opposite, they need being tamed, harnessed and exploited to the limit for the maximal benefit of the society. Ultimately, it is in the scope of policy-makers' and scholars' responsibility to work together in order to solve challenges arising in the sphere of national security using STI policy instruments.

REFERENCES

1. Caverley, J. D. United States Hegemony and the New Economics of Defense. *Secur. Stud.* **16,** 598–614 (2007).
2. Gholz, E. Globalization, Systems Integration, and the Future of Great Power War. *Secur. Stud.* **16,** 615–636 (2007).
3. Gilpin, R. *War and Change in World Politics*. (Cambridge University Press, 1981). at <http://ebooks.cambridge.org/ref/id/CBO9780511664267>
4. Goldman, E. O. & Andres, R. B. Systemic effects of military innovation and diffusion. *Secur. Stud.* **8,** 79–125 (1999).
5. Diebold, W. & Keohane, R. O. After Hegemony: Cooperation and Discord in the World Political Economy. *Foreign Aff.* **63,** 414 (1984).
6. Teske, P. & Thierer, A. D. The Delicate Balance: Federalism, Interstate Commerce, and Economic Freedom in the Technological Age. *CrossRef Listing Deleted DOIs* **29,** 163 (1999).
7. Taylor, M. Z. Toward an International Relations Theory of National Innovation Rates. *Secur. Stud.* **21,** 113–152 (2012).
8. Vogel, K. M. Intelligent assessment: Putting emerging biotechnology threats in context. *Bull. At. Sci.* **69,** 43–52 (2013).
9. International Monetary Fund. *World Economic Outlook, April 2014: Recovery Strengthens, Remains Uneven*. (International Monetary Fund, 2014). at <http://elibrary.imf.org/view/IMF081/20955-9781475571615/20955-9781475571615/20955-9781475571615.xml>
10. Cooper, R. N. & Maddison, A. The World Economy: A Millennial Perspective. *Foreign Aff.* **80,** 176 (2001).

11. Gordon, R. *The Demise of U.S. Economic Growth: Restatement, Rebuttal, and Reflections*. (National Bureau of Economic Research, 2014). at <http://www.nber.org/papers/w19895.pdf>
12. Carr, N. G. *The glass cage: automation and us*. (W.W. Norton & Company, 2014).
13. Baily, M. N. What Has Happened to Productivity Growth? *Science* **234,** 443–451 (1986).
14. United States. & Government Accountability Office. *Offshoring : U.S. semiconductor and software industries increasingly produce in China and India : report to congressional committees*. (GAO, 2006).
15. Manyika, J. & McKinsey Global Institute. Manufacturing the future the next era of global growth and innovation. (2012). at <http://www.mckinsey.com/insights/mgi/research/productivity_competitiveness_and_growth/the_future_of_manufacturing (date of access: 28.11.2014)>
16. President's Council of Advisors on Science and Technology (U.S.), United States. & Executive Office of the President. Report to the President on capturing domestic competitive advantage in advanced manufacturing. (2012).
17. Wiid, R., du Preez, R. & Wallström, Å. Coming of age: A 21 year analysis of Marketing Intelligence Planning from 1990 to 2010. *Mark. Intell. Plan.* **30,** 4–17 (2012).
18. Van Ours, J. Editorial Report 2013. *Econ.* **162,** 105–106 (2014).
19. Porter, M. E. & Heppelmann, J. E. STRATEGY & COMPETITION How Smart, Connected Products Are Transforming Competition Smart, connected products are changing how value is created for customers, how companies compete, and the boundaries of competition itself. *Harv. Bus. Rev.* **92,** 64 (2014).
20. Duncan E. & Ritter R. Next frontiers for lean. *McKinsey Q McKinsey Q.* (2014).
21. Building a Solid World. O'Reilly Radar. at <http://radar.oreilly.com/2014/03/building-a-solid-world.html (date of access: 28.11.2014)>

22. Here’s How Spotify Scales Up And Stays Agile: It Runs ‘Squads’ Like Lean Startups | Techcrunch. at <http://techcrunch.com/2012/11/17/heres-how-spotify-scales-up-and-stays-agile-it-runs-squads-like-lean-startups/ (date of access: 28.11.2014)>
23. Stefan Heck and Matt Rogers describe what companies must do when growth in capital and labor productivity is no longer enough. at <http://www.project-syndicate.org/commentary/stefan-heck-and-matt-rogers-describe-what-companies-must-do-when-growth-in-capital-and-labor-productivity-is-no-longer-enough (date of access: 28.11.2014)>
24. Стратегия национальной безопасности Российской Федерации до 2020 года. at <http://www.scrf.gov.ru/documents/99.html (date of access: 23.01.15)>
25. Энергетическая стратегия России на период до 2030 года, страница 4 \ Консультант Плюс. at <http://www.consultant.ru/document/cons_doc_LAW_94054/?frame=4 (date of access: 17.11.2014)>
26. Доктрина продовольственной безопасности Российской Федерации. at <http://www.scrf.gov.ru/documents/15/108.html (date of access: 02.03.2015)>
27. Доктрина информационной безопасности Российской Федерации. at <http://www.scrf.gov.ru/documents/6/5.html (date of access: 02.03.2015)>

ANNEX 1

Situational Analysis Methodology

The first step in the situational analysis, after the object of study has been determined (identifying and describing the main components of national security), is to identify their connections with technologies. This implies identifying technologies which most significantly affect each of the five national security areas.

