Programs and Investments in Disruptive[1] Technologies in Defence

DOI: 10.37458/nstf.22.1-2.6

Mirko Šundov*

Hybrid Threats and Wars in 21st Century - Making Society and Critical Infrastructure Resilient are extremely important for us to respond to different future threats and challenges.

Defence leadership has acknowledged that they must make significant and urgent changes to its people, processes, organisations and culture if they are to keep pace with its strategic competitors and sustain its national security posture. The changes are directed towards the goal of

[1] A Disruptive Technology is a technological development which changes the conduct of operations especially the rules of engagement significantly within a short time and thus has an impact on the long-term goals for concepts, strategy and planning". Source: NATO STO SAS-062 "Assessment of Possible Disruptive Technologies for Defence" and Security Technical Report

* **General (ret.) Mirko Šundov, PhD**, has been a volunteer in the Homeland War (HW) since 1991. He held a number of command positions in the Croatian Armed Forces, including the position of Commander of the 4th Guards Brigade and Chief of the General Staff of the Croatian Armed Forces (2016-2020). For participation in HW and for the results achieved after it, he was awarded with a number of decorations and medals. He completed several military schools and courses in Croatia and abroad, including the War School "Ban Josip Jelačić", a course for senior officials at the Center for Security Studies "George C. Marshall" in Germany, a course for senior officials in UN missions in Finland, NATO Defense College in Rome and others. General Šundov received his master's degree (1999) and his doctorate from the Faculty of Science (Geo.sciences branch), University of Zagreb in 2007.

innovation and digital transformation – to build an enterprise that is foundationally agile and equipped to rapidly identify, develop, test, and integrate new technologies continuously, and faster than its adversaries.

We are now in the era of Fourth Industrial Revolution where the nature of organizations and the Future of Work will change radically. The Fourth Industrial Revolution is characterized by a fusion of technologies that is blurring the lines between the physical, digital and biological sphere. New dimension of threats are shaping radically new questions for defence communities, which are, in turn demanding fundamentally new answers, underpinned by unconventional mind-sets and integration of methods that facilitate both.

When we think about technology, we often think about physical devices that are electrical or digital. In fact, technology encompasses more than that – methods, systems and devices.

Let me use this opportunity to mention some of the important topics that I find extremely important for further discussion. I will start with few sentences related to how Croatia is organized and respond to possible threats and crises.

Secondly, I would like to point out what is important for the decision-making process, staff training and stress some of the new technologies.

And thirdly, I will try to indicate some of the challenges ahead.

1. Croatian Organization - Response to Threats

Recently, Croatia adopted a new Defence and National Security Strategy (2017). With these documents, we have decided to establish a Homeland Security System as the new concept - Security Partnerships based on the experiences of the Homeland War of Independence and recent other events affecting national security.

Along with the prior adoption of the National Security Strategy, the Act on National Security System launched the Government's program in national security. Government level of coordination body was established at the same time. It was decided to be led by the Deputy Prime Minister responsible for national security. The main goal is to achieve synchronized, coordinated, and synergistic actions of all instruments of national power, including all state bodies, non-governmental organizations, media, private sector, and citizens.

This provides an effective responding mechanism to unforeseeable security challenges and natural disasters, providing a strong prevention, planning and, in particular, all kinds of crisis situations management.

Since the most important activities in this regard is the organization and conduction of exercises. We conducted Cyber Safety exercises related to the action of all instruments of national power with scenario including possible terrorist threats, the fight against fire, water pollution, and similar list of incidents.

These exercises have already confirmed that we are on the right path to develop reliable Homeland Security System and improve the level on internal interoperability.

At this stage, we are in the process of introducing and considering these new technologies in terms of their role and supporting the development of the Homeland Security

system. One of the most important is to introduce a new capability especially in the area of Cyber. We are going to establish Cyber Command and modernize and equip unmanned systems.

2. Importance of some elements concerning the process of decision making and staff training

2.1. People

This is important for the political leadership of nations and states, as well as for the military leadership. People are always the most important element. People make the difference. Being a leader means having a character. Leadership is merely a matter of character. Possessing virtue is the state of mind, will, and heart, which gives us strength of character and gives consistency to our personality.

Character is a series of classical human virtues - above all generosity, humility, prudence, courage, self-control, justness and faith.

These virtues increase capabilities:

Prudence: Increases our ability to make the right decisions.

Courage: Increases our ability to abide by our decisions and to resist all kind of pressure.

Temperance / self-control: Increases our ability to suppress our emotions and to devote ourselves to the accomplishment of our mission.

Justness: Increases our ability to give everyone what belongs to them.

Generosity: Increases our ability to strive for higher values, that encourage us and others.

