CMDR COE PROCEEDINGS 2024

10

September, 2024





TABLE OF CONTENT

RESILIENCE, CRISIS AND EMERGENCY MANAGEMENT: MEASURING, ANALYSIS AND SOLUTIONS

Mitko STOYKOV, Professor

Abstract: In this monograph are published the methodology and products of a scientific research on the institutional resilience and crisis and emergency management capabilities of the National Security System

Introduction

The main goal of this applied scientific research of the National Security System of the Republic of Bulgaria is the development of analytical and scientific-based tools to research institutional resilience in the area of security and defence. Another goal is to establish a sustainable partnership between the participated scientific and educational organizations in a joint program as a part of national and European international research networks, programs and projects, designed to support ensuring a transparent, predictable and favourable security environment for the development of society and the state.

The National Scientific Program "Security and Defence" (NSP S&D) was adopted by RMS No. 731/21.10.2021 in implementation of the National Strategy for the Development of Scientific Research 2017-2030. The Ministry of Education and Science (MES), according to Agreement No., finance the implementation of the NSP S&D. D01-74/19.05.2022. The main goal of the NSP S&D is to support increasing of scientific capacity and development of basic aspects of scientific research, and applied tools in the area of national security and defence. That is why one of the main thematic directions for realization of NSP S&D is "Defence and of the population in disasters and accidents: Concepts, doctrines and strategies; Equipment, equipment and training."

The main purpose of this multidisciplinary, strategic conceptual and science-applied research is to support enhancing Business Continuity and Resilience readiness of the NSS's institutions with providing a continuity of the adaptation of its state based legal-

normative and strategic conceptual and doctrinal fundamentals in the area of national security and defence. It is designed to lever strategic management documents to the requirements and continuous changes in the security environment, where the national institutions operate, as well to support the development new or to update the existing policies and practices for security and defence, as well to support development of new concepts, strategic programs and plans to better address state's response to the long-term challenges, risks and threats to national security.

The horizon of relevance and applicability of the results of a fundamental scientific research usually exceeds ten years and might be preceded by Strategic Foresight Analysis and development long-term visions and strategies for improvement functionality of basic state's sectors. Having In mind recent dramatic changes in the security environment in Europe and Middle East, the basic strategic vision is changed. To respond this change, experts exploit science-applied tools and approaches to develop instruments for ensuring the defence of the national strategic interests and realize NSS's main goals. That why it is appropriate the basic strategic documents to be periodically partially or completely updated and renewed in need through specially dedicated scientific and expert researches.

The need for conducting strategic studies of the national security and defence system is pre-determined by a political expert assessment of emerging new indications, based on the influence of technological, external and internal factors on the functionality of the institutions - significance and irreversibility of the influence of new challenges, risks and threats to the national security and, at the same time, an insufficiently up-to-date institutional capabilities for the of national interests and the realization of national security and defence goals. The periodicity of the implementation precedes assessments of the relevance and duration of the planned period of validity of the national strategic documents, as well as the need to update or change the scientific foundations for long-term political, management and resource binding of the efforts of state institutions to create a -good objective conditions for the realization of strategic goals in the field of security and defence.

An additional argument is the implementation of long-term national investment programs and projects for updating and building of the national security system's capabilities. Full synchronization of the national strategic planning with the alliances in NATO and the EU implies to follow common alliance horizons of relevance of national

planning documents. Such engagement is a significant prerequisite and motive for conducting analyses and comprehensive assessments of the entire security and defence sector in order to increase the synergy of institutional interaction and policy binding, coordination and synchronized building of institutional capabilities to counter challenges, risks and threats in all areas of national security.

The war near in Europe, in Ukraine, shows that, together with the allies in NATO and the European Union, the Republic of Bulgaria is entering a new, insufficiently known, difficult to predict and highly dynamic strategic security environment with ever-increasing geopolitical competition, in which successful adaptation to changes in the past is no a guarantee for future success. The country will continue to develop its defence capabilities and actively participate in Alliance collective efforts to sustainably new readiness by significantly increasing national defence and security spending. Within the framework of the Common Foreign and Security Policy (CFSP) and the Common Security and Defence Policy (CSDP), the main political commitments are to unite efforts and motivation and to implement common measures to increase the national security together with other member states. The model for a comprehensive Alliance approach to security enables a coherent and effective response to the rapidly changing threats in the strategic security environment and the implementation of strategic priorities through the implementation of crisis and emergency response measures and the integrated management of digital and physical risks in the alliance security system.

The last wold crises, resulting from the COVID-19 pandemic and the war in Ukraine, have significantly changed the perception of the multifaceted impact of security threats and policies/response measures, given the need for a significant simultaneous effort and future investments to ensure security in a new physical and digital environment. They emphasized the importance of the EU assistance provided to Ukraine, to achieve strategic energy autonomy and to sew up the supply chains of products, services, infrastructure and technologies. Raised the need for joint efforts to ensure the readiness and resilience of response mechanisms and tools.

The main purpose of the this analysis is to present scientifically based assessments of the current situation and to allow the formulation of scientific and applied proposals for concrete solutions to overcome identified problems in the field of crisis and emergency management in the long term, as well as to expand inter-institutional

interaction and cooperation with public organizations and citizens. The analysis is oriented to assess and evaluate the existing disaster, accident, emergency and crisis management systems and the development of scientific applied and conceptual proposals for their improvement when follow the logic of the need for a consistent settlement of public relations and emphasize the construction of the foundations of a unified National System to manage crises and emergencies. The proposals have a changed philosophy of the operation of the main legal norms. The current Disaster Management Act and the repealed Crisis Management Act govern the state's management during the crises and emergencies. Crises are extremely large-scale and destructive events for the state and society, and their management requires a continuous monitoring and preventive application of pre-planned measures and plans. Therefore, the basis for the management of crises and emergencies requires a preventive intervention of the institutions and the state in order to prevent and avoid their destructive manifestation with negative impacts over all public sectors of life.

In the case of crises and emergencies, measures are purposefully applied and search and rescue operations are carried out to have a positive impact on the functionality of the state/local/municipal institutors and the overall changes of the security environment. Therefore, the consequences of crises and emergencies could be not liquidated, not only because it is impossible, but also following the need to manage them until the achievement of a new acceptable state and normal functioning of the community, state and society, which is always different from what was before the manifestation of the particular crisis or emergency. In accordance with the Constitution of the Republic of Bulgaria, the management of the state is entrusted to the executive state power, and even in the case of the introduction of martial law and a state of war, there is no provision for derogating parts of the basic law of the state and changing the hierarchy of its management. Therefore, even in crises and emergency situations, the duties of decisions making and their implication in practice remain primarily for the authorized by the Constitution authorities - the Council of Ministers, ministers, regional governors, mayors of municipalities and heads of legal entities.

The analysis of the existing and conceptual proposals for the creation of new bodies for institutional resilience, Crisis And Emergency Management includes the Security Council to the Council of Ministers, the Security and Crisis and Emergency Management Councils to the Ministers, regional governors and mayors of

municipalities, Centres for Crises and Emergency Management, Situation Centres. All they are specialized expert and advisory bodies for monitoring and analysing the situation and for proposing solutions for implementing measures, plans and conducting operations for institutional resilience, Crisis And Emergency Management. The decisions themselves have to be taken only by the authorized bodies - Council of Ministers, ministers, regional governors, mayors. The expectations from the implementation of the current conceptual proposals and changes in the regulatory framework is a significant change of the philosophy of the settlement of public relations in an extremely important period, covering crises and emergency situations in states between peacetime and wartime of the functioning of the institutions and the state.

Measuring Institutional Resilience

The two first decades of the XXI century brought new and unknown challenges, risks and threats to the national security and peace when at the same time continuously increased their complexity, scale and areas of manifestation. The frightening synergy of the cascade effects of expression of many combinations of political, economic, social, informational, conventional and non-conventional, kinetic and non-kinetic, lethal and non-lethal security threats received a political name "hybrid war". Applied even in a real war in Europe, this name was intuitively embedded deep into all areas of functioning of modern society, including also expert community. Their study provoked a series of large-scale Allied researches that outlined the scale and complexity of the current and future security challenges and enriched their theoretical identity. The results provoke a new focus on civilian and military resilience, as a real foundation the nations to be continuously ready to prevent and manage crises, to deter and defend their independence and territorial integrity.

Resilience in an Alliance context refers to the capacity to prepare for, resist, respond to and quickly recover from shocks and disruptions. Civil preparedness is a central pillar of Allies' resilience and a critical enabler for the Alliance's collective defence, and NATO supports Allies in assessing and enhancing their civil preparedness. Rooted in Article 3 of the North Atlantic Treaty, national and collective resilience are an essential basis for credible deterrence and defence, and are therefore vital to NATO's efforts to safeguard its societies, populations and shared values[1].

[1] ttps://www.nato.int/cps/en/natohq/topics_132722.htm

The Article 3 of the North Atlantic Treaty provide for a principle view of resilience in NATO: “In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed

attack.”[2] Its leads to the need of development capabilities, needed to execute defined in NATO Strategic Concept 2022 core tasks: crisis prevention and management, deterrence and defence. In this context, resilience is estimated as national and collective responsibility. The nations need capabilities in order to be ready to respond the entire spectrum of crises and emergencies and at the same time effectively to contribute strengthening resilience and minimise vulnerability of NATO.

Military efforts to defend nation’s territory and populations is supported by number of civilian capabilities and an uninterrupted readiness to minimise the impact of possible manifestation of a broad spectrum of risks, treats and crises, as well to reduce vulnerabilities and consequences. Civil resilience has several areas of responsibility:

- Assured critical government services with a formalised plan for the provision of minimal governmental services, and secured and autonomous crisis management centres;

[2] https://www.nato.int/cps/en/natolive/official_texts_17120.htm

- Resilient energy supply with robust sustainable redundancy capabilities, prioritised critical supply chain and awareness protocols and procedures;
- Readiness to deal with an uncontrolled people movement, based on nation's integrated civil and military plan and detailed preplanning and exercising managing of the simultaneous movement of people;
- Provision of resilient food and water resources with real capabilities for food and water contamination and contingency food and water supply plan;
- Resilient public healthcare system, ready to deal with mass casualties, warning and reporting system, medical capabilities database and civil-military contingency plan;
- Resilient civil communication systems with sustainable redundancy capabilities and legal & physical arrangements for access;
- Resilient civil transportation systems with legal & technological arrangements, agile & robust transportation infrastructure and transportation IT systems.

The listed above critical specifications are organised in seven baseline requirements for national resilience hat provide the Allies with a system to measure their preparedness. Military forces, especially those ready for deployment during crises and conflicts, depend heavily on the civilian and private/commercial sectors of society for transport, communications, energy and even some basic supplies such as food and water, to fulfil successfully their missions. Effective civil preparedness ensures that these sectors are ready to withstand attacks or disruptions and can continue supporting NATO's military forces at all times. NATO's policy on resilience and civil preparedness is guided by the Resilience Committee.

The expected Armed Forces contribution to be resilient and prepare for an effectively countering new threats was systematically summarized in developing an overarching concept. The concept's thematic areas support civil preparedness to enhance nation resilience and stress on several military/defence system's advantages. The forces' management system is more developed and capable, better organised and exercised than its civilian equivalents for other sectors of society. Their capabilities are leveraged in support of ensuring nation's continuity of government, for coordination during crises and emergencies. A common resilient picture is based on situational understanding, provided by military intelligence and civilian information services. The quality of processing and dissemination information of the military capabilities usually prevail

those in the other state's institutions. At the same time, better orchestrated military Command and Control technical and IT capabilities could be enhanced with achievement of a better civilian knowledge of the area and the population that are essential for building situational awareness and understanding.

The military resilience is generally based of Armed Forces' Defence and Warfighting Capabilities. Their increasing ability to support the civil environment must be integrated into all five domains of military operations: land, air, maritime, space and cyber. An appropriate tool to support this effort of military capabilities is the Civil-Military Cooperation (CIMIC) in all possible domains of interactions and support civilians. Except crises and emergencies, military satellite constellations might support civil emergency communications, military cyber defence can help protecting and defending

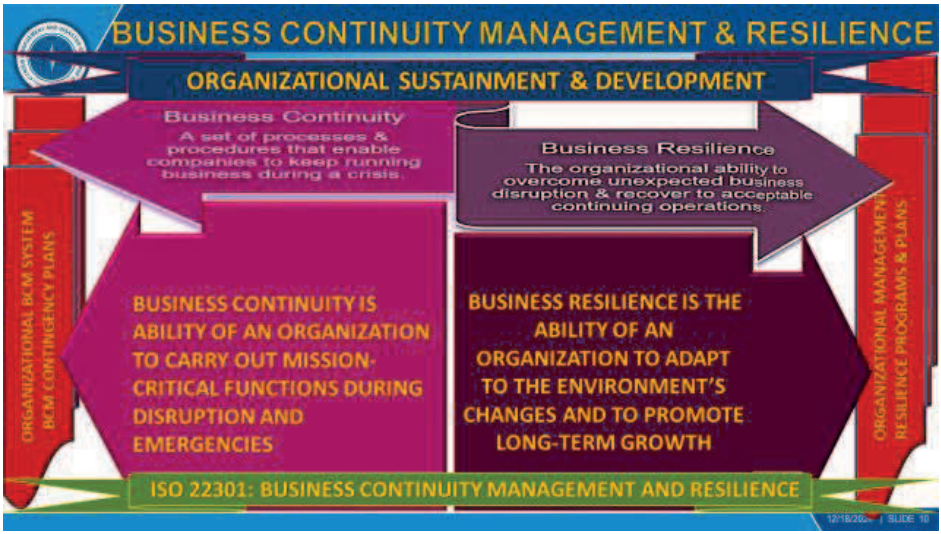
critical infrastructure, naval forces have better capabilities to protect civilian ports and undersea infrastructure, as well as commercial power, gas and communication lines.

The military logistics system is dependent on civil infrastructure and commercial entities for its equipment, supplies, repair parts and munitions. However, it has capabilities and expertise in movement and transportation that are scarce amongst civil entities. Military airlift capabilities are used to support humanitarian operations globally, often they are the only able to reach, land and support civilian authorities on some geographical areas (like Pakistan Mountain Floods). Nevertheless that these resources are designed for a heavy engagement during a conflict and war, civil entities may require their specialised logistics support if no other available options for Search and Rescue operations.

Military capabilities for a precise and responsive planning is a core competency of Command and Control System of military forces. Both military and civilian management entities might benefit from a collaborative participation in this endeavour, especially with regards to establishing of shared situational awareness and global picture that support a clear understanding of the common operational environment.

Resilience of the military personnel is designed to resist on all challenges and to cover the full spectrum of military mission requirements, including ability to respond to specifics of a civil environment. The main aspect of building personnel's perseverance is societal or social resilience. Military personnel with closer connections to their social base, families and communities are expected to be more resilient as they provide emotional support and rallying point for those on the front lines. Tightening these social connections might benefit both civil and military personnel with strengthening relationships, deepening mutual understanding and trust.

The design and completeness of the military infrastructure often relies on big parts of civil infrastructure. Military bases, their routes are usually designed with force that could provide for safety and security of civil authorities. They might be used to host displaced persons, to receipt and storage critical materials and supplies. Following a comprehensive view of interdependence of resilience, a concept for Layered Resilience is intended to respond to the conceptual shortfall and to integrate both civilian and military areas of resilience responsibility. As a concept, it also provides the



exclusive overarching framework for the development of needed subject related conceptual documents.

The most important for building, achieving and measuring resilience is its reliance on well-known international standards (ISO). For example, ISO 22301 is the international standard for Business Continuity Management Systems (BCMS) that defines requirements for Security and resilience of these systems. It provides a framework for planning and management BCM organizations. The standard list requirements to plan, establish, implement, operate, monitor, review, maintain, and continually improve all documentation of management systems that are designed to protect against, reduce the likelihood of, and ensure recovery from disruptive incidents. The implementation of this standard is beneficial and crucial for enhancing organizations' resilience when they prepare to respond to various emergencies, crises and disruptions, while providing an uninterrupted continuity of operations and services. Following it helps managers to identify risks, plan, and train preparation for emergencies, and improving recovery of functionality.

In International Glossary for Resiliency[3] Business Continuity Management (BCM) is defined as a "Holistic management process that identifies potential risks and threats to an organization and support to assess possible impacts to business functionality and products. It provides a standardised framework for building organizational

[3] International Glossary for Resilience, https://drii.org/resources/glossary;

resilience and capabilities for effective response. As a basic foundation, BCM integrates contingency planning, education and training, emergency response, crisis

management, consequences management and disaster recovery.

As a new discipline in NATO, BCM aims to provide provenance and direction for developing and implementing the NATO-wide BCM System (and BCM system for each NATO entity) that will provide policy and capabilities to prepare for, respond to, and recover from emergencies and disruptions. An application of system approach make BCM at NATO operates in a holistic “system of systems”, because each NATO body will develop own BCM System (based on common standard requirements) and will take into account all existing interdependencies. This system approach based on common both NATO Business Continuity Policy and International Standards (ISO) will provide for systematic competiveness, coherence, unity of efforts, will support avoiding duplication and reach a leveraged the Alliance and nations synergy.

Generally, the development of BCM systems and establishing BCM culture will provide for a better readiness for the anticipated future and change management where entities will have a strategic tool with proven effectiveness for an adaptive functionality and readiness to respond to the any change, disruption or emergency. This application of this discipline will support subject matter capability building and facilitating organizational resilience and sustainability.

Recognizing BCM as an effective tool to plan and response to disruptions, emergencies and crises where organization continues to be operational to execute its functions with planed effectiveness. More, based on increased resilience, the organizations will be ready to deal effectively with unknown emerging risks, threats, disruptions, and to manage future emergencies and crises. That is why the achievement of all dimensions organizational resilience has to be applied as a strategic management-driven approach to and response culture developer (SO 22313). Additionally, setting resilience as aim might be enhanced with a full integration and coordination of all applied disciplines, at all organization's levels: strategic, tactical, and operational. At the same time, the organizations will have a choice to integrate additional methods for reaction and responses while explore embedding resilience through business continuity in their business practices. According to the new NATO Strategic Concepts 2022, the Alliance and Nations' resilience is an obligatory strategic prerequisite for a successful execution of NATO core tasks. That is why an integration of all available efforts and capabilities into a common system of systems approach is dictated by the need to clearly distribute demands among all actors, and to unite all achieved results in a common respond to these demands based on every organization's business continuity maturity.

The ability to respond to any change in the security environment and get the product out before competition is inherent in any successful organization. Resilience is a continuous requirement and the support of its maintaining in organizations need they to be strategically adaptable, operationally ready, and tactically able to respond to any risk, threat, emergency and crisis.

In the previous decades, the unity of the Alliance effort of readiness to respond to unknown and unexpected threats was defined under the need of capabilities to counter hybrid threats. Based on the diversity of challenges and forces/institutional response these threats brought an expression of specialised NATO readiness was specified under the planning and building capabilities for military contribution to countering hybrid threats. At the same time, the European Union (EU) defined the need for capability building for an effective response to the manifestation of these threats and

increased the efficiency of the fight against them in a the EU Joint Framework[4] combined existing policies and suggested actions aimed at:

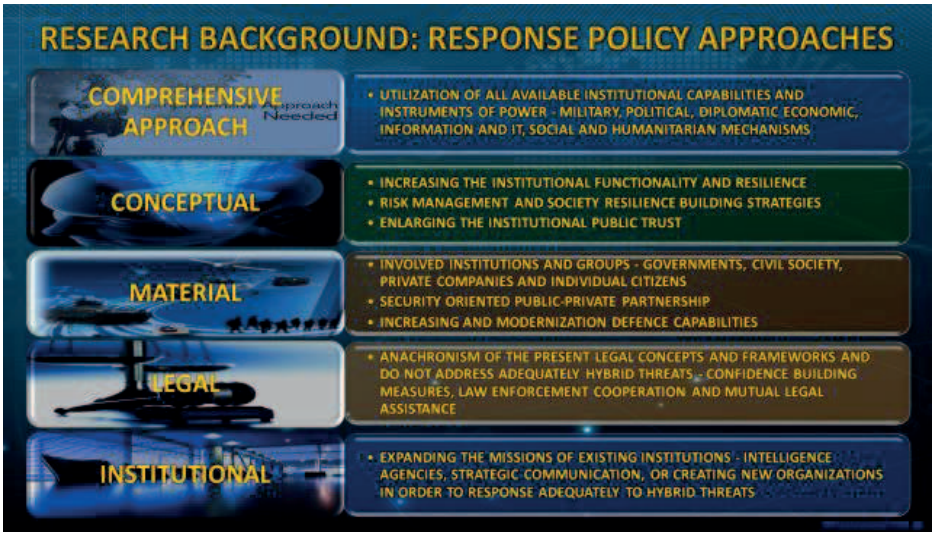
- increasing awareness with mechanisms for the exchange of information to deliver strategic communication;
- building resilience with accents on cybersecurity, critical infrastructures, of the financial system, public health, and countering extremism and radicalisation;
- preventing and responding to crisis and wide-ranging and serious hybrid attacks;
- cooperation and coordination between the EU and NATO and other International Organisations.

A strategy for NATO's role was adopted[5] in order to address the challenges and threats across the spectrum of diplomatic, informational, military, economic, financial, intelligence and law enforcement aspects. Later, a plan for its implementation was presented, focused on capability building for support a prompt decision making process, and maintaining the institutional stability and readiness to respond. The further effort was directed toward development of several high impact concepts that are aimed to focus on the need for increasing societal resilience and of civilians against new and unknown security treats.

A number of national publications also support the disclosure of the nature, characteristics and conceptualization of the subject area of countering hybrid threats. This topic was discussed at the forum of Chief of Defence Conferences. Following the Allied effort and proposals to conduct national scientific support tools for an improvement of institutional resilience and sustainability, a MOD lead an inter-institutional working group drafted a national Strategy to Countering Hybrid War. In line with the requirements to support improvement of the national expertise, the Defence Advanced Research Institute (DARI) at Rakovski National Defence College (NDC) conducted an applied science research project, named "Inter-Institutional and International Cooperation to Combat Hybrid Threats". The project was executed in two stages. The first - Expert assessment of institutional role and capabilities, and Second: the need for inter-institutional and international cooperation to combat hybrid threats – presented at international conference: "Inter-institutional and international cooperation

[4] http://europa.eu/rapid/press-release_MEMO-16-1250_en.htm;

[5]



to combat hybrid threats". This paper will briefly present the conducted scientific research nature and main findings. All these steps of a focused applied science are directed toward the development of science based instruments to support and measure institutional resilience in accordance with the requirements of national and allied strategic documents.

Research Background

This science-based research is based on a clear conceptual platform, which defines the background of the studied topics. It utilised available allied approaches in order to define more/precise clear understanding of changing security environment. NATO started developing a Capstone concept “Military Contribution to Countering Hybrid Threats” in order to define all new trends and possibility of simultaneous manifestation of the various combinations of harmful risks, threats and effects to the national security and defence - summarised as hybrid threats. The second goal was to enlarge the possibility areas for application of available military capabilities and countermeasures for their defeating.

The main task of this project of capstone concept was a security threats assessment, defining the needs of defence capabilities, and conceptual requirement to engage all levels of NATO, Nations and Partners strategic leadership. The concept was designed also to lead the future Armed Forces capability development and support establishing a Future Operations Framework document – that is aligning the defence strategy,

armed forces' structures and capabilities. This project of the concept tried to reveal key features of the new threats that are sources of potential risks and threats to the national security and defence:

- They are combined with a deliberate use of misinformation or false information, they utilise a diversity of effects, based on simultaneous use of lethal and non-lethal conventional weapons.
- The combination of negative effects after their manifestation is accelerated by an increasing possibility of proliferation of Weapons for Mass Disruption (WMD), diversity of terrorist actions, broadening the areas of information espionage and cyber-attacks, organized crime and information operations.

- The project stresses on the several most challenging to the national security and defence areas:
  - the weaknesses provoked by some imperfections of the international law and institutional legal bases;
  - the continuous diversification of the threats' sources;
  - a very low and almost invisible profile of their appearance and manifestation;
  - an intensive flow rate and large affected areas, based on access to new technologies and science achievements;
  - continuous adaptation and flexibility of the increasing number of state and non-state players.

- This concept also was expected to contribute for defining hybrid threats as posed by adversaries, with the ability to employ simultaneously conventional and non-conventional means adaptively in pursuit of their objectives.

The EU also brought some contribution into the further conceptualization of the response to new unknown threats to the national security and increasing resilience. The European Joint Framework on Countering Hybrid Threats defines hybrid threats as a phenomenon that results from the convergence and interconnection of different risks and threats elements, which forms a more complex and multidimensional threats to national security.

The document also defines the origin and nature of a Hybrid Conflict – a situation in which parties refrain from the overt use of armed forces against each other, relying instead on a combination of military intimidation (falling short of an attack), exploitation of economic and political vulnerabilities, and diplomatic or technological means to pursue their objectives.

The EU framework determines Hybrid War as a situation in which a country resorts to overt use of armed forces against another country or a non-state actor, in addition to a mix of other means (i.e. economic, political, and diplomatic, etc.). In the scientific research, these definitions were utilized to help establish a common understanding of the origin and nature of hybrid threats.

The Strategy on NATO's Role in Countering Hybrid Warfare is a response to the 21st century geopolitical evolution's influence over the extension of current conflicts by non-linear actions across the entire DIMEFIL[6] spectrum. The strategy determines NATO strategic scope in political, diplomatic, information, military, economic, financial, intelligence and law enforcement domains in order to ensure success of applied countermeasures, to increase readiness, and deterrence capabilities.

The strategy defines internal and external focuses of its implementation with guidelines to increase effectiveness of national strategic planning, to develop measures for cohesion in security and defence policy and strategic management, and to propose establishing a matrix of institutional responsibilities and reactions, including:

[6]Diplomatic, Information, Military, Economic, Financial, Intelligence and Law

- intelligence and early warning;
- faster decision making process;
- advanced capability development for future conflicts;
- exercises and training;
- readiness, flexibility, agility and responsiveness.

In order to utilise available countermeasures instruments, the project again steps on the basic NATO and EU conceptual documents. For the preparation to deter and defend hybrid threats, NATO prescribed the particular conditions for success and areas of the strategy application. The countermeasures include development and application of capabilities for detection, analysing and respond to the unknown risks and threats, special countermeasures to dissuade the opponents to use hybrid strategies, and proper use of NATO Strategic Concept instruments of collective defence.

The Recovery and Resilience Plans can be considered a general opportunity of EU resilience policy and practice, directed toward performing a deep structural transformation in the member states to reach the levels of planed resilience. The EU Commission deploys up €723.8 billion in banks loans and grants to support the implementation of needed reforms and investment packages to the member states in their national Recovery and Resilience Plans (RRPs). Especially for the management of this project was established a Recovery and Resilience Facility (RRF) that is a temporary instrument for the EU's plans the Union and nations to re-emerge stronger and more resilient from the current crises. The Commission raises funds by borrowing on the capital markets, that are available to Member States for implementation of reforms intended to:

- Support of the EU priorities to make states' economies and societies sustainable, resilient and prepared for the green and digital economy transformation;
- Address the identified challenges and Lessons Learned (LL) successful practices in specific recommendations in economic and social policy practices' coordination.
- Implementing the EU plan and the Commission's response to the socio-economic hardships and global energy market disruption caused by Russia's invasion of Ukraine.

- Align both the reforms and investments in nations' RRPs with the EU's strategic priorities when resolve country-specific challenges of economic and social policy coordination.
- Facilitate and accelerate a green and digital transitions in the member states economies with an execution of planned measures, while increasing resilience, cohesion and sustainable economic and social growth.
- Help member states preparation, planning and implementation of their national plans where more than 500 approved projects are linked to plan and implement of Member States' RRPs and their smooth implementation.

An effective application of NATO and the EU policy, strategy and framework requires a proper national response policy. The Alliance has already collected an extended experience for application of the comprehensive approach that allows the simultaneous utilization of many available capabilities and instruments, including military, political, diplomatic economic, information, social and humanitarian mechanisms. The application of a further deep conceptual approach will support and contribute to increase the institutional functionality and societal resilience, to establish proper risk management and building society resilience strategies, and to enlarge and increase the institutional trust. The development of resilient response capabilities needs an involvement of all institutions and social groups, including governments, civil society, private companies and individual citizens, and utilisation of available with proven effectiveness instruments, like security oriented public-private partnership, to help modernise, adopt and enlarge the needed defence and security capabilities.

A proper legal support to enlarge resilience and increase readiness, prevention, detection and response, could be directed toward minimising the anachronism of the current national legal concepts and frameworks that do not adequately address risks and threats from one side, and from another - to improve the effectiveness of resilience building measures, law enforcement cooperation and mutual legal assistance. It will support measures to expand the responsibility and missions of security and defence institutions including intelligence agencies, strategic communication structures; as well as to support building new organizations to optimise an adequate response to the threats. NATO Future Foresight Analysis describe the main characteristics of the future operating environment:

- Persistent;
- Simultaneously;
- Boundless;

The emerging new risks and threats will be ***persistent*** because the known today actors with higher influence power will increase in number. In addition, the development of science and ecologies will provide not only states, but also private organizations and individuals that will emerge and compete persistently in power, threatening member-states and the Alliance's security and military strategic interests.

The manifestation of destructive risk and trust can start ***simultaneously*** by potential adversaries so the Alliance might need to activate many different areas of capabilities against number of hostile attacks. To response to a deliberate simultaneous trial to harm common security and defence, member states can have a prevailing number of capabilities to deal with threats, emergencies and crises, where could be included all state instruments of power, science and technological advantages. Some practices will require to simultaneously pursuing cooperation in some areas (e.g. economy, arms control of proliferation) while at the same time the Alliance actively fighting in others (e.g. cyberspace or information, and proxies).

The persistency and simultaneity of emerging risks and threats will require a ***boundless*** reaction of all available military and state instruments of power. This reaction will merge political, economic, social, etc. capabilities with military power at

all levels – allied, strategic, operational and tactical defence with and military, strategic,

operational and tactical forces' capabilities to enrich traditional military operations and actions with non-military activities. The possibility to explore forces' advantages in all domains – Land, Sea, Air, Space and Info will provide to reach resilience and ascendancy of adversaries' concurrency in physical, space and geographically unlimited domains. This ability for operating in widening security environment enhances the Alliance and Nations possibility to build resilience and continuous readiness to prevent and manage crises, to deter and defend against adversaries.

National power[7] is defined as the sum of all resources available to a nation in the pursuit of national objectives. National power embeds basic state's elements, called instruments that generally are separated according their directions of influence and mean of origin where geography, resources, population are national, and derived from them - economic, political, military, psychological and informational are social. These instrument of state power are the biggest source of influence, owned nationally by states. In the United States policy and practice, for the long time as instruments of national power were considered Diplomacy, Information, Military, and Economic (DIME). In this row, the diplomacy is national instrument for engaging the state with other states in order to promote and advance declared states' values, interests, and objectives. It is working tool for formation and participation in coalitions and alliances. The information is nation's and organizations/actors strategic resource, especially in the area of security and defence. Today the states are competing with a big number of non-state actors, including terrorist and criminal organizations that own information's resources and capabilities. National military instrument of power is widely used to protect, deter and defend national interests. The military capabilities are one of the most important tool to compare states power, available for use for resolving crises and conflicts, to project power as well as to defend states territorial integrity, sovereignty, independence. The economic instrument of power is considered states'/nations' fundamental engine and critical enabler of development all instrument of national power, including wellbeing of nation's population/social capital.

