DOI: 10.53477/2668-6511-22-01

SCIENTIFIC SECURITY AND THE BACKBONE OF THE FUTURE ROMANIAN ARMED FORCES

Iulian CHIFU, Ph.D.,
Associate Professor, "Carol I[st]" National Defence University, Bucharest, Romania.
E-mail: keafuyul@gmail.com

Abstract: *Scientific security enters the forefront of the debates related to the evolution of security and military in the future. In that respect, the backbone of the Romanian Armed Forces should move more to fields of scientific research and technological achievements with direct applications and, maybe, a proper scientific and strategic tool at the disposal of the Chief of Defense. The most important fields of research should come from strategic studies, prospective studies, new technologies and their impact, applied military and security sociology, as well as Informational Warfare and impact studies.*

Keywords*: scientific security; strategic studies; prospective studies; informational warfare; impact studies.*

1. Scientific Security: how to securitise science?

Scientific security as a field of interest for securitisation is floating around for some time. But this has never come as a natural concept, since the idea of securitising any piece of a field where creativity and inventively are the leading characteristics seems impossible. But, on another point, huge steps have been made in opening the way for technological security, and that's a step forward. Moreover, the fact of protecting copyrights, licenses, brevets, research has already been a concern, even though this is far from the real meaning of scientific security which aims, according to our concept, to deal with the evolution of research, of theorisation, protecting them and inducing rules and norms according to common interests, shifting realities and perceptions and framing new markets as well as new environments for the new adapted World Order.

In that respect, we will refer here to the technological security, already a concept well developed and used, and which already enshrines more than technology, adding also research in fundamental fields, strategy and strategic thinking, prospective studies, horizon scanning and future studies, as well as important concerns in the sociological security field as in the impact studies as well as consequence management studies. We will also add the inputs that gave the scientific security new impetus coming from the recent QUAD[1] summit and the ways to approach China for a soft containment, as well as the transfer of technologies and instruments to deal with Beijing in the AUKUS[2] framework.

For us, the main fields of interest in scientific security would be: strategic studies/strategies and strategic thinking; prospective studies/horizon scanning/future studies; new technologies and their impact on the human being, society, politics, international relations and global security; impact studies and consequence management for the decisions so that they

[1] A.N.: The Qadrilateral Security Dialogue in the Indo Pacific, a format between the US, India, Japan and Australia founded in 2007 at Japan's proposal, reestablished in November, 2017.
[2] A.N.: A trilateral security pact between Australia, the United Kingdom and the United States, announced on 15 September 2021 for the Indo-Pacific region.

could not lead to man-made crisis; applied military and security sociology, the knowledge of the real society we are living in and attractiveness for the military service as well as the synergy of sociological cultures of people involved in the defense field – order, rigour, strict vertical of power versus hazard, random behaviour and special needs and millieux for computer, IT and cyber researchers and drone operators as well as creativity bubbles, music and silence for researchers in fundamental studies; Informational Warfare and study of perception and channelling perception formation towards a desired goal.

A very important reference in this direction is the US National Technology Security, a US Government supported initiative by a grant from the U.S. Air Force Office of Commercial and Economic Analysis (OCEA). The project, run by the Center for New American Security (CNAS), is aiming at far more that technological security, and, according to the objectives of the project, it will develop the intellectual framework for a national technology strategy for a successful, long-term American innovation and technological leadership through policies for accelerating American innovation, mitigating risk to US advantages, and contending with the technology strategies of competitors (The Center for a New American Security - CNAS. 2021).

The project is a clear reflection of the scientific security since it will also explore options for boosting innovation through research and development funding, developing and maintaining human capital (STEM education, high-skilled immigration, upskilling), technical standard-setting, and supplying public goods (data, computing resources). This project explores the institutional and bureaucratic processes through which the government should develop and execute an effective national approach. This project analyses measures such as increased supply chain diversity and security, improved visa screening, targeted export controls and investment screening, and increased and more effective counterespionage investigations (U.S. National Technology Strategy).