In the course of the situational analysis the Scenario Group developed a special methodology for identifying technology groups which have major effect on the rate and quality of economic growth, energy security, food security, information security, and quality of human capital, based on the nested matrices technique. Using this methodology, the Scenario Group obtained the following results.

The second step is to identify, out of the selected and presented above technologies, those in respect of which Russia is, firstly, already lagging behind the world leaders, and secondly, those where it potentially may begin to lag behind during the period until 2030.

Participants of the situational analysis are asked to comment on this selection and if necessary, indicate which technologies should be crossed out and which, on the contrary, added to it.

Participants of the situational analysis are also asked to identify technologies out of those most significantly affecting the five presented national security components, in respect of which Russia may lag behind the leaders during the period until 2030. Please name potential gap areas for each national security area, in the following format.:

- for economic development, Russia's potential lagging behind in developing the following technologies seems to be particularly important:_____
- for energy security, Russia's potential lagging behind in developing the following technologies seems to be particularly important: _____
- etc.

The third stage of the situational analysis is to identify and describe the risks which Russia's lagging behind (both actual and potential) in developing certain technologies creates to the relevant national security segment (each of the five). The risks should be identified for each national security area individually, i.e. their consideration should start from "national security segments", not from "technologies".

Since Russia's lagging behind in various technologies probably poses similar risks, participants of the situational analysis are not asked to identify risks for each specific technology.

Rather, it would make sense to identify the risks typical to Russia's lagging behind in respect of the technology groups relevant for particular national security areas (risks for economic development posed by Russia's lagging behind in ICT; risks for education posed by Russia's lagging behind in ICT; etc.).

Identifying the risks posed by Russia's lagging behind in developing specific technologies would be useful if such risks were different from the ones typical for the respective technology group, and potentially could significantly damage Russia's national security.

Risks should be identified and analysed in the following format (Tab. 1):

Tab. 1 - Questionnaire for expert panel (situation analysis)

Questionnaire for expert panel (situation analysis)
1. Risks for Russia's economic development posed by technology gap in:
Technology group 1: definition, description, and analysis of the risk
Technology group 2: definition, description, and analysis of the risk
Technology group 3: definition, description, and analysis of the risk
2. Risks for Russia's energy security posed by technology gap in:
Technology group 1: definition, description, and analysis of the risk
Technology group 2: definition, description, and analysis of the risk
3. Risks for Russia's food security posed by technology gap in:
Technology group 1: definition, description, and analysis of the risk
Technology group 2: definition, description, and analysis of the risk
4. Risks for Russia's information security posed by technology gap in:
Technology group 1: definition, description, and analysis of the risk
Technology group 2: definition, description, and analysis of the risk
5. Risks for Russia's healthcare system posed by technology gap in:
Technology group 1: definition, description, and analysis of the risk
Technology group 2: definition, description, and analysis of the risk
6. Risks for Russia's ability to minimise negative effect of environment degradation on people's health posed by technology gap in:
Technology group 1: definition, description, and analysis of the risk
Technology group 2: definition, description, and analysis of the risk
7. Risks for Russian education posed by technology gap in:
Technology group 1: definition, description, and analysis of the risk
Technology group 2: definition, description, and analysis of the risk

The fourth stage of the situational analysis is to prepare recommendations on minimising and (ideally) overcoming the risks in relevant national security segments posed by the technological gaps identified at the previous stage, and on using opportunities available to Russia in various national security areas. The experts are asked to answer the following questions:

- Which technologies must be developed first of all to minimise the risks (including those where Russia is already lagging behind, and where it potentially can lag behind during the period until 2030)?

- Which technological opportunities are available to Russia to improve the relevant national security segment?
- Which technologies or technology groups Russia must develop (or which technology gaps it must overcome) independently, on its own?
- Which technologies or technology groups should be acquired abroad (through purchasing or commercial espionage)?
- Which risks should be overcome not by developing/acquiring technologies and/or closing the technology gap, but asymmetrically? Exactly what this asymmetrical response should be?

As at the previous stages, the recommendations should be developed for each specific national security area individually.

The last stage of the situational analysis is to identify the effect of the Western countries' (USA, EU) unilateral sanctions on Russia's lagging behind in technologies which are particularly important for its national security.

As at the previous stages, the analysis will be conducted for each national security area individually.

Specifically, the situational analysis participants will be asked to answer the following questions:

- How the unilateral sanctions already imposed against Russia by Western countries can possibly affect technological gaps in relevant national security areas?
- What new sanctions against Russia can be expected if the objective is to maximise Russia's technological gap with the advanced countries in relevant national security areas?
- What are the ways to minimise damage from the sanctions (both the current and potential ones) concerning Russia's technological gap with advanced countries?

Alexander A. Chulok

National Research University Higher School of Economics. Institute for Statistical Studies and Economics of Knowledge. International Research and Educational Foresight Centre. Deputy Director;

E-mail: achulok@hse.ru

Dmitry V. Suslov

National Research University Higher School of Economics. School of World Economy and International Affairs. Center for Comprehensive European and International Studies. DeputyDirector;

E-mail: dsuslov@hse.ru

Evgeny IA. Moiseichev

National Research University Higher School of Economics. Institute for Statistical Studies and Economics of Knowledge. OECD – HSE Partnership Centre. Analyst.

E-mail: emoiseichev@hse.ru