JDST., vol. 3, no. 2, p7-p41, 2020
https://doi.org/10.46713/jdst.003.02

www.jdst.eu, e-ISSN 2534-9813

Research Article

Defence Strategy and New Disruptive Technologies Nexus: Implications for the Military Organisations

Yantsislav Yanakiev, Nikolai Stoianov, Dimitar Kirkov, Grigor Velev

Bulgarian Defence Institute "Prof. Tsvetan Lazarov"

2 Prof. Tsvetan Lazarov Blvd. 1592, Sofia, Bulgaria

https://www.di.mod.bg/

ABSTRACT

This article aims to investigate the role of strategy in the defence domain, with a special focus on how technology innovations can influence strategy development. The key question is how and in which ways technological advances may affect defence strategy development. It starts with an evolution of the concept of defence strategy in recent years, as well as its possible future transformation in parallel to the trends of new and emerging defence technologies. After that, it analyses different conceptual models of defence strategy based on case studies of strategic documents in the defence domain of the nations represented at EU project Predictive methodologY for TecHnology Intelligence Analysis (PYTHIA) consortium, as well as documents of EU and NATO. Finally, the article summarises some conclusions concerning the dynamic character of interrelation between the development of defence strategies and technology innovations. Besides, some ideas regarding how defence research can address operational needs by supporting with new knowledge the production and procurement of the most needed weapon systems are presented.

✉ Corresponding Author: Tel.: +359 2 9221862 Fax: +359 2 9221808; E-mail: y.yanakiev@di.mod.bg

ARTICLE INFO

RECEIVED: 01 Sep 2019
REVISED: 10 Nov 2019
ACCEPTED: 30 Dec 2019
ONLINE: 20 MAY 2020

KEYWORDS

PYTHIA, Defence Strategy, Disruptive Technologies, Defence Capabilities, Technology Foresight

I. INTRODUCTION

This article aims to investigate the role of strategy in the defence domain, with a special focus on how strategy can be affected by technology innovations. The key question is how and in which ways technological advances may influence defence strategy development.

To achieve this goal the article is structured in three main parts.

First, the evolution of the concept of defence strategy in recent years is examined, as well as its possible future transformation in parallel to the trends of new and emerging defence technologies. For that reason, the analysis starts with a description of the strategic context and identification of global trends in the field of technology. Besides, a summary of possible military implications that result from these trends is discussed.

Second, different conceptual models of defence strategy are examined based on case studies of strategic documents in defence domain of the nations represented at EU project Predictive methodologY for TecHnology Intelligence Analysis (PYTHIA) consortium, as well as the Global Strategy for the European Union's Foreign and Security Policy (2016), the 2018 EU Capability Development Priorities, the NATO Strategic Concept "Active Engagement, Modern Defence" (2010) and NATO Science and Technology Organization Tech Trends Report 2017.

Third, the report summarises some conclusions concerning the dynamic character of interrelation between the development of defence strategies and technology innovations. Besides, some ideas regarding how defence research can address operational needs by supporting with new knowledge the production and procurement of the most needed weapon systems are presented.

II. CHANGING STRATEGIC ENVIRONMENT AND GLOBAL TECHNOLOGICAL TRENDS

Strategic context

This section of the article summarizes main trends in the political, societal, economic, environmental and technological domains that will shape the future strategic context to derive implications for the EU security in the next couple of decades. It is important from the viewpoint of the evolution of the concept of defence strategy and identification of future operational needs.

The analysis is based on the review of 2018 NATO Strategic Foresight Analysis Report and the Global Strategy for the European Union's Foreign and Security Policy: "Shared Vision, Common Action: A Stronger Europe".

The Strategic Foresight Analysis Report (SFA) published by NATO Allied Command Transformation in May 2018 identifies convergence of several political, social, technological, economic, and environmental trends that are going to redefine the global security context [16].

It is instrumental to capitalize on what was done in NATO with the Long-Term Transformation Process which is based on the four-year cyclical process that sees NATO develop a Strategic Foresight Analysis Report (by-annually updated and The Framework of Future Alliance Operations (FFAO) [7] which lists the implications/impact that all (including technological) trends have on military operations and defence planning.

In the political domain, the most significant trends are related to:

- Redistribution of economic and military power towards Asia which is expected to challenge the EU and NATO regarding their influence;
- Greater influence of Non-state actors over national governments and international institutions;
- Increasing competition between major powers which may intensify the likelihood of confrontation and conflict in the future;
- Emerging alternative global governance institutions that are likely to challenge the existing international organizations;
- Public discontent has led to increasing polarization between political and social groups, further eroding of trust in governments and traditional institutions.

Social trends, defined in the SFA, which will most profoundly shape the future global security context are:

- The asymmetric demographic change, an ageing population in the most European countries which is related to nations' ability to allocate necessary funds for defence as well as may limit recruitment for the defence forces; Also, the high fertility rates in the developing countries may lead to youth bulges, unemployment, insufficient education opportunities for the young people, social unrest and increased emigration towards the EU;
- The rapid urbanization which might lead to resource scarcity and challenge the distribution of available resources;
- The increasingly polarized societies and growing interconnected human networks which may lead to important challenges for EU's security.

The main environmental trends are related to:

- Climate changes which are going to impose stress on current ways of life, on individuals' ability to subsist and on governments' abilities to keep pace and provide for the needs of their populations;
- Increasing impact of natural disasters in areas unaccustomed to such events;

- Governments and international institutions will be expected to provide humanitarian assistance and relief with increasing frequency.
- The main trends in the area of economics and resources are the following:
- An increasingly interconnected global financial system which is more vulnerable to attacks by both state and non-state actors;
- The demand for resources will increase paralleled with population and economic growth particularly in developing countries;
- Access to and control over natural resources will play an increasing role in power politics;
- Increased inequality is a catalyst for migration and can have second-order effects such as fractured and conflictual societies, violent extremism, nationalism, isolationism, and protectionism;
- The existing burden on national economies will grow due to the rise in competing demands for limited resources.

Finally, the main trends, identified in the SFA 2017 Report, related to new and emerging technologies are the following:

- Individuals, state actors and non-state actors will have greater opportunity to exploit readily available technologies in an innovative and potentially disruptive manner. The new and emerging technologies will offer huge opportunities for both civilian and defence sectors, but also present new vulnerabilities and security challenges;
- Interconnectedness and digitalization have increased the volume and value of information. The scale and speed of global networks will allow individuals and groups immediate access to information and knowledge but may also enable the dissemination of false or misleading information. Additionally, data will increasingly become a strategic resource. The Internet has promoted increased citizen advocacy and government transparency. Increased access to information, particularly via social media, can be a catalyst for social mobilization. Global networks provide the opportunity for the dissemination of information to large audiences for shaping global opinion;
- The number of sensors in the environment is increasing exponentially. Networks are becoming global, creating a denser and broader situational awareness. These networks will become embedded in our lives and interwoven into everything that we do. Furthermore, these networks are increasingly being created and used in a distributed manner;
- The commercial sector will be increasingly dominant in technological development. Commercial innovation has outpaced traditional defence Research and Development (R&D). Reductions in defence budgets have led to over-reliance on commercially available solutions, the loss of defence-focused R&D skills and may increase security risks. Reductions in defence-specific research brought about by reduced budgets, and the application of commercial innovations to military requirements has seen the commercial sector overtake defence research and development. The commercial

sector may not address some areas of science and technology that are critical for defence innovation;

- Operational effectiveness has become overly dependent on advanced technology and civilian infrastructure without redundant systems. Technological advancements will continue to open new domains of warfighting such as cyber and space. The scale, pace of advancement and cost have made it unattractive for governments to develop redundant technologies solely for military use.

The current EU Global Strategy for the implementation of the Common Security and Defence Policy (CSDP) "Shared Vision, Common Action: A Stronger Europe" clearly states that "We live in times of existential crisis, within and beyond the European Union. Our Union is under threat". The Strategy describes the world as "more complex", "more connected" and "more contested". Also, it is unquestioned that "Internal and external security are ever more intertwined: our security at home depends on peace beyond our borders." Therefore, the EU will be a responsible global stakeholder" [2] (pp. 3-4).

The main security risks to the Union today are terrorism, hybrid threats, economic volatility, climate change and energy insecurity endanger our people and territory. Therefore, the Union will enhance the efforts on defence, cyber, counterterrorism, energy and strategic communications protection [2] (pp. 9-10).

In this context, the EU needs to be strengthened as a security community. This means the European security and defence efforts to enable the EU to act autonomously while also contributing to and undertaking actions in cooperation with NATO. To achieve this end goal, the Member States need the technological and industrial means to acquire and sustain those capabilities which underpin their ability to act autonomously [2] (p .20).

