International Conference KNOWLEDGE-BASED ORGANIZATION
Vol. XXVII No 1 2021

THE NATIONAL SECURITY STRATEGY IN THE CURRENT ENVIRONMENT: FROM DIME TO A DIME-T APPROACH

Maria CONSTANTINESCU

"Carol I" National Defence University, Brașov, Romania
mconst_ro@yahoo.com

Abstract: *The contemporary security environment is characterized by Volatility, Uncertainty, Complexity and Ambiguity (VUCA), the use of hybrid warfare and grey zone conflicts, generating the need to adapt the national security strategies to the changes demands of the environment. In this context, the instruments of national power (diplomatic, information, economic, military) should be used in an integrated manner, in order to provide a more comprehensive approach to national security. The technology has become an integral part of the life of the society, and as such it should be taken into consideration as an instrument of power and highlighted as a major component of a national security strategy. The paper proposes a DIME-T approach to national instruments of power, by analysing the complex implications of technology on all the areas of security.*

Keywords: security, VUCA, DIME, instruments, technology

1. Introduction

The contemporary security environment is characterized by a combination of intense rivalry and competition, between state and non-state actors, in a high Volatility, Uncertainty, Complexity and Ambiguity (VUCA) environment. Most of the conflicts taking place in the last decade clearly highlight a tendency towards the use of asymmetric methods, across multiple confrontation domains, which are no longer limited to military actions.

In this context, the security strategies of many countries, including Romania, have tried to adapt to the changing environment, but they are still disproportionately focusing on the military side of the conflict and less on the asymmetrical, but not less dangerous threats. The threats to national security (that may also have military implications) can come from a variety of areas, which were not traditionally described in such planning documents: climate change, disinformation and influence campaigns, dependence on technology, economic dependence on a specific country or on a sole supplier, emergence of new technologies, high inequality, increased connectivity etc.

Providing a comprehensive and realistic approach to national security means changing the paradigm of what means security, to encompass all the novel risks and threats, regardless of their nature, but also developing an appropriate framework of response, involving the development of strategies and integrated responses from various ministries and agencies.

The purpose of this paper is to explore a more comprehensive approach to national security, including the significant impact the technological advance has on security. The paper is the result of a qualitative research, as main research methods the literature review, case studies in the form of various countries'security strategies and

DOI: 10.2478/kbo-2021-0004

interviews with experts from security and defence area.

2. From DIME to DIMET – a new approach to national security

According to George Kennan, national security can be defined as “the continued ability of the country to pursue the development of its internal life without serious interference, or threat of interference, from foreign powers” [1]. This definition sets the foundation for the modern perception of national security, but the current security environment is a lot more complex than the post WWII environment in which it was elaborated. Many countries now faced the dilemma of redefining the borders of what means security, through the use of concepts such as societal resilience or whole of government approach to national security.

The main purpose of a national security strategy is still viewed as providing the framework for the future use of the instruments of power (the famous DIME – diplomatic, informational, military and economic) for the achievement of the national interests, in line with the national values.

2.1. National security in the age of technology

One of the key features of the current security environment is the blurring of the line between war and peace, between competition and conflict, into what is called the grey zone. Conflicts in the grey area are characterized by intense competition, at political, economic, information and military level, beyond the normal inter-state relations, but below the threshold of a full armed conflict [2].

Within the grey zone conflicts, technology plays an important role. Although technology has influence warfare before, through the development of new weapons, communications, means of transport etc, what sets the current situation apart is the pace of technological advance and the implications of technology on the national security, deriving not only from the advances in the military area, but also from countless other areas, with implications on the whole society. Never before has the spread of technology developed by civilian companies and designed for civilian use (such as social media platforms, computer science, Artificial intelligence, autonomous vehicles, nanotechnologies, biotechnologies etc.) has had such an profound impact on the national security, generating novel threats, risks and opportunities.

Some of the current challenges to national security can still be defined using an adapted DIME framework, but others require new approaches and courses of action. The increased Volatility, Uncertainty, Complexity and Ambiguity of the security environment (VUCA) is exacerbated by the unprecedented pace of technological development, which that the national security strategies of modern states face challenges in clearly define the threats and risks (a difficult feat in an ever-changing environment), but also in outlining the courses of action using all the classical DIME tools. It can be argued that technology can be included in the I (information), E (economic) or M (military) areas of the DIME approach, but this view ignores the complex and interconnected nature of the technological changes modern society faces.