The last years brought an enrichment of the instruments of national power, because to the above mentioned were added financial, intelligence and law enforcement. The

[7] https://www.thelightningpress.com/the-instruments-of-national-power/?srsltid=AfmBOoqg1EgPuJ0x1TgfwoVow5rY7X8Re1pJKgeuzvcninKumZtsKE6g

sources and capabilities of national power with a more detailed list provide for better defend and advance national interests with applying the most powerful state's prerequisites to achieve strategic objectives. Each of these instruments of national power works effectively with the others elements, including diplomatic, informational, military, economic, financial, intelligence, and law enforcement.

The Layered Resilience Concept will express an ability to absorb shocks and fight-on, across all layers, military, civil-military and military-civilian. The intention is MIoP to support the Alliance's ability to anticipate and resist strategic shocks or surprises, manage consequences, fight through and ultimately out-last and prevail against adversaries. This requires mentioned above layered approach that comprising mutually reinforcing 'layers' of military resilience and civilian resilience and support NATO's comprehensive resilience agenda. The achievement of layered resilience needs to recognize the importance of the continuity of command, military forces' structures and processes, availability of reserve forces, redundancy and the balance between capability and capacity[8].

In this context, MIoP might be used in many options that vary in purpose, scale, risk, and combat intensity. These variations can be understood to occur across a continuum of conflict ranging from peace to war. Inside this continuum, it is useful from a strategic perspective to delineate the use of the MIoP into broad areas - from operational level of warfare that connects the tactical to the strategic, to broad campaigns. Except direct usage MIoP to build forces' and nations/Alliance superior power, these capabilities provide for utilisation better opportunities to identify and manage risks, to apply a preventive management of crises and emergencies, and to practice cognitive superiority and better understanding and operating inside the less-predictable future strategic environment. The future MIoP have to exploit opportunities like[9]:

- ***Out-think***, where the Alliance is excellent and agile, underpinned by unique military ethos, culture and diversity and take the initiative and win over any potential adversary under any circumstances;

[8] NATO Warfighting Capstone Concept, pag.18, https://www.act.nato.int/our-work/nato-warfighting-capstone-concept/

[9] NATO Warfighting Capstone Concept, pag.10, https://www.act.nato.int/our-work/nato-warfighting-capstone-concept/

- ***Out-excel***, where the Alliance decisively operates across domains, in concert with other instruments of power and actors and simultaneously conduct shaping, contesting and fighting activities;
- ***Out-pace***, where the Alliance is able to recognize risks, seize opportunities, decide and act faster than potential adversaries;
- ***Out-partner***, where the Alliance is able to foster and exploit mutually supportive and habitual relationships and partnership opportunities;
- ***Out-last,*** where the Alliance is able to think, plan, operate and adapt with a long-term perspective in mind to endure as long as it takes through strategic competition and any conflict situation.

The development of needed quality of MIoP is based on several imperatives that support to organize and synchronize the Alliance and Nations efforts:

- **Cognitive Superiority** needed to understand the future operating environment and potential adversaries/opponents relative to the own capabilities, capacities and objectives;
- **Layered Resilience** that represent the ability to absorb shocks and resist across all layers, military, civil-military and military-civilian;
- **Influence** and **Power Projection** in support of positively shaping security and defence environment, including generating positive options for the Alliance and imposing dilemmas on adversaries;
- **Cross-Domain Command** to keep operational, revitalize and enable C2 ability to understand the multi-domain operating environment and act rapidly and effectively;
- **Integrated Multi-Domain Defence** in support of protecting the Alliance's integrity to decide and act against threats in any domain, regardless of their origin or nature Layered Resilience.

Based on these imperatives, the MIoP will increase the Alliance's ability to anticipate and resist strategic shocks and surprises, to allow a better management of consequences, to fight through and ultimately out-last and prevail against adversaries. These are the main reasons that requires the mentioned layered approach, comprising mutually military and civilian resilience. To develop needed capabilities to manage security and defence risks and to counter nowadays and future threats, the Alliance stressed on the new mechanisms and instruments for increasing societal resilience. An appropriate level of institutional and societal resilience will be used as an essential basis for credible deterrence and effective support to fulfil NATO core tasks. Enhancing resilience through institutional business continuity management and preparedness will be a part of the Alliance and Nations capabilities to counter expected new threats and challenges. NATO effort helps to identify the presented Resilience

Guidelines and Evaluation Criteria as practical key to increase societal resilience. These guidelines are prescribed to lead and support the unification of NATO Nations effort to increase resilience and provide society with continuous and assured critical government services, development formalised plans for provision of minimal governmental services with use secured and autonomous Crisis Management Centres. A conceptual

response to the military resilience will be NATO Layered Resilience Concept.

Societal resilience will be impossible without availability of uninterrupted essential services, like energy supply with robust and sustainable redundancy capabilities, prioritisation critical supply networks and proved awareness protocols and procedures. The sustainability of society's functioning depends on the resilience of food and water resources, including contingency plans for food and water decontamination. The societal resilience is dependent on the availability of resilient civil communication and civil transportation systems and a safe critical infrastructure. A guaranteed provision of society essential services is the function of the resilience of lifesaving lines – first of all medical support and emergency medical support, civil services and facilities, capabilities to manage emergencies, to deal with mass casualties and to cope a possible uncontrolled movement of people.

The lack or insufficiency of presented in the research's background needed capabilities and public services may facilitate an unexpected and uncontrolled

manifestation of new and unknown security and defence risks and threats. Namely, this assumption is used to focus on the need of an assessment of the national and institutional capabilities that provide a needed of business continuity and continuous resilience of the National Security System's functioning. To measure resilience and capabilities to respond to the possibility of influence of arising new risks and threats in the so called grey functioning areas of society, the possibility to interrupt the continuous execution of the basic functions of National Security System, to predict the possible influence over the designated responsible leading institutions or state agencies, and needed capabilities to minimise the existence of missing, insufficient or outdated capabilities is develop a special scientific-applied framework. This scientific tool provides an expert assessment of the resilience and capabilities of NSS institutions, including the influence on the decision-making process and the need for inter-institutional and international cooperation.

Research Framework

For the exploring the first stage of the research project named "Inter-institutional and international cooperation to combat hybrid threats" was developed a special Expert Assessment Card. The main subject of it use was the assessment of institutional capabilities to safe resilience of functioning and the same time to counter arising hybrid threats. The Expert Assessment Card was also designed to measure the need for capability development based on institutional specialization, on inter-institutional and international collaboration. The main research goals were development of a subject matter scientific and expert platform:

- for assessment of the institutional resilience;
- to respond of new destructive characteristics of emerging unknown risks and threats to the defence and national security;
- to stimulate an expert discussion of the emerging security challenges in support of further development national strategic documents;
- to support establishing of an integrated approach to the institutional capability development;
- to provide scientific and expert support for an assessment, planning and development of the needed capabilities.

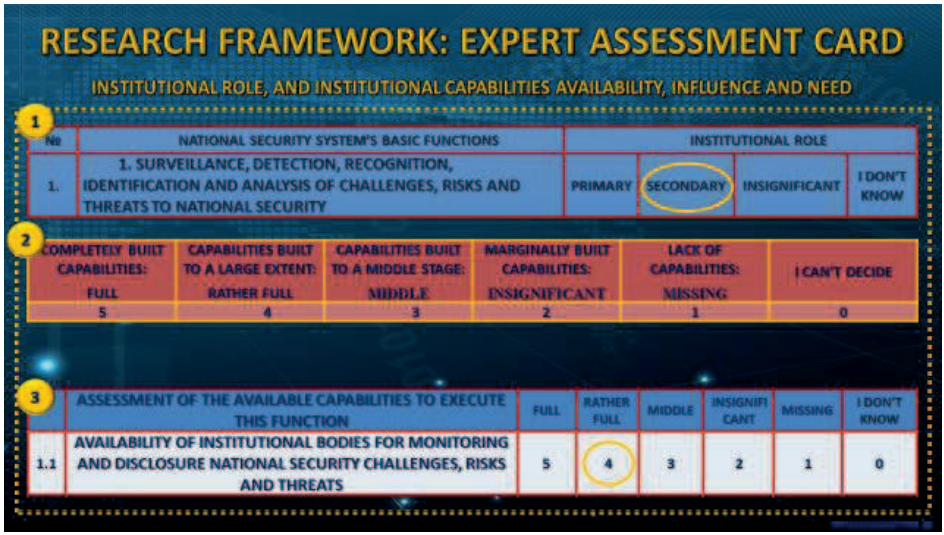
The First stage was executed in the format of expert assessment with application of a deliberately developed Expert Assessment Card, supported by a Business

Management Simulation Game. The Second stage was conducted in the format of an International Conference, and the Third on with publication of related with the project reports and findings.

This scientific research was focused on real expert assessment of the available and necessary institutional capabilities to measure resilience with implementation of basic NSS functions. Therefore, the research target group encompassed experts from ministries, state agencies and public organizations. Conventionally, this target group was divided into three subgroups:

- Group One – subject matter expertise participants from Ministry of Defence and Bulgarian Armed Forces;

- Group Two – experts from internal security and law enforcement leading institutions and organizations;



RESEARCH FRAMEWORK: EXPERT ASSESSMENT CARD

INSTITUTIONAL ROLE, AND INSTITUTIONAL CAPABILITIES AVAILABILITY, INFLUENCE AND NEED

1

No	NATIONAL SECURITY SYSTEM'S BASIC FUNCTIONS	INSTITUTIONAL ROLE			
		PRIMARY	SECONDARY	INSIGNIFICANT	I DON'T KNOW
1.	1. SURVEILLANCE, DETECTION, RECOGNITION, IDENTIFICATION AND ANALYSIS OF CHALLENGES, RISKS AND THREATS TO NATIONAL SECURITY				

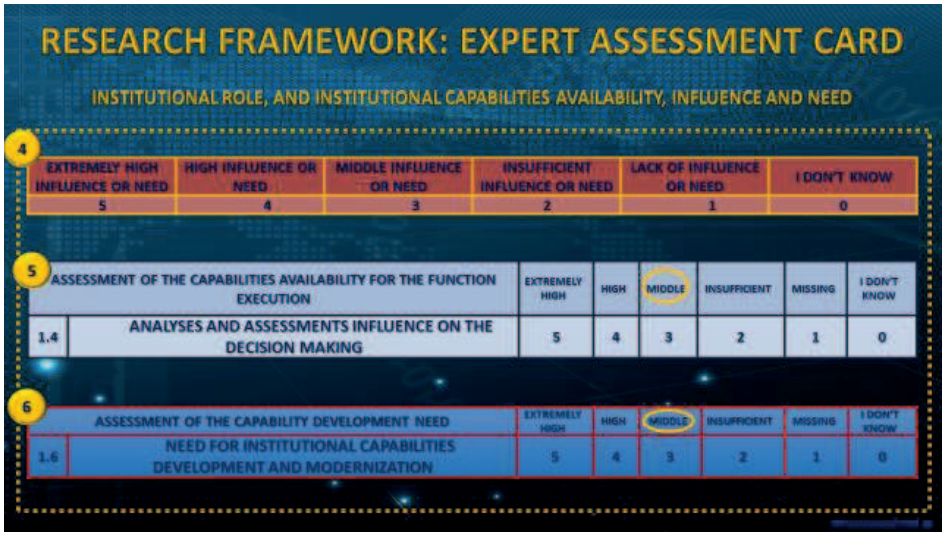
2

COMPLETELY BUILT CAPABILITIES: FULL	CAPABILITIES BUILT TO A LARGE EXTENT: RATHER FULL	CAPABILITIES BUILT TO A MIDDLE STAGE: MIDDLE	MARGINALLY BUILT CAPABILITIES: INSIGNIFICANT	LACK OF CAPABILITIES: MISSING	I CAN'T DECIDE
5	4	3	2	1	0

3

	ASSESSMENT OF THE AVAILABLE CAPABILITIES TO EXECUTE THIS FUNCTION	FULL	RATHER FULL	MIDDLE	INSIGNIFI CANT	MISSING	I DON'T KNOW
1.1	AVAILABILITY OF INSTITUTIONAL BODIES FOR MONITORING AND DISCLOSURE NATIONAL SECURITY CHALLENGES, RISKS AND THREATS	5	4	3	2	1	0

- Group Three - experts from the institutions or organisations with contribution and support to the National Security System functioning and capabilities development.



RESEARCH FRAMEWORK: EXPERT ASSESSMENT CARD

INSTITUTIONAL ROLE, AND INSTITUTIONAL CAPABILITIES AVAILABILITY, INFLUENCE AND NEED

4

EXTREMELY HIGH INFLUENCE OR NEED	HIGH INFLUENCE OR NEED	MIDDLE INFLUENCE OR NEED	INSUFFICIENT INFLUENCE OR NEED	LACK OF INFLUENCE OR NEED	I DON'T KNOW
5	4	3	2	1	0

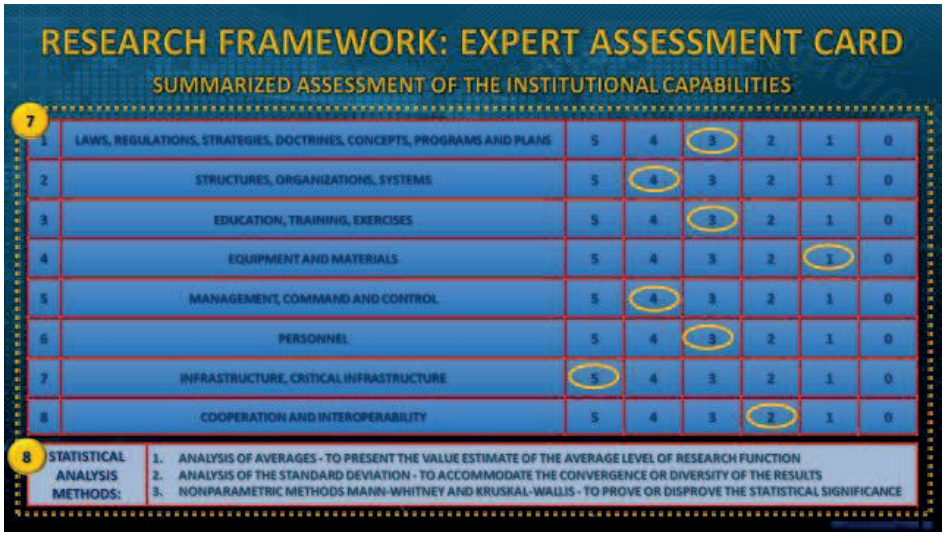
5

	ASSESSMENT OF THE CAPABILITIES AVAILABILITY FOR THE FUNCTION EXECUTION	EXTREMELY HIGH	HIGH	MIDDLE	INSUFFICIENT	MISSING	I DON'T KNOW
1.4	ANALYSES AND ASSESSMENTS INFLUENCE ON THE DECISION MAKING	5	4	3	2	1	0

6

	ASSESSMENT OF THE CAPABILITY DEVELOPMENT NEED	EXTREMELY HIGH	HIGH	MIDDLE	INSUFFICIENT	MISSING	I DON'T KNOW
1.6	NEED FOR INSTITUTIONAL CAPABILITIES DEVELOPMENT AND MODERNIZATION	5	4	3	2	1	0

The nature of this scientific research was focused on the NSS resilience and functionality, measured by an expert assessment, provided by the involved institutions with the possibility of the institutional capabilities to execute twenty one basic NSS functions. These functions were derived after a scientific and expert review of National Security System legal base and other normative documents of the NSS institutions.



RESEARCH FRAMEWORK: EXPERT ASSESSMENT CARD

SUMMARIZED ASSESSMENT OF THE INSTITUTIONAL CAPABILITIES

1	LAWS, REGULATIONS, STRATEGIES, DOCTRINES, CONCEPTS, PROGRAMS AND PLANS	5	4	**3**	2	1	0
2	STRUCTURES, ORGANIZATIONS, SYSTEMS	5	**4**	3	2	1	0
3	EDUCATION, TRAINING, EXERCISES	5	4	**3**	2	1	0
4	EQUIPMENT AND MATERIALS	5	4	3	2	**1**	0
5	MANAGEMENT, COMMAND AND CONTROL	5	**4**	3	2	1	0
6	PERSONNEL	5	4	**3**	2	1	0
7	INFRASTRUCTURE, CRITICAL INFRASTRUCTURE	**5**	4	3	2	1	0
8	COOPERATION AND INTEROPERABILITY	5	4	3	**2**	1	0

STATISTICAL ANALYSIS METHODS:

1. ANALYSIS OF AVERAGES - TO PRESENT THE VALUE ESTIMATE OF THE AVERAGE LEVEL OF RESEARCH FUNCTION
2. ANALYSIS OF THE STANDARD DEVIATION - TO ACCOMMODATE THE CONVERGENCE OR DIVERSITY OF THE RESULTS
3. NONPARAMETRIC METHODS MANN-WHITNEY AND KRUSKAL-WALLIS - TO PROVE OR DISPROVE THE STATISTICAL SIGNIFICANCE

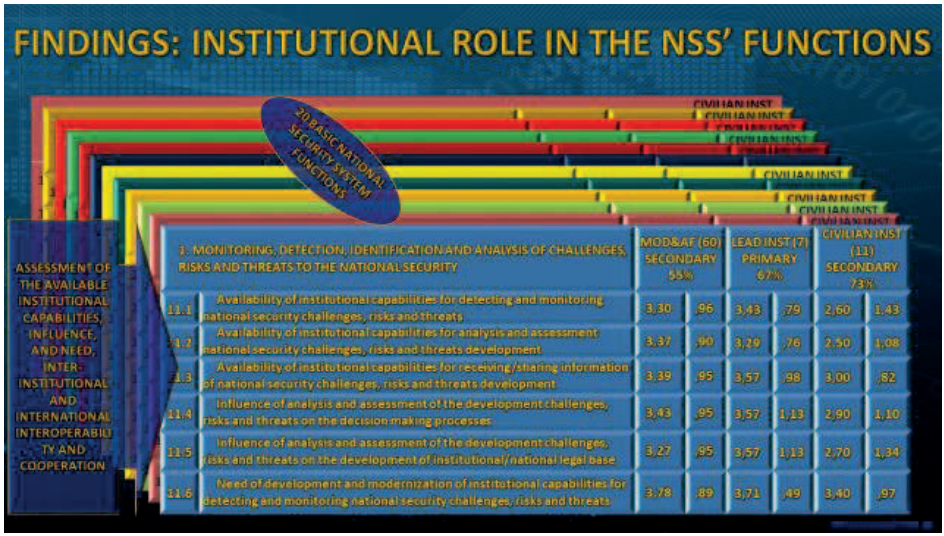
The application of the research methodology was conducted in two separate parts. The first one included filling out the specially designed Expert Assessment Card, following the procedures of scientific methodology "Delphi". The second includes an expert discussion on the particular topics in the framework of a Business Management Simulation Game. The specifics of the first stage's methodology, and the various forms of data processing and results analyses required application of different and separate steps for processing entire research results. The project team used several statistical methods for data processing and empirical analysis of the obtained from the assessment cards results:

- Analysis of averages[10] - to estimate the average level of the research functions;
- Analysis of the standard deviation from the mean value [11] - to accommodate the convergence or variance of the results for the evaluation of identical functions or capabilities;

[10] How To Analyze Data Using the Average, https://betterexplained.com/articles/how-to-analyze-data-using-the-average/

[11] Describing Data using the Mean and Standard Deviation, https://libraryguides.centennialcollege.ca/c.php?g=717168&p=5123683

- Nonparametric methods Mann-Whitney and Kruskal–Wallis[12] to assess the deviation from the normal distribution of the values in order to prove or disprove the statistical significance between the differences in the values of the studied outcomes



of institutions or organizations.

[12] The Kruskal–Wallis test is an extension of the Mann–Whitney test for more than two independent samples. Guide: Non-patametric Tests (Mann-Whitney, Kruskal-Wallis), https://www.learnleansigma.com/guides/non-patametric-tests-mann-whitney-kruskal-wallis/

The main research assumption is that National Security System functionality is based on the resilience and a continuous balance between the performance of the basic functions, and the availability of particular groups of institutional capabilities (on the right side) that allow the institutional performance.

The Expert Assessment Card includes 21 basic functions of the National Security System, identified and systematised through a deep analysis of national and institutional security related legislation base. The experts assessed their own institution role as primary, secondary or supporting, which they performed during the NSS functioning or when the institutions execute their designated by national legislation functions. The possibilities for the overall institutional resilience and ability to perform each of the basic NSS functions was assessed through the estimation of the availability of current institutional capabilities, divided into 5 to 7 key capability development areas, or the need for their further development.

The design of the first part of Expert Assessment Card provides an estimation of the institutional role (primary, secondary, contributing) to execute this function. The second part represents the measurement scale, applied from the expert for the assessments performance.

The third part is an Expert Assessment Card's tool, based on the capabilities imperatives, used for measuring availability of the researched groups institutional capabilities.

The forth part describes the research measurement scale rates that provide assessment of institutional capabilities. The fifth and sixth parts present a tool for measuring accordingly 5 - the influence of available capabilities on the decision making; and 6 - the need for future development and modernization of the measured groups of capabilities.

At the end of the assessment card, the availability of summarised institutional capabilities is assessed by measuring the eight imperatives of each group capabilities:

- strategic regulations, institutional legal base and internal normative documents;
- organization – organizational structure of the institutions;
- education and training;
- materials and resources availability;
- command and control or institutional management system;
- personnel or institutional social capital;
- infrastructure and facilities;
- interoperability.

The structure of the performed research during the second stage of the project as Business Management Simulation Game also was divided into several parts:

- The first one represents the group's discussion areas: possible threats, required capabilities in order institution to be resilient and to counter risks and threats, available capabilities, deficit of capabilities, and down the forms of inter-institutional and international cooperation to develop needed capabilities.
- The second part of the game summarises and discussion topics;
- The third one – discusses the evaluation of research findings.

Research Findings

Main Conclusions for the Methodology application

The research target group's structure encompasses the specialized expertise of three main sub-system groups of institutions in the National Security System, government agencies and public organizations. This classification of subgroups is based on a precise expert sign, oriented to ensure participation of the needed of institutional expert representation, as well as on the need of understanding the credibility and reliability of the research's findings. In order to obtain the highest representativeness

and credibility of the received empirical data and results, the subject matter experts were divided into three groups:

• First subgroup - Ministry of Defence and the Bulgarian Armed Forces;

• Second subgroup - institutions (without Ministry of Defence and Armed Forces) with a leading role in the implementation of the basic internal security and law enforcement NSS functions;

• Third subgroup - institutions and organizations with supporting role and contribution to the execution of the basic NSS functions.

The MOD expert group includes the largest number participants (60 experts) and it is the relatively most unified in term of the participants' expertise. Such composition of the subgroups forms a good basis as a prerequisite for a broad representation of statistical data and comparison of obtained data and findings after the assessments of the institutional role and capabilities of the researched institutions.

The other two subgroups were smaller. The second subgroup includes seven (7) experts from leading internal security and law enforcement institutions, and the third - eleven (11) experts from state institutions and organizations with contribution to the execution of the basic NSS functions. Their grouping into two separate subgroups forms two different subject matter expert platforms that included representatives of institutions with relatively common goals and tasks. At the same time, this wide profiling of subgroup composition allows the research results to be summarized with a number of conventions and the received empirical data to be adopted and further used only as guidelines for the analyses in support of already proven institutions role and capability development trends.

This explanation is necessary for interpretation of the research results and analysis for the NSS contributing institutions. Since the institutional subject matter expertise of each participant in the study is narrowly specialized and profiled, the received summary results and empirical data could be hardly considered as representative for each of the institutions and organizations in this subgroup. Such a specification is based on real research opportunities, for example to obtain an unexpected low assessment of available capabilities, because these groups of capabilities are available only in one of these institutions, and they are not related to the role and activities of all other institutions.

When analysing the aggregated data and results from the evaluation of the institutional role during their implementation for execution of some basic NSS functions, there is also a characteristic related to tripping of narrow specialization of the expertise, involved in the study. Therefore, the obtained results can and should be taken as representative for only one or for a limited number of the institutions from this subgroup. For example, leading (according to the state's legal requirements) institutional role for the implementation "Civil and of critical infrastructure", and " of public order, combating organized crime, law enforcement, investigation and court" functions should be considered as a primary responsibility only for institutions aside from the MOD. Nevertheless, because of mentioned reasons and in accordance with the obtained results, the roles of these institutions were assessed as minor or supporting/contributing.

On the other hand, the overall expert assessment results indicate that the available moderate-level capabilities are sufficient for the execution of the NSS function "Monitoring, control and of air and sea space, protecting the state sovereignty, independence and territorial integrity". Therefore, at this stage, the state should have built a reliable defensive potential for its national security and defence. At the same time, experts assessed as insufficient the obtained by average grade groups available institutional capabilities for the implementation the NSS function "Fight against terrorism, counterterrorism, counterterrorism, managing the consequences of terrorist acts".

During the assessment of each group's capabilities to accomplish these two basic functions, experts possibly subconsciously take into account:

- on the one hand Bulgaria's affiliation to the two security and defence related organisations - NATO and the European Union. This assumption in turn allows viewing as a common task provision of air and sea security and defence;
- on the other - state territorial integrity and defence - only in the context of international agreements and NATO collective defence.

During the capability assessment for the execution of the institutional role for the implementation of the second function, the expertise most probably takes into account timely increasing insecurity of Europe Nations, and the associated with the current

situation deficit and obsolescence of national and allied capabilities to counter terrorism.

Main Conclusions for the NSS Institutions

1. Conclusions for MOD and AF Capabilities

1.1. Regardless of legally delegated to MOD and AF execution of the NSS function "Monitoring, control and of air and sea space, protecting the sovereignty, independence and territorial integrity" in both national and Allied format, the average assessment summary of the available capabilities reveals a possibility for the institution to fulfil only the associated with this function basic tasks. Given a little higher aggregate evaluation of the need for building and improving these institutional capabilities, which are planned for realisation via large acquisition projects (e.g. basic Army, Air Force, and Navy platforms, provision of declared operational troops to the allied battle groups, monitoring and control systems, etc.) it is necessary that the MOD focus its management expertise for the realization of all these projects. At the same time, existing possibility of incomplete implementation of the institutional commitments to implement this function (in the areas of personnel, systems, weapons, communications, logistics and material support) creates real prerequisites for untimely and incomplete disclosure and realistic assessment, as well as slow response to new and unknown threats to national security.

1.2. A priority engagement of MOD and AF with the realization of the fundamental institutional role: “Implementation of Allied, International and coalition commitments to NATO and the EU reflected in relatively high aggregate assessment of existing institutional capabilities, compared with the assessment of available capability for execution of the previous functions. However, in future capability building and improvement MOD should take into account that the part of current obligations toward execution of this function are also performed with a number of constraints, resulting primarily from mandatory compliance to the national legal and regulatory frameworks, as well as from declared military formations capabilities for their participation in allied operations and missions.

1.3. The available MOD and AF capabilities allow the execution of their leading institutional role in NSS function “Crisis and Wartime Planning, State Reserves and Logistics”. The deployment of all assessment grades in the average levels of the measuring scale, as well as the need of assessing capabilities for higher availability mean that there still exists a possibility, in case of complex emergencies and an increasing external impact and influence, the institution to meet insurmountable difficulties during the implementation of this function. Additional obstacle could be considered a comparatively low level of sharing current NSS inter-institutional responsibilities and capabilities.

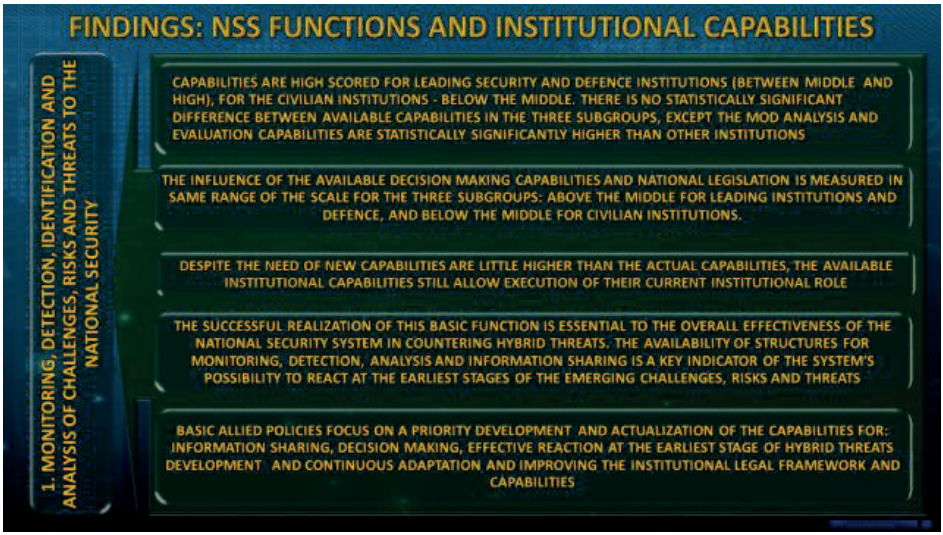
1.4. A relatively high degree of MOD involvement into state participation in Allied crisis and consequences management operations serves as a catalyst to maintain the current higher level of available capabilities that enable the realization of its institutional role. Accordingly, the summary of results estimates an average high need for the development and improvement of these institutional capabilities, suggested in turn by ever-increasing responsibilities of the Bulgarian Armed Forces to participate in such types of operations.

1.5. Although the MOD and AF institutional role is secondary in the realization of the NSS function “Consequences management in natural disasters, large industrial accidents and catastrophes”, the obligation for participation are result from the tasks to execute one of the three AF basic missions – “Peacetime Contribution to National Security”. It therefore calls for a continuous necessity to build and improve related institutional capabilities. The assumed average assessment of available capabilities on the one hand and the extremely high needs for development of these capabilities

on the other, point out that nowadays there is still a possibility of discrepancy between the need to respond to new challenges, risks and threats and limitations of the available capabilities. These assessments should be accepted as a real obligation of MOD leadership to devote more effort and resources to the modernization and upgrading of the institutional capabilities in line with the current real demands.

1.6. Given the proven necessity for continuous improvement of institutional capabilities to countering terrorism, and the continuously growing public interest and expectations call for expanding MOD and AF tasks in their secondary institutional role. The summary assessment results of the current institutional capabilities - below the average, and higher situated assessment results of the need for their building and upgrading suggest that an effective participation in the implementation of this function requires significantly more effort by the MOD and AF political and military leadership.

1.7. The continuously increasing demands and heightened public sensitivity to the realization of the NSS function “Public information, strategic communication, media and warning systems” require a particular attention to the formation of active MOD policy and the development of advanced capabilities for implementing all related institutional tasks.



1.8. Regardless of a legally prescribed institutional allocation of the responsibilities for implementation of the NSS function “Border security, border control and migration”, given the increasing demands of AF assistance to the Ministry of Interior on the one

hand, and research revealed statistically significant difference between the MOD capabilities availability and demand on the other, impose an immediate and effective response to building new and improving existing institutional capabilities.

1.9. The uniqueness of some Defence and Armed Forces capabilities for “Protecting people and critical infrastructure”, as well as a continuously increasing demand for capabilities for the implementation of this function require an increasing political and institutional military effort to respond to these needs.