Most critical capabilities that have to be developed at the EU level a related to "Intelligence, Surveillance and Reconnaissance, including Remotely Piloted Aircraft Systems, satellite communications, and autonomous access to space and permanent earth observation. As regards counter-terrorism, Member States must implement legislation concerning explosives, firearms and Passenger Name Records (PNRs), as well as invest in detection capabilities and the cross-border tracing of weapons". Besides, "Europeans must invest in digital capabilities to secure data, networks and critical infrastructure within the European digital space. We must develop capabilities in trusted digital services and products and in cyber technologies to enhance our resilience". Finally, "regarding high-end military capabilities, Member States need all major equipment to respond to external crises and keep Europe safe. This means having full-spectrum land, air, space and maritime capabilities, including strategic enablers [2] (p. 46).

To achieve strategic autonomy and for a credible CSDP, the Strategy stresses on building a sustainable, innovative and competitive European defence industry (p. 47).

To summarize, the EU Global Strategy clearly emphasizes the interdependence between strategy development and science & technology innovations. It identifies current and future security risks for Europe, the end state to be achieved - secure, resilient and prosperous Europe, the means and ways that include boosting innovations in the technological and industrial base to acquire and sustain the full spectrum of capabilities needed to counter the identified risks and threats.

Future technology implications in the defence domain

This part of the article focuses on the identification of potentially disruptive technologies and how science or technology (S&T) may affect the capabilities development of the EU. The analysis is based on two recent publications of the European Defence Agency (EDA) Defence Matters Magazine 14, "Defence Innovations: A Journey to the Future" and NATO Science and Technology Organization (STO) Technology Watch Cards report, AC/323-D (2017)0006, STO Tech Trends Report 2017).

The interdependence between strategy and technology is strongly defined in a recent publication of the European Defence Agency (EDA) titled Defence Innovations: A Journey to the Future [5]. The authors of this research come up with highlighted that the identified technology trends "are likely to have profound implications on the shape of future conflicts, in terms of actors, domains, duration and timing, and phasing, or, in short, ENDS, WAYS and MEANS" Moreover "In an increasingly connected, complex and information-rich global society, technological developments not only shape the ways and means by which wars are waged, but can also precipitate changes in what is perceived to constitute (military) conflict, and condition the role of defence institutions in preventing, preparing for, engaging in and moving away from conflict"; From the analysis of emerging technology trends the study states that, "technology trends outside of the military are moving quickly, profoundly and unpredictably. This may require a more innovative approach on behalf of European defence planners".

Indeed, the chapter Disruptive defence innovations a constant eye on the future: identifying Europe's capability requirements for 2035, presents an independent horizon scanning and technology watch activities to identify future technology trends whose applications are likely to have a significant impact on not only on societal developments but also on defence and security. Among the key disruptive technologies and technology trends that are expected to influence defence and security are the following:

- Sensors and network connectivity;
- Artificial intelligence & cognitive computing;
- Defence internet of things;
- Big data analytics for defence;
- Blockchain technology for defence;
- Artificial intelligence-enabled cyber defence;
- Robotics and autonomous systems;

- Future advanced materials for defence applications;
- Additive manufacturing (3d-printing);
- Next-generation sequencing for biological threat preparedness;
- The globalisation of technology and modularisation of systems;
- Space as a battlefield;
- Human enhancement;
- Renewable energy and energy weapons.

The NATO STO Technology Watch Cards Tech Trends Report 2017) [10] presents an extensive list of technology innovations that may have an important effect on the future battlespace and that are favourable to international collaborative research:

- Additive Manufacturing which military forces could use for rapid prototyping, in the situation of production and repair of deployed military equipment, precision, custom and unique parts production;
- Everywhere computing supported by military mobile networks and mission cloud computing has the potential to provide real-time decision support to the individual soldier at all times and all places;
- Predictive Analytics is very instrumental regarding the huge amounts of data in the future battlespace and provides the potential for analytics to deliver insight across all warfighting and defence domains, real-time decision support, early indicators and warnings of crises and real-time monitoring;
- Social Media applications in defence and security include population surveillance, sentiment analysis, knowledge and information sharing, low-cost means to stay in touch with families and strategic communications;
- Unmanned Air Vehicles applications in defence and security include allowing for access to unreachable areas, persistent surveillance, endurance, robots in support of soldiers, and cheaper, automated logistics deliveries;
- Advanced Materials that are manufactured using nanotechnology or synthetic biology may be used in coatings with extreme heat resistance, high strength body or platform armour, stealth technologies, advanced sensors and decontamination, and bulk production of food, fuel and building materials;
- Mixed Reality applications in defence domain include heads up or head-mounted displays for pilots and soldiers for real-time situational awareness, digital cockpits/windows, realistic training environments or providing hands-free job performance aids, etc.;
- Sensors are everywhere, which refers to the ability to detect and track any object, or phenomenon from a distance by processing data acquired from high tech, low tech, active and passive sensors as well as background sensors, essentially everything could be a sensor. The defence applications include universal air picture, underwater sensor nets, social media

exploitation, automated logistics planning, autonomous systems and soldier systems;

- Artificial Intelligence which refers to the ability of machines to match humans in terms of learning, reasoning, planning and acting in complex cyber-physical environments. Potential impact in defence domain includes replacement of human decision-makers, autonomous robot or vehicle control, automated information fusion and anomaly detection, psychological operations and intelligent tutoring for a variety of military and support (medical) missions;
- Electromagnetic dominance which is the ability to use more of the spectrum, to share the spectrum more efficiently, to protect own forces' use of the spectrum and to deny enemy use. The future will bring, among other things, faster, more reliable wireless/radio communications, electronic warfare resilience, secure streaming video and smaller deployed footprint;
- Hypersonic vehicles can be an aeroplane, missile or spacecraft. Potential defence applications include fast long-range strike of high value or high threat targets, ballistic missile defence and reusable space transport vehicles;
- Soldier systems, which refers to the augmentation of individual human abilities using artificial means such as robotic exoskeletons, smart textiles, drugs and seamless man-machine interfaces. Potential defence uses include the capacity to endure extreme environments, better health monitoring and care provision and decision making at the individual level.

To summarize, both EU and NATO documents demonstrate many common assessments regarding future technology trends that are going to influence military art, including future defence strategies.

Military Implications related to identified global trends in the defence technology domain

From the viewpoint of the topic of this research, it is of particular interest to identify plausible military implications resulting from the trends in defence technology domain, which are applicable in the EU allied format and for the Nations.

First, the growing access to new technology enables disruptive behaviours. The current near-monopoly held by major state powers on the possession of high-tech weapons continues to decrease, allowing smaller states and non-state actors to acquire disruptive technologies. A broad array of low-cost, unsophisticated technological advancements, such as drone and robotic technologies, are readily accessible and can be employed innovatively as weapons.

Second, the increasing number of sensors, access to data and global networks may generate operational vulnerabilities. States and non-state actors with malicious intent will have the ability to access information at an unprecedented rate. Additionally, as access to data continues to increase, procedures will need to be developed or amended to consider the growing vulnerability of information.

Third, adversaries will increasingly use global networks to disseminate false or misleading information to influence public opinion and decision-making. The EU will require an agile approach to strategic communications to maintain an edge.

Fourth, the reliance of the military on certain technologies, such as space-based communication and navigation systems, reduces the resilience of the force if these technologies are denied. Old skills may need to be relearned and less vulnerable analogue technologies could be considered as back-ups. Resilience needs to be considered in platforms' design and information exchange requirements.

Fifth, the rapid development of technology challenges interoperability due to the disproportionate rates of technological development amongst EU Nations.

Sixth, the increasing rate of technology advancement is expected to challenge the whole defence acquisition processes.

Seventh, the new technologies, such as offensive cyber, artificial intelligence, autonomous systems and human enhancement will expose divergent ethical and legal interpretations.

Finally, it is of key importance the EDA to foster innovation and multinational cooperation in defence R&D projects to mitigate the negative trends over the last decades related to R&D funding decline.

III. Case studies of different conceptual models of defence and S&T strategies at allied and national levels

The analysis in this chapter starts with the strategic documents in the security and defence domain of the EU and NATO.

The focus of the analysis is on how the issue of defence technologies is incorporated in the strategic documents and the character of the interrelationship between technological developments and defence strategy transformation.