Humility: Increases our ability to overcome our own selfishness and to endure in serving to others.

Faith: In God, yourself, other people - increases our ability to possess and use all these other virtues.

We need to be particularly focused on our younger generations, our "computer generation". They already operate and live in the depths of the information age –social networks, blogs and Facebook. We need to develop a digitally competent workforce, and the potential it offers.

People who will win the critical battles of the 21st century are not those who have mastered the processes and concepts of last century, or even of present time. They are people who will be able to look into the intense competition (particularly in the economic and defence domain) already arising in our world, and in future conflicts. We need people to think in new ways and see new opportunities, which can conceptualise, innovate and create winning solutions.

It would be comforting to think that human factor, which has always been a vital component in past wars, will still count decisively in the future.

During the development of technology, thousands of years ago it change a lot, but what has not changed is whether someone is good or bad person.

2.2. Technologies

Riding will always exist, and the car is just a temporary occurrence.

"Aircrafts are interesting toy but no military value"
French Marshal Ferdinand Foch, 1912

Since the beginning of the industrial age, we have seen innumerable examples of a new technology or product being feared for the change it might bring, rather than be welcomed for the benefits it could bring to society.

In the past there have been technologies that moved from the pages of science fiction into scientific reality, it is going to be the same in the near future.

When we look at the trends that are shaping our security environment, we immediately recognize the exponentially growing rate of technologies and its implications. NATO stress some of them in the Framework for the future operations

- Additive Manufacturing - is the process of making a 3D solid object of virtually any shape from a digital model in ways that are impractical to achieve using conventional manufacturing.
- Everywhere Computing - is computing that is available anytime and anywhere.
- Predicitive Analytics - is the process of generating understanding and providing insight for inference or forecasts of future states from data with volume, velocity variety or dubious veracity.
- Social Media - refers to the wide range of internet - based and mobile interactions where users participate in online-shared exchanges and contribute user related content or participate in online communities of mutual interest.
- Un-maned Vehicles (air, sea and land)
- Advanced Materials - are artificial materials with unique and outstanding properties.

- Mixed Reality - is the merging (stapanje, konsolidacija) of refers and virtual worlds to produce new environments and visualisation where physical and digital object coexists and interact in real time.
- Sensors are Everywhere - 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.
- Artificial Intelligence - refers to the ability of machines to match human in terms of learning, reasoning, planning and acting in complex cyber-physical environments. (Potential impact includes replacement of human decision makers, autonomuos robot or vehicle control, automated information, fusion and anomaly detection, psychological operations and intelligent tutoring(instruiranje) for variety of military missions.
- Electromagnetic Dominance - is the ability to use more of the spectrum, to share the spectrum more efficiently, to protect own forces use of spectrum and to deny enemy use.
- Hypersonic Vehicles - can be aeroplane, missile or spacecraft. They can move at a speed beyond Mach 5, the same speed regime as re-entry vehicle or space shuttle experiences as it reaches the lower atmosphere.
- Soldier Systems - refers to augmentation of individual human abilities using artificial means such as robotic exoskeletons, smart textiles, drugs and seamless man-machine interfaces.

- Energy - over the next 30 years, the global demand for energy will likely grow by 35 % Smart cities - By 2045 , 65 - 70 % of the world population - approximately 6.4 billion people - will live in cities; Food and water technology - Over the next 30 years, inadequate access to food and water will become a crisis point an many parts of the world; Space - The Space industry has entered a period of innovation and progres not seen since the space race of 1960s

Just like: Mobile Internet, Cloud Technology, Artificial Intelligence and Autonomous Systems, Gamification and virtual reality, Drones and UAVs, Digital twins, 3D Printing, The Internet of Thing, Meatless meats, Advanced Robotics, Cyber warfare, Automated Decision Making, Disruptive Tech Soldiers, Block Chain….

Those new technologies provide a solid basis for exchanging our views about the role of new technologies to our respective national defence and the Alliance.

The technology is the fastest growing and evolving trend, and it has already transformed our daily lives and the societies we live in. The surge in computing power, together with Artificial intelligence and autonomous systems, amongst other evolutions, will arguably continue to accelerate the pace of technological progress. The development of global networks simplifies the access to new technologies and information, as well as their dissemination down to the level of individuals.

According to NATO's Strategic Foresight Analysis, it is expected that governments will continue to lose their driving role in the development of cutting-edge technologies, leading to an over-dependency on the commercial sector, including in sovereignty areas such as defence and security

3.Challenges

The trends are showing that potential adversaries will reach technological parity with us. For us in NATO, the first consequence of this easier access to disruptive technologies is the threat posed by their exploitation by our potential adversaries. Consequently, we have to keep up with the tempo of these evolutions and adapt at the speed of relevance).