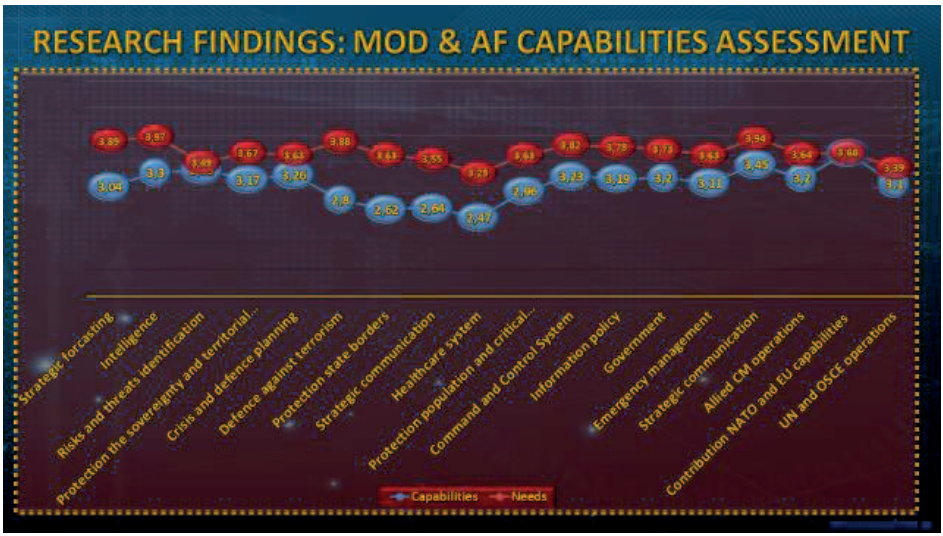
1.10. An effective response to the manifestation of new and unknown security risks and threats really require improvement of the institutional mechanisms to scientific research in order to increase pro-activity of military education and training.

1.11. A strong focus on the Allied effort growth to develop capabilities for the implementation of the NSS function “Horizon scanning, long-term forecasting, risk analysis and assessment, modelling and simulation” in order to follow the development and manifestation of security threats, as well as with an account of their importance to build real institutional capabilities for a preventive and proactive addressing new and unknown risks and threats, require a real review and reassessment of the NSS institutional roles, aimed to help concentrating all efforts on building the missing capabilities.

1.12. An increasing diversity of International Organisations’ operations and missions, and continuous expanding Bulgarian AF contribution in the UN and the OSCE operations, as well as the need for précising their participation commitments in other allied and international operations require a continuous improvement of defence capabilities for the execution of this NSS function.

1.13. The appreciation of the institutional capabilities influence for “Surveillance, detection, recognition, identification and analysis of development challenges, risks and threats to the national security” and the need for their updating and upgrading reveals the expected high importance of the execution of this function for the overall functioning of the NSS.

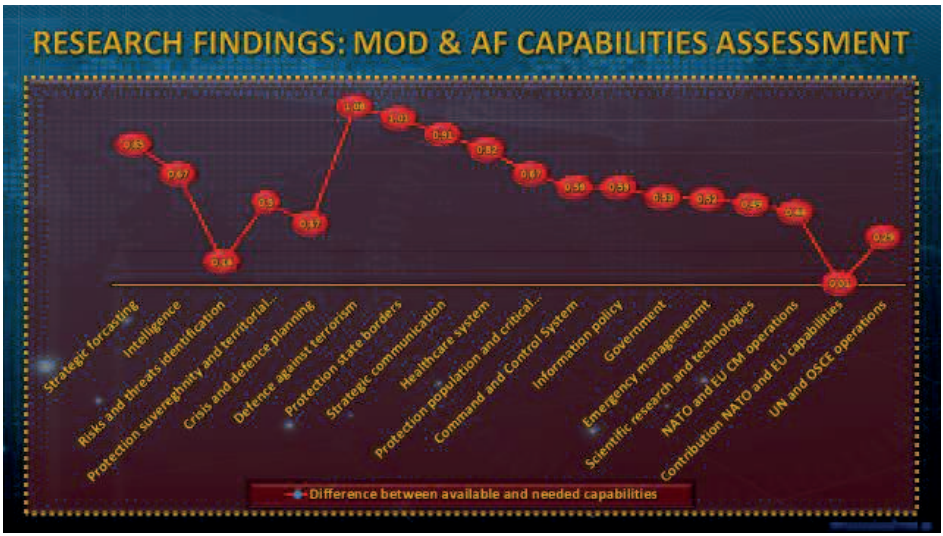
1.14. The strong influence of institutional groups capabilities of “Information policy, security and of information systems and networks” on all other institutions activities in operations in the information domain, as well as the growing need for information support to the implementation of each of the NSS functions, require first a reassessment and updating of current policies and capabilities, and second - a



continuous improvement of institutional and national measures to protect information and networks from unauthorized access and malicious use.

1.15. The unique responsibility of each NSS institution in National security and Defence Policy formation and capability building, as well as the need for planning and execution of their own institutional policies, require possession and continuous update of the needed capabilities. Accordingly, the specifics of formation and implementation of the institutional policy shall not affect the obligations of national executive authorities for the formation and coordination of the overall national security and defence policy priorities, like State Security Council, the National Assembly Commissions, and Presidency Advisory Council on National Security. Therefore, the revealed high need

for institutional capabilities improvement should be in deep correlation with other national institutions capabilities.



1.16. High expert assessment of “Intelligence” institutional capabilities, and the deep influence of the availability of these groups capabilities over the NSS management, as well as the continuous need for new capabilities, lay on a clear understanding of the military intelligence important role and the uniqueness of MOD and AF institutional capabilities. Given the specific development and functioning of intelligence systems, it is a pure institutional obligation to update continuously the existing and building new capabilities to execute this NSS function.

1.17. With a clear expert underestimation, the MOD and AF institutional role for the execution of one of the most important NSS functions “Command, control and coordination” was evaluated as secondary. Accordingly, the available institutional capabilities that assure its performance are rated slightly above the average, and the same evaluation receives the need for their improvement. A legally MOD and AF requirement is the responsibility to develop Command and Control System basic elements and relations in peacetime and wartime, as well as to maintain their interoperability with the other NSS institutional elements of these systems, including NATO and allies, the EU and partners C2.The estimated correlation between the actual availability and the need for institutional capabilities today could be taken as a guarantee for current operational readiness to identify, track, analyse and ensure an

expected adequate response to newly arising and unknown threats and risks to national security.

1.18. The relatively low assessments of the MoD and the Army capabilities of health care and response to the major emergency medical situations (like quarantines, epidemics, pandemics) are probably provoked by an incomplete consistency of the current AF medical support system with a strong concentration of all: pre-hospital, hospital treatment and rehabilitation in one medical structure - Military Medical Academy. At the same time, the assessments of a clear institutional necessity to build new and improve existing medical capabilities for the execution of this function are relatively high. Given the unique state capabilities and a very high MOD and AF responsibility to provide healthcare services and medical treatment, as well as the obligation to lead emergency management activities, an obligatory precondition for the institution is to perform an overall review and reassessment of the current AF medical support structures, and their obligation to build needed capabilities.

1.19. Regardless of the MOD effort, including a continuous update of AF development strategic plans, this aggregate assessment of current capabilities for the performance of the institutional role during the execution of the basic NSS functions reveals a clear need for a new strategic review of the overall institutional capabilities. The most appropriate period for its performance is 2018, along with planned interim review of "Armed Forces Development Plan 2020" as part of the implementation of the "Defence Capabilities Development Programme of the Republic of Bulgaria Armed Forces 2020".

1.20. A specific attention should be paid to the timely acquisition of the MOD and AF needed capabilities that ensure the execution of its primary institutional role during the implementation of basic NSS functions. The development of these operational capabilities could as well ensure a continuity and consistency of the technological, conceptual and material improvement of all other AF groups of capabilities. Given the unification of the development and use of defence capabilities – development and operational use of a single set of AF capability Packages to perform all their tasks in the NSS, an appropriate next step would be organising and conducting a specialised expert assessment of the overlapping and any duplication of the legally prescribed internal-institutional responsibilities for development of the NSS capabilities. It will support reviewing and clarifying also the needed levels of institutional stockpiles,

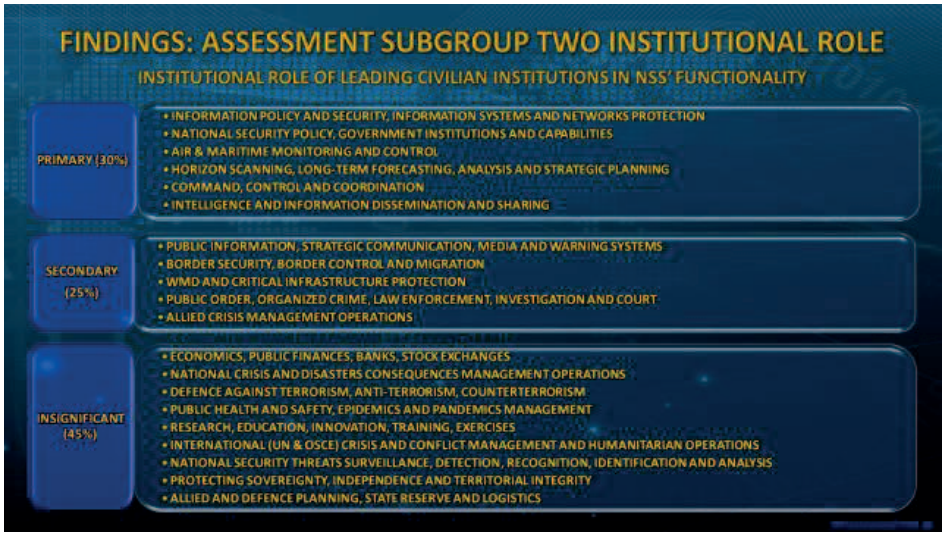
possible institutional inter-changeability and interoperability during the process of development and maintaining these institutional capabilities.

2. Lessons Learned from the evaluation resilience of the leading internal security institutions

2.1. Relatively high ratings to the institutional capabilities availability and demand for “Information policy, security and of information systems and networks” could be adopted as a result of understanding their high influence over the execution of all other NSS functions, including the overall information assurance of NSS operability. With an accent on expanding the influence of these capabilities, and the continuity of the information technologies and practice improvement, the plans for their further development should provide a continuous update of the information policy and capabilities, including information measures against unauthorized access and malicious use.

2.2. With a clear understanding of the strong influence of institutions with leading role in the NSS over the “Formation and implementation of all sector policies in the national security domain”, the generalized high rating of the availability and need for these capabilities, they could be seen as indicative when taking into account the specifics of policy formation and implementation, as well as their contribution and influence on the formation and coordination of national security and defence policy.

2.3. The relatively high evaluations of the availability and influence of the group capabilities on “Surveillance, detection, recognition, identification and analysis of development challenges, risks and threats to the national security”, as well as higher than average assessment of their upgrading need, reveal the perceived importance of an effective execution of this function and its impact on the overall NSS efficiency.

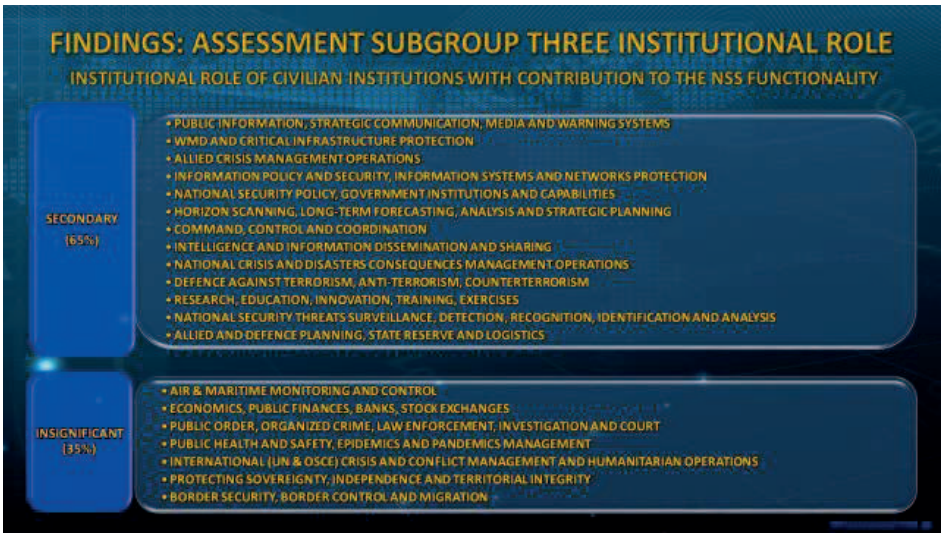


2.4. A relatively high expert assessment of the need for cooperation and interaction could be seen as support to the recognized need to increase the Allied effort in capability building to implement NSS function "Scan the horizon, long-term forecasting, analysis and risk assessment, modelling and simulation of the national security risks and threats". Although existing institutional groups of capabilities are assessed at middle level of the scale, their importance for maintaining the preventive and proactive NSS readiness to tackle new and unknown risks and threats need periodic reassessments of institutional roles of all NSS institutions, as well as a concentration of institutional efforts on the building of missing and modernizing existing capabilities.

2.5. The summary evaluation report which recognizes the importance of institutional contribution to the development and operation of national security management systems reflects the middle level assessments of institutional groups of capabilities for execution of NSS Command and Control function. This function is evaluated as secondary for the leading internal security and law enforcement institutions, although each of them has a direct responsibility for the development and operation of particular elements of the overall NSS architecture and management. The actual existence of available capabilities could be taken as a guarantee for the efficiency and continuous institutional readiness for identification, tracking, analysis and immediate response to the new and unknown national security risks and threats.

2.6. The summarised expert assessment of institutional “Intelligence” of the second subgroup institutions and their influence over the NSS management, as well as the assessment of the need for new capabilities are in the middle of the measurement scale. These results could be assessed as a confirmation of the intelligence important role for the NSS functionality. At the same time, a relatively greater appreciation of the need of new capabilities, as well as the need for a deeper institutional interaction during their development suggest that expert expectations for future institutional role and capabilities will continuously increase.

2.7. The evaluation of the groups institutional capabilities of state internal security agencies to implement “Crisis and wartime planning, state reserves and logistics” function revealed that their availability allows a conventional execution: the evaluations of current stocks are relatively low, situated in the range between low and moderate on measurement scale. The deployment of the need assessment are little higher than the availability estimates and reveal a likelihood during possible complex or emergency situations with a strong external influences and ultimate overloading that institutions might be involved in the execution of this function with possible conventions and difficulties.



2.8. The direct institutional responsibility of internal security and law enforcement organizations for the execution of “Public order and law enforcement” action allows the relatively low summary assessments of the available capabilities not to be

considered trustworthy. Although their evaluation is in the middle of the scale, only a relatively small number of institutions carried out the basic NSS tasks: Ministry of Interior, Ministry of Justice, and the National Security Agency etc. It means that in the wide-expert structured second subgroup, the assessments are fuzzy performed – i.e. they are dominated by a realistic assessment of a lack of capabilities outside the mentioned institutions. For the same reasons, the summary assessments of institutional capabilities demand for the execution of this function are relatively low and do not seem quite relevant to perform a leading institutional role.

2.9. The increasing demands and expanding public sensitivity towards the realization of the function “Public information, strategic communication, media and warning systems” require further attention on the evaluation of available capabilities for the execution of the institutional tasks of internal security agencies. Therefore, the assessments of availability and demand for institutional capabilities cannot be accepted with a full confidence either.

2.10. Already tagged reasons for received significant undercutting of the summary assessments of the institutional capability availability and demand to implement NSS function “ of population and critical infrastructure”, as well as the assessment of the increased need of capabilities building, cannot be accepted as a downgrading the expectations of the growing needs, as well as of additional institutional effort to build and improve these institutional capabilities.

2.11. The secondary role of leading internal security institutions for the implementation of NSS function “Implementation of allied, international and coalition commitments for participation in NATO and the European Union operations and missions” is performed with available institutional capacities assessed lower than middle of the measurement scale. The need for development and improvement of these capabilities is measured above the middle. These results allow concluding that there is an obvious likelihood the part of these institutional obligations to be implemented by conventions and restrictions.

2.12. Appropriate instruments to obtain more reliable assessment results for each of the institutions included in the subgroup of the leading internal security would be organizing and conducting a specialized expert assessment separately for each of them.

3. Main Conclusions for the Contributing to NSS Institutions

3.1. The estimated need for a continuous development and improvement of the institutional capabilities to “Counter terrorism” has not been vividly reflected in the evaluation of the summarised results of the currently available institutional capabilities. A clear statement of the institutional capabilities deficit is a difference between the summarised assessments of capabilities demand which substantially exceeds the available capabilities assessments. The results analysis reveals a growing need to lay more institutional efforts in order to overcome the disclosure deficit of institutional capabilities.

3.2. This institutions subgroup role for the execution of NSS function “Consequences management of natural disasters, large industrial accidents and catastrophes” was evaluated as a secondary. According to the expert assessments for performance of this role, the supporting institutions have middle level on the scale available capabilities. The significant difference between the assessment of middle level available capabilities and a much higher estimation of the needs for their development testifies that there is a high likelihood of an incomplete implementation of these institutional obligations provoked both by the deficit of available capabilities and the institutions inability to overcome existing limitations in case of need to address new and unknown challenges, risks and threats to national security.

3.3. Summarized average grades of availability and influence of the institutional group capabilities for the implementation the NSS function “Monitoring, detection, recognition, identification and analysis of development challenges, risks and threats to national security” and the estimated need for their upgrading reveal a clear correspondence between the availability and demands for these type of institutional capabilities.

3.4. The relatively low expert assessments of institutional capabilities on one side, and their impact over the entire NSS management, as well as the need for new capabilities for the execution of NSS function “Intelligence sharing, information and knowledge provision” are probably received because of the comparatively low institutional role and the insignificant number of tasks of this institution subgroup.

3.5. The inexpensive engagement of the contributing institutions to the implementation of the basic NSS function “Participation in Allied crisis and consequences management operations” also affects capabilities current status with a low grade of

their availability. At the same time, the estimated above the average need for the institutional capabilities development and improvement reveals a trend of continuously increasing responsibilities of all state institutions to further participation in these operations.

3.6. The growing influence of institutional capabilities on both the execution NSS function “Information policy, security and of information systems and networks” and the implementation of all institutional obligations and all system functions to protect national security suggest on the one hand maintaining a constant further update of current policies and capabilities, and on the other - implementing more effort for the coordination of institutional measures to protect the NSS information.

3.7. The participation of all institutions in shaping the NSS policies requires possession and constant update of necessary capabilities to execute “Government security policy and system capability building”. This policy implementation specifics for each NSS institution does not replace the highly acclaimed need to reconcile common priorities of the national security and defence policy. Therefore, in full compliance can be regarded the revealed from the expert assessments high demand for new capabilities and the inter-institutional need for further cooperation and interaction in the development of these groups capabilities.

3.8. Current status of the available capabilities (with an assessment above the average on the measurement scale) to perform a secondary role of the contributing institutions to the execution of NSS function “Crisis and wartime planning, state reserve and logistics” reveals a real opportunity for the execution of these tasks. The relatively high assessment of the need for development and improvement of institutional capabilities most probably takes into account the probability of the continuously increased needs to react to the complex emergencies or external influence and impact.

3.9. Relatively low assessments of available institutional capabilities and their impact on the decision-making process could be considered as a result of recognition the entailing role of this subgroup for the execution of NSS function “Scan the horizon, long-term forecasting, analysis and risk assessment, modelling and simulation the development and manifestation of national security threats”. Given the growing importance of the implementation of these tasks for the operability of all NSS institutions individually and the system as a whole, as well as in order to increase their

timely responsiveness in dealing with new and unfamiliar risks and threats, require institutional revaluation, planning and development of new and missing capabilities.

3.10. Although the aggregate assessment of institutional capabilities for the implementation NSS function “Command, Control and Coordination” is a little below the middle on the measurement scale, the increased needs to maintain a constant readiness and NSS management, the total evaluation of the need for increasing capabilities is relatively high. The understanding of the high importance of the availability of institutional capabilities for the implementation of this function stems from the need to maintain constant system operability and readiness to respond to new and unknown national security threats and risks.

3.11. The aggregate high assessments of the institutional capabilities for “Research, education, innovation, training, exercises” could be assumed because of the study reported needs for a continuous improvement of the measures to effectively counteract new and unknown security risks and threats. This expert assessment reveals that the capabilities improvement is possible through raising the level of scientific support to their development: scientific researches, innovations and continuous improvement of education and training intensity and quality.

3.12. Simultaneously increasing society demands and expectations for increasing efficiency of the implementation of NSS function “Public information, strategic communication, media and warning systems” presume the availability and timeliness of a sufficient institutional capacity (measured in a middle degree of the scale). The summary appreciation of these capabilities impact is probably a result of future expectations for their influence on public opinion (the assessment of the need for this group of institutional capabilities is above the average).

3.13. High grades of the need for capability development for the execution of NSS function “Civil and critical infrastructure ” most probably takes into account the increasing current NSS institutions liabilities and the ambition to continuously enhance their efforts to update and replenish the institutional capabilities.

3.14. The need for a continuous update of plans to support the implementation of all NSS basic functions in this expert assessment is revealed as a growing need for periodic reviews and evaluations of institutional capabilities. Particular attention should continue to be paid to maintain the needed capabilities to ensure the implementation

of institutional roles in the execution of basic NSS functions and to ensure a continuous technological, conceptual and material adaptation of existing institutional capabilities.

4. Conclusions from the Business Management Simulation Game

4.1. The discussion format of conducted Business Management Simulation Game allowed identification of a number of areas of state institutions functioning where is possible emergence of national security risks and challenges whose

combination and growth would be unexpected and they could turn into real threats with complex and damaging consequences to the national security. Their emergence, nature and characteristics could be qualified as hybrid, not only as manifestation, but also as final effects. The main tasks arising from the need to maintain a continuous NSS institutional readiness and resilience could be grouped into the following areas:

4.1.1. The actualization of NSS legal base in order to enhance the changes into institutional roles and responsibilities that allows the application of a comprehensive approach into capability development and using to build institutional resilience and to counter hybrid threats;

4.1.2. Need for an adequate resilience and countering hybrid threats' conceptualizations as a basis for development of working strategic documents and involvement of all state institutions and leadership with the development of a system of measures to enhance the institutional resilience, prevention and effective response to hybrid threats, disruptions, crises and emergencies;

4.1.3. Leveraging the national strategic documents with NATO and the EU requirements in order to improve the resilience against hybrid threats: Participation in the development of a capstone concept "Military contributions to countering hybrid threats"[13]; the strategy for NATO role to countering hybrid warfare; Action Plan for strategy implementation, and the EU Joint framework to counter hybrid warfare[14];

4.1.4. Government - policy, stability and influence over foreign policy orientation, violated management practices and public trust;

4.1.5. Crucial sectors of state economics - energy, resource management, banking and finance, internal security, defence, healthcare, social policy, etc.;

4.1.6. Information policy, cyber , media networks and information influence;

4.1.7. Threats to society political stability and integrity;

---

[13]http://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf;

[14]http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018;

4.1.8. Influence of external and internal factors - combating terrorism, crises, conflicts, migration, demography, ethnic separation, radicalization, unemployment, social exclusion;

4.1.9. Internal security and law enforcement - organized crime, against illegal migration, human trafficking and drug abuse, petty crime, corruption, legal , public trust in the law-enforcement bodies;

4.1.10. Implementation of EU and international obligations and agreements.

4.2. The discussion of potential areas and forms of manifestation of hybrid threats to national security reveals as the most significant opportunities a complementary, overlay or combination of the negative effect of internal and external security events with lower possibility to predict their long-term manifestations, effects and consequences. The sophisticated identification and countering their manifestations require a mandatory and permanent operability of specialized institutional structures for recognition, tracking, analysis and countering these threats to the national security.

4.3. The expert summarised assessment of the occurrence probability of such threats is ranging from moderate to high. The assessment suggests an immediate response to the urgent need of implementation of effective measures to enhance the preventive institutional readiness and to develop working NSS TTP (Tactics, Techniques, Procedures), contingency plans and other institutional capabilities in order to respond to unexpected development and evolving of hybrid security threats.

4.4. A strong emphasis was put on the need for further acceleration of the institutional reforms in order to better a complete development and subsequent absorption of the institutional and national potential by using all the possible instruments for inter-institutional, inter-institutional and international political dialogue, large-scale information campaigns, public diplomacy mechanisms, and combination of economic, information and social measures to increase the level of public awareness, confidence and institutional resilience.

4.5. As currently urgent was defined the need for proactive national strategy for enlarging inter-institutional and international cooperation and collaboration to build and share use of new and renewed capabilities to countering hybrid threats.

4.6. The continuously increasing role of modern education and training was acknowledged, as well as the need for comprehensive scientific research to support

institutions capability development in the subject matter area of countering hybrid threats, as well as to support, update and develop needed specialized expertise for NSS.

5. General Conclusions

1. The research results show that the execution of a relatively small part of the basic NSS functions (20 percent, or four of twenty) is performed with institutional capabilities, estimated at above the average level on the measurement scale.

2. The majority of the NSS functions should be performed with capabilities whose evaluation reveals a level of development and availability in the middle as a significant part of these capabilities are rated even lower than the average level of the

measurement scale.

3. The aggregated data of a comparative analysis of the assessments of MOD experts of the capabilities availability and needs to perform basic NSS functions revealed the existence of multiple groups of capabilities, which needed improvement and supplement because the assessments of the need for these group capabilities are significantly higher than assessments of their current stock.

4. Given the insufficient institutional representation in this scientific research as number of representatives from different NSS institutions with an exception for MOD and AF, and therefore used a wider expert profile of the participating groups, based on the expected institutional contribution to the NSS operability (derived from current

legal obligations of the institutions), the assessment results for the performed institutional role during execution of these basic functions could not be considered as fully representative for each of the grouped institutions.

5. Additionally, the assessment results reveal a narrow institutional and sector specialization of the participating experts. Because of that it could be assumed that the institutional role for execution of some basic NSS functions most probably has not been evaluated in full compliance with the prescribed legal requirements and there is probability that the assessments reflect the specific for each institution statutorily assigned responsibilities and tasks.

6. The summary also reflects a clear trend for the expertise to follow and reflect the current for the institutions political agenda. For example, the overestimation of some of the institutional needs is reflection of the prioritised institutional emphasis on the current department expertise responsibilities to support decision-making process on contemporary topical and important political issues as well as in building needed capabilities in order to enhance the NSS functionality.

7. The narrow specialization of most of the expertise could be seen as the basic motivation of MOD experts to allow the measurement of an adequate correspondence between the expert assessment highlights and the requirements of the actual institutional legislation and strategic documents. It also could be assessed as a reflection of the declared policy and current institutional commitment which are primarily directed toward increasing the effectiveness of participation and contribution to the Allied development and operational use of the Bulgarian AF capabilities.

8. Due to the specific expert response to the reasons for an apparently following the institutional prioritization during the execution of basic NSS functions in the area of security and defence, as well as the institutional commitment to the ongoing development of specific groups capabilities it could be considered as unappreciated the necessity to develop and update some of them for the execution of very important missions: to protect state territorial integrity and independence; to combat terrorism (regardless of the recent effort to adopt a special law); to support internal security; and to protect the population and critical infrastructure.

9. Given the narrow specialization and orientation of institutional expertise and the likelihood of underestimation of the need for Command and Control System capability

building for the execution of the function “Monitoring, identification and analysis of new security challenges and threats”, the research results allow to conclude that despite the institutional efforts there is still a high probability of occurrence of new and unknown hybrid threats to national security. The likelihood of their manifestation is particularly high in the area of implementation of shared institutional obligations to the basic NSS functions or in the common inter-institutional areas of building national security and defence capabilities.

10. The analysis of the survey results and conclusions also reveal that in order to overcome the capabilities deficit and increase the institutional and national readiness to deal with unknown security challenges, risks and threats, it is needed:

10.1. To present the research results at the MOD and AF councils.

10.2. A comprehensive review and update of the National Security System legal and regulatory framework.

10.3. To develop a detailed matrix with classification of the institutions roles and responsibilities for execution the basic NSS functions.

10.4. A priority development and improvement of the capabilities needed for the performance of leading institutional roles during the execution of NSS essential functions.

10.5. An update and inter-institutional prioritization of each institution commitment to the national capability building for the implementation of all legally prescribed responsibilities and institutional role to support NSS operability, including expanding the institutional contribution to the shared building of national and Allied capabilities.

10.6. To develop working operational mechanisms (political initiatives, strategies, programs, plans, courses, scenarios, exercises and training) in order to improve education and training quality of the institutional expertise to enhance the role of inter-institutional and international cooperation and collaboration during the capability development and use to support the execution of fundamental NSS functions.

11. Future opportunities for a practical application of the research methodology and results:

11.1. The research results allow a further practical application of this testified and proven scientific methodology with specially designed “Expert Assessment Card” for the review of developed institutional capabilities during the 2018 review of the implementation of "Armed Forces Development Plan 2020".

11.2. The study analysis is a confirmation of the need to perform an after 2018 assessment of the Military Education System capabilities, as well as the projects for their future development. The assessment could be based on improving legal regulation and system optimization in order to:

- line and use the education and training for the personnel of all security sector institutions;
- establish optimal conditions for the academic staff development;
- optimize the structure of the Defence College, National Military University and Naval Academy;
- change forms and terms of education and training;
- update their academic curricula and expand participation in national programs and projects;
- enlarge military education system contribution to improve the effectiveness of NSS capabilities and system interoperability.

The applied research methodology and obtained data and results reveal a number of National Security System limitations, shortages and incomplete groups of needed capabilities. A timely and prompt response to the importance of these research findings would be a review and update of NSS institutions legal base, missions and task. The results from the performance of this review might be used for the

actualization of current Armed Forces development programs, plan and projects. Already testified methodology with application of Expert Assessment Card could be included in the scientific support tools in case of planning and conducting a comprehensive review of National Security System roles, missions, and capabilities.

6. Analysis and Evaluation of the National Crisis and Emergency Management System

6.1. Analysis of the National Crisis and Emergency Management System

The information age is constantly changing the structures, behaviours and relationships in the globalized world and diversifying security threats. The attempt to reject the unipolar approach in the organization of international relations through changes in political geography (or changes in known in the past geopolitical areas) reflects the dynamics of the security environment. It forces the countries to look for new approaches to define in a new way needed capabilities to guarantee their national security, territorial integrity and sovereignty, as independent players or in collective security and defence systems. The destructive results from the shifting of the world's centres of gravity require building of new capabilities to improve resilience, to prevent risks and to respond to threats, arising crisis and emergency management into an integrating paradigm for a new conceptualization of the structuring, capabilities and responsibilities of the national security systems.

The past national and Alliance’s participation in the processes of crisis management: in Cambodia, in the Balkans, in Afghanistan, Iraq, current providing assistance to Ukraine, as well as support number of countries in the consequences management after crises and natural disasters, the increasingly growing responsibilities of the NSS require the implementation of proper scientific researches, analyses in support of development a new applied national mechanism for improving institutional resilience and state’s capabilities for crisis and emergency response.

The transformation of the Mechanism and process of Crisis and Emergency Management into a holistic integrated national package of capabilities can bring to a new, higher level the interagency mechanisms for generating complex management decisions, sending and receiving political messages and feedback from them. This approach will break the traditional decision-making formats and framework and will provide for an expanded presence of civil society in state governance process. A similar capability package will contain a new conceptualization of the institutional

responsibilities in a national Crisis and Emergency Management process, will support development of an unified national crisis response system, based on the standardized business continuity management, institutional and state's resilience, and increased response capabilities, measures and operations as an integrated mechanism for their implementation.

There is a danger the existing institutional capabilities, attitudes and practices in nowadays society, designed for a mental and practical alignment between the crisis and emergency management and consequences management, caused by natural disasters, major accidents and catastrophes, that might be fully incorporated into a newly adopted concept and law for institutional resilience, Crisis And Emergency Management. Therefore, the first task and an extremely responsible approach to the improvement of the national legal/normative base, require a formation of new public understanding and attitude, new conceptualization for the institutional responsibilities and design of the NSS as a National System for crises and emergency management. This system will be based on the modern requirements to the security systems and will take into account the past Lessons Learned, experimentation practices in order to reach new positive results in a new national legal framework.

