MULTINATIONAL APPROACHES IN MANAGING EMERGING AND DISRUPTIVE TECHNOLOGIES. CHALLENGES AND OPPORTUNITIES

Dragoș ILINCA, PhD[*]

Abstract: *The last decades were marked by substantial technological achievements with a constant expansions of applicability domains, including on security and defence. Generally, the new technologies are known under the title of emergent and disruptive which has a substantial note of generality. From this perspective, a particular sense of ambiguity is affecting the possibility of categorizing the new technological trends. There is a general consensus for several categories, especially artificial intelligence, autonomous systems, big data, which have a growing applicability supported by innovative approaches and use of dual-use capabilities. The challenge posed by EDTs are two folded, in terms of opportunities provided for overall progress of human society as well as regards the challenges and risks for contemporary society. Finding a balanced approach is one of the priorities for the coming period, whether we speak on national undertakings or multinational ones. The role of NATO and EU in this undertaking is incremental, especially for supporting national efforts and maintaining technological edge.*

Keywords: *NATO, EU, CSDP, hybrid, emerging and disruptive technologies, artificial intelligence, interoperability, defence capabilities*

There is no doubt that Emerging and Disruptive Technologies (EDT) is one of the most debated topics nowadays. To an equal extent, any discussions on this subject is a more complex than ever considering the overall industrial and economic dynamic and interlinkage between human factor and technological advance. Subsequently, approaching disruptive technologies requires certain conceptual clarification, especially from the perspective of a relative novelty of this feature.

[*] coordinator of research programs at the Institute for Political Studies of Defense and Military History, dilinca@yahoo.com.

From this perspective, the logic question is "what are disruptive technologies?". The existing literature indicates the absence of a generally agreed definition. The beginning is associated with Clayton Christensen (1952-2020), economist and Harvard scholar, which coined the terminology "Disruptive Technology" in the context of his research on the disk-industry development. This invention was further popularized through his reference book "The Innovator's Dilemma" (1997) in which outlined the fundamentals of disruptive theory. It was crafted from a solely industrial and economical perspectives by putting under close scrutiny the capacity of big companies to match constant diversification of market demands while maintaining technological superiority. His conclusions were that most often the big companies failed, even with a proper management, to maintain their competitive edge untouched.

That happened, according to Christensen, because of the way in which the companies are looking to the demands and their obsessive preoccupation to meet only the mainstream markets narrows the attention towards conventional development. This approach is speculated by competitors which acted asymmetrical and by employing more adaptive strategies which has the potential to disrupt, relatively fast, towards them considerable segments of markets and financial flows. From this perspective, Christensen theory proclaimed the dominance of disruptive technologies against the sustaining ones, by highlighting the innovation factor which is more practical in case of the first.

This conclusion is underpinned by a laborious work and statistical data on world largest company performance in comparison with much smaller companies that employed innovation by looking outside of the conventional toolbox. From this perspective, the main characteristics of disruptive technologies could be defined as being simpler, cheaper, smaller, and most important, much more convenient to use[1]. In particular, Christensen anticipated that "internet appliances" will become the leading disruptive technologies that will dominate the market. In this sense, he anticipated the potential of connectivity that internet provided, stimulating thus the development of disruptive technologies.

[1] Clayton Christensen. *The Innovator's Dilemma. When New Technologies Cause Great Firms to Fail*, Harvard Business School Press, Boston, Massachusetts, 1997, p.11.

In this context, the definition generated through Christensen theory describes a process employed by a company with limited resources managed to challenge the leadership on the market of bigger sustainment companies. The success of disruptive theory substantiated very fast, being introduced in almost every domain of our life at a global scale. From this perspective, the shapes and types of disruptive approaches grew exponentially, generating some difficulties in classifying by a given methodology.