Notably, there is an impressive history of extremist groups or individuals and insurgents in Iraq, Afghanistan, Syria and across the MENA region, leveraging commercially available technologies (software, encryption technologies, electromagnetic jammers, and drones, improvised explosive devices).

The employment of new technologies in operations will certainly require adaptive mind-sets, technological awareness and appropriate policies and legal frameworks to facilitate the adoption of new technologies, as well as to ensure the highest level of interoperability for capabilities that will be increasingly connected. We are well aware that the future security environment will bring about even more complexity and uncertainty.

Meatless meats / Artificial Food - Food producers are creating meat alternatives that look, feel, and most important taste like the real thing.

Industry 4.0 promises a more connected world in which machines carry out mundane tasks.

Digital twin is a simulation model that updates and changes in accordance with real world assets to enable better decision making and could be used to simulate a piece of complex machinery, for example predicting how it will

respond in certain scenarios and how to best optimise performance. Digital twins will provide businesses with the ability to respond to changes, improve operations and add value to the internet of things.

Many of us know what it is like to live in the shadow of nuclear weapons (to refer to the Cold War period). There are much bigger question-marks over how the rapid advances in emerging technologies will affect the way wars are fought, and perhaps even the way people think of war.

The big concern is that these technologies may be used in autonomous weapons systems that can make choices about killing humans independently of those who created or deployed them.

With new technology it is possible to create the perfect replica of any human being 's face alive or dead. Only those photographs or video clips of that person are needed. There is indeed a justified fear of abuse, and we need to be aware that could be such occurrences, which can have serious consequences. Everyone can be anyone. We will have no idea who is adversary, fake news, scandals ....

NATO Science and Technology organization already took in consideration, in its project portfolio, the use of advanced technologies in the decision-making process, teaming up humans and machines. Here we don’t talk about human versus machines but human and machines working together, while the human capital aspect remains essential.

NATO’s Allied Command Transformation (ACT) has produced an emerging disruptive technology road map that puts its focus on big data, AI, automation, command and control and hypersonic systems among others. The aim of the roadmap is to transform battlespace operations through technology and sustain a military edge across all its

capabilities, whether it involves adapting current capabilities or upgrade them. A key focus point for NATO is the interoperability between all member nations. A key crucial element is the Federated Mission Networking (FMN), a cost-effective capability that will reuse existing standards and capabilities, aiming to support command and control and decision-making in future missions through enhanced information-sharing

Imagine the inconceivable and change the established way of thinking. This can be a big trap for us but also a great advantage for our opponent who can use it. We have to change the established way of thinking; we must think unimaginable.

Emerging technologies would require the wholesale reinvention of current tactics and doctrine. Some researchers believe that the main tactical unit of the future will be a mixed human-robot team and that this will require fundamental changing the human soldiers. It means extending the physical and mental abilities of the soldier, improving his understanding and interpretation of the environment, and improving communication with other super soldiers and robotics systems.

New ways of thinking about new dimension of threat and contingencies, competitions and missions they produce will be required in order to mitigate risk and capitalize on opportunity. Operational and strategic planners must integrate and empower novel alternative analysis methods and mind-sets that challenge existing assumptions, expand analytical filters and enable more flexible planning efforts to meet the challenge and opportunities of the future.

We have to change the established way of thinking; we must think unimaginable.

4. Whole of Government approach and international collaborative research

The Integrated Review of foreign policy, defence, security and international development was unveiled in February 2020, with the aim to transform the UK's approach to foreign policy through a policy-led review conducted across Government.

The review will determine the UK's long-term strategic objectives for national security and foreign policy; understand how to work more effectively with allies; define the capabilities needed for the next decade and beyond; recognize the required reforms to the government's systems and structures to reach the review's goals. The review into defence and security industrial strategy, led by a cross-government team which will engage with industry, Parliament and other stakeholders, will define a more strategic approach to ensure the UK has "competitive, innovative and world-class defence and security industry sectors." It will focus on the impact of rapid technological change on industry, the necessity of innovation, partnership, and competition from abroad, and the challenge in having the right skills.

The Ministry of Defense (MoD) has highlighted five priorities:

- The integration of physical and information activity across all operational domains
- Agile command and control to enhance and accelerate decision-making
- The ability to operate and deliver military outcomes in contested domains
- Access defence people with the right skills, knowledge and experience
- Be able to simulate future battlespace complexity

We have to be, especially, focused on our younger generation, our cadets, students, younger officers and young people. They are already operating and living in the depths of the information age. We need to develop a digitally competent workforce and the potential it offers - the so-called digital generation. For the benefit of all of us.