An expert attitude toward the crisis as a "national or international situation in which there is a threat to the priority values, interests and goals"[15], allows defining the key elements of the Crisis and Emergency Management process:

- the receipt, processing and analysis of information;
- the assessment of the situation and definition of the state of crisis in accordance with the accepted criteria;
- the determination and planning of alternatives for resolving the crisis;
- bringing the crisis under control;
- the return to stability.

The modern crises and emergency management is considered as a system that has legal obligations to apply diplomatic, political, military, economic, humanitarian and other measures, needed to establish the signs of the emergence of a crisis, to lead

[15]Reported in the initial version of the repealed Crisis Management Law, http://www.maxiconsult.bg/pdf/ZUK.pdf ;

decision-making for application of anti-crisis/emergency actions/operations. The main goals to build a National Crisis and Emergency Management System are the needs:

- to increase the capabilities for the prevention and the impact of emerging tension and preventing the possibility of their turning into a large disruptive crisis;
- to arise effectiveness of crisis management of new and emerging crises with possibility to prevent them from overgrowth into armed conflicts;
- to provide for timely civil and military preparation to resolve a wide range of crises;
- to serve as a predictable mechanism to reduce violence and prevent escalation;
- to allow bringing the crisis under control and managing until an overall return to stability.

Crisis and emergency response options might be incorporated into standardized response measures. These measures allow from one side keeping organizational functionality, based on standard business continuity management practices, preserving resilience, enhancing national security and in the pre-crisis period, and from the other – a timely application of anti-crisis measures and crisis and conducting crisis and emergency response operations. They will cover a wide range of political, diplomatic, economic measures and initiatives and capabilities for conducting operations – peacebuilding, peacekeeping, humanitarian, information, psychological, counter-terrorism, support for application common Alliance measures of sanctions and embargoes, emergency management search and rescue, disaster relief, consequences management operations. As special measures of the NSS might be generalized operations against terrorism, to prevent from threats of using weapons of mass distraction, to reduce risk factors and prevent from possible actions of terrorist organizations and to expand the capabilities for consequences management after terrorist acts. This number of operations expands by the need of supporting provision of border security, arms control, and uncontrolled of mass movement of peoples/refugees. During the implementation of these measures and conducting crisis and emergency response operations, the NSS/Crisis Management System needs a continuous interaction with the national mass/social media.

The establishment of a national crisis management system, its compatibility and interaction with the NATO collective crisis and emergency response system, as well

as interaction on a bilateral basis with national systems and international organizations, are crucial for effective crisis and emergency prevention and management.

The National Crisis and Emergency Management System can be used as an integrating strategy for the country's security system for better construction and spending of resources through real-time information exchange, building shared awareness in the system, expanding the possibilities for crisis prevention, generating information superiority in a standardized decision-making process - resulting in increased management and response efficiency. To realize the benefits, it allows:

- mobilization of all national capabilities for the prevention or resolution of crises at the earliest stage of development;
- guarantees political/civilian control over the activities of all crisis and emergency management bodies and forces at each phase of crisis and emergency management;
- during its functioning, the results of the crisis management do not provoke an emergency to become a crisis with a different nature or in another region;
- guarantees the development of the necessary capabilities, the education and training of the system’s personnel, preparation of the institutions, state, population and the national economy to increase resilience and to protect during the crises and emergencies;
- ensures capability, technological and procedural compatibility with the NATO crisis and emergency management system, as well as with the EU crisis and emergency management mechanism;
- the emphasis on preventive activity and crisis prevention and conflict management with the use of the entire potential of the system, actively works with the media and development capabilities for conducting a wide range of information operations.

The crisis and emergency management system covers the management bodies and centres, communication and information system and crisis and emergency response forces. The operability of the individual elements depends on the functioning of the National Disclosure System and the interaction with the National Early Warning System.

The governing bodies carry out the monitoring, analysis and assessment of the risk and the situation, predict the potential opportunities for the occurrence of crises, prepare solutions, carry out preliminary and situational planning, announce and lead the implementation of standard measures and operations for responding to crises and emergency situations. They are structures of national, departmental and territorial management units.

A permanent expert information-analysis management body can be the National Centre for institutional resilience, Crisis And Emergency Management. It is intended for:

• discovering, monitoring and analysis of risks and emerging threats to defence and national security, middle-time forecasting for arising of potential crises;

• coordination of national efforts in crisis prevention measures;

• provision of an efficient infrastructure for institutional resilience, Crisis And Emergency Management;

• ensuring constant exchange of information on the management of crises and emergency situations between state's institutions;

• preparation of proposals for application of preventive measures and response operations to crises and emergency situations;

• development of cooperation in the area of crisis and emergency management.

In addition to specific analyses and forecasts during a crisis, the centre develops a general assessment of the situation, proposes preventive response options, coordinates the application of contingency plans and coordinates the response forces actions. The composition of a National Crisis and Emergency Management Centre would include:

- National Situation Centre;
- Department of Analysis and Forecasts;
- Administrative Department;
- Interagency Expert Group.

The strategic expert units of the ministries, departments and crisis and emergency response forces provide the expertise of the centre. For the management of crisis and

emergency response forces, a Joint Operations centre is established, based on the infrastructure of the National Crisis and Emergency Management Centre.

Crisis and emergency response forces and means ensure the practical implementation of anti-crisis measures and the conducting of crisis and emergency response operations. They include pre-announced personnel and structural units from the specialized national services, the armed forces, the forces of the Ministry of the Interior, the Ministry of Health, the Ministry of Transport and Communications, the Civil Defence Agency, other ministries and agencies, municipalities, legal entities and voluntary formations.

The implementation of preventive measures is carried out according to a standardized procedure and preliminary plans to ensure the of citizens, for urgent actions in the management of the consequences and for interaction with the bodies of the state administration and local government. Participation in the resolution of crises outside the country is in accordance with national, international law. In the conditions of an international military-political crisis and a clear mandate of international organizations, with a decision of the National Assembly on the proposal of the Council of Ministers, the forces can participate in peacekeeping operations and in other operations other than war.

The training of the crisis management bodies and the response forces is conducted according the requirements of the state legal basis. The training of the institutional management bodies and crisis and emergency response forces is carried out in accordance with the regulatory framework of crisis and emergency management departments, the international legal and regulatory framework, and the country's responsibilities in the collective security systems.

Building the necessary capabilities to ensure the of life, health, services and democratic values of civil society is a long and complex evolutionary process of simultaneous transformation of its structures and the national security system. The main criterion for measuring the effectiveness of this transformation is the actual practical state of security in the world. Despite the tremendous efforts of the international community, increasing insecurity and the growth of threats warrant close monitoring and urgent finding of appropriate solutions to reduce insecurity and threats.

The realization of the advantages of the crisis and emergency management system does not require the assumption of responsibility for significant changes in the legislation, for the development of additional administrative structures and for additional resource provision. The main duties of managing the National Crisis and Emergency Management System are delegated to the existing institutions for managing the country, and the implementation of anti-crisis measures and the conduct of crisis and emergency response operations - to the available institutional forces. The emphasis on crisis and emergency prevention and the use of standardized management steps applicable to a wide range of responses will further enhance the effectiveness of the National Crisis and Emergency Management System's actions.

The limited conceptual approach in the normative construction of the existing emergency management system partially uses the theoretical foundations and characteristics of emergency situations. A disaster as emergency situation is defined in the Disaster Act [16]: "A disaster is a significant disruption of the normal functioning of society, caused by natural phenomena and/or human activity and leading to negative consequences for the life or health of the population, property, economy and for the environment, the prevention, control and overcoming of which exceeds the capacity of the system to serve the usual activities of public ". In previously approved versions of this law, a disaster was defined as "an event or series of events caused by natural phenomena, accidents, accidents or other extraordinary circumstances that affect or threaten the life or health of the population, property or the environment to an extent that require the taking of measures or the involvement of special forces and the use of special resources'. In fact, a gap in the two presented versions of the law is the lack of a clear definition of an emergency situation. An emergency situation can be considered as a situation on a particular territory, arising as a result of a disaster, technological disaster, accident, natural disaster, the negative influence of which can raise or cause human casualties, human health and the environmental damages, significant material damage and disrupt the normal functioning of the institutions and society.

Additional provisions of the current law define some of the constituent elements of the disaster management process. Natural phenomena broadly summarized and without

[16]Disaster Protection Law, https://lex.bg/laws/ldoc/2135540282 ;

classification for possible degrees of potential for negative impact on people and the functioning of society. They are presented as phenomena of geological, hydro-meteorological and biological origin such as earthquakes, floods, mass movements, storms, hailstorms, large snow accumulations, frosts, droughts, forest fires, mass diseases of an epidemic and epizootic nature, pest infestations and others the like caused by natural forces. The incident is described as "an unpredictable or difficult to predict, limited in time and space action, with a high intensity of forces or as a result of human activity, endangering the life or health of people, property or the environment".

The accident is also defined as "an incident of a large scale involving roads, highways and air traffic, fire, destruction of hydraulic facilities, accidents caused by activities at sea, nuclear accidents and other environmental and industrial accidents caused by human activities or actions". The industrial accident is no longer considered as an accident, but as "sudden technological failure of machines, equipment and aggregates or carrying out activities with hazardous substances and materials in the production, processing, use, storage, loading, transport or sale, when this leads to danger to the life or health of people, animals, property or the environment".

Given the introduction of an extremely broad concept of disaster, its characteristics cannot be accepted for universal application, such as scope - area, duration, inevitably necessary volume, danger, vulnerability, etc. The imperfection of the legal norm is further deepened in the presentation of the emergency response process, which disaster management is summarized as "disaster management". The very essence of management is presented only as a process of coordinating the efforts of the various structures of the unified rescue system and their joint work to achieve the common goal - mastering the disaster and protecting the life and health of people, property and the environment. It lacks essential elements of the emergency management process such as planning, prevention, decision-making, implementation of standardized response measures, situational management, and consequences management.

In addition to the conceptual incompleteness of the Disaster Law and the deficiencies in comprehensively defining the main constituents, the same law has created a Unified Rescue System without proper conceptualization and comprehensiveness of scope, without applying a systemic approach. The main characteristic of the system is individualization only as a structure, in which the constituent elements retain their

structures, departmental affiliation and management. The normative incompleteness of the law is highlighted by the lack of regulations for its implementation. Such an act can be used not only to structure the management process, but also to introduce regulatory requirements to the participating institutions for preliminary planning, prevention measures, which is the basic element in the process of responding after indications of the occurrence and management of emergency situations, disasters and accidents.

An accident can be considered as an extraordinary accident, an unintended accident, an unwanted and unplanned event. In order to prevent it, the circumstances of its occurrence, the applied and non-applied measures for its prevention should be evaluated. The accident forms a negative potential for the destruction of an object, the environment, in which the possibility of a real threat to the health and life of people and animals is generated. Particularly dangerous for human life and health are large-scale technological accidents with the possibility of destroying buildings, structures, equipment, vehicles, disrupting a production process or transportation with a threat of damage to human health and the environment.

Unlike accidents, catastrophes are a sudden destructive event that causes human casualties, significant damage to human health, destruction or significant damage to material values, and serious environmental damage. Natural disasters can be described as large-scale natural threats or cataclysms with destructive geophysical, geological, hydrological, atmospheric, bio-spherical and other potential that can cause catastrophic consequences, sudden disturbances in the normal rhythm of life of the population, large-scale destruction and damage to material values, as well as fatal injuries to people. Natural disasters can cause various accidents and catastrophes.

A particular importance for determining the nature, measures, and management of emergencies is a classification, based on the causes/threats/sources of their occurrence. They can be the result of armed conflicts, wars, natural disasters such as earthquakes, floods, hurricanes, tsunamis, landslides, mudflows, man-made such as radiation releases, chemical, biological, medical - epidemics and pandemics, forest fires, explosions, building collapses, sewage treatment plant accidents, floods, transport accidents. Emergencies can find manifestation as environmental in the atmosphere, biosphere, hydrosphere and lithosphere. The World Health Organization defines as disasters the results of emergencies:

• meteorological - storms, hurricanes, tornadoes, cyclones, snow storms, cold, unusual heat, drought, etc.;

• topological - floods, snowfalls, landslides, mudflows;

• telluric and tectonic disasters - earthquakes, volcanic eruptions, etc.;

• accidents - damage to building and other structures - dams, tunnels, buildings, mines, etc., fires, shipwrecks, train wrecks, large explosions, etc.

The basis of the timely and efficient management of emergencies is prevention - application of preventive measures in case of discovered indications of occurrence based on preliminary contingency planning. Prevention is considered as the pre-emptive implementation of measures with the aim of minimizing the manifestation of risks of emergencies, to protect the health of people and animals, to reduce the amount of environmental damage and material losses. Emergency management measures also include purposeful containment of affected areas, minimizing the negative impact on a limited territory.

The analysis of the structure and application effectiveness of the existing crisis and emergency management system in comparison with the presented modern opportunities and practices reveals:

• a normative incompleteness in the settlement of public relations in the state in the field of crisis and emergency management;

• a normative neglect of the scope and powers of the institutions of the national security system until the structuring of the law enforcement institutions in the National Security System [17];

• an insufficient institutional representation of the Security Council to the Council of Ministers [18];

[17]Law on the Management and Functioning of the National Security Protection System, https://lex.bg/en/laws/ldoc/2136588572 ;

[18]Art. 8 of the Law on the Management and Functioning of the National Security Protection System, https://lex.bg/en/laws/ldoc/2136588572 ;

• a scientifically unfounded and complete association of the management of crises and emergency situations with the state's response to disasters, accidents and catastrophes [19];

• a lack of uniform criteria for monitoring and evaluating the sources, nature and potential of security risks and threats;

• an increased powers and legally insufficient legally clarified status of the national bodies for institutional resilience, Crisis And Emergency Management and their interaction with the bodies of the executive power, local self-government and non-governmental organizations;

• a lack of the legally established system of situation centres [20], a unified National system for institutional resilience, Crisis And Emergency Management, standardized management procedures, prevention measures and response operations;

• a lack of a National Early Warning System, a National Disclosure System and a unified communication and information structure ensuring the compatibility of all segments of national security;

• a lack of a unified system and criteria for determining the departmental response forces, the education and training of the personnel of the crisis and emergency management system;

• an incomplete compatibility of the national crisis and emergency management mechanism with international practices and the Alliance systems;

• a complex procedure for applying the national legal and regulatory framework in the process of managing crises and emergency situations in the country and in fulfilling the assumed international obligations;

• a need for a normatively established emphasis on risk prevention and increasing the efficiency of the system.

6.2. Assessment of the National Crisis and Emergency Management System

The impact of dynamic changes on the security environment reveals a need to expand the mechanisms of coordination and interaction between institutions in the National

[19]Disaster Protection Act,

[20]Art. 18 and 19 of the Law on the Management and Functioning of the National Security Protection System, https://lex.bg/en/laws/ldoc/2136588572

Security System to develop and implement coherent policies to counter modern challenges, risks and threats by affirming a comprehensive approach to the of national security. An appropriate practice for assessing the capabilities of the crisis and emergency management system was the Strategic Review of the National Security System and the Strategic Defence Review, which identified an urgent need to develop and update basic normative and conceptual documents to increase functionality of the National Security System.

The primary importance for overcoming the regulatory deficit and for development a legally established framework for the functioning of the National Security System was the revealed urgent need for the development and adoption of a Law on Crisis and Emergency Management. Crisis and emergency management is an essential element of the of national security[21], which is implemented by the Council of Ministers through the National Crisis and Emergency Management System[22]. The development of a concept for resilience and Crisis Management Law will remove the lack of uniformed criteria for assessing the sources, nature and potential of arising security threats, the increased powers and legally unclear status of the national crisis and emergency management bodies and their interaction with the authorities, local self-government and non-governmental organizations. It will overcome:

- the lack of a legally established unified National Crisis and Emergency Management System;
- standardized management procedures;
- prevention measures and response operations;
- will increase coordination between the National Early Warning System, the National Disclosure System on a unified communication and information structure that will ensure the compatibility of all elements of the System for the of national security in crises and emergencies.

The law will:

- establish a formal system and criteria for determining of the composition of response forces;
- organise personnel education and training for participation in crisis and emergency management system;
- help to overcome the incomplete compatibility of the national crisis and emergency management mechanism with international practices and systems;

---

[21]Art. 17, para. 1 of the Law on the Management and Functioning of the National Security Protection System, https://lex.bg/en/laws/ldoc/2136588572 ;

[22]Ibid., Art. 17, paragraph 3;

- reduce the complexity of the procedures for applying the national legal-normative base in the management of crises and emergencies inside the country and in during the implementation of international obligations;
- place an emphasis on prevention and increasing the effectiveness of the system,
- develop conditions for subsequent review, updating and improvement of legislation and institutional regulations in the field of crisis and emergency management to support the structuring of relationships between state institutions. private commercial companies with non-governmental organizations in the management of crises and emergencies, disasters and emergencies.
- integrate the capabilities of the National Security System to manage a wide range of crises, including the application of specialized measures in counterterrorism operations, intrusion response operations, air and the maritime space of the Republic of Bulgaria, for the of critical infrastructure, measures to manage the consequences of crises and to restore the stability of governance.
- help to overcome the legal vacuum that arose after its repeal in 2009, will serve as a basis for further improvement of the regulatory framework in the field of national security .
- require changes to the Law on the Management and Operation of the National Security System to harmonize the conceptual apparatus and allow synchronization of the conceptual framework, prevention, preparation and conduct of operations in response to crises in the allied systems of NATO and the European Union.

A response of the significant need for an Act of the Council of Ministers to build the national system of situational centres - national, institutional and regional will respond to the requirements of Art. 19 and 20 of the Law on the Management and Functioning of the National Security System. The establishment under the Council of Ministers of the Republic of Bulgaria a National Situation Centre for institutional resilience, Crisis And Emergency Management will allow usage of an independent expertise from state institutions and academic structures. It will have opportunity to structure all specialized expertise in support of decisions making and proposals for crisis and emergency measures applications directly to the Security Council and the Ministerial Council and will be used for coordination the activities of institutional and territorial situational centres during the crisis and emergencies. The establishing of the need situation

centres - national, departmental and regional, will support the implementation of the basic principles in the performance of functions and tasks.

In response to the need of a uniform state standards for education, training and improvement of the expert qualification of the experts and managers from the state administration in the area of national security and defence, will be conducted specialized pilot courses for joint education, training, exercises at the operational and strategic level by all institutions of the state administration. A specialised targeted training will be organized for all bodies of the state administration and local government to increase the population and the readiness of the institutions for managing crises and emergencies. The establishing of an expert position "expert on national security and defence" will support the structuring of the labour market, the optimal distribution of positions in the administration, taking into account the needs for knowledge, skills and competences for the implementation of the specific functions. This approach will create conditions for an adequate response to crises and emergencies, cyber-attacks, unknown or hybrid threats, incidents, etc., and will improve coordination between state administration, local self-government bodies and local administration, and increase compatibility with NATO alliance systems and the European Union.

An urgent need has been revealed to improve the communication and information infrastructure of the institutions inside the National Security System and to develop a National Early Warning System, which will respond to the requirements of the Law on the National Security System.

Pursuant to the proposals of previous annual reports on the state of national security, an urgent need has been identified for the development of a National Register of Critical Infrastructure, which will facilitate the identification of national critical infrastructure sites and help prioritize the distribution of institutional responsibilities and obligations, the funding plans and the implementation of safeguards.

A need has been discovered to create a mechanism to support the financing of prevention in crisis and emergency management and disaster , as well as to ensure planned and targeted building of the capabilities of the National System for institutional resilience, Crisis And Emergency Management and to respond to the obligations under The Disaster Management Act.

The results of the Strategic Review of Security and Defence reveal the need for the development and approval of a draft of a new National Security Strategy, which will form a future strategic framework for the improvement of the legal and regulatory frameworks, and the construction of a National Crisis and Emergency Management System. It is necessary for the National Security Strategy to be developed based on an established National Security Concept that includes general guidelines for the strategic leadership of the country to defend national interests and achieve national goals. The strategy will define the characteristics of the environment, the main policies and practices for their implementation in the planning period.

The need for a common national policy in the field of education, training and qualifications in the area of national security and crises and emergencies management of has been confirmed. In response the need of increasing the operational efficiency of the National Security System, based on a new realism and new management bodies and response forces, a need for joint institutions participation in conducting national and Alliance exercises with appropriate overall coordination and coordination has been revealed. The scenarios for conducting these exercises have to be usable both for national the allied crisis and emergency management systems.

Crisis and emergency management is an integral part of national security and an essential element of its activities. The strategic goal of the crisis and emergency management policy is to prevent their occurrence, limit the negative consequences and quickly restore the functioning of state and public life from before the crisis occurred. Effective management of crises and emergencies, disasters and other emergencies to protect citizens, property, critical infrastructure and the environment requires building capacity to assess and impact risks through planning and implementation of measures for prevention, preparedness, response and recovery in ministries, departments, municipalities, commercial companies and citizens united in the National Crisis and Emergency Management System. The system provides the necessary institutional framework and tools for interdepartmental cooperation in fulfilling the responsibilities of crisis and emergency management. Moving from a reactive to a proactive approach to crisis and emergency management, covering the whole process – before, during and after the crisis, is essential to building resilient institutions and civil society. The policy is in the initial stage of implementation, as legislation is needed to regulate this high-risk activity. The initial phase in its

implementation is the adoption of a modern law on crisis and emergency management and the development of a system of situation centres as the operational and informational basis of crisis and emergency management. Based of the experience in the area of crises and emergency management within the frameworks of NATO and the EU, it is expedient to synchronize the national legal framework with the documents and procedures for responding to a crisis of a political-military nature with the crisis and emergency management systems of NATO (NRS) and the EU.

A primary importance for overcoming the regulatory deficit and for creating a legally established framework for the functioning of the National Security System is the revealed urgent need for the development and adoption of a legal framework for institutional resilience, Crisis And Emergency Management (including through the development of a new law for institutional resilience, Crisis And Emergency Management). The management of crises and emergency situations is an essential element of the of national security (Article 17, Paragraph 1 of the Law on the Management and Functioning of the System for the of National Security), which is implemented by the Council of Ministers through the National Crisis Management System and emergency situations (Art. 17, para. 3). The development of the law will remove the lack of uniform criteria for assessing the sources, nature and potential of security threats, the increased powers and legally unclear status of the national crisis and emergency management bodies and their interaction with the authorities, local self-government and non-governmental organizations.

It will overcome the lack of a legally established unified National Crisis and Emergency Management System, standardized management procedures, prevention measures and response operations, which will increase coordination between the National Early Warning System, the National Disclosure System on a unified communication and information structure ensuring the compatibility of all elements of the System for the of national security in crises and emergency situations.

The legislation will establish a standard system and criteria for determining the composition of the response forces, education and training programs for personnel in order to be ready for participation crisis and emergency management system activities and operations. It will

- help to overcome the existing incomplete compatibility of the national crisis and emergency management mechanism with the international practices and systems;
- reduce the complexity of the procedures for applying the national legal-normative base in the management of crises and emergency situations in the country and in the fulfilment of international obligations;
- emphasize on prevention and increasing the effectiveness of the system, creating conditions for subsequent review, updating and improvement of legislation and institutional regulations in the area of crisis and emergency management
- support the structuring of relationships between state institutions, private commercial companies, with non-governmental organizations in the management of crises and emergencies, disasters and emergencies.

The adoption of this law will integrate the capabilities of the National Security System to have more management options to response to a wide range of crises, including the application of specialized measures in anti-terrorist operations, operations to respond to violations of the state borders, air and sea space, for protection of critical infrastructure and consequences management, to resist and restore security and stability. The crisis and emergency management legislation is a condition without which the legal vacuum created by the May 2009 repeal of the Crisis and Emergency Management Act passed in 2006 cannot be overcome, and will serve as basis for the further improvement of the regulatory framework in the field of national security . Adoption of this legislation will require changes to the National Security System Management and Operation Act to harmonize the conceptual apparatus and allow for the synchronization of conceptual frameworks, prevention, preparation and conduct of operations in response to crises in NATO allied systems and the European Union.

The significant need has been confirmed by a Decree of the Council of Ministers for the construction of the system of situation centres - national, departmental and regional, which will answer the requirements of Art. 19 and Art. 20 of the Law on the National Security System. The development a National Situational Centre under the Council of Ministers as expert body will attract experts from state institutions and academic structures will support specialization and expertise for support of decision making and application of response measures from the Security Council and the Ministerial Council. It will be used for management and coordination of the activity of departmental and territorial situational centres in crisis and emergency situations. The

construction of the situation centres - national, departmental and regional will support the implementation of the basic principles in the performance of the functions and tasks.

A number of examples reveal the existence of unified systems for the prevention and management of emergencies, within which the safety of the population is ensured and the amount of damage to the national economy and the established way of life of the society is reduced. An appropriate conceptual framework for applying a standardized approach to the management of all emergencies is the establishment of a national crisis and emergency management framework, including in close cooperation and interaction with NATO and EU allied systems. Without being exhaustive, the main tasks that can be legally assigned are the scope of the entire process by distinguishing both the prevention and the management of emergencies and their consequences:

- development and implementation of legal and economic standards to ensure the of affected citizens and territories;
- implementation of measures to prevent emergency situations and increase the sustainability of the functioning of institutions and facilities for civil in emergency situations;
- building and using systems for early warning and notification of the population in emergency situations;
- readiness for actions of the governing bodies, forces and means to prevent the occurrence and minimize the negative impact of emergency situations;
- collection, processing and exchange of information in the field of the of the population and the territory in crises and emergency situations;
- population training;
- forecasting and assessment of the socio-economic consequences of emergency situations;
- building financial and material reserves for responding to crises and emergency situations;
- provision of expertise, management and control in the field of of the population and the territory from emergency situations;

- implementation of emergency and crisis response measures;
- implementation of measures for social of the population affected by emergency situations, provision of humanitarian aid;
- international cooperation in the field of of the population and the territory in crises and emergency situations.

The basis for the development and run operational such a system is based on the principles:

- full coverage of the population and objects, material and immaterial values subject to,
- an account of the division of responsibilities, competences, forces between institutions and management bodies at all levels in the state
- an advance specialized planning of measures to protect the population and the territory in emergency situations and their continuous application both in peacetime and in war
- the reasonable sufficiency of the volume and conditions for implementation, consistency and complexity of the approach applied measures of the population and the territory in the management of crises and emergency situations.

7. Development of science-based tools to improve the National Crisis and Emergency Management System

7.1. A conceptual framework for institutional resilience, Crisis And Emergency Management

The experience in the construction of conceptual frameworks with scientific applied and practical-expert application in the field of national security[23]allows his purposeful concentration on the construction of the State's Conceptual Framework for institutional resilience, Crisis And Emergency Management. A confidence in obtaining desired final results for the application of a scientific approach in the integration of all constituent aspects of the national regulation of emergency and crisis management is provoked by the positive results from several past successful projects:

- development of the Law on Crisis Management and emergency cases;

[23]In this part of the study, the results of the application of scientific and applied scientific methods were used to develop conceptual frameworks in the dissertation work for obtaining the scientific degree "Doctor of Sciences" of Professor Mitko Stoykov in 2018.

- the activity of a sector with the same name in the Ministry of Defence;
- the presentation of the country's participation in the NATO and EU governance systems;
- building the Centre for institutional resilience, Crisis And Emergency Management and Disaster Response;
- a broad scientific and teaching experience in the country and abroad in the subject area of crisis and emergency management.

All realized projects, including the development of the specified legal norms, are based on a clear theoretical basis, called a concept. The definition of a concept is located in a broad scientific-theoretical framework and varies from an idea to carry out some activity or conduct an operation, to a purposefully developed and approved plan for their implementation. The scientific essence of **the concept** is represented by **a specialized theoretical construction, tied to the achievements of science and technology, structured on the descriptions of the context, environment, goals, structure, relationships and responsibilities of specialized research and expert structures**.

Basic constituents of any conceptual framework are concepts and the connections between them, purposefully forming the theoretical-conceptual foundations of a certain scientific-applied and expert subject area. The concepts are used to define, characterize and build a common, integrated theoretical space from a certain set of unique, heterogeneous and at the same time indivisible components, which are used to develop, characterize, and construct each of the constituent concepts. The simultaneous use of a set of different completed concepts to describe theoretically the structure, connections, relationships, operability and behaviour of the complex systems of systems could practically be realized by building a unique intellectual or integrative conceptual framework that would allow a synergistic integration of the capabilities of each constituent concept.

In this context, a conceptual framework can generally be defined as a research and applied scientific construct in which a specially selected set of interrelated concepts is incorporated, together providing a comprehensive and comprehensive understanding of a given phenomenon or phenomenon. Expanded to increase comprehensiveness, the conceptual framework is defined as**:**

A comprehensive, multidisciplinary scientific-research and scientific-applied construct to support the incorporation into management decisions of the requirements of guiding policy directives, strategies, doctrines, plans and programs in a unique set of interrelated and integrated concepts for guaranteeing quality scientific and expert assurance of processes: decision-making; planning and management, building capabilities and synchronizing efforts to increase interoperability, institutional approaches to protecting national security, and asserting sustainability of governance systems of modern society.

Each of the constituent concepts included in the composition of the conceptual framework, in addition to its main purpose of solving specific scientific research, scientific applied, expert, legal-normative and other problems in the processes. It also serves to expand the subject matter area, to support and/or ensure the application and guaranteeing the functionality of any of the other concepts integrated into the framework when taking into account at the same time both its own and the other concepts' contributions to the formation of the uniqueness of the unified and specific only to this framework theoretical foundations, philosophy and methodology. Towards the creation of a similar theoretical-applied intellectual framework for planning and building a structure, functional connections and operability, for the distribution of duties and responsibilities, of management and provision of the products of highly specialized scientific-expert systems or organizations (such as the national security system) could be approached through an analysis of good practices and lessons from the application of similar approaches to research and applied science in other subject areas .

Good practices and the products of the application of such approaches show that a careful selection of the constituent concepts allows the formation of the necessary set of ontological, epistemological and methodological foundations, for which each of the constituent concepts is assigned a unique methodological, ontological or epistemological role.

In such conceptual frameworks, ontological statements are used to justify, clarify and guarantee the connection between the applied research methodology and the investigated reality, confirming the truth of the origin and the availability of proven theoretical foundations that form the conceptual framework. Epistemological statements are applied to guarantee the scientificity, operability or functionality, as well

as the possibilities of each of the concepts to integrate with the others, as well as the framework as a whole, including the possibilities of application in updating and future use of the entire newly built theoretical construction. Accordingly, the methodological statements are used for scientific and applied justification of the selected structure, techniques, tactics and procedures for the process of building the conceptual framework, for evaluation and guarantee of its constant compliance with the basic characteristics, mission and tasks of the built system laid down in the project.

The hierarchical structure, strong interdependence and dependence of the entire theoretical and conceptual base of national security systems require detailed knowledge of the essence, processes and tools for concept development and verification. Following the outlined scope and structure requirements and taking into account the need for a clear allocation of institutional responsibilities for institutional resilience, Crisis And Emergency Management, the approach to building a new unique framework should be proven scientific, holistic or comprehensive, integrative, comprehensive, confidence-inspiring and ensuring the receipt of real results, while allowing for continuous adaptation, conceptual enrichment, expansion and refinement.

Summarizing the requirements to a specific subject area of application in the context of the immediate purpose, the conceptual framework for institutional resilience, Crisis And Emergency Management could be defined as:

A comprehensive, multidisciplinary scientific research and scientific applied construction to support the incorporation into theoretical-conceptual foundations, into legal norms, in management decisions, in tactics, techniques and procedures, the application of national and institutional policies, strategies, doctrines, programs and plans in the formation of a unique scientifically based integrated set of interrelated concepts, the application of which can guarantee a new and higher quality of scientific - the expert provision of crisis and emergency management processes .