Analysis of defence and S&T strategies at EU and NATO level

European defence research & technology strategy

The European defence research & technology (EDRT) Strategy, endorsed by the European Defence Agency (EDA) Steering Board on 10 November 2008, is focused on addressing the Research & Technology needs of the Common Security and Defence Policy (CSDP) as it stands now and develops in the future. The vision of the EDRT strategy is "to enhance and develop more effective research collaboration in science, technology and demonstrators to deliver in time the right technologies in support of military capabilities for short, medium and long term needs" [1] (p. 4).

It covers two phases -planning and implementation and defines the ends, the means and the ways to achieve a technological breakthrough on new defence capabilities acquiring. First, the ends represent a prioritised European list of key technologies in which to invest to improve the European defence capabilities.

The Strategy is by virtue an example of a capability-driven approach in research and technology programming and implementation. The ends should be accomplished through collaborative S&T projects in the EU context. The means describe the tools, which may improve efficiency and accelerate the implementation of the ends. Finally, roadmaps and action plans will be crucial tools to describe the ways and connect the planning and the implementation phases of the EDRT Strategy.

The key achievement of Defence EDRT Strategy is the fact that it postulates Research and Technology (R&T) spending to be 2% of total defence expenditure. Besides, the Strategy envisages European collaborative Defence R&T spending to be 20% of Defence R&T Expenditure in the Union.

Over the past 10 years after the endorsement of the EU Defence R&T Strategy in 2008, profound changes in the global security environment took place, as well as substantial developments in defence technologies. Therefore, it is important to analyse the evolution of the concept of defence strategy in the context of new emerging technologies and more specifically, how the EU R&T strategic documents have been updated to be adequate to the foreseeable security challenges.

A clear example of the process of aligning strategic research agendas with Member States' operational needs and requirements is the Overarching Strategic Research Agenda (OSRA) [12].

The OSRA provides a systematic and clear mechanism for collaborative European Defence Research for the future, such as the upcoming EU framework programme and Preparatory Action. Also, it offers a rationale for investment in defence R&T at an EU level that supports capability needs.

The overall aim of OSRA is to establish a framework that helps to reduce the level of effort that the Participating Member States (PMS) and EDA have to put into updating and keeping Strategic Research Agendas (SRAs) and their roadmaps up-to-date, by creating a digital 'live' SRA/OSRA portal that supports more frequent and systematic interaction between EDA and PMS in the Capability Technology Groups (CapTechs).

The 2018 EU Capability development priorities

The European Defence Agency produces updated Capability Development Plans (CDPs) since 2008, in close cooperation with its Member States and with the active contributions of the EU Military Committee (EUMC) and the European Union Military Staff (EUMS). The purpose of the periodic CDP revision, a key tasking of the Agency, is to provide a full capability picture that supports decision-making at EU and national levels regarding defence capability development. The overall objective is to increase coherence between Member States' defence planning and to encourage European cooperation by looking together at future operational needs and defining common EU Capability Development Priorities. The CDP revision benefits from several inputs such as the Headline Goal Process, studies on long-term trends, lessons from operations and information on current plans and programmes.

The CDP is regularly updated and the EDA Steering Board in Capability Directors formation in June 2018 endorsed the latest version. It is of particular strategic significance as it serves as a baseline and reference for the implementation of major European defence initiatives launched following the 2016 EU Global Strategy: The Coordinated Annual Review on Defence (CARD), the Permanent Structured Cooperation (PESCO), and the European Defence Fund (EDF).

The most tangible output of the 2018 CDP revision are the 11 new EU Capability Development Priorities, developed together with the Member States. They are the result of an in-depth assessment conducted based on contributions provided by the Member States, the EUMC and EUM) on short-term, mid-term and long term trends: capability shortfalls analyses and lessons learned from recent CSDP operations; planned capabilities and the potential for future European cooperation in each of the capability domains; and a study into the long-term capability-related and technological trends and needs (2035 and beyond) [15].

The 2018 new EU Capability Development Priorities cover the process of transformation of the EU Global Strategy in capabilities development in several critical for the EU security areas [6]:

- Enabling capabilities for cyber responsive operations;
- Space-based information and communication services;
- Information superiority;
- Ground combat capabilities;
- Enhanced logistic and medical supporting capabilities;
- Naval manoeuvrability;
- Underwater control contributing to resilience at sea;
- Air superiority;
- Air mobility;
- Integration of military air capabilities in a changing aviation sector;
- Cross-domain capabilities contributing to achieving the EU's level of ambition.

The NATO Strategic Concept and technology impact

The NATO Strategic Concept is a key document that outlines NATO's enduring purpose and security tasks. It also identifies the central features of the security environment, specifies the elements of the Alliance's approach to security and provides guidelines for the adaptation of its military forces.

The current NATO Strategic Concept "Active Engagement, Modern Defence" (2010) defines three core tasks of the Alliance: collective defence, crisis management and cooperative security.

The following technology influences on Security environment are identified in the NATO Strategic concept (2010) [11].

- Nuclear weapons and other weapons of mass destruction, and their means of delivery, threatens incalculable consequences for global stability and prosperity;

- Modern technology increases the threat and potential impact of terrorist attacks, in particular, if terrorists were to acquire nuclear, chemical, biological or radiological capabilities;
- Cyber-attacks are becoming more frequent, more organised and costlier in the damage that they inflict on government administrations, businesses, economies and potentially also transportation and supply networks and other critical infrastructure; they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability. Foreign militaries and intelligence services, organised criminals, terrorist and/or extremist groups can each be the source of such attacks;
- Several significant technology-related trends – including the development of laser weapons, electronic warfare and technologies that impede access to space – appear poised to have major global effects that will impact on NATO military planning and operations.

What are the main defence and deterrence capabilities, related to technology threats that are identified in the NATO Strategic concept?

- Maintain an appropriate mix of nuclear and conventional forces;
- Ensure the broadest possible participation of Allies in collective defence planning on nuclear roles, in peacetime basing of nuclear forces, and in command, control and consultation arrangements;
- Develop the capability to defend NATO's populations and territories against ballistic missile attack as a core element of the collective defence, which contributes to the indivisible security of the Alliance.
- Further develop NATO's capacity to defend against the threat of chemical, biological, radiological and nuclear weapons of mass destruction;
- Develop further NATO's ability to prevent, detect, defend against and recover from cyber-attacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations;
- Ensure that the Alliance is at the front edge in assessing the security impact of emerging technologies and that military planning considers the potential threats.
- From the technology point of view, one can conclude that the 2010 NATO Strategic concept gives significantly higher importance to new security challenges – cyber-attacks and capabilities to prevent, detect, defend against and recover from them.

Case studies of different conceptual models of defence strategies at national level

This section presents a review of different concepts and models of defence strategy of the MS represented at PYTHIA Consortium, as well as the U.S. and Germany concerning the dynamic character of interrelation between the development of military/defence strategies and technology innovations. The focus is on how the development of a strategy can be affected by defence technology innovations.

We are going to highlight two key components of defence strategies: 1) assessment of strategic defence environment; and 2) formulation of key defence priorities:

Under the first area of analysis, strategic defence environment, we are going to focus on identified risks and threats to national and EU Defence. Besides, we will identify what is common and what is different in the national conceptual approaches to develop defence strategies.

Under the second area of analysis, key defence priorities, we will look for how the national defence and R&T strategies view the role of technology innovations in defence policy, planning and defence capabilities development, as well as approaches to stimulate defence innovation.

Bulgaria

The updated National Defence Strategy of the Republic of Bulgaria from 2016 [8] describes the strategic security environment as complex and dynamic with many dimensions, which are difficult to predict. Many factors influence the strategic environment among which the process of globalization; financial and economic crises; the proliferation of weapons of mass destruction and the means of their delivery; climatic and health problems; demographic, ecologic and energy problems; asymmetric risks and threats; information security threats; failed states; internal and regional conflicts; The security environment in the Middle East and North Africa is of paramount importance The situation in Central Asia, especially in Afghanistan [8] (pp. 3-8).

Among the key security risks and threats to the Bulgarian national security are the following:

- Risks of weapons of mass destruction (WMD) proliferation as a result of the increased interest of some non-state actors end extremist groups to acquire WMD and the comparatively easy access to new technologies;
- The asymmetric and the other transnational risks and threats, particularly trans-border terrorism and religiously motivated violence;
- The danger to ecological security which stems from climatic changes and their consequences, natural disasters and catastrophes, industrial accidents involving leakage of dangerous substances, trans-border pollution of the air;
- The problems related to the deficiency of energy and natural resources (energy dependency);
- The dynamic development of ICT and their widest application in all domains of the public life poses information security risks and threats of cyber-attacks against strategic civilian and military communication and information systems and forces participating in missions and operations beyond the borders of the country;
- Failed states;

- The conflicts in the Middle East and North Africa, as well as the crisis in Ukraine with the application of hybrid strategies.