2. Technological security as a part of Scientific security

In order to launch the debate about technological security as part and parcel of the scientific security, we've analysed the main strategic documents of the US, NATO, EU, UK, as well as the Report on World Economic Forum from 2021. We've done so looking at the American strategic documents (President Joseph R. Biden Jr. 2021; Annual Threat Assessment of the US Intelligence Community 2021; America's Place in the World 2021; A Foreign Policy for the American People 2021; Global Trends 2040. A more contested World 2021) (Biden National Security Strategy hasn't appear yet); NATO strategic documents and assessments (The Secretary General Annual Report 2020; NATO 2030: United for a New Era 2020; NATO 2030: new technologies, new conflicts, new partnerships 2021); EU strategic documents (Fontelles 2021; The geopolitical implications of the Covid-19 pandemic 2020) – of the High Representative for Foreign Policy, another one from the Foreign Affairs Committee – AFET – of the European Parliament; two British strategic documents – along them the integrated Strategy till 2030, the one supporting the idea of a scientific security per se, since it grants UK the status of Technological and Scientific Superpower until 2030 (Cabinet Office 2021); and finally, the Report of the World Economic Forum (World Economic Forum 2021), The Global Risks Report 2021.

Those documents introduce different concepts and nuances of interpretation, a direct proof that the field involving technological security, not talking about scientific security, is still on the making. The concepts presented in those documents are: scientific power, emerging and disruptive technology, technological supremacy, technological advantage, technological and scientific leadership, technological superiority or development, all could be found in these documents. Moreover, the self-assumed status of scientific and technological superpower by

the Great Britain document is of first importance; it is also about the side effects of technology as it is about the strategic advantage (coming from the technological development); about both technological and scientific power and rapid technological change that transforms science and technology in a modality to measure the power.

In spite of different concepts and nuances in addressing this sphere of understandings of the thematic linked to technological security, there is a convergence of the approaches based on several pillars (Chifu 2021 - 1, 13 - 23):

– science and technology become multipliers and referentials for power, at a global level;

– there is a real competition on research and access to technology, that could lead also to wars and limits of the development widening of the differences on economic growth and development and even creating possibilities for niche developments in the emerging economies that could resettle global hierarchies;

– technology is an advantage and creates opportunities, but could also be a subject of vulnerability for an actor and source of threats for the mankind;

– technology polarises and creates alliances for technological exchange as well as constraints, containment, limitations for the access to technologies or for the alternative options for the sources of technology;

– the space that usually is referred as technology implied in the area and could also be found in technological security, as in science and scientific security, refers also to IT, artificial intelligence, cyber, nano-technologies, biotechnologies, big data, quantum computers, space technology;

– we do not have in hand or in the international law norms and ethical limitations for the exponential development of new technologies, which could turn out to be-disruptive or even destructive technologies;

– chassing new technologies could mean, in the case of an autocracy, the race towards a kind of supreme weapon, used to dominate the World;

– we do have enemies already identified, not only technological or scientific competitors, since those actors or countries aim at dominating the World, absolute control, or channelling and constraining our normal way of thinking. China and Russia are considered here, each with its own merits, nuances and major differences between the two actors concerning the degree of identified danger each of them are representing for us.

As we have seen before, technological security is just a slice of the scientific security. In the other part are situated the rights and values of the ethics of research, but also securing money for the research, genuine discovery and respecting the copyrights and primacy in discovery in the scientific research. It is also about fair competition and correct attribution of merits in the research, but also the very pragmatic ways to get to targeted results in the scientific research, combined with the legitimacy and opening in accepting the side effects of a discovery and the impact study, as well as the consequences of such a leap into knowledge or the effects of the excessive use of a technology or discovery without accepting its limits and by-products that need to be also addressed and presented in full transparency.

The ethics of using scientific research are a completely different and difficult subject since, in some cases, the technology is used in a different direction then a virtuous constructive one: limiting human rights, controlling the ways of thinking or the behaviour of individuals all over the world, not only on a nations' own citizens; as on another point, there are ways to control, limit or monopolise the ingredients or needed parts, if not the knowledge, instruments of research and means to build critical technologies, or it is possible to completely ban the access to specific technologies for some states. As we could see, the complexity of scientific security is far broader.