7.2. Characterstics of the Conceptual Framework for Institutional Resilience, Crisis and Emergency Management

The design, construction, management and continuous operationalization of the conceptual framework form a foundations of a theoretical-conceptual construct with the behaviour of a complex system of systems. Following the practice of describing complex systems of systems, the theoretical description and behaviour of this

framework could accordingly be constructed with a predicted operationality by foregrounding the constituent common and strictly identifiable characteristics. The theoretical presentation of these characteristics is needed for the formation of specific analytical tools for understanding the essence, clarification and prediction of aspects of behaviour in the mentioned operationality of the conceptual framework. In the conceptual framework, for the scope of the organization and activities of the MOD Working Group for the analysis of the transformation and interoperability of the Armed Forces, with the help of the basic characteristics, both the uniqueness of the built scientific research and practical-applied mechanism, as well as the possibilities for forecasting are presented and evaluating the relevance of its behaviour and the quality of the resulting products in practical use.

Briefly and without claiming to be exhaustive, the main features can help to present the conceptual framework as:

• **Joint**. The conceptual framework does not follow and cannot be considered as a mechanically collected set of concepts, but as a specially designed scientific construction - a set of selected concepts, in which each of the constituents is assigned a specific role for presenting conceptual/theoretical aspects, factors, elements or variables, as well as to justify the possible relationships between them. In contrast to the usage of similar techniques to develop a research model that emphasizes factors, constituents, and relationships, the emphasis in constructing a conceptual framework is on providing opportunities for comprehensive application of each of the constituent concepts. Without being considered as a random and mechanical sum, when summing up the possibilities and qualities of each of the selected constituent concepts, viewed as a unity, synergistically new possibilities and qualities of the constructed conceptual framework are formed.

• **Descriptive**. The conceptual framework does not only provide an analytical disclosure of the causal relationships between the concepts, capabilities and products of the framework, but creates conditions for describing the current reality, the expected state and behaviour of the studied systems/capabilities in the system or environment.

• **Explanatory**. In contrast to the purpose of quantitative models, which offer theoretical explanations from a different perspective, the mechanisms and tools of

conceptual frameworks are formed to provide a detailed understanding of all aspects of the nature and operation of the systems or capabilities under study.

• **Analytical**. Through the integration of proven operational or workable concepts, the conceptual framework is designed to form a unique platform for the analysis and selection of workable options of expert opinions to support decision-making, planning and capability management and enhance the interoperability of the armed forces.

• **Interpretive**. The construction and tools of the conceptual framework show that it can be used not only to provide information and knowledge for managing capabilities, but also as a science-based analytical tool to interpret and interpret the expected behaviour of capabilities throughout their life cycle.

• **Multidisciplinary**. The unique design, scope, qualities and purpose of each specially designed framework predetermine the wide variety of scientific disciplines and research techniques that could be applied in the use of the composite concepts, in the analyses and in the preparation of expert assessments.

• **Broad**. The scope of the conceptual framework is focused on the identification of concepts, the use of which contributes to the comprehensive implementation of the planned research methodology, provides balanced management and control of the functionality of information and knowledge to achieve the goals of the framework. In the presence of new concepts and the need to integrate them into the conceptual framework, and in the absence of the need for outdated concepts, the scope of the framework can be expanded and contracted.

• **Flexible**. The conceptual framework can be considered as a sustainable and flexible scientific research and scientific application tool, since its construction allows for quick and unhindered construction, integration and use of the constituent concepts.

• **Open**. The construction of the conceptual framework is intentionally left open to allow at any time, as needed, additional use of concepts whose operability can serve to complement the mix of research and applied science tools needed to solve the tasks and achieve the main objectives of the framework.

• **Integrative.** The construction of the conceptual framework forms a model for the integration of all constituent concepts, in which the independent application of each of the concepts is guaranteed and does not create conflicts with the application of each

of the others, as well as the entire framework as a scientific research and applied science tool.

• **Synergistic**. The specialized integrative construction builds a unique design of the conceptual framework, which operability allows the absorption of the advantages of each of the contained concepts to generate a synergistic effect, in which both the total value and the quality of the obtained scientific research and applied scientific results will be different and with higher dimensions of the mathematically summed results of the single application of each of the concepts individually.

• **Established**. The scientific-theoretical construction of the framework forms and implements a recognizable methodology, objectives, defined management and resources, while maintaining independence in the operationality, objectives, tasks, provisioning and management of each of the constituent concepts.

• **Internally interdependent.** Due to the strong interdependence of the elements of the framework, any change in the construction and design of the conceptual framework is determined unique by the quantity, quality, modification, integration and interaction of each of the constituent concepts with the others in the framework.

• **Manageable**. The framework integrates a purpose-developed construct of concepts that is built to solve planned tasks and achieve defined goals, thus requiring continuous centralized management of its composition and operability. Regardless of the fact that individual component or constituent concepts retain their ability to be applied independently, when using them as part of the overall structure, the management of their independent operability must be continuously directed towards solving tasks and achieving the goals of the conceptual framework.

• **Operationally focused**. The management of the functionality of the conceptual framework should be continuously aimed at achieving the initially formulated set of operational objectives by using concepts whose individual objectives may or may not be fully aligned with the objectives of the framework.

• **Uncertainty reducing**. The construction of the conceptual framework is built to perform analyses and fill the need for knowledge in a specific context and dynamic environment with a high degree of uncertainty, therefore the results of its functionality cannot be automatically compared, correlated or applied comprehensively and universally to other similar research and applied research tools.

• **Specialized database**. The application of the set of concepts aimed at individual segments of the subject area of the framework's functioning allows them to be used as sources for extracting data, which, structured and summarized in a common database, could, if necessary, be transformed into a set or empirical data base for conducting qualitative analyses within the conceptual framework.

In “2021 Deloitte Global resilience report” [24] are described several basic characteristic in building a resilient institution/organization. In order to reach exsustiveness for needed resilience of the conceptual framework, they are included to the list of basic characteristics:

• **Prepared.** The conceptual framework need to be ready for immediate application.

• **Adaptable**. Conceptual framework need a full flexibility/adaptability as the most critical requirement to the built organizations’ resilience.

• **Collaborative**. This basic characteristic indicated the importance of collaboration within the organization, to support decision-making, mitigating risks, and an increased innovation.

• **Trustworthy**. Conceptual framework support focusing of each of the institutions on improving communication and transparency with other institutions.

• **Responsible**. Help the organizations to quickly adapt and pivot in response to disruptive risks, threats, crises and emergencies.

The presented characteristics of the theoretical-research construction conceptual framework are defined as a component of an in-depth scientific study and are defended in a dissertation work for obtaining a scientific degree "Doctor of Sciences"[25].

7.3. Science-Based Approach to the Development a Conceptual Framework for institutional resilience, Crisis And Emergency Management

The experience of building specialized research instruments and applied research frameworks for the scope and integration of concepts with applicability in the field of social sciences shows that there is a clear tendency in the use of such approach in the given subject area. They help to emphasize theoretical explanation/description,

[24] 2021 Deloitte Global resilience report , https://www2.deloitte.com/se/sv/pages/about-deloitte/articles/characteristics-resilient-organization.html

[25]Practical Guide to Grounded Theory Research, https://delvetool.com/groundedtheory ;

scientific justification and interpretation of the obtained results in order to incorporate them into theoretical bases for the formation of a new concept or theory. The use of similar procedures for a detailed research of available information and data allows the formation of specialized conceptual or theoretical categories, which facilitates and supports the extraction of new knowledge about the studied objects and systems.

The similar research approach using the tools of a conceptual framework as a basic methodology for conceptually describing data in order to create new theoretical constructs is known as Grounded Theory Methodology[26]- as a qualitative method for studying specific phenomena or processes and developing new theories based on gathering and environmental data analysis. In this scientific research, the main phases are preparation, creating a database; continuous comparative, thematic, conceptual, semiotic, metaphorical and discourse analysis (from the position of the context and environment in which the framework operates); keeping records and their systematization; review of results, conceptual selection and generalization to form new theory.

Applying the approach of a conceptual framework, based on Grounded Theory Methodology, requires recognizing the essential difference between concept and scientific description. Concepts are typically used for theorizing or for theoretically informed problem solving, regarding the structure and functionality of described systems. There the information and knowledge are grouped behind an individual/unique conceptual paradigm and could only be interpreted within a specific context, strictly defined for the application of each of contained concepts, and operational environment. On comparison, in theoretical description, information is usually organized thematically, and individual topics can be conceptualized with corresponding interpretations as needed. The main difference being these topics usually serves as universal theoretical explanations that's why therefore they are not used to develop conceptual schemes.

7.4. Analytical Techniques for Usage a Crisis and Emergency Management Conceptual Framework

In the practical use of the tools of the conceptual framework, an extended methodology for conducting qualitative analyses could be applied, such as content analysis, thematic analysis, conceptual analysis, discourse analysis, comparative analysis, meta-analysis, expert analysis, morphological analysis, Delphi analysis, uncertainty analysis, deductive analysis, maximum likelihood and influence analysis, operational analysis.

Regardless of the fact that the majority of the indicated analyses represent and are used as qualitatively oriented analytical techniques, the need to determine strict relevance/correspondence to the studied objects, systems, capabilities and the presence of mandatory guarantees for the applicability of the developed expert assessments may require additional use of quantitatively oriented methodologies. They are needed for analysis, construction of conceptual models and simulations, which would support the conduct of specialized experiments to test the operability and validate the applicability of the products obtained from the framework. The interdisciplinary nature of the conceptual framework implies a comprehensive understanding of the inherent need to apply a wide variety of analysis techniques. Taking into account the uniqueness of each framework, these analyses would serve as a testimony to the strict specialization of the methodology and the limitation of extending the full validity of the results of the analyses only on the object/objects/systems of the particular study.

A particular importance to the use of a wide variety of qualitative and quantitative oriented analytical techniques would be a systematized organization of the information used and the results obtained in an accessible database. The specialized data and information at the entrance of the study, on which the selected research and analytical methodologies are applied in the functionality of the conceptual framework, should also be provided in an appropriate format, to be reliable, sufficient in quantity, accessible, comprehensive for completeness, comprehensiveness and the most - effective representation of the studied capabilities and systems, the environment in which the studied objects operate, and in accordance with the context in which their construction, implementation, etc. are studied.

When preparing expert assessments at strategic level, it is undesirable and inadmissible to have ambiguities, to carry out assessments outside of the reported operational environment and context. Therefore, research inputs can and should be derived from the institutional regulatory framework for building and deploying capabilities and armed forces (laws, regulations, doctrines and concepts), strategies, plans and programs for building and development. Given the multidisciplinary nature of the framework and the possibility of linking or relating/comparing available data from used conceptual/theoretical frameworks of the operational use of capabilities and forces, regardless of form, the credibility/validity of the data would allow them to be considered as empirical data from the analyses of the conceptual framework for the studied objects and systems. Since the process of building and applying the analytical techniques of the framework is continuously iterative, its constant enrichment and updating is essential for the topicality of the content of the database.

7.5. Process of Building Conceptual Framework for Institutional Resilience, Crisis and Emergency Management

In order to reduce the complexity of the process of building a scientific construction of the conceptual framework, an appropriate approach would be to structure it in different phases, where its application would not establish restrictions and would not prevent/restrict the possibilities laid down in the methodology for returning to previous phases or repeating any of them if necessary. Without pretensions to universal exhaustiveness and comprehensiveness of the process of building the conceptual framework, but with a clear understanding of the need to form reliable foundations for the construction of a specialized research methodology, in general, the phases of the process of building the conceptual framework should include:

- mapping of the selected sources of information;
- detailed familiarization and categorization of the selected data;
- identification and selection of framework concepts;
- review and categorization of the constituent concepts;
- integrating the concepts into the framework;
- synthesis and summarization of information and data, deduction and systematization of results;
- validation of the conceptual framework;

• evaluation, refinement and development of the conceptual framework.

The formation of shared knowledge and understanding of the complexity of the process, as well as of the compliance of the purpose with the requirements for creating scientifically substantiated conditions for the overall realization of the purpose of the conceptual framework requires a sequential brief description of each of the presented phases.

7.5.1. Mapping of Selected Sources of Information

The main task of the first phase of the process of building the conceptual framework is the mapping and selection of information from the entire multidisciplinary spectrum of sources. Structured as an independent process, the first phase covers identification and systematization of information and data by type, quality, direction of use, scientific discipline, on the one hand, and formation of specialized information arrays depending on a previously created taxonomy, on the other. The phase begins with an extensive expert review of the available sources and the information and data contained in them, continues with a discussion and analysis of the characteristics of the information, such as completeness and relevance/relation to the researched problems, with the participation of experts and scientists from the various disciplines whose work is focused on the subject areas of the framework's functioning. The progress of the first phase in the presented sequence helps to reveal incompleteness and the need for complementary and additional information and data.

The process in the first phase is iterative and ends only after receiving a positive assessment of compliance of the availability and suitability of the mapped information and data. Of particular importance for the quality of the final products of the analysis in the conceptual framework is compliance with the requirements for comprehensiveness and completeness in the collection and classification of the information necessary for the study. That is why the mapping must create prerequisites for a full scope of the characteristics and qualities of the investigated problems in the targeted subject area, and subsequently will contribute to an unimpeded and impartial validation of the obtained results.

7.5.2. Detailed Familiarization and Categorization of Selected Data

The purpose of this phase is familiarization with the available information and data, their categorization and evaluation for compliance with the requirements for use. If missing or insufficient information needs to be added, the process could iteratively

return to the first phase. To assess the quality of information and data, it is desirable to select a system of criteria that would determine their place and significance within the scope of each discipline/concept. Such an approach would help set a precedent for accelerated and comprehensive application of research techniques, thereby positively influencing the overall effectiveness of research using the conceptual framework, as well as the quality of the resulting research and analysis results or products.

7. 5.3. Identification and Selection of Composite Concepts

In accordance with the chosen methodology and taking into account the complexity of the structure and functionality of the conceptual framework, the purpose of this phase is to carry out a comprehensive and comprehensive selection of the concepts necessary for its composition. Its implementation presupposes a highly expert knowledge of all concepts related to the construction and functioning of the studied ability or system. When selecting concepts, their compliance with the operational environment and the context in which the studied capabilities are evaluated and expected to function must be taken into account.

As a result of the implementation of the activities in this phase, it is expected to obtain a taxonomy of many multidisciplinary, unifying concepts, which may sometimes contain competing and even contradictory elements. In the development of new capabilities or significant upgrades and refinements of existing ones, it could be that some concepts are missing, for example for operational use, or as a result of the development of science and technology, it is necessary to make significant changes to existing concepts, the application of which would also bring the conceptual basis for building and using capabilities to a qualitatively higher level.

In response to such needs, the iterative nature of the method of constructing the conceptual framework should be used, which allows returning to previous phases, modifications, refinement or development of missing concepts, of course, with the application of the relevant mechanisms for their validation. The requirement for a qualitative orientation of the end products of research, analysis and expertise using the complex tools of the conceptual framework presupposes a deep knowledge of the theoretical and conceptual basis of building the studied capabilities and systems, as well as paying special attention to the activities in the maintenance phase of the necessary completeness of the set of concepts used.

7.5.4. Overview and Categorization of Constituent Concepts

The purpose of this phase is to deconstruct each of the concepts that make up the framework in order to examine, identify and use in the analyses its structure and its main qualities: requirements, purpose, rationale, purpose, scope, principles, characteristics, roles and responsibilities, individual elements of the structure or the overall structure of the capabilities, resources for building and ensuring the operability, conditions for the implementation of the concept, evaluation of the applicability, conclusions and the need for its improvement over time. The next step of the phase involves the systematization and categorization of the concepts and elements of the concept that would help identify the need for new or refinement of current core features of the studied capabilities in their future conceptualization or their expert evaluations of operational applicability.

A suitable form for presenting the results in the phase is the table, which, when arranged, allows grouping with an emphasis on compliance with the studied characteristics. When revealing incompleteness or lack of information for a complete description of main characteristics, as well as for a description of the expected functionality of the studied abilities, the process of building the conceptual framework allows a "return" to any of the previous phases, including, if necessary, supplementing the set of the studied concepts with new ones. As a result of the phase of categorization of the concepts, according to the assessment of the scientists and experts conducting the research, the quantity and quality of the detailed systematized information should provide and guarantee that all the necessary prerequisites are created for the subsequent integration of the main elements of the concepts in the framework.

7.5.5. Integration of the Constituent Concepts into a Common Conceptual Framework

The goal of one of the most important phases of the process of building the conceptual framework is to integrate and group the elements of the environment in which the capabilities or system operate/function; the main theoretical statements, concepts and processes of the operational framework; the responsibilities for the management of the functionality and the improvement of the conceptual base, including the possibility of selection according to certain criteria of similarity if it is necessary to create a new concept. This requires integration to create appropriate conditions for revealing and representing both the interdependencies between the constituent elements of the

concepts and the likely consequences for the ability when further implementing strategies to increase the semantic and interoperability of the abilities. In addition, it is necessary that the procedures in the phase create conditions for matching and comparing information with different characteristics in order to provide conditions for understanding the nature and potential limitations of the research approach.

During the operationalization phase, the conceptual framework can be applied iteratively or repeatedly to reduce uncertainty, overcome identified limitations, and fill in gaps or absences of information needed for research.

In order to speed up the process of integration of concepts and increase the effectiveness of the functioning of the framework, it would be useful to create conditions in which the integration of information contributes to the accelerated flow of information through the constant expansion of the possibilities of access to systematized, structured information resources in the conceptual, organizational and functional boundaries of the framework. The rapidity, extended access and completeness of information in the constituent concepts would support the formation of the necessary prerequisites for increasing the quality of the final products of the framework, created in a common and truly integrated information environment. Additionally, the integration process could be accelerated by initially considering the interrelationships, steps and phases of process implementation in the framework, which would enable its products/services to be constantly, comprehensively and comprehensively monitored and controlled. Regardless of the overlap and complementarity of the framework's concepts and process integration practices, their application can contribute to providing a clear scientific and applied understanding of the possible consequences and products of the framework's operationalization. The complexity and duration of the steps in the concept integration phase could be reduced by using previously developed expert judgments and, if possible, concepts from the higher hierarchical level for the capability/system under study in order to reduce the number of concepts that make up the framework.

7.5.6. Synthesis of Information, Summarization of Data, Deduction and Systematization of Results

The purpose of the phase is to synthesize the information and data from the concepts into the conceptual framework. The synthesis and summarization of the obtained data and information is done with the aim of reliable integration of the set of data,

information and knowledge extraction that describe the structure and behavior of the studied system, capability or object in the necessary context, in a real operational environment and in a consistent, accessible to use form. Depending on the complexity of each of the steps, assessing the speed of individual stages of information and data processing, their synthesis and summarization, it could be characterized as low, medium or high. Of particular importance for the successful running of the phase is the exact observance of the quality requirements and the use of information and data with the necessary characteristics, because, for example, in a process of synthesizing and summarizing raw information or information and data in an inappropriate format in addition to low speed of the phase could produce results of low application value. In compliance with the requirements and high-speed processing of quality information, it should be expected that the information and new knowledge obtained will be of a higher quality than that at the entrance of the phase.

During the phase, researchers and experts need to be sufficiently open-minded, unbiased, tolerant, consistent and flexible in summarizing and theorizing the information and data to obtain new knowledge, concepts or theoretical justifications. Mastering the available opportunities to repeatedly repeat the steps of synthesis, generalization and deduction of information would allow the development of a high-quality, new, recognizable concept or theoretical framework, the application of which would support the achievement of research and applied goals. Qualitative answers to the presented requirements can only be achieved with comprehensive, in-depth and detailed knowledge of the concept development process by the research participants.

7.5.7. Validating the Conceptual Framework for Institutional Resilience, Crisis and Emergency Management

The aim is to validate a conceptual framework by checking the consistency of the integrated constituent concepts, concepts and products with the plans and expectations not only of the research and expert team, but also with the possibilities of applying the framework in future research and practice in the subject areas of its functionality. Validation of the conceptual framework is a process that can start with structuring and using a toolkit applied in proven scientific research, and end with analyses and expert evaluations to confirm the future applicability of the resulting products. In addition, the application of iterativeness and the assimilation of the possibilities for supplementing the theoretical foundations of the framework in the

process of its construction and functioning will constantly contribute to the enrichment of scientific research, applied scientific and expert practice.

The validation process is conducted to obtain confirmation that the concept or framework covers and corresponds to the definitions and functions that are planned to be obtained by conducting the research, i.e. the validated concept or framework must be sufficiently well theoretically grounded and reasoned, and its compliance with expectations can be measured. The importance of validation and compliance with planned parameters, as well as guarantees of applicability of products can be argued by using a set of criteria for their measurement:

• The use of a criterion such as plausibility is suitable for forming an assessment of the validity of the implementation of outlined plans or ideas. The plausibility or consistency of the products of the framework could be demonstrated through the mechanisms of logical confirmation or deductive inference from proven working research or theories, or arrived at through observation or induction. Applying such a criterion helps to establish and confirm that the resulting new concept, product or research result is not intended as fictitious ideas or assumptions.

• The application of a feasibility validation criterion could demonstrate that the resulting concept or products conform/have the necessary characteristics to be assessed as feasible, workable or operational, thereby in addition to the plausibility the guarantee of realization or feasibility of the concept or the products of the framework imply the mandatory functionality embedded in their construction.

• The efficiency criterion is introduced to validate the high quality of implementing the operational concept or using the products of the conceptual framework. A number of tools can be used to measure product performance. They serve as a real assessment of the organization's operability, using descriptions of the relationships between plans, intentions, processes, results, and the quality of management decisions laid down in the conceptual framework. As a result, performance assessment helps to systematize all available options for strategic planning and management of capabilities and system.

• Proven effectiveness is a guarantee of applicability of the framework and products in other research and evaluations. The criterion of pragmatism can be used to measure and validate the limits of applicability of the obtained results and as a

guarantee of a predetermined unlimitedness for the application of other important concepts in the framework, emphasizing the need for connections and correspondence or coherence with other concepts in the subject area.

• Applying a criterion of empiricalness to the obtained data and results would provide the conceptual framework validation process with evidence of measurability of integration and practical arguments for the operability of the resulting concepts or products of the framework. • To demonstrate the conformity of the behavior of the operationalized conceptual framework products or capability/system assessments with the intended expectations of researchers and experts, the framework behavior predictability criterion can be used.

• Having a criterion allowing for multi-subjective certification would allow multiple testing of the framework and the resulting products by different researchers and experts in order to validate them.

• The use of another similar criterion – for multi-methodological certification, would ensure that when building the framework and obtaining reliable products, opportunities are foreseen to verify their validity by applying other research and applied tools.

The presentation of new or improved existing concepts, theoretical propositions or management practices, obtained from the operationalization of the conceptual framework at various specialized scientific-expert forums such as workshops, seminars, conferences, symposia would provide excellent opportunities for researchers and experts to discuss, debate, maintaining contacts and obtaining feedback both with the scientific and expert community and with future potential users of the methodology and products of the conceptual framework.

7.5.8. Evaluation, Refinement and Development of the Conceptual Framework for Institutional Resilience, Crisis and Emergency Management

The operational dynamism and multidisciplinary construction of the phenomenon "conceptual framework" implies that, if necessary, the methodology of its construction can always be revised, supplemented and changed in accordance with new achievements, discoveries, comments and publications. Since the practice of scientific research with the application of a conceptual framework spans multiple scientific disciplines, the resulting new concepts and results will have meaning and significance for the applied scientific disciplines as they work for their enrichment, refinement and

prospective development. The main goal of the first part of the implementation of the approach to building a conceptual framework for the analysis of transformation and interoperability is to develop and present a theoretical description of a method for extracting knowledge and increasing the quality of expertise by using multiple concepts that operate in different disciplines of a common subject area. Its main tasks are the formulation of concepts and conceptual framework related to the operational environment and the context of construction and use of the studied capabilities, as well as a description of the process of construction and functioning of a conceptual framework.

In this part, the definition of a concept is presented as a specialized theoretical construct tied to the achievements of science and technology, and structures the description of the context, environment, goals, structure, relationships and responsibilities of specialized research and expert structures created to solve specific research and scientific and applied problems in the process of transformation management and interoperability of defence and security systems. The specific conceptual framework is presented as a comprehensive, multidisciplinary research and applied science construct to support the incorporation of management decisions and requirements of guiding policy directives, strategies, doctrines, plans and programs into a unique set of interrelated and integrated concepts that is constructed to ensure quality scientific-expert assurance of the decision-making processes, planning and management of the transformation of defence and security, building the capabilities and the efforts made to increase the interoperability of the armed forces.

Adhering to the requirement to describe complex systems of systems with their main characteristics, as the basic qualities of the framework are determined jointness, descriptiveness, explanatory, analytical, interpretation, multidisciplinarity, wide coverage, flexibility, openness, interpretation, synergy, entrenchment, internal dependence, controllability, operational focus, uncertainty reduction and database synthesis. To create an opportunity for increased understanding in the conditions of complexity and uncertainty, the process of building the conceptual framework is presented as systematized, consistent, iterative, passing through each of the described phases. Regardless of the many limitations formed by the set requirements for mandatory product validation, in the construction of the conceptual framework for the analysis of the transformation and interoperability of the armed forces, sufficient

flexibility, opportunities for changes and upgrades, the full absorption of which would guarantee the maintenance of a permanent relevance of similar scientific research tools.

7.5.9. Operability of the Intellectual Framework for Institutional Resilience, Crisis and Emergency Management

The institutions of the modern state are under increasing pressure to ensure high efficiency of the performed functions and optimal value of public expenditures. On the one hand, institutional obligations are constantly increasing, and on the other, public expectations for cost reduction are increasing, especially for the activities of institutions in the national security system. The trends of increasing the diversity and number of security threats and challenges set requirements for the optimization of the institutionally ongoing processes of forming the national and institutional security policies on common national interests, priorities, goals while at the same time institutionally developed and shared capabilities. The operability of the universal institutional framework follows the implementation of the basic principles laid down in its construction to become an integral part of the universal intellectual platform for national security management.

In response to the national and union requirements and the public expectation for increasing institutional efficiency, the development and functioning of institutions, it would follow that the construction, integration and use of institutional capabilities should be carried out on standardized generally applicable science-based models and techniques for strategic planning, evaluation, analysis and development. A suitable platform for structural and functional improvement of institution models is the application of systems engineering techniques or an architectural approach . Such an approach provides an opportunity for a comprehensive assessment of the current and future perspectives of the structure and functionality of each institution on a universal but unique business model for each institution. The institutional business model binds the normative, strategic, conceptual, functional requirements and through interconnected architectural perspectives implements them in the institutional processes of planning, building and managing institutional capabilities in a common transparent and accountable financial framework of all current and future core products and services of the institution, consistent with its contractual obligations and obligations.

7.5.10. Institutional Business Model for Engineering of a National Crisis and Emergency Management System

The institutional business model is applied to a simplified representation of the structure and operation of a particular institution. Linking institutional outputs or outcomes to institutional functions through the institutional structure is used. Although each institutional business model is unique, it can be used to represent the universality of possibilities for describing the functionality of a real complex organization or public system. It is used to describe and map the main purpose of the institution without the need for an in-depth presentation of the complexities, underlying principles, characteristics and relationships.

Modern institutions really need a business model for a clearer presentation and distribution of their main and auxiliary roles and responsibilities in the management of the state, for describing the internal and external dependence of the functionality of the modeled institution. As an intellectual product of systems engineering, the business model can be used to increase the efficiency of the institution, optimize the organizational structure and reduce unnecessary intra-institutional bureaucracy. Therefore, the business development of each of the institutions in the national security system can be considered as applying a science-based approach to avoiding functional duplication, more clearly defining and distinguishing the functional areas and responsibilities of the institutions to achieve the desired results in the subject area of security and defence.

In addition, the application of the business model approach in the strategic management of the institutions of the national security system would help:

• The disclosure of the connections between the performed institutional duties and the contributions of each institution to achieve the main results of the national security system;

• Ensuring the implementation of a unified process of strategic planning and implementation of existing arrangements and agreements with other institutions in the system;

• Increasing understanding and supporting the internal structuring of the institution's responsibilities and accountability for its activities in the national security system;

• Consideration of all opportunities for optimization of the organizational structure to ensure the most effective and efficient achievement and delivery of the institutional results in the security system;

• Support and increase the possibilities for forecasting the manifestation of future risks for the institutional functionality and for the achievement of the institutional results that are important for the entire security system.

The unified construction and functioning of the business models of institutions in the security system is based on the need for the readiness of each institution to provide (contribute to the construction of) system capabilities key to the operation. The capabilities are built, managed and integrated to ensure the performance of the main functions, operations, missions to maintain the continuous overall operationality of each institution individually and the system as a whole. Therefore, the development of the institutional business model should take into account the complexity of the structure of the national security system, the high degree of interdependence of all institutions in the system, the obligations to build individual and system-wide capabilities, as well as the requirements for transparency and accountability in the functioning of the model (laid down in the requirements of the constitution and other legal and regulatory documents).

The use of the business model for the unification of institutional sustainability, functionality and contributions to the national security system [27]requires taking into account the course of all internal institutional processes and the unique institutional contribution to the course of external processes, the integration of which with the activities of other institutions forms the foundation of activities that is critical to the functionality of the entire system. Unified generalized for all institutions, these processes can be systematized in several areas: enabling processes – performance of the functions of unified development of strategic intra-institutional guidelines, formation of institutional policies, activation of the governing documents for managing the construction and use of institutional capabilities; management of institutional capabilities – implementation of institutional functions for building, preparing and maintaining the specific capabilities of the legally prescribed mandatory levels of

[27]Mitko Stoykov, Institutional sustainability of the national security system, monograph, AvangardPrima, 2018.

readiness for use in the national security system; integration of capabilities – implementation of institutional functions for integration of institutional and system capabilities in readiness for operational use; delivery of the final institutional products in the system – performance of the institutional functions to provide ready-to-use capabilities in accordance with the legally prescribed requirements for each institution.

Characteristic of the activation of the institutional business models of the elements of the national security system is the use of system-wide strategic documents - security strategies, defence or military strategies, White Paper on defence, documents from periodic strategic reviews, annual reports on the state (of security and defence), planning guidelines, budget guidelines. In the activation of the core institutional functions, the practices related to the fulfillment of alliance obligations are carried out by independently or participating in the collective construction and use of alliance defence and security capabilities.

The unified set of the main functions institutional functions, which affects the internal-institutional structuring and determines the internal and external functional connections for the institution can be generalized to: initiators to ensure the activation of the institutional functionality; strategies and policies to provide strategic guidance; budget management for financial assurance of the processes; science and technology for scientific assurance of ongoing processes; building and developing abilities to guide all functional processes and links to the achievement of the final institutional products; management of human capital (human resources) for hiring, training and securing the personnel of the institution; management of the infrastructure to materially ensure the progress of the processes; security function – for guaranteed management of functionality-related risks and threats; an acquisition function to provide the institution with systems and materials throughout their life cycle; control and audit to guarantee the institution's independence and accountability in the implementation of the main functions; logistic – for overall material and technical provision of ongoing processes; education and training to ensure the continuity of the improvement of the qualification of the personnel; health and social insurance for personnel; legal provision to guarantee the normative compliance of the functionality with the requirements of the legal-normative institutional base.

The application of a business model for the management of institutional functionality and integration in the national security system orients all institutional processes

towards final products and provides an opportunity to continuously follow the chain to increase their value. It ensures the implementation of established practices for strategic decision-making and management, as well as strategic engagement with all other institutions in the national security system. In detail, the security system engineering process is represented by the Security System Engineering Intellectual Framework.