The key priority of the Bulgarian National Defence Strategy is the development of a modern defence institution, based on an integrated system for effective and transparent defence management with potential for institutional flexibility, timely planning and effectively responding.

To achieve this goal the Strategy envisages the establishment of modern defence management; capabilities-based planning; education and training of the personnel following modern standards; technological re-armament of the Bulgarian Armed Forces and the defence system, applying the lessons learned from operations and the results from defence research activities; increasing the share of structures, programs and projects, jointly implemented with the allies and partners in NATO and EU framework; integrating into a system the resource and investment planning and the material resources allocation; updating the concepts and doctrines for the development and employment of the military and civilian defence components in operations [8] (p. 12).

The importance of technology innovations in defence policy, planning and capabilities development is emphasised in the Strategy. Besides, all activities in S&T and acquisition should be focused on the achievement of Required Operational Capabilities. It clearly states that the investment policy and the acquisition of defence-related products are conducted after a comprehensive technological and economic analysis of their effectiveness for the Required Operational Capabilities development, taking into consideration the lessons learned from the current operations [8] (p. 19). Moreover, the National Defence Strategy of the Republic of Bulgaria considers the success in current and future operations as a result of the employment of modern information technologies[8] (p. 21).

Particular attention is devoted to guarantee permanent and unlimited access to the cyber-space and to secure the integrity of its critical systems. Therefore, the Republic of Bulgaria continues to develop national capabilities for prevention, detection, protection and recovery from cyber-attacks and jointly with the allies takes part in the process of establishment of a common integrated cyber-threats detection, warning and response system [8] (p. 21).

There are no explicit recommended approaches to stimulate defence innovation in the text of the Bulgarian National Defence Strategy, but this topic is covered by another document called Strategy for research and technologies in security and defence which horizon is until 2020 [14].

This document presents the key defence technology research areas that are allied to the priorities of the European defence research & technology strategy1. In this way, not only the national priorities in these areas are specified, but also the

[1] A European defence research & technology strategy, https://eda.europa.eu/what-we-do/our-current-priorities/strategies/ResearchandTechnology

contribution of our country to the satisfaction of the European defence capabilities and the capabilities of NATO.

The Strategy creates conditions for ongoing monitoring and coordination on security and defence research and technology. Also, it establishes an Interdepartmental Centre for research and technology coordination on security and defence under the Council of Ministers of the Republic of Bulgaria.

The focus of the efforts will be focused on priority technology areas, sub-areas and technologies nationally and in the interests of NATO and the European Union for:

- Research and technology to support new capabilities in security and defence development;
- Effective spending of resources;
- Efficiency in transforming research and technology in line with changing operational capability requirements;
- Participation of R&D structures in decision-making processes for research and technology in the interests of security and defence forces;
- Direct participation in the scientific and research activity of the defence industry.
- The priorities for investing in research and technological monitoring are:
- Information and communication technologies, sensors, radiolocation and radio navigation;
- Armaments, ammunition and defence equipment;
- Research and technologies for nuclear, chemical, biological and radiation protection and ecology;
- Research and technology related to the role of the human factor in security and defence.

France

The security threats and risks identified in the 2013 White Paper have been realised more rapidly and more vigorously than expected and, the French Republic issued a new Defence and national security strategic review in 2017 [3].

Among the key security risks and threats to the French national security that are identified in this latest strategic document are the following:

- Direct attacks on the national territory - Jihadist terrorism, which struck France and its European neighbours, is evolving and expanding to new regions;
- The concentration of threats and crisis in Europe - a migration crisis, the persistent vulnerability in the Sahel-Sahara region, enduring destabilisation in the Middle East, tensions on Europe's eastern and northern flanks;
- The effects of climate change, pandemic risks, energy rivalries, trafficking and organised crime are creating further vulnerability and destabilisation;
- The risk of the emergence of a new virus spreading from one species to another or escaping from a containment laboratory is real. Similarly, interconnected food industries generate risks to human health, and

increase the potential for "agroterrorism". Even worse, the spread of biotechnologies might enable terrorist organisations to carry out sophisticated biological attacks;

- In cyberspace – the ability to operate anonymously (TOR network) and the creation of electronic currencies (ex. Bitcoin) are opening up new opportunities for crime, with a potential for development that seems exponential;
- The capacity to take action in cyberspace and the informational domain is becoming increasingly accessible. As a result, the societies, populations, government services and businesses are more directly exposed to interference or malicious actions that may have major consequences.

The key defence priorities of France are related to strengthening the European defence based on shared security interests. France supports the Common Security and Defence Policy, including both permanent structured cooperation and the European Defence Fund. Besides, the country will continue to shoulder its full responsibilities within NATO, including collective defence and reassurance [13].

The French military will continue maintaining a full-spectrum and balanced armed forces model. This model is considered critical for France's national independence, strategic autonomy and freedom of action. More specifically, the full-spectrum and balanced armed forces model should make it possible to engage in high-intensity operations on land, at sea, in the air, and to operate in the cyberspace. The document postulates that France's armed forces should be capable of autonomous action concerning nuclear deterrence, the protection of its territory and approaches, as well as to intelligence, operations command and control, special operations and cyberspace. To achieve this goal, the new investment programmes should focus on certain forms of readiness, especially resources for intelligence, command and control, first entry, combat and support. Innovation is viewed as the core of the approach pursued by the Ministry and the Armed Forces.

In the context of this operational requirement, the French Defence and national security strategic review lays special attention to the role of disruptive technologies which give rise to new opportunities and new vulnerabilities. Among them are the following:

- Technological disruption contributes to instability in the strategic environment because sophisticated weaponry and the rapid spread of many technologies are now enabling medium-sized states, groups and even individuals to acquire or develop capabilities previously only accessible to a limited number of countries;
- Most technologies with the potential to radically change future defence systems are still state-funded (e.g. hypersonic and hyper manoeuvrable missiles, improved and networked sensors, active stealth systems, directed-energy weapons, etc.), but the civilian public and private sectors are generating an increasing number of technologies with military applications;

- Genetic engineering and more specifically synthetic biology (with genome engineering), as well as technologies derived from neuroscience and human augmentation, are extremely promising;
- In the space domain, broader access enabled by the New Space movement opens up multiple opportunities, including miniaturised systems and new services, available at ever-lower costs;
- Hyperconnectivity, big data technologies, the Internet of Things and robotics are examples of fields offering major opportunities for defence applications;
- Artificial intelligence, in particular, is expected to play a central role in defence systems, where it will make a significant contribution to operational superiority while entailing new risks;

At a time of global re-arming, major powers are stepping up their efforts to develop leading-edge systems (such as hypersonic and stealth), creating a risk of Europe lagging. Furthermore, a growing number of countries are acquiring sophisticated weapon systems (including missile defence, air defence and even anti-satellite weapons). The increase in missile range and speed, multiple sensor combinations and networking make targeting easier, reduce the effectiveness of stealth and offer harder-to-counter anti-access and area denial capabilities;

The spread of new civilian and dual-use technologies is enabling all types of actors without industrial bases to acquire advanced resources previously only available to states (e.g. cryptography, GPS navigation, telecommunications and jamming technologies). In a booming global market, the risks of loss of control or misappropriation of such technologies are numerous and proven;

The current transformation in the space sector is already resulting in denser traffic (including small satellites constellations) and a growing risk of collision with space debris, making it necessary to develop space situational awareness and the resilience of the space capabilities;

All of these changes, together with rudimentary modes of action and more innovative methods (e.g. drone-mounted improvised explosive devices) tend to even out the balance of military forces, particularly as the underlying technologies are not adequately covered by control mechanisms.

Particular attention in the Defence and national security strategic review is given to the growing threats in cyberspace. It identifies the main risks and vulnerabilities, as well as possible mitigation strategies. Among them are the following:

- Cyberattacks have ramped up considerably over the past decade, reflecting the dissemination of increasingly sophisticated means of attack. States have played a direct role in these changes by propagating cyber-weapons that, once known, may be studied, re-engineered and reused, but also indirectly, by allowing such attacks to be developed in or deployed via their territory;
- Over the same period, the increasing exposure of developed societies to digital technologies and interconnection has increased their vulnerability. Cybernetic tools can be used to inflict significant industrial damage or to

impair networks and infrastructures critical to the proper functioning of societies or states;

- Major systemic risks ensue from the difficulty of managing such attacks and their vectors and consequences. Controlling the propagation of attacks, of tools and weapons, and their consequences, is difficult, which entails major systemic risks. These risks are exacerbated by the fact that action in cyberspace can achieve global effects using limited resources. In the military domain, the increasing dependency of weapon or command systems on digital technologies makes them even more sensitive to such threats;
- Difficulty in attributing actions and the combination of direct actions with opinion influencing and propaganda techniques make numerous manipulation scenarios possible, whether for destabilization purposes or in support of more conventional operations. Addressing constantly changing cyber-threats is particularly complex since the response must extend beyond the scope of defence, due to the intertwined nature of the challenges faced and of the public and private actors.