The categories which can be called as being “classical” includes: artificial intelligence (AI); 3D printing; smartphones; blockchain; ride-sharing applications; GPS systems; streaming entertainment; social media networks. But this is should be treated only as an indication of the enhanced multidisciplinary of disruptive technology which is facilitated by globalization and general use of the internet as the main communication instrument. Security and defence is one of the most attractive area for implementing disruptive technologies on a variety of aspects, including operational and capabilities development ones. Of course, implementing new approaches in this area is meant to increase the efficiency of the military employment, while changing the general patterns in which future warfare is conducted.

Nevertheless, there are certain side-effects associated or generated by disruptive technologies which require careful consideration. The initial expectations that facilitated the use of this instrument were largely in the economic competitiveness area, concentrated on using the opportunities and advantages offered by disruptive technologies. But implementation exceeded this approach, by creating additional uncertainties regarding the potential negative use of the new instruments. As it was anticipated in the initial stages of disruptive theory development process the contemporary world is under a structural change of the security paradigm. Nowadays, the technological progress is no longer the apanage of states and multinational organization. The high degree of connectivity creates the conditions for a relatively easy access to disruptive technologies of the non-state actors with undefined consequences for the common security. Additional complexity is induced by the extensive geographical profile of disruptive technologies in which transnational character is the dominant pattern.

From this perspective, a particular attention should be devoted to the risks of using disruptive technologies as a weapon with undefined impact on the international security stability. Managing this challenge is placing additional burden on national security efforts, while asking for conceptual adaptation and upgrading the required capabilities. In this quest there are additional questions related to the individual capacity of states to manage adequately this challenge and generate the right type of capabilities. This particular aspect is more difficult to tackle, taking into account the high degree of versatility employed by disruptive technologies which can be depicted in dual-use capabilities.

Furthermore, the technological development pace and constant expansion of the EDT's applicability areas associated with security and defence challenge the overall ability of the states to maintain technological edge. There is a certain agreement on how the profile of emergent and disruptive technologies will evolve for the next decades. In this sense, it can be envisaged four main types&categories in which future EDTs could be integrated, namely:

- Intelligent – will manifest through an integrated exploit of artificial intelligence and will generate knowledge-focused analytic capabilities, and symbiotic AIhuman intelligence to provide disruptive applications across the technological spectrum.
- Interconnected – focused on exploiting the network of virtual and physical domains, including networks of sensors, organisations, individuals and autonomous agents, linked via new encryption methods and distributed ledger technologies.
- Distributed – employing decentralised and ubiquitous large-scale sensing, storage, and computation to achieve new disruptive military effects.
- Digital – trough digitally blend human, physical and information domains to support novel disruptive effects[2].

[2] Science & Technology Trends 2020-2040, NATO Science & Technology Organization, 2020.

NATO approach

All of these aspects, bring into the light once more the relevance of multinational approaches in managing efficiently the implications of disruptive technologies on national security. From NATO perspective, the topic of disruptive technologies in international context was one of the most important features addressed in the Strategic Concept, adopted in 2010, in the aftermath of Lisbon Summit. In this sense, the strategic framework indicated that "A number of 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 NATO military planning and operations"[3].

In addition to the operational related aspects, disruptive technologies were approached from their impact on NATO's capacity to project and sustain its defence and deterrence posture. In this respect, a special emphasis is placed on internal ability to evaluate permanently the implications of technological advance and, subsequently, the way in which these evolutions are properly reflected in the overall context of defence planning system.

From this perspective, the NATO Summit in London (3-4 December 2019) made the very first steps in developing a comprehensive strategy on disruptive technologies. The need to ensure the North Atlantic Alliance technological edge it was highlighted in connection with the overall undertaking to enhance resilience of member states[4]. In this vein, it was adopted a roadmap, including the necessary steps both conceptual and institutional ones. For the last aspect, NATO internal architecture was further consolidated by creating a dedicated structure, NATO Innovation Board, which will be responsible with overall coordination of this topic in the Allied context. At the same time, it is responsible for integrating and disseminating, at NATO level, guidance and recommendations for this topic being also the main interface with civil society and private sector on

[3] NATO Strategic Concept for the Defence and Security of the Members of the North Atlantic Organisation "Active Engagement, Modern Defence", available at https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf, accesed at 14.10.2021.