8. Products of the Conceptual Framework

8.1. Institutional Business Continuity Management Policy[28]

The 2022 Strategic Concept reaffirms the Alliance key purpose to ensure collective defence of the member states. NATO's effectiveness as a vision, military alliance rests on its ability to successfully deliver these core tasks: to deter and defend against the full range of threats, to respond to and manage crises beyond NATO territory, and to enhance international security through cooperation. The Alliance is not immune to threats and hazards that could potentially degrade its effectiveness. Disruptions of different scales and types have affected, and will continue to affect NATO in the future so that the North Atlantic Council (NAC) recognized the need to establish Business Continuity Management (BCM) as a discipline. The BCM discipline is strongly related to other NATO disciplines such as incident management, emergency response, risk management, and crisis management.

NATO BCM policy[29] provides the vision, aims, leading principles, requirements and governing structures, as well conditions for development NATO BCM System and alignment of BCM activities across NATO drawing on guidance based on the International Standards.

In response of NATO BCM Policy minimum requirements, CMDR COE develops and applies a CMDR COE Department Head of NATO BCM Discipline Business Continuity Management Policy Statement.

[28] This concept is specially developed for Crisis Management and Disaster Response Centre of Excellence

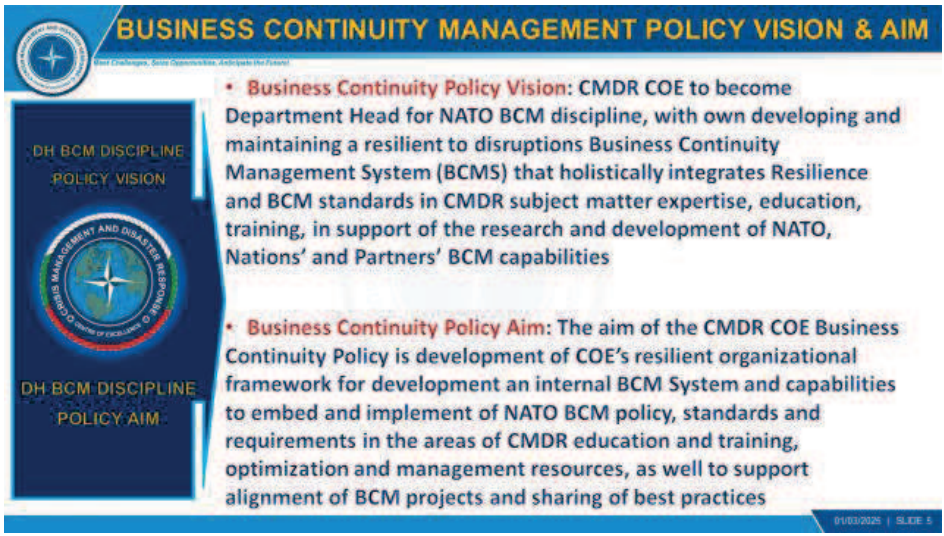
[29] PO(2020)0166, 20 May 2020, NATO Business Continuity Policy

Vision

Following the requirements of NATO BCM policy, the vision for the establishing CMDR COE Business Continuity Policy is:

CMDR COE to become Department Head for NATO BCM discipline, with own developing and maintaining a resilient to disruptions Business Continuity Management System (BCMS) that holistically integrates Resilience and BCM standards in CMDR subject matter expertise, education, training, in support of the research and development of NATO, Nations' and Partners' BCM capabilities.

Aim



The aim of the CMDR COE Business Continuity Policy is development of COE's resilient organizational framework for development an internal BCM System and capabilities to embed and implement of NATO BCM policy, standards and requirements in the areas of CMDR education and training, optimization and management resources, as well to support alignment of BCM projects and sharing of best practices.

Purpose

CMDR COE Department Head BCM is established to promote the execution of the COE critical functions in the event of a disruptive incident, in accordance with the

requirements and aligns with the requirements of ISO 22301 Security and Resilience – Business Continuity Management System.

Applicability

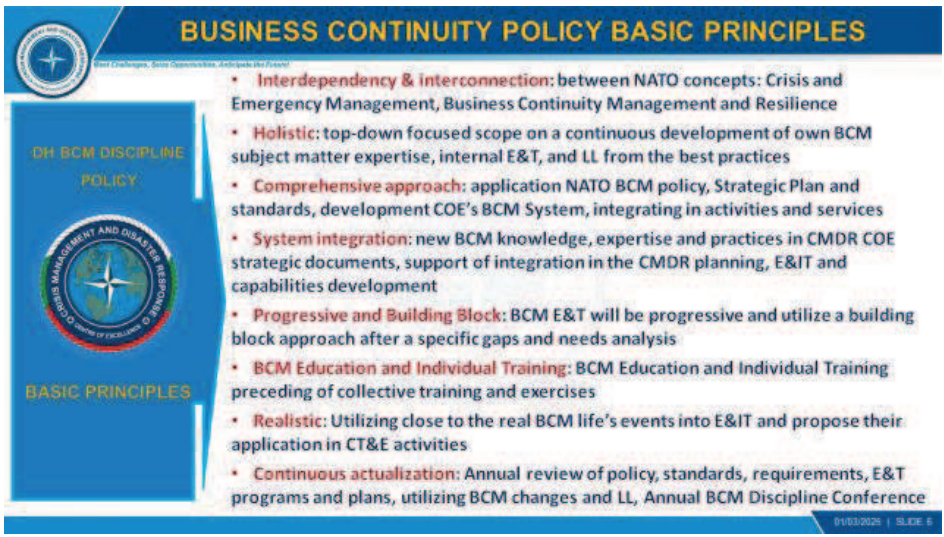
This policy is applicable to CMDR COE employees as part of the internal BCM system and in particular, those involved in the fulfilment of the duties of the Department Head NATO BCM discipline.

Policy requirements

The CMDR COE adopts an integrated Business Impact Analysis and Risk Management based approach to the operation of Centre's internal BCM system and develops plans to ensure the continuity of its critical business functions. Planning and training activities and the process for incidents management are outlined in the CMDR COE BCM Framework.

Basic Principles

The implementation of the CMDR COE BCM policy is based on NATO BCM basic principles: leadership engagement; coherence, focus on outposts; System of Systems Approach.



Additionally, when perform its functions and POW activities, CMDR COE will apply the following principles:

- Conceptual and practical interdependency and interconnection between the NATO concepts of Crisis and Emergency Management, Business Continuity Management and Resilience;
- Holistic top-down focused scope on a continuous development of own BCM subject matter expertise, internal E&T, and LL from the best practices;
- Comprehensive approach in application NATO BCM policy, Strategic Plan and standards in development a CMDR COE's BCM System, as well all integrating it in all COE's activities and provided services;
- System integration of available and new BCM knowledge, expertise and practices in CMDR COE strategic management documents and support integration of BCM in the Alliance CMDR planning, E&IT and capabilities development;

As Department Head for the NATO BCM discipline, in E&T activities CMDR COE will apply the following NATO ETEE Policy principles[30]:

- BCM E&T should be progressive and utilize a building block approach after a specific gaps and needs analysis;
- BCM Education and Individual Training preceding of collective training and exercises;
- Utilizing close to the real BCM life's events into E&IT and propose their application in CT&E activities;
- Annually based review of BCM policy, standards, requirements, E&T programs and plans, utilizing BCM changes and LL at the Annual BCM Discipline Conference.

BCM Framework

The CMDR COE will maintain an up-to-date standardised BCM Framework that provides assurance to the Centre's Director, Searing Committee, Chefs of Branches and SD&BCM Section that disruption related risks are clearly identified and managed appropriately, with consideration to the CMDR COE capabilities and objectives, and that business continuity can be maintained should a disruption occur.

CMDR COE branches are responsible for undertaking planning activities outlined in the BCM Framework, when following key components:

[30] MC 0586/1, Policy for Allied Forces and their use for Operations, 9 Aug 12;

- Risk identification and assessment
- Business impact analysis
- Business continuity planning
- Regular audits, testing and training.

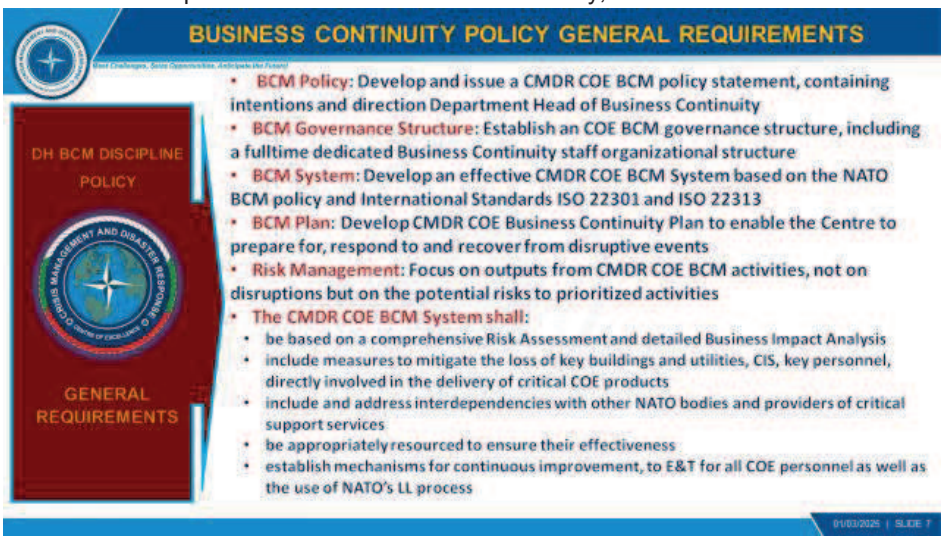
This includes maintaining up-to-date business continuity plans (BCPs) which define the priorities and processes to respond, recover, restore and resume the CMDR COE's critical business functions (CBF) to a pre-defined level of operation. Critical events are escalated to the department's business continuity team (BCT) which is responsible for management of the branches response and recovery from critical events. CD&BCM Section is responsible for planning and execution of DH NATO BCM Discipline activities.

CMDR COE Requirements

General Requirements:

In development and application of CMDR COE BCM policy, the Centre will comply with the following BCM standard minimum requirements:

- Develop and issue a CMDR COE BCM policy statement, containing intentions and direction Department Head of Business Continuity;



- Establish an COE BCM governance structure, including a fulltime dedicated Business Continuity staff organizational structure;

• Develop an effective CMDR COE BCM System based on the requirements on NATO BCM policy and International Standards ISO 22301 and ISO 22313

• Develop CMDR COE Business Continuity Plan to enable the Centre to prepare for, respond to and recover from disruptive events;

• Focus on outputs from CMDR COE BCM activities, not on disruptions but on the potential risks to prioritized activities.

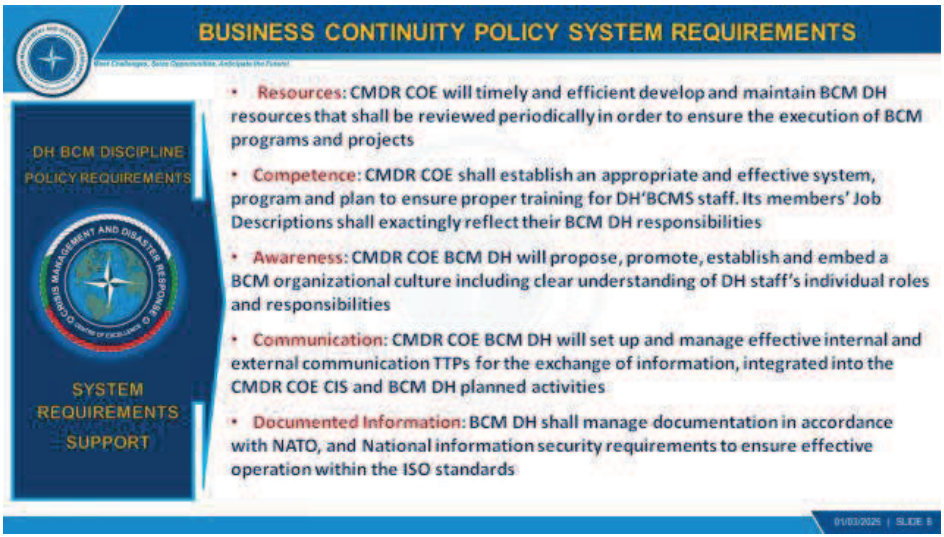
• The CMDR COE BCM System shall:

- be based on a comprehensive Risk Assessment and detailed Business Impact Analysis;
- include measures to mitigate the loss of key buildings and utilities, Communication and Information Systems, key personnel, directly involved in the delivery of critical COE products;
- include and address interdependencies with other NATO bodies and providers of critical support services;
- be appropriately resourced to ensure their effectiveness;
- establish mechanisms for continuous improvement, to E&T for all COE personnel as well as the use of NATO's Lessons Learned process.

BCM DH System Requirements

Support Requirements

• ***Resources***. CMDR COE will timely and efficient develop and maintain BCM DH resources that shall be reviewed periodically in order to ensure the execution of BCM programs and projects.



• ***Competence***. CMDR COE shall establish an appropriate and effective system, program and plan to ensure proper training for DH'BCMS staff. Its members' Job Descriptions shall exactingly reflect their BCM DH responsibilities.

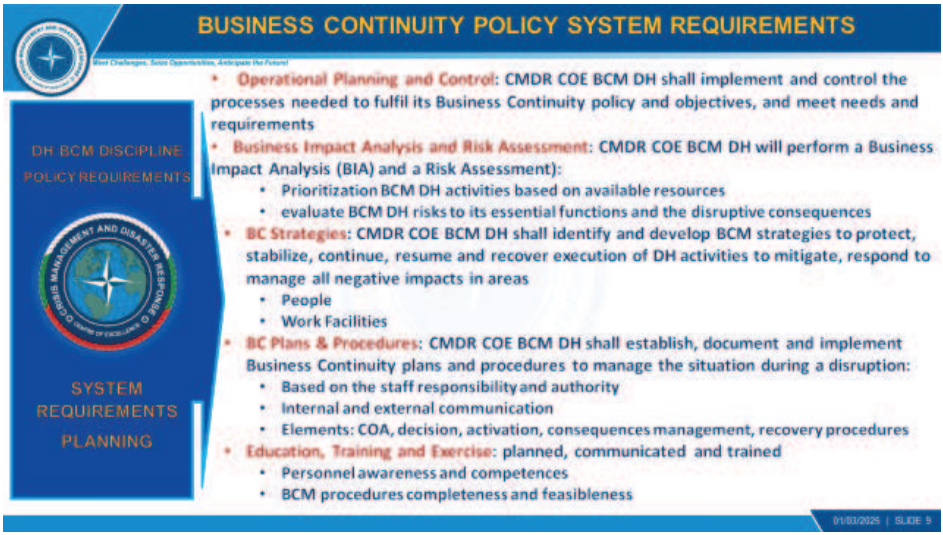
• ***Awareness***. CMDR COE BCM DH will propose, promote, establish and embed a BCM organizational culture including clear understanding of DH staff's individual roles and responsibilities.

• ***Communication***. CMDR COE BCM DH will set up and manage effective internal and external communication TTPs for the exchange of information, integrated into the CMDR COE CIS and BCM DH planned activities.

• ***Documented Information***. BCM DH shall manage documentation in accordance with NATO, and National information security requirements to ensure effective operation within the ISO standards.

Planning Requirements

• ***Operational Planning and Control***. CMDR COE BCM DH shall implement and control the processes needed to fulfil its Business Continuity policy and objectives, and meet needs and requirements.



• ***Business Impact Analysis and Risk Assessment***. CMDR COE BCM DH will perform a Business Impact Analysis (BIA) and a Risk Assessment (RA):

- The BIA shall identify prioritized BCM DH activities based on available resources to maintain these activities. The BIA shall be revised and endorsed by CMDR COE SC;
- The RA shall evaluate the specific BCM DH risks to its essential functions and the potential disruptive consequences, as well will propose appropriate Risk Management action.

• ***Business Continuity Strategies***. Based on BIA and RA, CMDR COE BCM DH shall identify and develop BCM strategies to protect, stabilize, continue, resume and recover execution of DH activities as well as to mitigate, respond to and manage all negative impacts, grouped in areas:

- People: Avoiding DH staff single points of failure by planning, implementing, testing and improving the necessary arrangements, TTPs, BCM DH plans' backup and alert mechanisms.
- Work Facilities: Arrange available alternate working area for prioritized activities and BCM DH staff including distance working and teleworking capabilities.
- Communication and Information Systems and Infrastructure: CIS and other information infrastructure of BCM DH will be planned and resourced to provide BCMS's resilience including data back-up and recovery infrastructure.

• ***Business Continuity Plans and Procedures***. CMDR COE BCM DH shall establish, document and implement Business Continuity plans and procedures to manage the situation during a disruption: including:

- DH will respond to disruptions, using staff responsibility and authority;
- DH will document and maintain procedures for Internal and external communication as well as the necessary information infrastructure;
- DH Business Continuity Plans shall provide guidance and information to respond to disruptions with the following elements:
  - Course of actions to undertake by the teams;
  - Activation criteria (decision points) and processes; and
  - Guidance to manage the immediate consequences of a disruption.
  - Recovery procedures to restore activities.

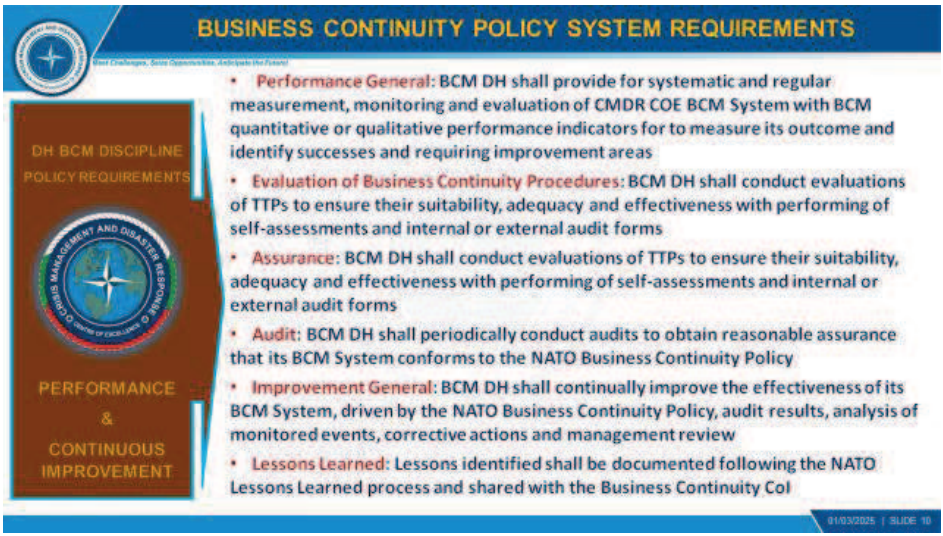
• ***Education, Training and Exercise***. CMDR COE DH Business Continuity Plans and procedures shall be planned, communicated and trained regularly:

- to promote personnel awareness and competency development;

- to ensure completeness and feasibleness of BC procedures.

Performance Evaluation Requirements

- ***General***. BCM DH shall provide for systematic and regular measurement, monitoring and evaluation of CMDR COE BCM System with BCM quantitative or qualitative performance indicators for to measure its outcome and identify successes and requiring improvement areas.



- ***Evaluation of Business Continuity Procedures***. BCM DH shall conduct evaluations of TTPs to ensure their suitability, adequacy and effectiveness with performing of self-assessments and internal or external audit forms.

- ***Assurance***. BCM DH control self-assessment will be supplemented by a certification letter, signed and annually reported to the Business Continuity Board.

- ***Audit.*** BCM DH shall periodically conduct audits to obtain reasonable assurance that its BCM System conforms to the NATO Business Continuity Policy.

Continuous Improvement Requirements

- ***General***. BCM DH shall continually improve the effectiveness of its BCM System, driven by the NATO Business Continuity Policy, audit results, analysis of monitored events, corrective actions and management review.

- ***Lessons Learned***. Lessons identified shall be documented following the NATO Lessons Learned process and shared with the Business Continuity CoI.

CMDR COE BCM Discipline DH Management

Clear organizational roles, responsibilities and authorities are essential to the successful implementation of the CMDR COE DH BC Policy. The BCM DH governance structure shall include the CMDR COE DH BCMS with the following components:

- BCM DH Policy;
- DH structure, people and responsibilities;
- BCM DH management processes:
  - policy;
  - planning;
  - implementation and operation;
  - performance assessment;
  - management review;
  - continual improvement;
- BCM DH documents in support of operational control and performance evaluation.

BASIC BCM DEFINITIONS

Based on ISO 22300 Security and Resilience (2021), ISO 22301 Business Continuity (2019) and Business Continuity Institute Good Practice Guidelines (2018)

Activity	One or more tasks undertaken by an organisation that produces or supports the delivery of products or services.
Analysis	A professional practice within the business continuity management cycle that reviews and assesses an organisation to identify its objectives, how it functions and the constraints of its operating environment.
Audit	One or more tasks undertaken by an organisation that produces or supports the delivery of products or services.
Business Continuity	Capability of an organisation to continue to deliver products or services at acceptable predefined levels following a disruptive incident.
Business Continuity Management	Holistic management process that identifies potential threats to an organisation and the impacts to business operations those threats, if realised, might cause and which provides a framework for building organisational resilience with the capability of an effective response that safeguards

	the interest of its key stakeholders, reputation, brand and value-creating activities.
Business Continuity Management Lifecycle	The ongoing cycle of activities of a business continuity programme that builds organisational resilience: policy & programme management; embedding; analysis; design; implementation; validation.
Business Continuity Management System (BCMS)	Part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity.
Business Continuity Plan (BCP)	Documented information that guides an organisation to respond to a disruption and resume, recover and restore the delivery of products and services consistent with its business continuity objectives.
Business Continuity Programme	Ongoing management and governance process supported by top management and appropriately resourced to implement and maintain business continuity management.
Business Impact Analysis (BIA)	Process of analysing activities and the effect that a business disruption might have upon them.
Competence	Action to eliminate the cause of a non-conformity and to prevent recurrence.
Conformity	A situation with a high level of uncertainty that disrupts core activities and/or credibility of an organisation and requires urgent action.
Continual Improvement	Recurring activity to enhance performance.
Correction	Action to eliminate a detected non-conformity.
Corrective Action	Action to eliminate the cause of a non-conformity and to prevent recurrence.
Design	A professional practice within the business continuity management lifecycle that identifies and selects appropriate solutions to determine how continuity can be achieve in the event of an incident.
Document	Information and its supporting medium.
Documented Information	Information required to be controlled and maintained by an organisation and the medium on which it is contained.
Effectiveness	Extent to which planned activities are realised and planned results achieved.
Embedding	A professional practice within the business continuity management cycle that defines how to integrate business continuity awareness and practice into business-as-usual activities.
Event	Occurrence or change of a particular set of circumstances. It could be one or more occurrences. An event can consist

	of something not happening. An event could also be referred to as an incident or accident. An event without consequences may also be referred to as near miss.
Exercise	Process to train for, assess, practise and improve performance in an organisation.
Implementation	A professional practice within the business continuity management cycle that implements the solutions agreed in the design stage. It also includes developing the Business Continuity Plans and a response structure.
Incident	Situation that might be, or could lead to, a disruption, loss, emergency or crisis.
Infrastructure	System of facilities, equipment and services needed for the operation of an organisation.
Interested Party	Or Stakeholder. Person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity.
Internal Audit	Audit conducted by, or on behalf of, the organisation itself for management review and other internal purposes, and which might form the basis for an organisation's self-declaration of conformity.
Invocation	Act of declaring that an organisation's business continuity arrangements need to be put into effect in order to deliver key products and services.
Management System	Set of inter-related or interacting elements of an organisation to establish policies and objectives, and processes to achieve those objectives.
Maximum Acceptable Outage (MAO)	See also maximum tolerable period of disruption. The time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable.
Maximum Tolerable Period Of Disruption (MTPD)	See also maximum acceptable outage. The time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable.
Measurement	Process to determine a value.
Minimum Business Continuity Objective (MBCO)	Minimum level of services/products that is acceptable to the organisation to achieve its business objectives during a disruption.
Monitoring	Determining the status of a system, a process or an activity.
Mutual Aid Agreement	Pre-arranged understanding between two or more entities to render assistance to each other.
Non-Conformity	Non-fulfilment of a requirement.

Objective	Result to be achieved. An objective could be Strategic, Tactical or Operational. It could be expressed in other ways as, for example, a goal, an aim or target.
Organisation	Person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives.
Organisational Culture	Values, attitudes and behaviour of an organisation that contribute to the unique social and psychological environment in which it operates.
Organisational Resilience	The ability of an organisation to absorb and adapt in a changing environment.
Outsource	Make an arrangement where an external organisation performs part of an organisation's function or process.
Performance	Measurable result.
Performance Evaluation	Process of determining measurable results.
Personnel	People working for and under the control of an organisation.
Policy	Intentions and direction of an organisation as formally expressed by its top management.
Policy And Programme Management	A professional practice within the business continuity management cycle that establishes the organisation's policy relating to business continuity and defines how the policy should be implemented throughout the business continuity programme.
Prioritised Activities	Activities to which priority must be given following an incident in order to mitigate impacts.
Procedure	Specified way to carry out an activity or a process.
Process	Set of inter-related or inter-acting activities which transforms inputs into outputs.
Products and Services	Beneficial outcomes provided by an organisation to its customers, recipients and interested parties.
Record	Statement of results achieved or evidence of activities performed.
Recovery Point Objective (RPO)	Point to which information used by an activity must be restored to enable the activity to operate on resumption. Can also be referred to as maximum data loss.
Recovery Time Objective (RTO)	Period of time following an incident within which a product or service must be resumed; or an activity is resumed; or resources are recovered.
Requirement	Need or expectation that is stated, generally implied or obligatory. Generally implied means that it is customary or common practice for the organisation.

Resources	All assets, people, skills, information (whether electronic or not), technology (including plant and equipment), premises and supplies that an organisation has to have available to use, when needed, in order to operate and meet its objective.
Risk	Effect of uncertainty on objectives. Often expressed in terms of a combination of consequences and likelihood.
Risk Appetite	Amount and type of risk that an organisation is willing to pursue or retain.
Risk Assessment (RA)	Overall process of risk identification, risk analysis and risk evaluation.
Risk Management	Coordinated activities to direct and control an organisation with regard to risk.
Stakeholder	Or Interested Party. Person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity.
Test	Unique and particular type of exercise which incorporates an expectation of a pass or fail element within the aims or objectives of the exercise being planned.
Testing	Procedure for evaluation. A means of determining the presence, quality or veracity of something.
Threat	Potential cause of an unwanted incident which may result in harm to individuals, assets, systems or organisation, environment or the community.
Top Management	Person or group of people who direct(s) and controls an organisation at the highest level.
Validation	A professional practice within the business continuity management cycle that confirms that the business continuity programme meets the objectives set in the policy, and that the plans and procedures in place are effective. It includes exercises, maintenance and review activities.
Test	Unique and particular type of exercise which incorporates an expectation of a pass or fail element within the aims or objectives of the exercise being planned.

Bibliography

1. A MC 0458/4 (Final), NATO Education, Training, Exercises, and Evaluation (ETEE) Policy, dated 03 January 2023.
2. AC/335-N(2017)0025-REV1-AS1, dated 27 August 2017, Resource Policy & Planning Board (RPPB) IBAN Performance Audit Report to Council on the Lack of Policy and Standards for Business Continuity Planning within NATO
3. ACT 2NU-40/13.03.2024 BCM MoA BETWEEN HQ SACT AND CMDR COE CONCERNING APPOINTMENT OF DEPARTMENT HEAD FOR NATO BCM DISCIPLINE
4. ACT/JFD/ETPPITT-7150/SER: NU, CORRIGENDUM 1 TO BUSINESS CONTINUITY MANAGEMENT STRATEGIC TRAINING PLAN
5. Allied Command Operations Comprehensive Operations Planning Directive;
6. Allied Joint Doctrine for Civil-Military Cooperation;
7. Allied Joint Doctrine for Non-Article 5 Crisis Response Operations;
8. Business Continuity Institute Good Practice Guidelines (2018)
9. EM(HQST-BCO)(2021)0024, NATO Business Continuity Guidelines
10. Handbook on EU CSDP Missions and Operations, The Common Security and Defence Policy of the European Union;
11. ISO 22300 Security and Resilience (2021)
12. ISO 22301 Business Continuity (2019)
13. ISO 22301 International Standard: Security and resilience — Business continuity management systems — Requirements
14. ISO 22301:2019 Security and Resilience - Business Continuity Management Systems - Requirements
15. ISO 22313:2020 Security and Resilience - Business Continuity Management Systems – Guidance
16. MCM-0203-2023, 28 November 2023, Appointment of Department Head for Business Continuity Management Discipline
17. MCM-0308-2021, 2022 Bi-SC Comprehensive List of Disciplines, dated 14 April 2022.
18. NATO Strategic Concept;
19. PO(2020)0166, 20 May 2020, NATO Business Continuity Policy
20. Practical Guide to Grounded Theory Research, https://delvetool.com/groundedtheory;
21. Директиви на НАТО по сигурността;
22. Доклад за състоянието на националната сигурност на Република България 2021 г.;
23. Доклад от Стратегическия преглед на системата за защита на националната сигурност и Стратегическия преглед на отбраната 2021 г.;
24. Закон за водите;
25. Закон за Държавна агенция "Национална сигурност";
26. Закон за защита при бедствия,
27. Закон за защита при бедствия;
28. Закон за МВР
29. Закон за опазване на околната среда;
30. Закон за отбраната и въоръжените сили на Република България;
31. Закон за противодействие на тероризма;
32. Закон за управление и функциониране на системата за защита на националната сигурност;
33. Закон за управление и функциониране на системата за защита на националната сигурност, https://lex.bg/en/laws/ldoc/2136588572;
34. Закон за управление на отпадъците;
35. Конституция на Република България
36. Митко Стойков, Институционална устойчивост на системата за национална сигурност, АвангардПрима 2018.
37. Национална стратегия за противодействие на престъпността;
38. Отбранителна стратегия на Република България;
39. Регламент (ЕС) № 513/2014 НА Европейския парламент и на Съвета от 16 април 2014 година за създаване на инструмента за финансово подпомагане на полицейското сътрудничество, предотвратяването и борбата с престъпността и управлението на кризи и извънредни ситуации като част от фонд „Вътрешна сигурност“ и за отмяна на Решение 2007/125/ПВР на Съвета;

40. Регламент (ЕС) № 514/2014 на Европейския парламент и на Съвета от 16 април 2014 година за определяне на общи разпоредби за фонд „Убежище, миграция и интеграция“ и за инструмента за финансово подпомагане на полицейското сътрудничество, предотвратяването и борбата с престъпността и управлението на кризи и извънредни ситуации;
41. Решение (ЕС) 2017/342 на Европейския парламент и на Съвета от 14 декември 2016 година относно мобилизирането на средства по линия на Инструмента за гъвкавост за финансиране на незабавни бюджетни мерки за справяне с продължаващата криза с миграцията, бежанците и сигурността;
42. Стратегия за национална сигурност на Република България;

BASELINE REQUIREMENTS FOR NATIONAL RESILIENCE AND PLANNING

Orlin NIKOLOV, PhD
Ralitsa BAKALOVA

Abstract: This article presents a comprehensive approach to building national resilience through integrated civil-military collaboration and a "whole-of-society" strategy. It emphasizes the need for coordinated response frameworks to address both immediate crises and long-term threats, including climate change and critical infrastructure vulnerabilities. Key components discussed include establishing robust baseline requirements, enhancing civil-military coordination, and fostering public awareness and preparedness. The article highlights actionable short-, medium-, and long-term strategies that strengthen infrastructure, promote community engagement, and encourage international cooperation, aiming to create resilient societies capable of withstanding modern security challenges.