Italy

The Italian "White Paper for International Security and Defence", published in May 2015, outlines strategic priorities and the military capabilities needed to implement these priorities.

A shift in the global balance of power, the massive transformation, potential of new technologies and greatly increased technological interdependency, and the low rate of defence investment are factors that influence Italian defence.

The document discusses the current international situation and identifies several factors, which influence the future international security scenario [22]:

- Increased influence and widespread technologies;
- The current speed of research and use of technologies, together with the innovation process resulting from the integrated use of existing and emerging technologies leads to a faster rate of change. Likewise, the traditional margin of technological superiority held by the military has been eroded in favour of technologies for civilian use. This will increase the possibility of technology being used by non-state actors;
- The centrality of computer networks.
- The world is becoming increasingly connected and integrated making possible universal access to knowledge and information. The West is particularly dependent on information network systems so that it is essential that these systems are functional, secure and resilient and this results in the emergence of a new operational domain, the cybernetic domain, which must be protected and defended. The effects of cyber-attacks on networks or computer services are particularly destructive for Western countries producing the same impact as those resulting from the war fought with conventional weapons.

- Urbanization: It is estimated that in 2040, 65% of the world population will live in large built-up areas and that 95 % of the increase in urban population will occur in the mega-cities of the developing countries. This process will have a significant impact on the dynamics of security management in those states.
- Scarcity of natural resources: Nations in the developing world need ever-increasing levels of energy and raw materials to sustain their growth. Competition for these resources could produce a higher level of international tension leading to possible conflicts. However, the increasing scarcity of vital resources such as water and food due to population growth, climate change and irrational use of territories is a much more serious problem. It is the cause of the migration phenomena and could pave the way to strong competition, even armed, for the possession of such resources.
- Local Identities: The progressive birth of local different groups or organisations causes an increasing weakening and fragmentation of existing states, which are unable to centrally manage the twenty-first-century complex phenomenon. In some cases, this weakness opens the way to non-state transnational religious or criminal organisations. The violence and diffusion rate of such organisations have a significant impact on the condition of regional or global security. The consequences arising from the possession of chemical, bacteriological, radiological or nuclear offensive tools are particularly serious in these territories.
- The decrease in defence investment: This phenomenon is common in the western world while the opposite is true in the rest of the world, particularly concerning regional powers. For Western countries, the reduction in military spending is the result of a widespread diminished awareness regarding the importance of defence issues compared to other economic and social problems.

The 2015 Italian White paper contains a chapter, which discusses the scientific, industrial and technological innovation policy of the MoD. Among the most significant trends identified are the following:

- Italian national defence cannot renounce to a certain level of industrial and technological autonomy, coupled with Armed Forces able to express the proper and necessary capabilities, to satisfy at least part of military needs either at the national level or through the participation to multinational initiatives of development and acquisition;
- Technological innovation in civilian markets also makes technologies, spare parts and equipment used for military needs available for new suppliers. It is important, to monitor overall technological development and to consider civil needs to become potentially associated with military ones;
- The Defence and Security industry contributes to technological development through programmes and investments in research and

development and, more generally, to economic growth through the direct, indirect and induced effects on GDP and the creation of skilled jobs;

- A comprehensive system of Defence and Security also requires a wealth of scientific-technological and industrial knowledge which allows the development of products and systems based on distinct technological competence that is as autonomous as it is collaborative, to create a strategic competitive advantage for the nation;
- The 2015 Italian White paper recommends the identification of strategic industrial and technological activities in the field of Defence and Security through a specific "plan" to be kept regularly updated. On the one hand, this evaluation must consider the needs of the armed forces, and, on the other, the effective technological and industrial capabilities.

According to this strategic document science, technology, and research and development are crucial elements of reference for the development of a national strategy for growth, to which the Defence will contribute actively. To improve and strengthen dual research and to allow the nation to benefit from initiatives of collaboration, the Defence will advocate a substantial adjustment of financial resources for R&D concerning specific projects and initiatives to strengthen capability in the field of Defence and Security where priority projects are identified at European level.

The National Plan for Military Research has to be integrated with the National Plan on Research and in this way will be possible the cooperation at the national level of industry organizations with private and public research centres, Universities.

Poland

In the Defence Strategy of the Republic of Poland from 2009, the Polish MoD outlines the international security environment and identifies global and national security risks and threats. Among them are the following [4]:

- The growing international interdependency of today's world often results in the inability to predict many phenomena and their developments, the extent of which is not limited by geographical barriers or political and economic systems. In such an arrangement of relations, the emerging threats and risks are global, while non-state entities that could disrupt this arrangement, are gaining importance;
- The security environment is marked by the concurrence and two-way penetration of military and non-military threats, often asymmetrical. The risk of a large-scale conflict has been drastically reduced, but the threat of regional and local conflicts has not disappeared;
- Nuclear and missile technology development programmes implemented in breach of UN Security Council resolutions also remain a significant threat to international security. The disruption of a regional military balance resulting from such programmes could pose a significant threat to global security;

- Economic security risks, especially those relating to energy security, top the list of non-military threats. Growing demand for energy resources accounts for the fact that they are used to exert political pressure and increasingly replace military power as a state's policymaking instrument. The integration of the global economy, apart from its undeniable benefits, also carries the risk of economic crises and the destabilization of financial markets. Climate change carries both humanitarian and political consequences and the struggle for access to natural resources has become a growing cause of conflicts. Other areas of potential global risks include uncontrolled population migrations from less developed countries and infectious disease epidemics;
- Asymmetrical threats feature prominently among security risks. In most cases, they are generated by failing or failed states. The most serious threats continue to be: international terrorism, including cyber terrorism and terrorism that uses weapons of mass destruction; the proliferation of weapons of mass destruction and means of transporting them; organized international crime involved in the smuggling of arms and dual-use materials, drugs and human trafficking, illegal financial operations and maritime piracy.

The Defence strategy points out that to ensure the realization of national interests and strategic goals in the area of security, the Republic of Poland organises and develops an integrated system of national security. The state's defence system established to counteract threats to vital national interests has been integrated with the NATO security system through common operating procedures in crises and during wartime and by participating in Allied defence planning. The Armed Forces of the Republic of Poland (AFRP) constitute the fundamental element of the state defence system, designated to effectively conduct the security and defence policy. The role of technologies in defence policy is discussed in the context of the required operational capabilities of the AFRP. Among the critical tasks to be achieved are the following:

- To ensure command capability, an integrated, fully automated and efficient class C4ISR (command, control, communications, computers, intelligence, surveillance and reconnaissance) system has to be implemented and gradually developed. Such a system has to be based on modern information and communication technologies and comprises all levels of command and types/components of armed forces;
- Acting in conditions of future network-centric warfare, the system should integrate weapons, reconnaissance and decision-making centres, make available information about resources and use mechanisms enabling data transmission in real-time, while at the same time ensuring continuity of work and the required level of security. This aim is served by electronic counterintelligence operations and cryptographic protection measures;
- The development of troop survivability and protection capabilities will aim at increasing the operational effectiveness of means of combat

identification system by improving resistance to jamming, increasing the probability of correct identification of targets, expanding the information potential of the system and ensuring electromagnetic compatibility of installations;

- To ensure an effective defence against weapons of mass destruction, priority will be given to the creation of an integrated system, operating in a data communications network, of agent detection, telling, warning and alerting troops. It will also be important to gain the capability of detecting biological agents, including remote detection, as well as the capability to neutralize explosive materials and hazardous items containing weapons of mass destruction;
- To ensure effective means of air defence, the capability to operate in a national and Allied integrated system of air defence will be developed to enable detection and destruction of aerial attack vehicles, including unmanned aerial vehicles (UAV), cruise missiles and tactical ballistic missiles.