3. QUAD and AUKUS as frameworks for technological transfers and sources of scientific security

QUAD recent first in person summit, held at the White House, with the chiefs of state and governments of the four member countries – US, Japan, India, Australia – has brought a new impetuous for scientific security, with different uses. Created with the purpose to contain China, a type of soft containment, as we put it (Chifu 2021 - 2), the institutionalisation of the agreement and deepening of the links came with an impetus for practical cooperation that includes also technological transfers or common efforts for: ending Covid-19 pandemic (the first official global document where this formulation appears, as well as the final deadline, 2022), including research in this field with security impact; rising the production and access safe and effective vaccines; promoting high standards infrastructure; fighting climate crisis; partnership on emerging technologies, space and cyberspace (The White House 2021 - 1). All include pieces of scientific security and in the subtext is referring to China, China's behavior and Chinese responsibility.

At the same page are the references to build a global pandemic radar and fight future pandemics, even though the document does not mention any responsibility of China for the Covid-19, or an appeal for a correct and in depth investigation of the first moments of emergence of a pandemic. High standards, transparency in constructions, high standards and Build Back Better World (B3W) – as an alternative programme to One Belt One Road project is also about scientific security, technological security and compete China at a different level including a different approach to quality as a difference from cheap and low quality infrastructure attributed to China. It comes also with a green component of the infrastructure build by the QUAD and assistance to third countries in the region. Green ports and green corridors in the Indo-Pacific region is also a challenge to China's dominance in the region, with an added value. As it is the case with the clean energy, controlling emissions, decarbonisation and how to reach this through innovation, adaptation, resilience and preparedness in front of civil emergencies created by extreme weather.

Last but not least, in the field of scientific security, there's a new innovation about finding, agreeing and using common standards and norms between QUAD states and their partners. This comes also from new discoveries in the technological field through scientific research in a technological ecosystem open, accessible and safe in order to create competitive standards, diversify 5G sources and providers, creating correct chains of suppliers and technology and developing horizon scanning – needed studies for anticipation and preparedness. As is the case with emerging and disruptive technologies that need to be subject to control and respect for the democratic values and human rights, another standard that forfeits Chinese competition.

A declaration of principles of the QUAD on standards to design, develop, govern and use technologies is another important tool for the soft containment of China using just diplomatic approaches and technical and scientific achievements (Chifu 2021 - 2). A new form of technological and scientific security comes exactly from the standards imposed and observed globally in several domains. Advanced telecommunications, artificial intelligence, chain of providers safe for semiconductors and monitoring of the evolutions in biotechnologies are also pieces that could be assumed under the framework of scientific security.

As interesting as the QUAD final document, related to technological and scientific security, is the approach to military assistance and technological transfer from the US and UK to Australia, via the AUKUS agreement. Sitting in the framework of the China soft containment, the assistance for Australia and the global fight of democracies against autocracies as the QUAD, the AUKUS prove to give birth to numerous miss-understandings with France and the EU (Chifu 2021 – 3). But it also represents a huge transfer of technology and an important instrument of scientific security in support for Australia, but also holding an

important significance for South China Sea region and Taiwan. As it announces support for the small island states from the Pacific, all being subject to different types of pressure from China (The White House 2021 - 2).

This agreement noted the coordination of signatories in cyber area, in advanced technologies for the defense, first and foremost in nuclear propulsion for submarines – the first transfer of sensitive technologies in the last 50 years and plus. But it involves also other capabilities and submarine activities, instruments against modern security submarine challenges including first hand key technologies of primary importance for the effectiveness of the military activities of the future: artificial intelligence, disruptive technologies from the cyber sphere, and high precision capabilities with long range (The White House 2021 - 2), all with an important content of scientific research and accomplishments, another component of the proposed concept of scientific security.