Separating the various aspects of technology between the three aforementioned tools of national security leads to a lack of integration and correlation. Technology now crosses the boundaries between the military and civilian applications, can be used in new and unexpected ways by state and private actors alike. Mitigating the VUCA aspects of the security environment starts with the development of an integrated and comprehensive grand strategy, supported by sector related strategies: an economic strategy, a military strategy, an information strategy, a societal development strategy, a technology development strategy etc. These strategies should serve as a guidance for the coordinated activities of various state structures, in close cooperation with the civilian companies and NGO'S.

2.2. Adding the Technology to the DIME approach

A national security strategy should take into consideration all time horizons, as the risks, threats and required ways of action may be different. Usually, on short term, the internal political environment (the policy of the ruling party or coalition) and the most pressing threats will be the most important factors to shape a country's security strategy. On medium term, factors such from the DIME framework (diplomatic factors, economic inequality, social trends, increased connectivity, the development of societal resilience to information warfare etc) will gain predominance. The classical approach to developing a security strategy tends to relegate complex issues like social issues, demographics, environmental issues and technological issues to the long term approach to national security. The reason derives both from the complexity of measures required to tackle such complex issues, but also from the fact that security strategies are political documents, endorsed by specific political parties, which leads to the tendency to postpone less popular measures, or measures which take longer time to show results, in an effort to placate the electorate.

Nevertheless, the current pace of technological advance signifies that technology can no longer be viewed as a long term component of national security, but as a medium and even a short term factor of influence.

Modern societies face a myriad of challenges to their security, some of them completely novel:

- a rearranging international order,
- emergence of new technologies and technology leaders, combined with inequalities between countries regarding the access, control and distribution of technology,
- enhances world wide access to information and communication, increased digitalization of societies,
- increased interconnectedness of the world economies, combined with a high specialization,
- expansion of competition and conflicts in novel spaces, from the physical and economic space to the information, cognitive, or cultural space, in a grey zone conflict paradigm..

Technology can influence national security in all the above mentioned areas. One of the most obvious spheres in which technology influences security is the *military area*, in which the access to high technology weapon systems can be a distinct advantage. The rapid pace of the technological advances in recent years and the spectacular ways in which new technologies (such as UAV's) have shaped the operational environment makes a long term approach to technology in a national security strategy, unsupported by short and medium term measures, no longer realistic. It would be tempting to consider that only the large countries with strong economies should be concerned with this issue, as they have the resources to invest in research and development and the acquisition of modern, high tech equipment and weapon systems. Nonetheless, small and medium-sized countries cannot afford to ignore the implications of this phenomenon on the operating environment, even if they do not have the same resources at their disposal. The example of the use of drones by Azerbaijan against Armenian land forces in the Nagorno Karabah conflict is a case in point.

Advances in technology will likely influence the operating environment of the future in direct and indirect ways, that should be identified in the national security strategies and for which further ways of action should be outlined. The *direct implications* derive from the development of new types of weapons systems, but also from their increased complexity and degree of integration, through innovative concepts such as autonomous weapons swarms or the Internet of Battlefield Things.

Globalization will definitely play a catalyst role, through the increased accessibility of technology deriving from diminished costs due to economies of scale and the development of less sophisticated versions of extremely expensive equipment by several other countries, among which China and Turkey can be mentioned. Developing countries are moving into the field of research, development and production of military systems that were until recently the prerogative of Western countries, using a variety of methods (from sending students to prestigious universities or to work as interns to economic and industrial espionage) [3] to obtain know how. Technological advancement can also have *indirect*, but no less significant, implications on military security through technologies developed for civilian use, but which can also be used for military purposes, such as IT technology, nano-robots, the use of discoveries in the field of neuroscience and biology for increasing the physical, cognitive or endurance abilities of the military and the human-technology integration (the concept of soldier of the future), to name just a few.

Advances in information technology will create new synergies between combinations of advanced precision weapons, improved C4ISR systems and widespread use of artificial intelligence and robotics. As a special category of emerging technology with potential military implications we can mention the advanced biotechnologies, which have the potential to provide improved physical and cognitive performance of the military of the future.

Economic security is another area directly influenced by the technological advances. The impact of technology and innovation on the economic development has been extensively studied by economists. In the words of Sachs and McArthur "technological innovation is almost certainly the key driver of long-term economic growth." [4] A country's economic development can no longer be separated from the access to advance technology, from IT to industrial robots, the use of 3 D printers, nanomaterials etc. Unfortunately, the VUCA acronym also applies to the economic environment, increasing the challenges states have to solve in short and near term. The need for a clear strategy for technology and innovation based economic growth is even greater, as the lingering effects of the 2008 financial crisis, the effects of the COVID 19 pandemic, the increased competition between states increase the uncertainty and slow down economic growth. Many states are faced with difficult choices in this respect, between short term decisions to mitigate the effects of disruptive events that may have medium and long term negative impact on technological development and economic security. The budgetary constraints generate the temptation to focus solely on the present, but investments in long term sources of economic security and development (education, research, technology, infrastructure, societal resilience) should not be overlooked. Technology, innovation and creativity should be acknowledged not only as crucial factors for economic development, but also as essential components of national security.