The Defence Strategy identifies the role of national research and industrial potential in the Polish defence policy in the following way:

- The Polish defence industry remains the main source of supply of materiel and military equipment to the armed forces and Polish R&D institutions are the main suppliers of production technology and engineering ideas in the area of defence technology;
- The integration of the Polish research and industrial potential in the area of defence should be directed at EU and NATO Member States. The European Defence Agency and NATO Science and Technology Organization should be platforms for the exchange of experience and the procurement of state-of-the-art production technologies. The procurement of state-of-the-art defence technologies for the AFRP and strengthening Poland's research and industrial potential should be the main goals of integration;
- Research and industrial units should focus their efforts in the area of defence technologies at developing production technologies that enhance the security of troops, providing a big deterrent effect, permanently raising their combat potential and ensuring manoeuvrability of armed forces.

Romania

The National defence strategy, 2015-2019 of the Republic of Romania a Strong Romania within Europe and the World defines the national security interests and objectives, and lines of action and main ways to ensure Romania's national security. Besides, it assesses the international security environment and outlines threats, risks and vulnerabilities. Among the identified risks and tasks in the strategy are [9]:

- The actions performed to destabilize the Eastern vicinity causing regional instability and possible negative phenomena, amongst which we can mention migration, organized crime, and also the alteration of the economic growth potential;

- The distortions on the energy markets and the competitive projects of some state or non-state actors;
- The cyber threats initiated by hostile entities, state or non-state actors, upon informational infrastructures, the cyber-attacks performed by cybercrime or extremist groups;
- The proliferation of the weapons of mass destruction and the bearing vectors, as well as the traffic of dual-use products;
- The hostile informational actions, which trigger the development of some support points on national territory, especially with an influential purpose;
- Risks of social nature that persist on the background of some trends such as the demographic fall, the migration of the active population, the degradation of the environmental factors, the shortcomings/deficiencies in the national health, education and social assistance systems, but also the distortions on the labour market;
- The radicalization of the extremist entities present on Romania's national territory may occur in the context of the intensification of the extremist flows of ethnic or religious nature or any other nature;
- Border criminality from drugs, people, armament and goods smuggling, illegal migration to economic-financial criminality;
- Illegal smuggling of conventional armament which may derive from some state or non-state actors' interest to perform such operations, targeting conflict areas or areas having a potential to turn into armed conflict;
- The ability of the state institutions to assess and diminish the impact of risks and threats, which is limited by the persistence of some vulnerability in the absorption of European funds, using public funds, energy, critical infrastructure, agriculture, environment protection, justice, health, education and scientific research.

To achieve the national security and defence goals, the strategy points outlines of action, that aim at:

- Consolidating the national defence capacity, which includes the efficient use of NATO mechanisms;
- Continuing the transformation, modernization and procurement of Romania's armed forces, by allotting at least 2% of the GDP to the defence budget, yearly, for 10-year time;
- Developing the capacities required to respond in case of asymmetric and hybrid threats;
- Deepening the security dimension of the Strategic Partnership with the US, by consolidating military cooperation, including the national territory and the Black Sea region;
- Reaching performance standards needed to achieve interoperability with the military of the other member states and bringing in line legal and normative provisions regulating the training instruction of armed forces;

- Adapting the security industry to the armed forces' equipment requirements and the competitive environment;
- Developing cooperation in the field of the security industry with states of the Euro-Atlantic space, by capitalizing on multinational cooperation opportunities, amid NATO and EU initiatives;
- Consolidating the national role and presence in civil missions and military operations through participation in monitoring missions and crisis management in areas of priority interest for Romania.

The United Kingdom

The UK International Defence Engagement Strategy [17] defines the security environment that as complex and dangerous for the UK and the national interests. Besides, it stipulates that no country can address all the challenges alone.

The Strategic Defence and Security Review 2015 2 (SDSR) [20] considers as the key threats to UK national security terrorism, extremism and instability; cyber; and the weakening of the rules-based international order, making it more difficult to achieve the consensus needed to deal with global threats. To respond to these threats, the British defence policy is defined as "International by Design" which means as close as a possible collaboration with allies and partners.

Besides, the SDSR announced that a new Joint Force 2025 would be developed to tackle a wider range of more sophisticated potential adversaries and to increase the Armed Forces' ability to work with the rest of government and internationally. The British Force 2025 is a joint, integrated and combined force because the UK is unlikely to fight overseas against a sophisticated adversary on its own. The ability to work within combined (international) formations is a vital factor of success in future wars.

In this context, the British strategic defence documents consider the process of developing new technologies as a key priority of defence policy and planning. The collaboration with allies and partners in defence-related multinational projects is an important avenue to help develop valuable new technologies and defence capabilities.

Furthermore, the SDSR sets out the Government's approach to innovation in Defence and Security, emphasizing the need for a step-change in the management approach allocating £800M over the next 10 years to fund innovation activities. A practical example of the management change is the establishment of a new Emerging Technology and Innovation Analysis Cell (ETIAC) with to purpose to keep close links with external partners and experts in the private sector and academia to improve the Government's ability to identify and understand the implications of new, potentially game-changing technologies. Besides, the UK MoD will continue to prioritise Science and Technology by maintaining investment at 1.2% of the

[2] UK Strategic Defence and Security Review, 2015, Available at www.gov.uk, accessed on 17.07.2018.

Defence budget, to ensure our Armed Forces sustain operational advantage against increasingly technologically advanced adversaries [20] (p 34).

It is important to underline that obviously, the UK defence strategists consider the role of the new technologies as a key element of winning future wars. In the same time, the SDSR assumes that “although better integration of emerging technologies and capability development will be essential, we must also address our organisation, workforce, processes and culture to be successful. This will require innovative operational concepts, strategic planning, and reward of innovative behaviours. Defence’s success in this endeavour will require significant cultural change, strong leadership, the continuous pursuit of adaptation across the Department and continued investment in S&T” [20] (p. 31).

We will conclude this review of UK strategic documents in the defence domain with a brief quote from the UK Science and Technology Strategy from 2017 [19]. According to this document, the Ministry of Defence’s (MoD) vision for S&T is that S&T plays a central role in Defence thinking and culture, directing and applying innovative research and thinking to meet the current and future strategic needs of Defence and Security (point. 1). It clearly states that S&T must be mainstreamed into MOD’s strategic policy and decision making because S&T is a critical force multiplier: whilst it makes key contributions to overseas operations, the nuclear deterrent and homeland security, it also enhances UK strategic understanding, develops disruptive and affordable winning edge technologies and identifies alternative solutions to address Defence’s strategic challenges [19] (point 10).

The United States of America

The 2018 National Defense Strategy of the United States of America describes the global security environment as “an increasingly complex, characterized by overt challenges to the free and open international order and the re-emergence of long-term, strategic competition between nations”[21] (p. 2).

The central challenge to U.S. prosperity and security is the re-emergence of long-term, strategic competition by what the National Security Strategy classifies as revisionist powers. The focus is on Russian adventurism and the attempts of China to become a global player. Another change to the strategic environment is resilient, but weakening post-WWII international order. Challenges to the U.S. military advantage represent another shift in the global security environment. The Strategy describes the battlefield as “more lethal and disruptive, combined across domains, and conducted at increasing speed and reach—from close combat, throughout overseas theatres, and reaching to our homeland”. The security environment is also affected by rapid technological advancements and the changing character of war.

The National Defence Strategy puts special attention to the development of new technologies such as advanced computing, “big data” analytics, artificial intelligence, autonomy, robotics, directed energy, hypersonics, and biotechnology [21] (p. 3).

Also, it undoubtedly sets the goal to modernize key defence capabilities “in order to solidify the U.S. competitive advantage”. The priority is given to the nuclear forces; space and cyberspace as warfighting domains; command, control, communications, computers and intelligence, surveillance, and reconnaissance (C4ISR); missile defence; joint lethality in contested environments; forward force manoeuvre and posture resilience; advanced autonomous systems and resilient and agile logistics [21] (p. 6). The focus of U.S. armed forces’ modernisation is on creating a lethal force. However, some of the emerging technologies that will be invested in for potential high-end warfare could also have value in the counterterrorism fight, such as artificial intelligence for target identification.

The U.S. National Defense Strategy is a textbook illustration of the dynamic character of interrelation between the development of defence strategies and technology innovations. The above-mentioned game-changing technologies certainly evolve innovative operational concepts. Therefore, it noticeably states that “Modernization is not defined solely by hardware; it requires a change in the ways of organisation and employment of forces. Besides, it “must anticipate the implications of new technologies on the battlefield, rigorously define the military problems anticipated in a future conflict, and foster a culture of experimentation and calculated risk-taking.” [21] (p. 8). Furthermore, the Strategy puts a strong emphasis on the process of cultivating workforce talent in parallel to new technologies development and capabilities acquisition. “Recruiting, developing, and retaining a high-quality military and civilian workforce is essential for warfighting success. Cultivating a lethal, agile force requires more than just new technologies and posture changes; it depends on the ability of our warfighters and the Department workforce to integrate new capabilities, adapt warfighting approaches, and change business practices to achieve mission success” [21] (p.8).