[4] London Declaration available at https://www.nato.int/cps/en/natohq/official_texts_-171584.htm, accesed at 14.10.2021.

subjects related with disruptive technologies. It is placed under the Deputy Secretary General coordination authority which consolidated the comprehensive character of its work. Furthermore, the innovation aspects were consolidated at the level of Strategic Commands as well as in the structure of NATO's agencies, creating, thus, an integrated matrix for managing the complexity of this subject.

In July 2020, NATO created Advisory Group on Emerging and Disruptive Technologies (EDTs) designed as a strategic reflection task force including 12 members with relevant background in private and academic sectors. The main job for this entity was to provide recommendations on the priorities on which NATO should focus in relation with disruptive technologies. This approach was a two-ways street, aiming both at identifying the opportunities on which NATO should take it into account as well as to depict the challenges and threats that could be induced by the EDT development.

All of these aspects, were approached by EDT Group the practical recommendations covering both potential operating models to be assumed in NATO activities as well as the ways for increasing the level of technical literacy across NATO structure[5]. In September 2020, the reflection group presented its recommendations which were taken into account in developing the NATO strategic approach. Based on the mandate provided at the outset, the recommendations covered institutional aspects by taking the necessary steps to create a network of Innovation Centers developed by member states as well as to develop and support financing mechanism focused on innovation. At the same time, the idea of consolidating the partnerships conducted by NATO was underlined in the recommendations made by reflection group with a special focus on creating cooperation formulas in relation with private sector and academia.

Special attention was paid during ministers meeting that took place in 16-17 February 2021 by agreeing the general framework of a NATO innovation defence initiative underpinned by an Allied strategy on emergent and disruptive technologies. Under the name "Foster and Protect: NATO's

[5] NATO Advisory Group on Emerging and Disruptive Technologies, Annual Report 2020, available at https://www.nato.int/nato_static_fl2014/assets/pdf/2021/3/pdf/210303-EDT-adv-grp-annual-report-2020.pdf, accesed at 14.10.2021.

Coherent Implementation Strategy on Emerging and Disruptive Technologies" the new strategy has two main priorities. First, to optimize the way in which NATO is approaching EDTs, from the perspective of strengthening its technological edge, especially on dual-use capabilities development. Second, foster relevant reflection process to aim at creating best practices for ensuring adequate protection against threats emanating from the use of these technologies.

As Secretary General emphasizes during this event, a particular focus was placed on capitalize the advantages of technological edge in order to increase the interoperability[6] in terms of forces and capabilities provided by member states. In this sense, it was underlined the need of a dedicated initiative in this area, supported collectively by member states contributions and, most of all, the adequate resource investment. In support of this undertaking, the primary rationale was to avoid creation of potential gaps between member states in the light of EDTs. This situation is likely to appear in case of deepen asymmetry between the state of technological development at national level. From theoretical point of view this is a case one of the most challenging aspects regarding the development of a concerted approach in multinational formats. The risks of unequal development of capabilities that use EDTs is omnipresent, being directly influenced primarily by the economic potential of every member state. From this perspective, the plea of NATO Secretary General was focused on maintaining an adequate level[7] of investment in these technologies at individual level.

The second pillar of the new initiative was in line of reflection group recommendations regarding the partnership formulas that can be developed by NATO, especially in relations with private sector and academia. From this perspective, it was envisaged the leading role of NATO's undertakings in maintaining technological superiority to support the creation of a positive framework for using emergent and disruptive technologies. Being one of the

[6] Preview of defence ministers meeting by Secretary General, Jens Stoltenberg, available at https://www.nato.int/cps/en/natohq/opinions_181427.htm, accesed at 15.10.2021.