Another sphere of security directly influenced by technology is the area of societal security, defined as "the ability of a society to persist in its essential character under changing conditions and possible or actual threats" [5]. Apparently related to the modern buzzword of resilience, societal security can be viewed as encompassing all the factors that threaten a society's collective identity and cohesion, thus partially overlapping with the areas of cultural security and information security. The unprecedented spread of information and disinformation, the use of information warfare tools, the emergence of social media platforms and of concepts such as post truth, alternative facts and fake news can generate extensive damage to a society's fabric, and technology is a key enabler. In the authors' opinion, technology should have a separate place as a tool of national power, as it can be used in numerous other areas that may threaten societal security, beyond the realm of information security. For instance, the combination of bio-engineering with artificial intelligence technology, the concept of the "bio-enhanced human" (an individual endowed with a capacity in a specific field that goes beyond the normal functional range of humans in general) [6] can create the premises of fundamental changes in a society and even in the concept of human identity itself.

3. Conclusions

The multipolar VUCA security environment, characterized by hybrid warfare, grey zone conflicts and unprecedented technological change requires an approach to national security that integrates all instruments of power into a comprehensive framework.

Consequently, all the tools of national power (including the use of technology) should be used in an integrated manner and national security could be considered as the ultimate strategic level joint capability – developed based on a common goal and ways of actions through the integration of efforts of all the state entities.

Governments can play a crucial role in using technology as a instrument of national power, by creating the regulatory framework, providing a clear, whole of nation vision and strategy, stimulating and supporting private companies, research institutes and other structures to enhance innovation. A clear vision and the will to implement technology and innovation oriented medium and long term policies in the fields of education and training, human capital development, entrepreneurship, infrastructure, tax reform are crucial for a country's security.

Technological advances originate predominantly from the civilian society, but the state entities have the responsibility of encouraging, sustaining and providing the framework for the use of these advances for the provision of national security. This approach encompasses a broad range of actions, from improving the technical education, providing opportunities for young researchers to remain in the country, providing facilities for start-ups and technology companies, increasing the cooperation between the armaments industry and civilian companies etc.

Besides the usual ministries and agencies (ministry of defence, ministry of internal affairs, intelligence services, ministry of foreign affairs) which are traditionally involved in developing and implementing the security strategy, other state bodies should be involved. The ministry of education, for example, can play a very important role in developing societal resilience, through increasing the level of education and computer literacy and decreasing the level of vulnerability of the population (and especially of the younger generations) to disinformation. The ministry of culture can play a role in reasserting clear values and constructing a national identity that does not need a common enemy (in a counterproductive us versus them approach), that can mitigate the divisive effects of information warfare tools. The ministry of health should also play a crucial role in developing societal resilience (during unforeseen events such as a pandemic, but also during more "normal times"), by promoting public medical education and presenting a reliable, scientific view on artificially generated controversies such as the effectiveness of vaccines.

The modern society is the most technological advanced and the most technological developed society in the history of mankind. Technology has permeated all the aspects of the society and the security sphere is no exception. Consequently, technology, in all its aspects, should be viewed as a crucial security factor and as such treated as a priority area of the national security policy.

References List

[1] Kennan, G. Comments on the General Trend of U.S. Foreign Policy, George F. Kennan Papers, Princeton University, dated 20 August 1948. Vol. XVIII, No. 66 - 2012 XXIII (80) – 2017. Accessed on 10.03.2021. Available from https://library.princeton.edu/special-collections/divisions/public-policy-papers

[2] Votel J, Cleveland C, Connett C, Irwin W. Unconventional Warfare in the Gray Zone. Joint Force Quarterly 80, 2016. Accessed on 04.03.2021. Available from https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-80/jfq-80_101-109_Votel-et-al.pdf

[3] Hannas W, Mulvenon J, Puglisi A, Chinese Industrial Espionage Technology Acquisition and Military Modernisation, Routledge, 2013

[4] Sachs J, McArthur J. Technological Advancement and Long-Term Economic Growth in Asia, editor Bai C, Yuen C. Technology and the new economy. MIT Press. 2002. 157-185

[5] Buzan B. People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era. Rienner L. ECPR Classics Series. 1991.

[6] Vassiliou A. The Bio-enhanced Soldier In International Law: classification and obligations. Accessed on 19.04.2020. Available at https://finabel.org/the-bio-enhanced-soldier-in-international-law-classification-and-obligations/