Introduction

The importance of civil-military collaboration in building robust national resilience frameworks cannot be overstated. Effective partnerships between military institutions and civilian agencies are crucial to enhancing operational readiness and ensuring coordinated responses to disruptions. During discussions, participants emphasized the need for integrated strategies that address both immediate crisis management and long-term preparedness, particularly in safeguarding critical infrastructure. NATO's guidance has been pivotal in shaping responses to modern security threats, including climate-related challenges and supply chain vulnerabilities, which require resilient civil communications and transportation systems.

Given the evolving nature of global threats, there is a growing consensus on the need for a "whole-of-society" approach to resilience. This approach integrates military and civilian efforts to strengthen preparedness, facilitate rapid response, and build trust among all stakeholders. By fostering greater understanding and cooperation between military and civilian sectors, nations can ensure a more unified, resilient response to contemporary security challenges, particularly those exacerbated by climate change.

Chapter I: The Connection between Climate Resilience and NATO's Baseline Requirements for Resilience

The connection between climate resilience and NATO's Baseline Requirements for Resilience arises from the recognition that climate change significantly threatens national security and the stability of member states. NATO's Baseline Requirements provide a structured framework for enhancing preparedness against various threats, including those intensified by climate change.

Here are NATO's 7 Baseline Resilience Requirements:

1. Assured continuity of government and critical government services: The ability to make decisions, communicate them, and enforce them during a crisis.
2. Resilient energy supplies: Ensuring backup plans and power grids are in place, both internally and across borders.
3. Ability to manage uncontrolled movement of people: Effectively addressing population movements that may conflict with military deployments.
4. Resilient food and water resources: Safeguarding supplies from disruption or sabotage.
5. Capacity to deal with mass casualties and health crises: Ensuring civilian health systems can cope and that sufficient medical supplies are stocked and secure.
6. Resilient civil communications systems: Maintaining the functionality of telecommunications and cyber networks even under crisis conditions.
7. Resilient transport systems: Ensuring rapid movement of NATO forces across Alliance territory and reliable transportation networks for civilian services during crises.

These requirements highlight the interdependence of climate resilience and national security. By integrating climate considerations, NATO adopts a holistic approach that includes military, civilian, and environmental factors, recognizing climate resilience as a collective responsibility requiring cross-sector cooperation. Member states are encouraged to develop strategies to enhance resilience against climate-related challenges, such as natural disasters, food and water scarcity, and population displacement, which can lead to social unrest.

The 2022 NATO Strategic Concept emphasizes resilience as a core issue, advocating for a robust response to disruptive threats, including climate change. This focus

reinforces the importance of climate resilience within NATO's security framework and promotes a "whole-of-society" approach, necessitating collaboration among governments, civil society, and the private sector.

Climate resilience is the capacity of communities, economies, and ecosystems to prepare for and recover from climate-related hazards. In terms of national security, it is essential for maintaining stability amid environmental changes. NATO's Baseline Requirements provide a vital framework for member states to enhance their resilience against various threats, including those intensified by climate change.

Chapter II: Challenges in Climate Resilience

As the effects of climate change intensify, the need for effective resilience strategies becomes increasingly urgent. However, integrating climate considerations into security frameworks faces significant obstacles, including issues with policy implementation, public awareness, and cross-sector coordination.

One major challenge lies in **policy implementation**. Incorporating climate considerations into security policies can be difficult because many existing frameworks prioritize immediate threats over long-term climate impacts. For effective integration, policymakers must recognize climate change as a multifaceted issue with profound implications for national security, economic stability, and public health. This shift requires a proactive, rather than reactive, approach, with policies designed to anticipate future climate-related disruptions and address their root causes.

Raising awareness of climate risks among both the public and government officials is also critical. A limited understanding of climate threats can hinder resource allocation and weaken the political resolve needed to support resilience initiatives. Educational programs play a crucial role in promoting a culture of preparedness, helping to ensure that climate resilience receives the attention it deserves within policy agendas.

Lastly, **coordination and response timing** pose further challenges. Effective responses to climate crises require seamless collaboration across government levels and sectors, which is often hampered by inadequate communication channels. By developing integrated response frameworks and conducting regular training exercises, stakeholders can improve reaction times and enhance their ability to work together efficiently. Strengthened coordination across sectors and consistent training

will ensure a more robust, unified response to climate-induced crises, bolstering overall resilience in the face of growing environmental threats.

Chapter III: Key Actors in Climate Resilience

With the impacts of climate change becoming ever more apparent, it is essential to adopt strategies that build resilience across communities and sectors. This approach to climate resilience is organized into short-term, medium-term, and long-term actions, each addressing critical needs to strengthen preparedness and adaptive capacity.

Short-Term Actions

In the short term, immediate actions can significantly enhance preparedness and response capabilities in the face of climate-related threats. Conducting risk assessments is a foundational step, allowing communities and agencies to identify vulnerabilities in infrastructure and services. By understanding potential impacts, decision-makers can prioritize areas needing intervention and allocate resources more effectively.

Another crucial short-term strategy involves establishing dedicated emergency response teams trained in disaster response protocols and equipped with the necessary resources. These teams ensure a rapid, coordinated reaction when climate-related emergencies arise, reducing potential damage and supporting affected populations.

Ensuring the resilience of critical infrastructure—such as transportation, energy, and water systems—is also essential. This requires assessing and upgrading these systems to withstand climate stresses, implementing resilient design standards, and retrofitting existing structures where needed.

Medium-Term Actions

Medium-term strategies focus on capacity building and fostering engagement across communities. Public education and social programs are vital in this regard. By raising awareness about climate risks and resilience strategies, these programs empower citizens to take proactive measures and contribute to a community-wide culture of preparedness.

Strategic action development is another key medium-term priority. By creating adaptable plans for responding to climate threats and incorporating feedback from past events, organizations and communities can ensure that resilience strategies stay relevant and effective amid changing conditions.

Research and implementation of best practices in climate resilience, informed by lessons from previous events, drive continuous improvement. Partnerships with academic institutions and research organizations can support the development of innovative solutions, bringing new insights into resilience-building efforts.

Encouraging shifts in societal attitudes toward climate resilience and sustainability through advocacy and outreach also plays an important role. Campaigns that promote sustainable practices and emphasize resilience help create a culture that values preparedness and adaptive capacity.

Long-Term Actions

For sustaining resilience over time, long-term strategies are crucial. Consistency and adaptation are key here—regularly reviewing and updating resilience plans to respond to evolving climate threats keeps them effective and relevant as new challenges emerge.

Investing in resilient infrastructure and advanced technology is fundamental to climate adaptation efforts. This includes green technologies, renewable energy, and sustainable urban planning, all of which can strengthen long-term resilience by making infrastructure less vulnerable to climate impacts.

Regional coordination is another essential long-term strategy. Establishing or reinforcing regional emergency management agencies can facilitate cross-border climate resilience efforts, promoting collaborative resource sharing, information exchange, and coordinated responses among neighboring jurisdictions.

Together, these short-, medium-, and long-term actions form a comprehensive approach to building climate resilience, ensuring that communities, infrastructure, and governance systems are better prepared to withstand and adapt to the growing challenges of a changing climate.

Chapter V: Collaboration between International Organizations

As climate challenges continue to intensify, collaboration among international organizations has become essential for strengthening global resilience. Effective partnerships and coordinated efforts are critical to addressing climate-related threats on a global scale. This chapter explores the key strategies that drive successful collaboration and foster collective responses to these pressing challenges.

One primary strategy is resource pooling. By combining financial, technical, and human resources, countries and organizations can maximize the efficiency of climate response efforts. Shared resource pools enable rapid responses to emergencies and foster a spirit of solidarity among nations that face similar climate challenges, allowing them to tackle crises with a united front.

Strengthening partnerships among international organizations, member states, and key stakeholders is equally essential. Building robust collaborative frameworks promotes joint training, consistent information sharing, and coordinated action plans. These frameworks lay the groundwork for a unified approach to climate threats, ensuring that all parties are prepared and equipped to manage crises effectively.

A commitment to continuous learning enhances resilience efforts by allowing organizations to analyze past experiences and refine their strategies. Workshops, conferences, and shared case studies enable stakeholders to identify successful approaches and pinpoint areas for improvement, thus building a foundation for adaptive resilience that evolves with each challenge.

Data sharing and transparency are also fundamental to effective climate collaboration. Establishing common platforms for real-time data exchange allows all parties to make informed decisions, as shared data improves situational awareness and prepares stakeholders to respond to climate-related events with precision and agility.

To stay ahead of evolving climate threats, investing in innovation is crucial. International organizations play a significant role in supporting research and development initiatives focused on resilience-enhancing technologies. By fostering innovation, they help communities build the adaptive capacity necessary to face climate impacts, from developing sustainable infrastructure to advancing predictive climate modeling.

Broader international cooperation on climate initiatives is essential for a truly comprehensive response. Integrating climate considerations into security policies and aligning with sustainable development goals enables organizations to address climate risks in a multifaceted way, considering both immediate and long-term implications.

Finally, monitoring progress is vital to ensure accountability and to facilitate continuous improvement in resilience strategies. Establishing standardized metrics for assessing progress fosters transparency, encouraging a committed approach to resilience and helping organizations adapt their strategies as they gain new insights.

By working together through these collaborative approaches, international organizations and their partners can build a more resilient global community, prepared to face the complex and interconnected challenges posed by a changing climate.

Conclusion

Enhancing climate resilience within NATO and its member states is an urgent challenge that requires a comprehensive and coordinated approach. As climate change increasingly impacts global security, nations must recognize its implications for national stability. Integrating climate considerations into existing security frameworks is critical, although it faces challenges such as policy implementation gaps and coordination difficulties. NATO must monitor the impact of climate change on security and increase situational awareness of emerging threats. To address these challenges, NATO and its allies should adopt a whole-of-government approach that fosters collaboration among military, civilian, and public sectors. Actionable strategies should focus on immediate preparedness, public education, and investment in resilient infrastructure.

Establishing baseline requirements for climate resilience is crucial, supported by regular risk assessments and training programs. NATO's commitment should include securing supply chains, ensuring the resilience of critical infrastructure, and addressing risks associated with emerging technologies. Improved communication and joint exercises will strengthen stakeholder coordination, while public engagement will foster societal support. Collaboration among NATO, member states, and international organizations is vital for pooling resources and sharing expertise. By building partnerships and enhancing collective resilience strategies, nations can better prepare for the challenges posed by climate change.

Ultimately, enhancing climate resilience will bolster national security and contribute to societal well-being. Integrating climate resilience into NATO's strategic framework is both a necessity and an opportunity to enhance collective security. Through collaboration, innovation, and a commitment to resilience, NATO can safeguard its future and that of its member nations against climate-related threats.

Bibliography

1. NATO. (2022). Call for Proposals: “Increasing Societal Resilience: Innovative Ways to Counter Disinformation and Hostile Activities.” Brussels, BE: NATO Headquarters. Retrieved from NATO Headquarters: https://www.nato.int/structur/pdd/2022/220411-ResilienceContentGuidelines.pdf.
2. NATO. (2022). General Terminology: Resilience. NATO Term: The Official NATO Terminology Database. Retrieved from NATO Terminology Database: https://nso.nato.int/natoterm/Web.mvc.
3. NATO. (2022). NATO Standard AJP-01 Allied Joint Doctrine. Edited F Version 1 with UK National Elements. Brussels, BE: NATO Standardization Office.
4. NATO. (2023). July 11th Vilnius Summit Communiqué. Press Release #001. Retrieved from NATO: https://www.nato.int/cps/en/natohq/official_texts_217320.htm.
5. NATO. (2021). Brussels Summit Communiqué. Retrieved from NATO: https://www.nato.int/cps/en/natohq/news_185000.htm?selectedLocale=en.
6. NATO. (2021). Developing a Whole-of-Society, Integrated and Coordinated Approach to Resilience for Allied Democracies. Retrieved from NATO Parliamentary Assembly: https://www.nato-pa.int/document/resolution-466-developing-whole-society-integrated-and-coordinated-approach-resilience.
7. NATO. (2016). Commitment to Enhance Resilience. Retrieved from NATO: https://www.nato.int/cps/en/natohq/official_texts_133180.htm.
8. NATO. (1949). The North Atlantic Treaty Washington D.C. - 4 April 1949. Retrieved from NATO: https://www.nato.int/cps/en/natohq/official_texts_17120.htm.
9. NATO. (2021). Climate Change and Security: Implications for NATO. Retrieved from NATO HQ.
10. NATO. (2022). Increasing Situational Awareness and Early Warning Capabilities Regarding Climate Change. Retrieved from NATO HQ.
11. NATO. (2021). Securing and Diversifying Supply Chains in the Context of Climate Resilience. Retrieved from NATO HQ.
12. United Nations. (2015). Paris Agreement. Retrieved from UNFCCC: https://unfccc.int/sites/default/files/english_paris_agreement.pdf.
13. Intergovernmental Panel on Climate Change (IPCC). (2021). Climate Change 2021: The Physical Science Basis. Contribution of Working Group I to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change. Cambridge University Press. Retrieved from IPCC: https://www.ipcc.ch/report/ar6/wg1/.
14. World Bank. (2016). Climate and Disaster Resilience: The Role of the Private Sector. Retrieved from World Bank: https://www.worldbank.org/en/topic/climatechange/publication/climate-and-disaster-resilience-the-role-of-the-private-sector.
15. European Commission. (2020). European Green Deal. Retrieved from European Commission: https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal_en.
16. National Oceanic and Atmospheric Administration (NOAA). (2020). Climate Resilience Toolkit. Retrieved from NOAA: https://toolkit.climate.gov/.
17. United Nations Office for Disaster Risk Reduction (UNDRR). (2019). Global Assessment Report on Disaster Risk Reduction. Retrieved from UNDRR: https://www.undrr.org/publication/global-assessment-report-disaster-risk-reduction-2019.
18. National Institute of Building Sciences. (2019). Natural Hazard Mitigation Saves: 2019 Report. Retrieved from NIBS: https://www.nibs.org/page/mitigationsaves.
19. World Economic Forum (WEF). (2021). Global Risks Report 2021. Retrieved from WEF: https://www.weforum.org/reports/the-global-risks-report-2021.

ADAPTING TO ENVIRONMENTAL THREATS: NATO'S STRATEGIC FRAMEWORK FOR CLIMATE RESILIENCE AND SECURITY

Orlin NIKOLOV, PhD
Ralitsa BAKALOVA

Abstract: This article examines strategic adaptations to the growing security challenges posed by climate change. As climate disruptions impact military operations, infrastructure, and regional stability, defense organizations are intensifying efforts toward climate resilience. This includes integrating advanced technologies like AI, predictive modeling, and environmental monitoring to enhance preparedness against both natural and engineered threats. Additionally, the article addresses risks related to environmental manipulation, such as geoengineering and cyber vulnerabilities in monitoring systems. This comprehensive approach reflects a commitment to safeguarding global stability and security in an increasingly climate-impacted world.

Introduction

The rising threats associated with climate change are reshaping the defense strategies of international organizations, with NATO at the forefront of adapting its policies to counter these environmental challenges. Climate change affects not only ecological balance but also international security, making the resilience of military operations, infrastructure, and regional stability increasingly critical. This article explores NATO's strategic approach to climate security, examining how the Alliance integrates advanced technologies like AI, predictive modeling, and environmental monitoring to enhance preparedness for both natural and engineered disruptions.

Additionally, it addresses NATO's efforts to fortify environmental monitoring systems against cyber threats, tackle the implications of geoengineering, and uphold environmental governance in the face of rapid climate shifts. Through comprehensive policies and forward-thinking initiatives, NATO aims to maintain global stability and security in an increasingly unpredictable climate landscape.

The Strategic Impact of Climate Change on NATO

Climate change is increasingly recognized as a significant threat multiplier that exacerbates existing security challenges faced by NATO. As the global climate continues to change, the implications for international peace and security are profound, necessitating a comprehensive reassessment of NATO's strategic posture and operational capabilities.

One of the most pressing concerns is the impact of climate change on military operations. Armed forces are likely to encounter extreme weather conditions more frequently, which can hinder operational effectiveness and readiness. This reality demands that NATO adapt its training, equipment, and operational planning to ensure that its forces can operate effectively in diverse and challenging environments. The ability to respond to climate-induced challenges is essential for maintaining NATO's operational integrity and effectiveness.

Moreover, NATO's military infrastructure is increasingly vulnerable to climate-related impacts. Critical installations, including bases and logistical networks, face risks from flooding, extreme temperatures, and severe weather events. To safeguard its military capabilities, NATO must assess and enhance the resilience of its infrastructure, ensuring that it can withstand these challenges and remain operational under adverse conditions.

The intersection of climate change and resource scarcity presents another layer of complexity for NATO. As climate change affects the availability of essential resources, such as water and food, the potential for conflict may increase both within and between nations. NATO must be prepared to respond to these emerging security threats, which could manifest as humanitarian crises or increased migration pressures resulting from environmental changes.

In response to these challenges, NATO has developed a range of adaptation strategies. These strategies include conducting comprehensive assessments of climate change impacts on the Alliance's strategic environment and military capabilities. By integrating climate change considerations into military planning and operations, NATO can enhance its preparedness for the multifaceted challenges posed by a changing climate. Additionally, enhancing training and education programs will equip personnel with the knowledge and skills necessary to navigate climate-related challenges effectively.

Collaboration with partner nations and international organizations is also crucial in addressing climate-related security challenges. By sharing knowledge and best practices, NATO can enhance its collective response to the impacts of climate change on security. This collaborative approach not only strengthens NATO's capabilities but also fosters a sense of shared responsibility among member states and partners.

NATO is committed to sustainability and reducing its greenhouse gas emissions. The Alliance recognizes the importance of transitioning to more sustainable practices within its operations, including exploring renewable energy sources and improving energy efficiency. By minimizing the environmental impact of military activities, NATO can contribute to broader efforts to combat climate change while enhancing its operational effectiveness.

The strategic impact of climate change requires NATO to engage in long-term planning and foresight. Anticipating future challenges and developing proactive strategies to mitigate risks associated with climate change is essential for ensuring that the Alliance remains prepared for a rapidly changing security environment. By integrating climate considerations into its strategic planning, NATO can safeguard the security of its member states in an increasingly uncertain world.

The Consequences of Global Warming and Human-Induced Aerosols on the Atmosphere

Climate change, driven primarily by human activities, has led to significant alterations in the Earth's climate system. These changes include the increase in greenhouse gases, deforestation, and the widespread use of fossil fuels. One of the most profound impacts of human-induced climate change is global warming, which has triggered a cascade of environmental effects that are felt across the globe.

Global warming, resulting from the accumulation of greenhouse gases like carbon dioxide and methane in the atmosphere, has led to a significant rise in global temperatures. This warming has numerous consequences, including the melting of polar ice caps, rising sea levels, and the increased frequency of extreme weather events. These changes not only disrupt ecosystems but also pose direct threats to human infrastructure and livelihoods, particularly in vulnerable regions.

In addition to greenhouse gases, human-induced aerosols play a significant role in climate change. Aerosols are tiny particles or droplets suspended in the atmosphere,

which can have both cooling and warming effects depending on their type. The presence of these aerosols in the atmosphere affects cloud formation and precipitation patterns, leading to further disruptions in weather and climate systems.

These atmospheric changes have far-reaching impacts on global weather patterns, making the environment more unpredictable and leading to conditions that can be exploited as weapons in geopolitical conflicts. The manipulation of weather through techniques such as cloud seeding or other more advanced geoengineering methods has raised concerns about the potential for weather to be weaponized. This possibility represents a new frontier in the nexus between climate change and security, with significant implications for international stability and the strategic operations of military alliances like NATO.

Weather as a Weapon: The Emerging Threat

The concept of using weather as a weapon has moved from science fiction to a real strategic concern. Advances in geoengineering and environmental modification technologies have raised the specter of weather being weaponized to achieve military objectives. The potential for more sophisticated weather manipulation techniques poses a significant threat to NATO's operations. Adversaries could theoretically induce droughts, floods, or other extreme weather events to disrupt NATO missions, damage infrastructure, or create unfavorable conditions for military engagements. Such actions could have severe and long-lasting impacts on civilian populations, agriculture, and ecosystems, further destabilizing regions of strategic importance to NATO.

The intersection of cyber threats and climate change also presents a complex security challenge. Cyberattacks on environmental monitoring systems could manipulate weather data, hindering NATO’s ability to forecast and respond to extreme weather events effectively. This adds another layer of complexity to the threat of weaponized weather, requiring NATO to enhance its cyber defenses alongside its climate resilience strategies.

Implications for NATO's Resilience and Preparedness

The potential weaponization of weather requires NATO to reevaluate and strengthen its resilience strategies. This includes enhancing its ability to monitor and respond to

environmental changes that may indicate hostile weather modification. To achieve this, NATO must develop advanced detection systems and incorporate climate risk assessments into its strategic planning and operational frameworks.

Additionally, NATO's preparedness must extend to the adaptation of military infrastructure and equipment to withstand the increasing frequency and intensity of extreme weather conditions. The NATO Greenhouse Gas (GHG) Emissions Mapping and Analytical Methodology emphasizes the importance of energy efficiency and emissions reduction, both of which are crucial for maintaining operational effectiveness while mitigating the environmental impact of military activities. This approach not only supports the sustainability of NATO's missions but also ensures that they are capable of operating in increasingly volatile climates.

Moreover, building climate resilience is essential to ensure NATO forces can function effectively under changing climate conditions. This involves fortifying military infrastructure, especially in vulnerable regions like coastal areas, and improving the Alliance's ability to respond to climate-induced disasters. NATO's strategic foresight must now account for the possibility of weather manipulation being used as a weapon, demanding a comprehensive approach to resilience that encompasses political, institutional, and operational dimensions.

Research by the RAND Corporation highlights the pressing need to integrate climate resilience into NATO's strategic frameworks. RAND specifically advocates for joint military exercises simulating extreme weather scenarios as a crucial method for enhancing interoperability and strengthening NATO's capacity to respond to diverse climate-related threats. Similarly, the NATO 2022 Strategic Concept underscores the importance of incorporating climate adaptation into defense planning, stressing the necessity of climate-focused drills to maintain operational readiness. Reports from the NATO Parliamentary Assembly further support this approach, calling for comprehensive, simulation-based training to better equip NATO forces for climate-induced crises. Collectively, these studies emphasize that robust climate resilience planning is vital for ensuring NATO's long-term strategic preparedness and adaptability in the face of emerging climate-related challenges.

NATO's Position on Geoengineering and Ecocide

Geoengineering, which involves large-scale technological interventions aimed at counteracting the effects of climate change, presents both opportunities and significant security concerns for NATO. While these technologies could potentially mitigate some aspects of global warming, they also pose serious risks, including unintended ecological consequences, the escalation of geopolitical tensions, and the misuse of such technologies for military purposes. NATO emphasizes the need for rigorous international oversight and governance to manage the deployment of geoengineering technologies and advocates for comprehensive risk assessments to prevent these technologies from being weaponized.

Ecocide, defined as the intentional destruction of the natural environment, has also emerged as a significant security concern for NATO. The Alliance views ecocide not only as an environmental issue but as a serious threat to global stability. The deliberate targeting of ecosystems, whether in conflict zones or as a form of climate terrorism, can lead to humanitarian crises, economic disruption, and long-term destabilization of regions. NATO's strategy to address ecocide involves advocating for stronger international legal frameworks that define and penalize such acts, while promoting the integration of environmental protection into military operations.

NATO’s involvement in supporting the establishment of legal frameworks on environmental crimes, including ecocide, demonstrates its commitment to addressing environmental destruction as a serious security issue.

Weather Manipulation: A Revolutionary Approach. Cloud Seeding and Nanotechnology in Weather Control

Geoengineering technologies, such as Solar Radiation Management (SRM) and Stratospheric Aerosol Injection (SAI), offer potential solutions to address climate change but carry significant risks, especially with regard to military misuse and geopolitical instability. These methods are designed to modify the climate for environmental purposes, but they also present opportunities for strategic military advantages.

Cloud seeding, for example, involves dispersing substances like silver iodide or sodium chloride into clouds to stimulate precipitation. While this technique has been implemented to combat water shortages in regions such as India, Mexico, and China,

the results have been inconsistent, and the long-term ecological effects remain uncertain. Adjusting precipitation in one region could lead to water scarcity in neighboring areas, potentially leading to geopolitical tensions over shared water resources.

Cloud seeding is one of the most researched weather modification techniques. By dispersing substances into clouds, cloud seeding stimulates precipitation. However, the effectiveness of this technique remains debated, with mixed results in regions such as Mexico, where rainfall increases could not be definitively linked to human intervention. Furthermore, the long-term ecological effects of cloud seeding raise concerns, especially as altering precipitation patterns in one region may reduce water availability in others, creating the potential for geopolitical conflicts over shared resources.

Nanotechnology, the manipulation of matter at the molecular or atomic level, could revolutionize weather control, promising strategic advantages for military applications by 2030. Through precise manipulation of atmospheric conditions, forces could gain capabilities to disrupt enemy surveillance and defend against directed energy weapons (DEWs). Central to these innovations are nano-enabled balloons with diamond-coated skins, designed to create localized microclimates by reflecting or absorbing solar radiation. These balloons, equipped with nano-scale solar cells, generate high-pressure zones, which influence weather patterns by controlling air movement. Their potential for generating artificial clouds or fog could prove useful in obscuring military assets or disrupting enemy sensors. By releasing nano-aerosols, nanotechnology enables controlled cloud formation, while electrolysis of water molecules enhances atmospheric humidity, further aiding cloud development. Real-time control of these conditions relies on advanced 4D-Var atmospheric modeling, updated continuously by nanometer-scale sensors embedded in the balloons. Operated in autonomous swarms, these devices utilize AI and machine learning to make precise, real-time adjustments. In addition to weather modification, nanotechnology offers a defense mechanism against DEWs: artificial clouds scatter and absorb energy from high-energy lasers (HELs) and high-power microwaves (HPMs), providing a protective shield. Looking forward, advances in self-organizing nanomaterials and intelligent sensor networks could allow the creation of entirely new weather systems, as demonstrated by NASA's Autonomous Nanotechnology Swarms (ANTS) program. However, these capabilities raise ethical and environmental

concerns, especially with potential impacts on regional climates. The Environmental Modification Convention (ENMOD) prohibits the hostile use of environmental modifications, emphasizing the need for regulations to ensure responsible application. Challenges in energy efficiency and computational power requirements remain, highlighting the need for advancements in solar-powered nano-cells, PEM batteries, and quantum computing to achieve real-time control. In summary, while nanotechnology holds immense potential to reshape weather control and defense, its development requires careful consideration of ethical, environmental, and regulatory frameworks.

Advancements in AI and Weather Modification

In recent years, Artificial Intelligence (AI) has become an essential tool in advancing weather modification efforts. AI is primarily used in predictive modeling, pattern recognition, and data analysis to improve the accuracy and efficiency of weather interventions such as cloud seeding. AI systems can process vast datasets from satellites, weather stations, and radar systems to provide better real-time predictions and to simulate the effects of weather modification interventions.

Machine learning (ML) models, a subset of AI, have been particularly useful in refining the effectiveness of cloud seeding by helping to determine the most opportune conditions for successful precipitation. Through AI-driven simulations, scientists can forecast the impact of cloud seeding, accounting for complex factors like cloud dynamics, atmospheric conditions, and regional weather patterns. This ability to model outcomes in real-time enhances decision-making and reduces the risks associated with large-scale weather modification projects.

AI is also crucial in monitoring unintended consequences of weather modification, such as downwind effects of altering precipitation in one region. By analyzing changes in atmospheric moisture content and jet stream patterns, AI can predict how interventions like SRM and SAI could shift weather patterns on a global scale. These advancements allow military and civilian entities to better understand the security risks associated with geoengineering and to anticipate geopolitical impacts.

In a military context, AI-powered simulations are critical for NATO's ability to prepare for potential geoengineering-driven disruptions. The use of AI to monitor and protect

against adversarial weather manipulation also forms a key aspect of NATO's cybersecurity initiatives, which aim to protect environmental monitoring systems from cyberattacks that could manipulate weather data, leading to further security challenges.

Cybersecurity and Climate Intelligence

Securing environmental monitoring systems from cyber threats is increasingly essential for maintaining situational awareness and readiness. Cyberattacks on these systems can distort climate and weather data, leading to inaccurate forecasts that may undermine both military and civilian responses to natural and artificial climate events. In a defense context, compromised data could result in operational setbacks, such as misinformed troop deployments or disrupted strategic planning, highlighting the need for robust cybersecurity measures.

As a countermeasure, cybersecurity frameworks prioritize safeguarding environmental monitoring data, ensuring adversaries cannot exploit these systems to weaken military infrastructure or disrupt civilian resilience efforts. Advanced defenses incorporate encryption and continuous monitoring to detect and neutralize threats before they impact data integrity.

To enhance predictive security, these systems integrate with numerical weather prediction (NWP) models, augmented by artificial intelligence (AI) and machine learning (ML). This combination not only secures environmental monitoring but also offers resilience against climate-based threats by predicting impacts of interventions like geoengineering or cloud seeding, which could affect regional climates. In an era where both cyber and environmental threats are intertwined, these technologies are essential for creating real-time, secure responses.

The evolving field of climate intelligence further strengthens security by consolidating large datasets from satellites, sensors, and historical climate records. This capability, which has been described as "business intelligence for climate," enables precise, location-specific insights that are critical for risk management in defense, energy, and infrastructure. By anticipating climate-induced disruptions, these tools support informed decision-making and preemptive responses, ensuring that both cyber and

environmental threats are contained effectively. This proactive stance helps fortify national security in an age of complex, climate-related challenges.

International Legal Frameworks on Geoengineering and Ecocide

Despite technological advances in geoengineering, the legal frameworks governing these practices remain limited. The 1976 Environmental Modification Convention (ENMOD) prohibits the military use of weather modification techniques, but it does not adequately cover non-military or dual-use applications of geoengineering, leaving significant gaps in governance.

Additionally, the United Nations Convention on Biological Diversity (CBD) introduced a moratorium on large-scale geoengineering projects in 2010, though this is non-binding and does not regulate small-scale or experimental projects.

The concept of ecocide—the large-scale destruction of ecosystems—has gained traction as an emerging legal discourse. Environmental activists and scholars have pushed for ecocide to be recognized as an international crime under the jurisdiction of the International Criminal Court (ICC).

NATO's Strategic Approach to Geoengineering and Environmental Threats

NATO's position on geoengineering and ecocide reflects its proactive stance on climate and environmental security as integral to global stability. NATO views geoengineering—deliberate large-scale interventions in Earth's climate—as a potential factor in the security landscape, particularly as climate change accelerates environmental pressures that could destabilize regions.

However, while geoengineering may offer mitigation possibilities, it carries significant risks and uncertainties, especially around governance, unintended ecological impacts, and possible misuse by state or non-state actors. Consequently, NATO's approach includes strategic monitoring of these activities to understand their security implications and prepare for potential challenges they may introduce.

NATO's Allied Command Transformation emphasizes the threat multiplier effect of climate change and biodiversity loss. Unchecked environmental degradation, including possible ecocide (the large-scale destruction of ecosystems), could drive

regional conflicts, resource scarcity, and displace populations, exacerbating existing geopolitical tensions. NATO is working to integrate environmental resilience into military strategies, equipping forces to operate in climate-altered environments while enhancing safeguards against any actions that may weaponized environmental degradation as a tool for coercion.

Overall, NATO's Climate Change and Security Action Plan and related assessments promote a comprehensive approach to environmental security, from monitoring potential geoengineering activities to fostering climate resilience across Allied infrastructure. This approach is part of a broader commitment to addressing the complexities of modern environmental threats, including ecocide, within the framework of international security cooperation.