[7] The target commonly used in this regard it is around of 20% allocated to investment out of the total expenses on defence sector.

beneficiaries of using the EDTs, NATO made available its expertise and potential to contribute in drafting adequate guidelines and ethical standards.

Under these guidelines, the practical implementation of the agreed strategic approach on EDTs was structured along several priorities like: artificial intelligence (AI), data and computing, autonomy, quantum-enabled technologies, biotechnology and human enhancements, hypersonic technologies, and space. Implementation process for NATO objectives in every area of priorities it was placed under the coordination of Innovation Board which will ensure a coordinated approach along the main functionalities of North Atlantic Organization.

Furthermore, the Brussels NATO Summit that took place on 14 June 2021 adopted additional measures in support of implementation of the objectives assumed under the new strategic framework. In this sense, it was agreed the creation of a civil-military Defence Innovations Accelerator for NATO (DIANA) in order to stimulate the conceptual and practical cooperation between member states as well as with external actors, especially private sector and academia. DIANA is based on two-pillars structure, encompassing Europe and North-America by gathering various offices and test centres, contributing to a more efficient investment in the new technologies as well as to the overall connectivity across the Alliance in these areas. In the same spirit, decisions adopted during Bruxelles summit included creation of a financial instrument to support the implementation of the new strategy. Under the name "NATO Innovation Fund" it will function based on member states contributions on an opt-in basis, to invest in start-ups working on dual-use and emerging and disruptive technologies in areas that are critical to Allied security[8].

EU approach

Interests for maintaining the technological edge of EU in a globalized world represented a constant feature for the entire process of developing defence and security component. This aspect was underlined by the EU Global Security Strategy adopted in June 2016, in close relation with the undertaking to enhance the EU profile in the international security

[8] *NATO 2030,* available at https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/-pdf/2106-factsheet-nato2030-en.pdf, accesed at 16.10.2021.

context. Emphasizing the specific parameters of globalization and the need to promote active multilateralism EU has to cope with new technologies such "biotechnology, artificial intelligence, robotics and remotely piloted systems in order to avoid related security risks and reap their economic benefits"[9].

Implementing this objective was conducted steadily at EU level by taking into account the very nature of this institution, especially in terms of civil-military interaction under the Common Security and Defence Policy (CSDP) with a proper reflection in terms of capability development as well as operational commitments. In this respect, the problem of taking grasp of technological progresses followed every stage of CSDP development, being integrated in various conceptual and practical undertakings in the field of European cooperation in the field of defence industry.

Corresponding with institutional design of EU after adoption of Lisbon Treaty, the central role in promoting this agenda was shared between EU Council and European Commission with a specific responsibility granted to European Defence Agency as a vehicle for transformation in capability development area. Furthermore, it should be noted the parameters generated in the wake of intergovernmental nature of CSDP which are based on the consensus between member states and voluntary participation in European security and defence cooperation. From this perspective, the initiatives taken in the field of EU technological development followed specific patterns in terms of melting and increasing synergies between various strands of work in industrial development, by ensuring cross-fertilisation between civil, defence and space industries, including improvement use of dual-use technologies. On this path, the Action Plan adopted by European Commission in February 2021, proposed an ambitious agenda regarding an integrated matrix in industrial cooperation. Also, known as "Three-Point Belt Plan", the overarching objectives of this initiative were related with:

▪consolidate the synergies between various programs and initiatives developed in the last decades with applicability in the field of security and

[9] *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*, p.43.

defence and in support of the political agreed objectives by EU Global Strategy;

▪optimize the financial support and increase the technological dividends of research and development undertakings in defence and space;

▪facilitate the use of civil industry achievements and innovation in defence cooperation projects[10].