4. Scientific security and research in Russia: EW and autonomous and robotic systems for modern warfare

The concerns are not at all trivial since, on the other side, the investments and achievements are important in the technological and scientific fields. We will only discuss here about some achievements of Russia, since the scientific literature confirms this approach to scientific security that Russian Army holds. And we will look at two directions, electronic warfare and unmanned robots. The lessons learned are coming from the last Zapad 2021 exercises and presentation of the new achievements, but also the integration of those technical and scientific projects in the warfare landscape.

Electronic Warfare (EW; in Russian, *radioelektronnaya borba*, or REB) has involved forming specialist EW structures, including at the brigade level, and populating all branches and arms of military service with EW-trained personnel and equipment. It targets capabilities to disrupt, jam and interfere with potential enemy command-and-control (C2) systems, communications, radars, or weapons (Petrenko 2021). EW assets entering service over the past four years, are dominated by Divnomorye-U offering EW protection from radar reconnaissance across an area of several hundred kilometers by generating an "umbrella" of EW interference. The EW complex detects and then analyses the target signal and type, alongside its power and direction of radiation, using artificial intelligence (AI) for suppression plan and selection of the most effective jamming methods (McDermott 2021).

According to military specialists (Vitaly 2021), The Divnomorye-U is designed to emit high-powered radiation that neutralizes enemy radar, regardless of type. It is reportedly capable of jamming both ground-based radars and radars of aircraft such as E-8 JSTAR, E-3 AWACS, E-2 Hawkeye, as well as radar equipment aboard helicopters and unmanned aerial vehicles (UAV) (Nikiforov 2021) EW capabilities were made public in late 2017 by then–deputy defense minister Yury Borisov. This related in particular to the Palantin, Rtut-BM and the Tirada-2S systems proving a level of knowledge implying scientific security that could influence any future NATO-Russian conflict (McDermott 2021).

At the same time, Zapad military exercises have proven another capability, the Russian unmanned robots. Russia has employed unmanned ground vehicles in combat formations for the first time, a significant step in the country's quest to develop an effective all-robot military unit, experts say. Two remote-controlled vehicles have been presented, according to Russia's Defense Ministry statement (Wellman 2021): The Uran-9, a tracked vehicle equipped with a 30 mm autocannon, a machine gun, anti-tank missiles and a flamethrower and the smaller Nerekhta unmanned ground vehicle, firing at targets with a mounted machine gun and a grenade launcher. Both were used for fire support and reconnaissance work, performing tasks that would be dangerous for troops, such as delivering ammunition and equipment in combat, seeking to

obtain greater lethality and survivability. Other machines were being used for mine clearing and urban warfare.

5. Lessons learned for the Romanian Armed Forces

The Romanian Armed Forces should consider those evolutions in technological and scientific security and try first to create an understanding on the field. Theoretical approach and a full presentation of the content of both concepts, especially scientific security, should be of first importance. Then, an update of existing instruments and an assessment of what the Romanian military needs, in terms of technology, research, strategies and capabilities should come up, in a different scientific transdisciplinary program.

Coping with the difficulties of building up such capabilities and preparing the institutional framework would be next, including the consequence management of this development and problems with integrating different cultures in the military framework. And here, too, the MoD should allocate at least 2% of its budget to scientific research of this kind.

It is clear that the Chief of Defense and appropriated bodies should consider to develop a proper scientific and strategic tool at their disposal, to be integrated in the existing institutional framework and chain of command, but allowing resources to reach this project and launching the proper interface to engage, attract and hire human capabilities, experts and needed minds, in a transdisciplinary effort, in order to achieve such an important objective.

BIBLIOGRAPHY:

BIDEN Joseph, R. Jr. (President). 2021. Interim National Security Strategic Guidance, March 2021. URL: https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf

BLINKEN Antony J. 2021. America's Place in the World. 4 February. URL: https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/02/04/remarks-by-president-biden-on-americas-place-in-the-world/

BORRELL, FONTELLES, Joseph. 2021. European Foreign Policy in Times of Covid 19, Luxembourg: Publications Office of the European Union, 2021, ISBN 978-92-9238-927-7. URL: https://www.euneighbours.eu/sites/default/files/publications/2021-03/european_foreign_policy_in_times_of_covid19.pdf

Cabinet Office. 2021. Global Britain in a Competitive Age. The Integrated Review of Security, Defence, Development and Foreign Policy. URL: https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy

CHIFU, Iulian. 2021 - 1 Securitate tehnologică. Un nou domeniu de strictă actualitate a securității viitorului, Revista Infosfera, nr 2/2021: 13-23, ISSN 2065-3395.