Germany

The White Paper on Security Policy and the Future of the Bundeswehr [18] is the current key German document on security policy. It is a strategic review of the current state and future course of German security policy and the development of the Armed Forces.

The document identifies a broad range of previously unknown challenges to Germany’s security. They differ in terms of the intensity of potential damage, the immediacy of their impact on countries’ security, and the long-term consequences. Besides, the range of risks to German security is becoming broader, more diverse, and increasingly unpredictable.

Among the most important security challenges are defined, the transnational terrorism; challenges from the cyber and Information domain; the use of digital communication to influence public opinion; interstate conflict; the renaissance of traditional power politics, which involves the use of military means to pursue national interests; hybrid warfare strategies and methods; fragile states and poor governance; threats to Information and Communication Systems, Supply Lines, Transportation and Trade Routes as well as to the Secure Supply of Raw Materials and Energy; Climate Change; Uncontrolled and Irregular Migration; Epidemics and Pandemics; radicalisation potential as a result of limited prospects in rapidly growing societies [18] (pp. 35-45).

To respond to this wide spectrum of security risks, Germany will pursue the following strategic priorities:

- Guaranteeing a Whole-of-Government Approach to Security;
- Strengthening the Cohesion and Capacity to Act of the North Atlantic Alliance and the European Union
- Unhindered Use of Information and Communication Systems, Supply Lines, Transportation and Trade Routes as well as the Secure Supply of Raw Materials and Energy;
- Early Recognition, Prevention and Resolution of Crises and Conflicts;
- Commitment to a Rules-Based International Order (pp. 48-52).

The White Paper places particular emphasis on the goal to define national key technologies, the availability of which must be ensured for reasons of national security and, if necessary, through coordination and cooperation with our European partners. These key technologies are based on the military requirements of the Bundeswehr, on foreign, security and European policy interests, on Alliance commitments, and Germany’s responsibility. They are subject to regular review [18] (pp. 74-76).

Innovation is indicated as a key to the future of the Bundeswehr to deliver effective protection and ensure the superiority of armed forces. Therefore, the Bundeswehr needs to be receptive to this new notion of innovation in armaments.

To achieve this goal, the White Paper recommends in the long term:

- to focus more on the innovation outside the Armed Forces own R&T;
- to approach new drivers of innovation, such as start-ups and the digital economy as a whole;
- to develop strategic management and target system for the R&T and innovation portfolio; to make available resources for explorative, disruptive research that is not based on specific individual developments;
- to engage in a debate, together with parliament, about a new risk management culture that is appropriate to more complex developments;
- to consider the development of an agency or enterprise that functions as an interface to innovative actors and, where necessary, also manages resources for investment in studies or start-ups in key technologies [18] (pp. 131-132).

Defence strategy – technology developments interrelations

In this last section of the second chapter, we are going to present some conclusions based on the review of defence and R&D strategies of the countries under scrutiny related to the dynamic character of interrelation between the development of military/defence strategies and technology innovations. They can be summarised as follows:

First, most of the analysed strategic documents follow the common ENDS – MEANS – WAYS paradigm described in the previous section of this chapter. The ends include determination of national interests, the means – represent the calculation of the resources needed to protect those interests and the ways to describe how to achieve the identified strategic goals.

Second, there exists a shared assessment of the international security environment as complex, dangerous and unpredictable. Besides, the MS share a common perception of security risks and threats, as well as the understanding that no MS alone will be able to cope with the situation. Therefore, the analysed strategies emphasise their international character and the will to cooperate in achieving strategic defence objectives.

Third, the analysis confirmed the fact that the technologies presented in table 1 fundamentally and directly influence defence strategy development at grand strategic and theatre strategic levels. The influence on the lower levels – operational and tactical is not so clearly presented. This conclusion does not mean that defence technology innovations do not affect tactical and operational levels. On the contrary, this effect will be seen with the modernisation of tactics to apply new military equipment, organisational transformation and restructuring of the military formations, changes in recruitment and retention of military personnel, education and training, etc. There might be postulated also a reverse correlation, namely the new type of conflicts may inspire defence strategy thinking and development of innovative tactics of modern warfare which may call for new technologies development. The rapid technological developments will require very short reaction time and even pro-active strategic studies to forecast emerging disruptive technologies and their implications on the defence strategy advancement.

Fourth, the analysis confirmed the hypothesis concerning action-reaction dynamics that unfold within each layer of defence strategy because of the impact of new technology. Clear examples in this regard are the development of strategic nuclear missiles and missile defence systems, capabilities for cyberattacks and cyber defence, etc. The process of development of new defence technology is coupled with the improvement of technologies to counter possible threats and this implies new concepts, strategies, doctrines and tactics development to be adequate to the changing strategic environment.

Fifth, the analysed strategic documents, both at EU and national level, put particular attention to the role of defence innovation and R&D programmes to develop new defence capabilities and to achieve the strategic defence goals. Some documents clearly define the central role of science as a "force multiplier". Therefore, it must become a key priority of defence policy and planning and an inevitable part of the strategic policy and decision-making process. The review confirmed the dynamic character of interrelation between the development of defence strategies and technology innovations.

Sixth, the leading role of emerging technologies in the process of defence strategies and capability development is undisputed and indispensable, but at the same time, a holistic approach is applied that addresses the full spectrum of defence capabilities development, namely organisation, people, processes and culture.

Seventh, in most of the analysed strategic documents there is a firm commitment to the developing cooperation in the field of defence industry within EU, by capitalizing on multinational cooperation opportunities in the framework of NATO and EU initiatives. The focus is put on the integration of the research and industrial potential in the area of defence of the EU and the Member States.

Eight, some of the analysed documents worn about possible negative implications from the rapid technological developments that must be taken into account when new defence strategies are developed because of this trend can contribute to rising instability in the strategic environment. The rapid spread and availability of various technologies are now enabling medium-sized states, groups and even individuals to acquire or develop capabilities previously only accessible to a limited number of countries.

Ninth, along with the identified common understanding on how defence strategy can be affected by technology innovations and common approaches in dealing with emerging security challenges, some differences in defence strategy development have been identified. The differences are at the level of investments in R&D and approaches to develop the national industrial base.

Tenth, obviously the ICT have the most influential impact on the development of defence strategies in the context of rapidly growing cyber threats and hostile informational actions. The new ICT have important advantages, but also they can create information dependence on the military command systems. Besides, the increasing exposure of modern societies to digital technologies and the interconnection among people and organisations can increase their vulnerability. This is another important lesson that has to be incorporated into the defence decision-making process.

Improving research & technology – defence strategy relationships

The review of different EU and national defence and R&D strategies made in the previous sections allows conveying some recommendations on how to improve science & technology – defence strategy relationships.

First, in some of the analysed strategic documents, the issue of lack of scientific-technological and industrial knowledge in the EU defence sector is alarmed which rises the risk lagging behind the US and other global actors. Therefore, the issue of attracting, retaining and motivating of qualified R&D experts is of key importance for the future of EU defence capabilities acquiring.

Second, the identified trend that technological innovations in civilian domain outpaced the traditional defence R&D also deserves attention to military strategists and decision-makers because they have to choose or combine two approaches: 1) to take advantage of technologies designed for civilian use; 2) to find a way to stimulate defence innovation and R&D sector which means to identify strategic industrial and technological activities in the field of defence and security and to keep the list regularly updated.

Third, it is of crucial importance for the military analysts and strategic thinkers to conduct constant horizon scanning to understand evolving technology opportunities and threats to provide scientific evidence, advice and coherent multi-disciplinary analysis to support strategic decision-making in defence domain. One of the best possible approaches to achieve this goal is to create and maintain a pool of Subject Matter Experts in the technology and defence strategy domains to evaluate different alternatives for policy options [23].

VI. Conclusions

This final section of the article presents, in brief, the outcome from the study on the evolution of the concept of defence strategy in the light of the identified global trends in the political, social, economic, environmental and technological domains. Besides, it summarises also the findings regarding defence strategy – technology development nexus at different layers and dimensions of the strategy and some recommendations to defence strategists at the EU and its MS.