In implementing this ambitious agenda, consolidation of innovation character of European cooperation is instrumental for increasing the competitiveness and strategic relevance of capabilities. There were envisaged several instruments to be developed under the coordination of European Commission. First, the creation of an "Innovation incubator" design to maximize the innovation output across the priority industrial areas and potentially increase the connectivity with other sectors. The anticipated shape of this undertaking is a network type, connecting different EU structures and institutions with relevant responsibilities in these areas. Another initiative is related with the creation of "Defence Innovation Networks" which will facilitate the cooperation in academic field, acting as intermediaries and facilitators between customers and civil companies which would have additional opportunities to valorize their products and technologies.

As regard cyber security and cyber defence, the main priorities are focused on setting-up the Cybersecurity Competence Centre (CCC) and the Network of National Coordination Centres. These structures will contribute to the protection of European economies and societies, while maintaining and promoting research excellence and reinforcing the competitivity of European industries in the field of cyber security. In addition to these elements, there are several flagship projects that are to be developed under Commission coordination in the field of: drone technologies, space-based global secure communication system and space traffic management. Under this approach, there were defined a substantial set of critical technologies that are relevant in terms of consolidating synergic approach between these domains, as follows:

[10] COM(2021)70, 22.2.2021 – Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Action Plan on synergies between civil, defence and space industries, p.1.

▪On electronic & digital – artificial intelligence, advance analytics and big data; cybersecurity and cyber defence; digital forensic technologies; high-performance computing, cloud and data spaces; photonics; ultra-low power micropocessors, lightweight printed or flexible electronics; quantum technologies; secure communications and networking; sensors.

▪On manufacturing – advanced and additive manufacturing; advanced materials technologies and sustainable materials by design; nanotechnologies; robotics; semiconductors and microelectronics.

▪On space & aeronautics – space technologies; secure precisions timing, positioning and navigation technologies; high-definition Earth Observation technologies; satellite – based secure communication and connectivity.

▪On health – biotechnologies; CBRN.

▪On energy – energy technologies (incl. storage, resilience, renewables, hydrogen and nuclear).

▪On mobility – autonomous system.[11]

Under these auspices, the approach on EDTs is equally ambitious and multidisciplinary. In the same vein, it can be argued that EU is approaching these technologies from a wider civilian and military user's perspective. As European Commission President, Ursula von der Leyen stated in September 2001, "The nature of the threat we face is evolving rapidly; from cyber-attacks to the growing arms race in space. Disruptive technologies have been a great equalizer in the way power can be used today by rogue states or non-state groups"[12]. In the last years this topic was approached structurally as it is the case of Artificial Intelligence for which it has been developed an extended inventory of conceptual support.

Furthermore, in 2018 was published the first Coordinated Plan which has the primary role to consolidate the interaction public-private partnerships and research and innovation network, all of these at the national level. This initiative, updated in 2021, is underpinned by a sound financial mechanism provided through different programs financed through

[11] *Ibidem* p.8-9.

[12] State of the Union Speech, 15 September 2021.

EU budget programs with extended applicability for other areas such cyber security, supercomputing, resilience and infrastructure connectivity (e.g. Digital Europe, Horizon Europe, Recovery and Resilience Facility, Connecting Facility). At the same time, EU approach on EDTs is focused on creating the ethical governance in associated domains, by taking into account the high-risks and challenges to the security of EU citizens posed by new technologies.

This approach should be analyzed in complementarity with the development of defence capability undertaken under CSDP aegis. The guidance is provided by the Capability Development Plan (CDP) which is an overarching instrument developed by EDA in close cooperation with member states. The last CDP was adopted in 2018 providing 11 priorities for capability development in the field of security and defence, including: cyber response operations; ground combat capabilities; space-based information and communication services; enhanced logistic and medical supporting capabilities; information superiority; naval maneuverability; underwater control contributing to the resilience at sea; integration of military air capabilities in a changing aviation sector; air superiority; air mobility; cross-domain capabilities. These elements derived from EU Global Strategy provisions and associated Level of Ambition encapsulate a particular focus on innovative technologies for enhanced future military capabilities, giving priority to a few key domains such as: artificial intelligence, unmanned systems, remotely-operated or autonomous medical systems, autonomous and automated guidance, navigation-control and decision-making techniques for manned and unmanned systems, multi-robot control or advanced materials, processes and technologies[13].