CHIFU, Iulian. 2021 - 2. Îndiguirea soft a Chinei: de la Război Rece la schimbarea piețelor, standarde și comportamente alternative. Adevărul, 27 September 2021. URL: https://adevarul.ro/international/asia/Indiguirea-soft-chinei-razboi-rece-schimbarea-pietelor-standarde-comportamente-alternative-1_6151555a5163ec4271af690b/index.html

CHIFU, Iulian. 2021 - 3. Pentru un contract ratat cu submarine, Franța împinge UE spre confruntare transatlantică, Adevărul, 20 septembrie 2021. URL: https://adevarul.ro/international/europa/pentru-contract-ratat-submarine-franta-impinge-ue-confruntare-transatlantica-1_614813845163ec42716ddb20/index.html

EU. 2020. The geopolitical implications of the Covid-19 pandemic. URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/603511/EXPO_STU (2020)603511_EN.pdf

McDERMOTT, Roger. 2021. Russia's Military Boosts Electromagnetic Spectrum Capability, Eurasia Daily Monitor. Jamestown Foundation. Volume 18. issue 144. 22 September 2021. URL: https://jamestown.org/program/russias-military-boosts-electromagnetic-spectrum-capability/

National Intelligence Council. 2021. Global Trends 2040 - A more contested World. URL: https://www.dni.gov/files/ODNI/documents/assessments/GlobalTrends_2040.pdf

NATO. 2020. NATO 2030: United for a New Era. 25 November. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf

NATO. 2021. February. NATO 2030: new technologies, new conflicts, new partnerships. URL: https://www.ndc.nato.int/news/news.php?icode=1527

NIKIFOROV, Sergey. 2021. The three most important technologies of the Russian Armed Forces in recent years are named. Politexpert.ru. 4 June 2020. URL: https://politexpert.net/199331-nazvany-tri-samye-vazhnye-tekhnologii-vs-rossii-poslednikh-let

Office of the Director of National Intelligence. 2021. April. Annual Threat Assessment of the US Intelligence Community. URL: https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf

PETRENKO Olga. 2021. "Sobering signals": the US is looking for ways to combat Russian electronic warfare systems, 25 January 2021. URL: https://discover24.ru/2021/01/otrezvlyayuschie-signaly-ssha-ischet-sposoby-borby-s-rossiyskimi-kompleksami-reb

PHILLIP, Walter, Wellman. 2021. Zapad military drills showcase Russian unmanned robots' battlefield breakthrough, Stars and Stripes, September 15, 2021. URL: https://www.stripes.com/theaters/europe/2021-09-15/russia-robots-war-games-zapad-ugv-2897317.html

The Center for a New American Security - CNAS. 2021. U.S. National Technology Strategy. URL: https://www.cnas.org/u-s-national-technology-strategy

The Secretary General Annual Report. 2020. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2021/3/pdf/sgar20-en.pdf

The White House. 2021-1. Fact Sheet: Quad Leaders' Summit, September 24, 2021. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/24/fact-sheet-quad-leaders-summit/

The White House. 2021-2. Joint Leaders Statement on AUKUS, September 15 2021. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/15/joint-leaders-statement-on-aukus/

US Departament of State. 2021. 3 March. A Foreign Policy for the American People. URL: https://www.state.gov/a-foreign-policy-for-the-american-people/

VITALY, Orlov. 2021. War is invisible and effective. Voyenno Promyshlennyy Kuryer, 24 August 2021. URL: https://vpk-news.ru/articles/63516

World Economic Forum. 2021. The Global Risks Report 2021. 16th Edition, ISBN: 978-2-940631-24-7. URL: http://wef.ch/risks2021