First, the analysis of the strategic documents of the EU and the MS reviled a tendency towards broadening of the understanding of the term "strategy". An overarching term appears that covers in addition to the military also political, economic, diplomatic, technological etc. components of the strategy. This trend is visible in the EU Global Strategy for the implementation of the Common Security and Defence Policy. Besides, the analysis shows that most of the authors identify several layers and dimensions of strategy: grand strategy (ends, national interests), theatre strategy, sectoral strategies (military, diplomatic, economic, information, technological, etc.). Moreover, they identify strategic, operational and tactical levels of war. Finally, yet importantly, the military scholars broadly accept the ENDS - WAYS and MEANS paradigm and analyse the complex interrelationships among these three core elements of strategy.

Second, the analysis confirmed the hypothesis that the new emerging technologies have not the same effect on different layers and dimensions of defence strategy. Most powerful is the influence on the grand strategic and strategic levels. Concerning operational and tactical levels, the new technologies also have their outcome, which can be seen in innovative approaches to planning and caring out military operations, modernisation of tactics, techniques and procedures to use advanced technologies, etc. Additionally, the analysis confirmed the hypothesis that the defence strategy – technology development nexus may be viewed as double-sided. On the one side, the emerging disruptive technologies directly and powerfully influence defence strategy development. On the other side, the dynamic and unpredictable strategic environment requires innovative defence strategies that need new technologies to achieve the strategic goals of the EU and its MS. Finally, the impact of technology on different layers of defence strategy should be analysed alongside two directions: a vertical one, consisting of the different actions across the different layers, and a horizontal one, which represents action-reaction dynamics that unfold within each layer, because of the impact of new technology.

Third, the analysis of the trends in the development of new and emerging technologies shows that they will significantly change the nature of the war in the Information age. In such a situation the interconnection among science, strategy transformation and warfare will grow extensively. The analysis of future technology trends shows that the tomorrow's warfare will be dominated by digital battles carried out by machines (some of them autonomous), interconnected in global networks, and fuelled by the enormous amount of data. This will pose a sober question about the vulnerability of information and the ways and means to protect it.

The key question to be faced by the defence strategists is to clearly define the ways & means to transform the defence system from the current state (AS-IS) to the required end-state (TO-BE) to be effective and efficient in a digital war. This major shift in the nature of warfare imposes requirement the strategy to take into account the innovative applications of new technologies in combination with fundamental changes in doctrine, operational practices, organizational processes and the human factor.

Fourth, the new character of the warfare and the growing access to new technologies, particularly disruptive ones, will require changes in the strategy to be able to mitigate effectively the growing threat that can be posed by non-state actors, terrorist groups, etc.

Fifth, the finding that the rapid development of technology might challenge interoperability in a coalition deserves also particular attention on behalf of defence strategists because the coalition operations are the most probable format of using forces in the future. In this respect, it is critical to focus on the whole spectrum of interoperability in coalition format (doctrine, technology, organization, training, materiel, leadership and education, personnel, etc.).

Sixth, the identified trend of application of new technologies in the warfighting such as artificial intelligence, autonomous systems and human enhancement techniques also needs the attention of defence strategists and planners because of the rising ethical and legal concerns. If a non-state actor can neglect these issues, for the EU and the MS it is essential to follow the international law and the ethics/moral criteria. The future defence strategies must give also answer to this question.

Finally, yet importantly, the main goal of future warfare will be to win the hearts and minds of the people. In this regard, it deserves attention identified risk potential adversaries to use global networks to disseminate false or misleading information and to "create" fake news to influence public opinion and decision-making in the MS and at EU level. Besides, the heavy reliance of the military on digital technologies in case of denied access as a result of cyber-attacks, calls for innovative strategic vision and action to prevent such threats and to respond effectively.

ACKNOWLEDGEMENTS

This article is based on the results achieved in the framework of the EU project Predictive methodologY for TecHnology Intelligence Analysis (PYTHIA).

PYTHIA has received funding from the European Union's Preparatory Action on Defence Research under grant agreement No 800893.

The information contained in this document reflects only the author's view and the European Defence Agency is not responsible for any use that may be made of the information it contains.

REFERENCES

[1] A European defence research & technology strategy, available on https://eda.europa.eu/what-we-do/our-current-priorities/strategies/ResearchandTechnology, accessed on 10.07.2018.

[2] A Global Strategy for the European Union's Foreign and Security Policy: "Shared Vision, Common Action: A Stronger Europe" (2016). Available on: https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf, accessed on 12.09.2018.

[3] Defence and national security strategic review, 2017; available from https://www.defense.gouv.fr/english/layout/set/print/media/documents-telechargeables/pdfdefense/defence-and-national-security-strategic-review-20172, accessed on 17.07.2018.

[4] Defence strategy of the Republic of Poland, 2009; available from https://www.files.ethz.ch/isn/156791/Poland%202009.pdf, accessed on 24.07.2018.

[5] EDA Defence Matters Magazine, Issue 14, 2017, "Defence Innovations: A Journey to the Future", Available from https://www.eda.europa.eu/webzine/issue14, accessed on 12 September 2018.

[6] EU 2018 Capability Development Priorities, available on https://eda.europa.eu/info-hub/press-centre/latest-news/2018/06/28/new-2018-eu-capability-development-priorities-approved, accessed on 04.07.2018.

[7] Framework for future alliance operations 2018 Report, Technology implications, pp. 46-48, Available from http://www.act.nato.int/images/stories/media/doclibrary/180514_ffao18-txt.pdf, accessed on 12 September 2018.

[8] Ministry of defence of the Republic of Bulgaria. The National Defense Strategy of the Republic of Bulgaria, 2011, updated in 2016. Available from: www.mod.bg, accessed on 10.06.2018.

[9] National defence strategy 2015-2019 – Romania, the Presidential administration; available from http://www.presidency.ro/files/userfiles/National_Defense_Strategy_2015_-_2019.pdf, accessed on 17.07.2018.

[10] NATO Science and Technology Organization Technology, AC/323-D (2017)0006, STO Tech Trends Report 2017. Available from http:// www.sto.nato.int/, accessed on 10 July 2018.

[11] NATO Strategic Concept "Active Engagement, Modern Defence", available from https://www.nato.int/cps/en/natohq/topics_56626.htm?selectedLocale=en, accessed on 23.07.2018.

[12] Overarching Strategic Research Agenda and CapTech SRAs Harmonisation (OSRA), Available from https://eda.europa.eu/docs/default-source/brochures/eda-osra-brochure.pdf, accessed on 12.09.2018.

[13] Strategic review of defence and national security 2017, Key points; available from https://cn.ambafrance.org/IMG/pdf/strategic_review_of_defense_and_national_security_2017_-_key_points.pdf, accessed on 17.07.2018.

[14] Strategy for research and technologies in security and defence of the Republic of Bulgaria, Council of Ministers of the Republic of Bulgaria, 2015.

[15] The EU Capability Development Plans, Available from https://www.eda.europa.eu/what-we-do/our-current-priorities/capability-development-plan, accessed on 12.09.2018.

[16] The Strategic Foresight Analysis (SFA) 2017 Report. Available from: http://www.act.nato.int/images/stories/media/doclibrary/171004_sfa_2017_report_hr.pdf, accessed on 17.07.2018.

[17] The UK International Defence Engagement Strategy, Ministry of Defence UK, available at www.gov.uk, accessed on 17.07.2018.

[18] The White Paper on Security Policy and the Future of the Bundeswehr, 2016, Available from

https://www.google.bg/search?q=The+White+Paper+on+Security+Policy+and+the+Future+of+the+Bundeswehr&rlz=1C1CHBF_enBG794BG795&oq=The+White+Paper+on+Security+Policy+and+the+Future+of+the+Bundeswehr&aqs=chrome..69i57j69i59j0.1272j0j9&sourceid=chrome&ie=UTF-8, accessed on 12.09.2018.

[19] UK Science and Technology Strategy, 2017.

[20] UK Strategic Defence and Security Review, 2015, Available at www.gov.uk, accessed on 17.07.2018.

[21] United States of America National Defense Strategy Sharpening the American Military's Competitive Edge, Available from https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf?mod=article_inline, accessed on 12.09.2018.

[22] White Paper for International Security and Defence, 2015, available from https://www.difesa.it/Primo_Piano/Documents/2015/07_Luglio/White%20book.pdf, accessed on 24.07.2018.

[23] M. Bozhilova, Approach on an expert-based assessment of alternatives, Proceedings of Scientific Conference with international participation Military Technologies & Systems 2013 (MT&S-2013), Sofia, 2014, II-143 - II-153, ISSN 2367-5942 (in Bulgarian).