These priorities are reflected in other cooperation initiatives developed under CSDP in the capability development area such is the case of Permanent Structured Cooperation (PESCO), European Defence Industrial Development Program (EDIDP) and European Defence Fund (EDF). In this context, EDTs representing one of the priorities of cooperation between member states benefiting, also, from the financial opportunities dedicated to this area, such is the case for EDF provisions for

[13] 2018 CDP revision. The EU Capability Development Priorities, EDA, Bruxelles.

ensuring up to 8% from the budget to support disruptive technologies[14]. A special note should be added to the financial aspects related to defence in the context of current Multiannual Financial Framework (2021-2027). For the very first time in the development of European security and defence cooperation there were agreed financial opportunities to support cooperation activities conducted between member states under dedicated instruments. In this sense, EDF allocations through MFF are 8 billion € out of which 5.3 billion which are allocated to capabilities development and 2.7 billion for collaborative defence research to address emerging and future challenges and threats[15].

Conclusions

There is no doubt that emerging and disruptive technologies are one of the most important topics that it should be addressed properly in the next period. As this strand is developing with the speed of light the cost-advantage analyses indicate a complex picture in which the border between the positive aspects and challenges is blurring. Given the magnitude of their impact at societal level, it goes without saying that it would be very difficult, for most of the countries, to cope individually with challenges posed by new trends in technology development. But this would not imply that national approaches should be neglected. Quite contrary, it deserves special attention being one of the most complex process involving an extended number of actors, such as economic entities, institutions, academia a.s.o. The main challenge is how to design a functional and integrated matrix able to generate necessary approaches on using efficiently national resources and capabilities.

As regards multinational solutions, there are certain benefits to serve the purpose of taking advantage of opportunities provided by EDT as well as to design adequate governance typologies to manage the security shortfalls. Although EDTs are a relatively new topic in the current debates, there were substantial undertakings to formulate adapted strategy and multinational approaches. As it was described above, a particular relevance

[14] EDF Regulation in Official Journal of European Union, L170, 12.05.2021.

[15] *Ibidem.*

is attached to the NATO and EU's approaches on EDTs and, subsequently, on the formulas designed in this respect. Of course, there are a lot of similarities and conceptual convergence as regards institutional design and practical undertakings assumed by two organizations.

But there is a lot of opportunities to be explored in terms of consolidating the partnership and cooperation between them by taking into account the reciprocal interests in generating adequate responses and most appropriate type of capabilities required by new technologies. From this perspective, EDTs should be perceived as an opportunity to identify the most cost-effective approach in managing unexpected challenges by leveraging existing and new instruments in the wake of increasing the coherence of national perspectives under the auspices of EU and NATO. In this sense, actional synergies between practical measures and programs adopted by these organizations should be further stimulated, with a special focus on interoperability and force generation as regards operations and missions.

BIBLIOGRAPHY

CHRISTENSEN C.*, The Innovator's Dilemma. When New Technologies Cause Great Firms to Fail*, Harvard Business School Press, Boston, Massachusetts;

LELE A., *Disruptive Technologies for the Militaries and Security*, Springer, Singapore, 2019;

OSINGA F., SWEIJS T., *Deterrence in the 21st Century – Insights from Theory and Practice*, Springer, Berlin, 2021;

1997 European Defence Fund Regulation in Official Journal of European Union, L170, 2021;

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Action Plan on synergies between civil, defence and space industries, 2021;

EU Global Security Strategy, 2016;

NATO Advisory Group on Emerging and Disruptive Technologies, Annual Report 2020;

NATO 2030, available at https://www.nato.int/nato_static_fl2014/assets/-pdf/2021/6/pdf/2106-factsheet-nato2030-en.pdf, accesed at 16.10.2021.