Conclusion

In conclusion, NATO's evolving strategy reflects its commitment to addressing climate change as a central component of global security. By integrating climate resilience into its operational frameworks and advancing capabilities through AI-driven predictive models, NATO is proactively enhancing its preparedness for climate-induced disruptions. The Alliance's focus on securing environmental monitoring systems, managing the risks associated with geoengineering, and adhering to international environmental governance illustrates a comprehensive approach to managing climate threats. This strategic response not only safeguards NATO's operational readiness but also underscores its leadership in promoting global stability in a world where climate and security are increasingly intertwined. As climate impacts continue to influence global dynamics, NATO's actions set a crucial precedent for the role of defense organizations in adapting to and mitigating environmental risks.

Bibliography:

1. Arctic Climate Change Assessment and Implications for NATO Operations (2023). NATO Headquarters.
2. Arctic Council. (2021). Arctic Climate Impact Assessment: Key Findings. Retrieved from Arctic Council Secretariat.
3. Bakalova, R., & Bosilkov, R. (2019). Human-Induced Climate Change and Real Consequences. In Climate Change and Security.
4. Boger, M. C. (2009). Operational Defenses through Weather Control in 2030. Air University, Maxwell Air Force Base.
5. Environmental Modification Convention (ENMOD). (1977). United Nations.
6. European Environment Agency. (2020). Climate Change, Impacts and Vulnerability in Europe 2020. EEA Report No 1/2020. Retrieved from https://www.eea.europa.eu/publications/climate-change-impacts-and-vulnerability-2020.
7. Garstang, M., et al. (2004). Weather Modification: Finding Common Ground. Bulletin of the American Meteorological Society, 86(5), 647-655.
8. Hall, J. S. (2005). Nanofuture: What's Next for Nanotechnology. Prometheus Books.
9. Hoffman, R. N. (2004). Controlling the Global Weather. NASA Institute for Advanced Concepts (NIAC).
10. International Criminal Court. (2021). Policy Paper on Environmental Crimes. Retrieved from https://www.icc-cpi.int/itemsdocuments/2021-policy-paper-on-environmental-crimes.
11. Lanicci, J. (2015). Weather Operations and Military Planning: A Historical and Strategic Perspective.
12. NASA Goddard Space Flight Center. (2009). Autonomous Nanotechnology Swarms (ANTS).
13. National Research Council. (2003). Critical Issues in Weather Modification Research. The National Academies Press.
14. Nature Climate Change. (2021). Global Consequences of Aerosol-Driven Climate Change. Nature Climate Change, 11, 334-343. Retrieved from https://www.nature.com/nclimate/.
15. NATO. (2022). Strategic Concept 2022. NATO Headquarters.
16. NATO. (2023). Environmental Modification Techniques and NATO Policy. NATO Headquarters.
17. NATO. (2023). Greenhouse Gas (GHG) Emissions Mapping and Analytical Methodology. NATO Headquarters.
18. NATO. (2024). Advanced Detection Systems for Weather Modification. NATO Headquarters.
19. NATO. (2024). Climate Change and Security Impact Assessment. NATO Headquarters.
20. NATO. (2024). Cybersecurity and Climate Risks: NATO's Integrated Approach. NATO Headquarters.
21. NATO. (2024). NATO's Leadership in Climate Security. NATO Headquarters.
22. NATO. (2024). Strategic Foresight Analysis. NATO Headquarters.
23. Palazzo, M. (2017). Climate Change and National Security: Understanding the Role of Weather in Military Operations.
24. RAND Corporation. (2022). Building Climate Resilience in NATO Forces: Strategic Priorities for Adaptation. Retrieved from https://www.rand.org/pubs/research_reports/RR2022.html.
25. Thill, M. J. (2008). Penetrating the Ion Curtain: Implications of Directed Energy Integrated Air Defense Systems in 2030. Air University.
26. World Meteorological Organization. (2023). Weather, Climate, and Cybersecurity: Emerging Risks in the 21st Century. WMO Bulletin. Retrieved from https://public.wmo.int/en/bulletin/weather-climate-and-cybersecurity.

LEVERAGING LESSONS LEARNED THROUGH THE INTEGRATION AND CONTINUOUS IMPROVEMENT OF BCM IN NATO-WIDE SETTING

Dobromir KODZHEYKOV
Ralitsa BAKALOVA

Abstract: While the BC Policy opens the gate for LL Capability employment in BCM, it is only through analysis of the PDCA cycle and the LL process itself, that the practical use and value of the capability in this context becomes evident. As noted in AJP-3 "LL describe more than just learning from experience, learning must be used to justify changes that will lead to improved performance. The purpose of LL procedures is to learn efficiently from experience and to provide validated justifications for amending the existing way of doing things, to improve performance". In the review of the PDCA cycle, it is highlighted that the principle of continuous improvement is initially set-up during the "Plan" phase, and later produces changes and potential improvements during the "Act" phase, however the LL process is ongoing during the two interim phases "Do" and "Check", to identify areas which meet or exceed expectations and ones that are not up to par. Therefore, Lessons Learned act as a trigger for the continuous improvement of the BCMS per se.

Introduction

Defined by the International Organization for Standardization as the "capability of an organization to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption" , business continuity (BC) has long been not only a matter of survival, but also a source of competitive advantage and resilience in a dynamic and uncertain environment. A multitude of organizations around the world regardless of their size or field of operations, have been utilizing this approach to tackle the uncertainties of the ever-changing world, protecting their operational capabilities, core outputs and stakeholder interests. Business continuity management (BCM), on the other hand, is a holistic management process that identifies potential threats to an organization and the impacts to business operations

that those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response.

For most corporate entities, the critical processes to be protected might be the delivery of a specific service or a product, where an interruption might occur following an incident, causing potential financial and reputational damages, but a swift recovery may even result in a bounce-back and unexpected opportunities. What if, however, an organization's mission and output are the security and physical protection of millions of people? What if an interruption to its activities is unacceptable to begin with?

As the "most successful Alliance in history" NATO's purpose for the past 75 years has been to guarantee the freedom and security of its members through political and militarySo means. However, as big, and powerful as it might be, the Alliance is not immune to threats and hazards that could potentially degrade its ability to deliver its core tasks. Disruptions of different scales and types have affected and will continue to affect NATO in the future. By adopting a NATO-wide Business Continuity Policy in 2020, the North Atlantic Council recognized that: "Under no circumstances, can the Alliance be unable to execute its essential mission, nor can it afford loss of reputation by failing to ensure continuity of its critical outputs." The core tasks of the alliance being: to deter and defend against the full range of threats, to respond to and manage crises beyond NATO territory, and to enhance international security through cooperation, it becomes evident, that any interruptions or disruptions in delivery, defeat the purpose of the Alliance itself. Considering that, the vision NATO Business Continuity Policy sets a clear path ahead of integrating an enterprise BCM framework: 'NATO continues its essential mission under all circumstances and becomes increasingly resilient to disruptions through continuous improvement'

In 2019 the NATO Business Continuity office was established, with the task of developing a sound and effective BCM framework for NATO at the enterprise level. The foundation of this framework was laid with the Policy mentioned above in 2020, however, in order to provide coherent guidance to the various NATO bodies' business continuity management activities additional Guidelines and A&C Framework (as well as other tools) have been drafted since. The approach chosen for the drafting of the Policy and the surrounding framework is rather unique, as it is built upon already existing, widely recognized in the corporate world standards and practices, such as ISO 22301 and ISO 22313 , adapting the NATO setting to the fullest, covering all of

the preset requirements, despite the nature of its unconventional output. For example, the NATO Business Continuity Guidelines states that “any reference to the term “business” is intended to be interpreted broadly to mean those activities that are core to the purposes of an organization's existence. For NATO, this encompasses all of the Alliance’s operations, missions and activities conducted under the provisions of the Washington Treaty.”

Sticking to an already well-established standard in the field, when drafting an entirely new policy is indeed a sensible solution, (especially when we consider the fact that most NATO members are a part of CEN) however it is also indicative of the fact that NATO recognizes the value it could acquire by delving deep into the practical experience of the private sector. That is not to say that the whole topic is brand new for the Alliance, of course, emergency response and contingency plans would be vital to any military entity, however BCM as a holistic managerial approach has a long history of development and improvement in the corporate sector, and has been utilized by public entitles for the past decade or two. By building upon the experience, lessons, and good practices already embedded in ISO 22301, the Policy manages to use a readily available template of sorts, filling it up with NATO aims and requirements, but most notably – principles. What sets the Alliance apart from the private sector, when utilizing same standards and practices, is the fact that the drive for constant change and improvement is engraved in the DNA of the organization itself as adaptation is a cornerstone for security.

In its effort to avoid “reinventing the wheel” NATO’s BCM Policy integrates a “System of systems” approach, in which each NATO Body develops a BCM System to meet its own individual needs. The system on Enterprise level is based upon the Business Continuity Management System requirements set in ISO 22301 and ISO 22313. A Business Continuity Management System (BCMS) is defined as ‘part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity. ISO Standards describe the functioning of a BCMS using the Plan-Do-Check-Act (PDCA) cycle, also known as the Deming cycle, which is a methodology for continuous improvement of processes. To develop an effective BCMS, the PDCA cycle outlines the requirements, allocates resources, and sets the conditions necessary for its continuous improvement and operational effectiveness.

BCMS Lifecycle in accordance to ISO 22301

The "Plan" phase lays the foundation for robust business continuity processes. It begins with the establishment of a Business Continuity policy and the setting of specific objectives for the organization. This phase involves identifying the necessary resources and setting up the continuous improvement processes. Such resources might be the role of management in terms of demonstrating commitment, defining policy, and establishing roles, responsibilities, and authorities. Key activities include conducting a Business Impact Analysis (BIA) and Risk Assessment to understand potential threats and their impacts on critical business operations. Additionally, it focuses on the context of the organization, as it sets out what the organisation should do in order to make sure that the BCMS meets its requirements, taking into account all relevant external and internal factors, including: the needs and expectations of interested parties; its legal and regulatory obligations; the required scope of the BCMS.

The "Do" phase consists of four critical steps: Analyse, Design, Implement, and Validate. During the Analyse step, critical business functions and the potential impact of disruptions are identified through a detailed assessment of risks and vulnerabilities. The Design step involves developing strategies and solutions to mitigate identified risks, including the creation of continuity and recovery plans tailored to the organization’s needs. The Implement step focuses on executing these strategies and solutions by putting in place the necessary procedures, resources, and training to ensure preparedness. In the Validate step, the plans are tested and exercised to ensure their effectiveness and reliability during an actual disruption. Roles and responsibilities for executing business continuity solutions are clearly defined in this phase, ensuring that everyone knows their part in maintaining continuity according to the established plans and procedures.

The "Check" phase involves a performance evaluation against the policies and objectives set during the "Plan" phase and the outcomes of the "Do" phase. This performance review includes regular monitoring and measurement of BCMS activities to ensure they meet the intended goals (set by the Policy). The results of these evaluations are reported to management, who then authorize any necessary remediation and improvement measures.

In the "Act" phase, the corrective actions necessary, that have been identified during the "Check" phase are implemented. This phase allows for revisions to the scope, and objectives of the BCMS as necessary, ensuring that the BCMS remains relevant and effective while adapting to changes in the organization and its environment. Continuous improvement is a key aspect of this phase, ensuring that the BCMS evolves and improves over time.

Going back to the System of systems approach, it is important to point out, that every NATO entity (described above) shall create and follow a BCMS which fits its needs. In order for these systems to operate holistically, they shall be based on common requirements; they shall be coordinated between relevant NATO Bodies, and a top-level governance structure shall provide oversight, coherence, and direction. What is more, during the development of such BCMS, NATO bodies shall support each other by leveraging interdependencies, optimising collective resources, ensuring complementary Business Continuity strategies, and by sharing best practices and lessons identified/learned.

Among others, two core principles stand out after a review of the PDCA system prescribed by ISO 22301/ 22313 and NATO's strategic documents, such as the BC Policy or the Allied Joint Doctrine. The first one revolves around the fact that the context in which the Alliance operates is constantly evolving, and so should NATO, through its capabilities, strategy and plans in order to adapt and meet the challenge of enduring strategic competition. Commitment to continuous improvement is a core principle in building and operating a robust BCMS, but it is also a core principle to the Alliance, which should potentially ease the integration of BCMS in all its entities. In the sense of this principle, it should be consistently emphasized throughout the organization that Business Continuity is a living process that is continuously improved and adjusted. For instance, as lessons are learned through responses and exercises, or a change occurs in the risk environment, the BCMS should react and adapt. In addition, periodic evaluations are beneficial to program management, and stakeholders because it confirms where the program is working correctly and where improvements are required. Information compiled from an evaluation can be used to assess the system performance and aids in setting priorities for improvements. The "Plan" phase of the PDCA cycle, establishes all elements required to operate solid Business Continuity processes. It starts with the establishment of a Business

Continuity policy and objectives for the organisation. Continuous improvement processes are established in this phase. The BC Guidelines drafted by NATO BCO note that a 'Business Continuity mind-set' shall be adopted by all, at all levels, all the time. Business Continuity should be embedded in all processes across the organisation and should become part of NATO's organisational culture. In line with that, Continuous Improvement Requirements placed in the BC Policy, stating that:" Each NATO body shall continually improve the effectiveness of its BCM System. Continuous improvement operates at all levels and shall be driven by the NATO Business Continuity Policy, audit results, analysis of monitored events, corrective actions, and management review. Shortfalls and risks to BCM shall be identified and reported to the top leadership of the respective NATO Body."

NATO LL (Lessons Learned) Process implications on constant improvement of BC

The second most prominent principle laid in the BC Policy is inevitably connected with continuous improvement, being the main tool to achieve it, and a whole new capability on its own – identifying and learning lessons from experience. Not once, was it already pointed out, that each NATO entity shall establish mechanisms for continuous improvement utilizing the already well-established Lessons Learned (LL) process. The term lesson learned (LL) is broadly used to describe people, things, and activities related to the act of learning from experience to achieve improvements. The experience may be positive, as in completing a successful task or procedure, or negative, as in mission failure. A lesson must be significant in that it has a real or assumed impact on operations; valid in that it is factually and technically correct; and applicable in that it identifies a specific design, process, or decision that reduces or eliminates the potential for failures or reinforces a positive result. Frequently, lessons highlight strengths or weaknesses in preparation, design, and implementation that affect performance, outcome, and impact. Using lessons learned, either through academic work or experience in practice, in order to mitigate potential negative impacts to core outputs and processes in the future, is the embodiment of the concept for BCM in an organization. As already mentioned, NATO has a well-established LL capability, described in the Allied Joint Doctrine for the Conduct of Operations (AJP-

03) , which should be used to optimize and assist the BCM integration process by sharing lessons and good practices across different bodies, developing their own BCMS. The BCO at NATO HQ is in charge of maintaining a Business Continuity Community of Interest (classified and unclassified levels) to enhance collaboration and promote the sharing of best practices and lessons learned using the NATO Lessons Learned process , meaning it is the primary tool for exchange of observations and information between different NATO entities.

The idea of LL in an organization is that, through a formal approach to learning, individuals and the organization can reduce the risk of repeating mistakes and increase the chance that successes are recurring. When the LL process is put in the context of business continuity being the ability of an organization to maintain or resume its essential functions and operations in the face of a disruptive event, such as a natural disaster, a cyberattack, or a pandemic, it becomes evident, that LL is vital in planning, preparing, and implementing strategies and procedures that can ensure the continuity of critical business processes and minimize the impact of disruptions on the organization. While the BC Policy opens the gate for LL Capability employment in BCM, it is only through analysis of the PDCA cycle and the LL process itself, that the practical use and value of the capability in this context becomes evident. As noted in AJP-3 “LL describe more than just learning from experience, learning must be used to justify changes that will lead to improved performance. The purpose of LL procedures is to learn efficiently from experience and to provide validated justifications for amending the existing way of doing things, to improve performance “ . In the review of the PDCA cycle, it was highlighted that the principle of continuous improvement is initially set-up during the ”Plan” phase, and later produces changes and potential improvements during the “Act“ phase, however the LL process is ongoing during the two interim phases ”Do” and ”Check”, to identify areas which meet or exceed expectations and ones that are not up to par. Therefore, Lessons Learned act as a trigger for the continuous improvement of the BCMS per se.

NATO’s LL process, described in Annex E of AJP-3 goes through several stages, starting with analysis, through gathering observations. An individual within NATO makes an observation: "a comment based on something someone has heard, seen or noticed that has been identified and documented as an issue for improvement or a potential best practice." Everyone within an organization needs to be involved in a LL

process for it to be successful. The observer, supported by lessons learned staff officers and subject matter experts within the chain of command, then analyses the observation to identify its root cause. During this analysis, the observer (with additional support) is to identify a remedial action, addressing the root cause and potentially correcting the problem, or sustain success. A remedial action is an activity or set of activities that corrects an issue identified for improvement or facilitates the implementation of a best practice. Additionally, the person or organization which should execute the remedial action will be identified during the analysis step. The output of the analysis is a lesson identified (LI). After a lesson has been identified, the remedial action goes through several consecutive phases of endorsement, implementation, monitoring, and validation, to become a lesson learned. Verification may involve further work and analysis, using exercises or experiments. Dissemination of the LL enables all parties to put the improvement into practice.

The “Do” phase of the larger BCMS lifecycle, is often described as the process of business continuity management, which essentially builds BC solutions (whether that be BC or contingency plans). Therefore, BCMS creates BCM that develops solutions, but as BCMS is constantly evolving, so is the inner BCM cycle and the produced solutions. When the LL process is compared to the "Analyse-Design-Implement-Validate" steps formulating the “Do” phase of the PDCA cycle described above, the structure suggests that lessons could be identified at the “Validate” stage, as this is the stage in which every BC solution is tested to ensure effective response to disruptions. Testing a solution will verify its function and suitability. Every solution can be validated individually through a local test or small-scale exercise. Several solutions can be tested together through a large-scale exercise. The lessons identified as a result of the validation phase, and the remedial actions suggested, are what triggers the revolution of the cycle into the initial stages of analysis and design, where lessons identified should result in tangible changes and be revalidated, to become LL. Through validation, supported by LL in the process, solutions gain strength and become more resilient. Building upon that notion, the BCO at NATO HQ has laid out the idea of ”being ready to fail fast, learning faster, and remaining open to new solutions” in its BC Guidelines. The ”fail fast, learn fast” approach utilizes the idea of the constantly revolving cycle, which refines solutions in an effective way, based simply on the speed and number of revolutions. In practice, that means that even an unsatisfactory solution

is a good starting point, as it will tumble in the cycle of revalidation and redesign, eventually getting polished by lessons learned throughout the process. ISO 22301 clearly describes that same process, by adopting the requirement for all organizations to implement and maintain a programme for testing and revalidation of the business continuity solutions. Although LL capability is not explicably mentioned," formalized post-exercise reports that contain outcomes, recommendations and actions to implement improvements" shall be the outcome of test and exercises in the organization. Additionally, the organizations are to act on the result of the tests, implementing remedial actions.

After a brief review of the LL process in NATO and its implications on refining business continuity solutions, the same could be done for the wider BCMS cycle, subjecting the developed solutions to a check against the initial strategic objectives. The "Check" phase deals with the performance review, and it summarises requirements necessary to measure business continuity performance and BCMS compliance both with ISO 22301 and the overall strategic vision set in the "Plan" stage, in the case of NATO, being described by the BC Policy. Same principles as the ones described above apply to this consecutive round of validation, however in this case, the overall results from previous stages are evaluated against the initial expectations and requirements, meaning that the lessons identified eventually feed in the "Act" stage, to trigger positive changes on a system level. While the assessment described in the previous cycle is done through test and exercises, the strategic level review of the BCMS calls for performance evaluation done through monitoring, analysis, and audits. Each NATO body shall periodically conduct audits to obtain reasonable assurance that its BCM System conforms to the NATO Business Continuity Policy. Heads of NATO bodies shall communicate BCM audit results to the NATO Business Continuity Board. What's more, with the addition of requirements such as "evaluations shall address the possible needs for changes to the NATO Business Continuity Policy, objectives, strategies and other continuity elements" , the Policy directly addresses the transition from identified lessons to lessons learned, through remedial actions, building a bridge to the last step of the PDCA - "Act" where they are actually implemented. The fourth and last phase is "Act". In this phase, the corrective actions defined in the Check phase are implemented. It allows for revision to the scope, the policy, and the objectives of the BCMS as defined during the "Plan" phase.

Learning lessons from foreign experience

Through analysis of the Lessons Learned process, it has been proven that it is an integral part of the BCMS cycle, applicable in all its phases, keeping the cycle revolving, refining business continuity solutions. With that, however, several critical questions remain to be answered. Even if a fully developed BCMS is considered, for the sake of this study, as a virtual perpetual motion machine, spinning in a never-ending cycle, producing organizational resilience, the problem of the "first push" is still in place. What triggers the constant cycle? Implementation of learning lessons through external expertise, as opposed to lessons learned from own experiences, could be a step towards resolving that problem. As with most organizations, NATO's BC journey did not start spontaneously. Through constant, extensive analysis and horizon scans of the security environment, a rather simple notion was identified: "The Alliance is not immune to disruptions that could potentially degrade its ability to deliver on its core tasks. Therefore, Business Continuity Management is very important and has to be a discipline in its own right across NATO." The concept of BCM has now officially been around for more than 70 years, yet it emerged from an identified need for a comprehensive approach, to tackle disruption of normal business operations in organizations through different fields. Decades of trials and errors, collection of best practices, legislation and eventually standardization drove the constant improvement of the concept. NATO also identified the need for such approach back in 2018 , however, being a knowledge-intensive organization it took an educated approach towards developing and integrating a BCMS – learning from foreign experience.

NATO's BC Policy sets the requirement for each NATO body to develop an effective BCM System based on the requirements by the International Standards outlined in ISO 22301 and ISO 22313 , moreover, the Guidelines for its practical implementation, refer to Business Continuity Institute Good Practices Guidelines and Disaster Recovery Institute Professional Practices, as complementing the standards. In practice, these sources are the largest unified bodies of knowledge in the BCM field, however, that knowledge has been accumulated over years of practice, analysis, and identification of lessons to be learned. Much like the BCM CoI (Community of Interest), managed by the LL office in NATO, the Business Continuity Institue (BCI) and Disaster Recovery Institute (DRI) are professional communities of interest, on the two

sides of the Atlantic, in which practitioners are incentivized to share experiences, as well as to develop, evaluate and validate BC solutions that were implemented in their own organizations to promote operational resilience, resulting in the mentioned Good / Professional Practices. Through their BCM experts' membership in such communities, organizations support each other in the same manner that different NATO bodies should support each other in the BCMS integration.

The implementation of good practices, lessons learned and external expertise from the corporate world in the field of BCM, might be both the fastest and the most cost-efficient way of building an effective BCMS in the NATO Enterprise. Corporate goals, aims and needs, however, cannot be fully aligned, to the unique operating environment that NATO (being a political-military alliance) must function and maintain continuity in. As stated above "reinventing the wheel" was never an option for the organization's development and maintenance of a BC system, therefore the expertise of external defence sector entities is crucial for the initial stages of BCMS setup. In their shared effort towards collective defence and for the preservation of peace and security, NATO member states have agreed to "separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack" as article 3 of the NAT points out. This article is effectively used as a tool in building NATO capabilities based on the ones already built by the member states. As mentioned above, the NATO BC Policy was developed adhering to the ISO 22301 standard, however it was also built upon the foundation laid down by the armed forces of some member states, that integrated BCM in their practice as early as the late 90's. For the purposes of this research, the BC policies of the British Ministry of Defence and the of the U.S. Army are reviewed, both developed, published and tested in practice before the official release of a NATO policy, yet highlighting the crucial role an integrated process of continuous improvement of the BC solutions through learning from lessons identified in the BCM cycle.

Lessons Learned from member states

The U.S. Army Regulation 500-3 on Continuity of Operations Program Policy and Planning is the proponent policy document for the U.S. Army Continuity of Operations

Program. The regulation establishes responsibilities, policies, and planning guidance to ensure the effective execution of critical Army missions and the continuation of mission essential functions under all circumstances including crisis, attack, recovery, and reconstitution across a wide range of potential emergencies. Essentially, the regulation describes all the undergoing processes in building and operating a fully functional BCMS in all the U.S. Army entities, much like the aim of the NATO BC Policy. The program requires annual testing, training, and/or exercising of COOP capabilities through tabletop, functional, or full-scale exercises etc., but what is more important is that the regulation's requirements include utilization of a lessons-learned process post-testing and auditing. "The senior Army official will determine what corrective actions, lessons learned, metrics, and tracking mechanisms are necessary and what formats and procedures will be used by their organization" . The BCMS operated by the U.S. Army even goes as far as introducing a tool, used for lesson identification and implementation of corrective actions, similar to the NATO LL process, reviewed earlier. An after-action report is required after an actual COOP event or exercise done in the testing phase. AARs include lessons learned, that are analysed, and subsequently corrective actions are prescribed triggering the next revolution of planning and validating BC solutions.

While the U.S. Army BC process focuses on ensuring mission essential functions are prioritized during disruptions, the approach of the British MOD is focused on Critical Outputs, like the wider NATO understanding. MOD Publication on Business Continuity Management under JSP 503 underlines the fact that," MOD plays a key role in defending the UK and its interests and in strengthening international peace and stability. The Department also has a unique set of responsibilities within Government that must continue to be met regardless of what may occur" . Additionally," BCM supports the achievement of the Defence Aim and the delivery of the Strategy for Defence by ensuring that MOD can continue to deliver or recover critical outputs (particularly operations) in the event of disruption." The three areas that are vital to MOD's ability to continue to deliver critical outputs following a disruptive event are described as:" people, processes and resources". Similarities to the NATO BC Policy are evident, as the British MOD's publication is based on a civilian BCM standard - The British Standard for Business Continuity Management BS25999 . British Standardization Institue published BS25999 in the early 2000's but it was replaced in

2012 by ISO22301, which built upon the foundation of the old standard, developing a more comprehensive approach to business continuity as a management system. In a comparable manner, JSP 503, released in 2011 acted as a field-tested platform for the Allied BC Policy, which adapted it to the requirements of ISO22301 and its own unique operational environment.

The MOD's BCM model, which is based on the British Standard's BCM lifecycle, has six elements as opposed to the 4-step PDCA management cycle, described by ISO 22301 and integrated into NATO's Policy. However, same core principle apply – BCM is only effective if the solutions it produces are a subject to constant improvement and revalidation. Exercising, Maintaining, Reviewing and Assurance phase, implemented by the British MOD, translates to the "Check" phase of the PDCA cycle described above, aiming to address any Issues of concern that arise during the assurance and validation process, thereby leading to improvements in BCM arrangements. Similarly to the U.S. Army Regulation 500-3, the tool for constant improvement of BCM arrangements in the organization, is none other, but the LL process itself. JSP 503 goes even further, implying responsibility for all staff in an entity, when it comes to opportunities for improvement of BCM by securing that lessons identified are incorporated into BCM activities and products.

Above review of the BC policies, implemented by two of the most capable militaries in NATO has highlighted the fact that although the BC Policy of the Alliance is relatively new, the significance of the topic is evidently not new to the public defence sector. What is more, defence institutions have effectively used their Lessons Learned capabilities to implement and gradually advance their BCM systems, as is the intention laid out in the NATO BC Policy. Identifying and utilizing external experience, good practices and expertise is crucial to the development of a sound business continuity system in an organization of this calibre. At the same time, identifying internal challenges, unique problems and solutions, through the LL process, and consequentially applying changes, corresponding to the identified problems, is the driver for continuous improvement of the BC system in place. Through a detailed analysis of the BCMS lifecycle described in ISO 22301 and implemented in the Allied BC Policy, accompanied by examples of this "battle-tested" method of improvement in defence institutions, the place of LL was identified in the NATO-wide BCM setting. Essentially, organizational resilience and continuation of operations, regardless of the

challenges and disruptions faced, is the basis of delivering NATO's core missions, but none of them would be achievable if the business continuation tools don't evolve as fast as the threads do. The ability to "bounce forward", to learn and emerge stronger after every disruption is only attainable through rigorous training, implementing lessons learned and continuous improvement.

Bibliography

1. International Organization for Standardization (ISO). (2019). ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements. Retrieved from ISO: https://www.iso.org/standard/75106.html.
2. International Organization for Standardization (ISO). (2012). ISO 22313:2012 Societal security — Business continuity management systems — Guidance. Retrieved from ISO: https://www.iso.org/standard/50038.html.
3. NATO Headquarters. (2020). NATO Business Continuity Policy. NATO Document Library.
4. NATO Standardization Office. (2017). Allied Joint Doctrine for the Conduct of Operations (AJP-3). Retrieved from NATO: https://nso.nato.int/natoterm/Web.mvc.
5. Ministry of Defence (MOD), United Kingdom. (2011). JSP 503: Business Continuity Management (BCM) Policy. Ministry of Defence.
6. British Standards Institution (BSI). (2007). BS25999: British Standard for Business Continuity Management. Retrieved from BSI: https://www.bsigroup.com.
7. U.S. Army. (2018). Army Regulation 500-3: Continuity of Operations Program Policy and Planning. U.S. Department of the Army.
8. Business Continuity Institute (BCI). (2018). Good Practice Guidelines (GPG) 2018. Retrieved from BCI: https://www.thebci.org.
9. Disaster Recovery Institute (DRI). (2019). Professional Practices for Business Continuity Management. Retrieved from DRI: https://drii.org.

PROJECT 33: THE NAVPLAN AND THE FUTURE OF THE US NAVY

Gonzalo VÁZQUEZ ORBAICETA

Abstract: The current Chief of Naval Operations in the U.S. Navy, Admiral Lisa Franchetti, published in late September 2024 the new Naval Plan for the Navy. Focused on preparing the Navy for war with the People's Liberation Army Navy (PLAN) by 2027, the new plan seeks to address the different problems currently faced by the Navy, as well as to maximize the performance of each and every component of the service (manpower, capabilities and logistics). However, in the midst of an increasingly competitive and challenging maritime environment, successfully achieving the goals set forth in the new plan will require notable effort and dedication. In light of this, it is convenient to put into perspective the place where the Navy stands today, examining its antecedents and its future projection.

Introduction

The importance of the sea for the security and prosperity of nations, far from losing its prominence in international relations, has been gaining increasing international attention. As today's highly interconnected global society has become increasingly dependent on the sea for its functioning, the strategic importance of the use and exploitation of its resources has been consolidated as one of the central pillars of the current international economic order. A quick glance at some of today's most prominent conflict hotspots reveals a maritime component in all of them.

In the Russia-Ukraine conflict, naval warfare in the Black Sea has become a scenario of significant technological advances in naval technology, with the extensive use of unmanned surface vessels (USVs) which has allowed Kiev to dispute Russia's control of the sea. Maritime trade in the region has been severely affected by the strife, causing major setbacks to the flow of trade in grain and other products on which many developing countries depend.

As a result of the conflict in the Gaza Strip between Israel and its regional adversaries, the Red Sea, one of the world's most important shipping lanes (connecting the Indian Ocean and the Mediterranean Sea) has become a high-risk area for global maritime

traffic. The Houthi rebels, materially supported by Tehran, have succeeded in sinking or damaging numerous ships over the last eight months, eventually leading to the deployment of two multinational naval operations: Operation Prosperity Guardian (led by the United States) and Operation Aspides (launched by the European Union).

In the Indo-Pacific, a region bound to become the center of gravity of the global economy (many would argue it already is), the stability of the regional order is constantly threatened by territorial disputes (mostly maritime) between the PRC and its neighboring countries –Japan, South Korea, the Philippines, Taiwan, Vietnam and Malaysia, among others. Moreover, Chinese leader Xi Jinping's ambition to incorporate Taiwan into the PRC – something he has instructed his military to try to achieve by 2027– makes this region another potential focus of conflict.

Against this backdrop, the United States and its allies are facing with the need to significantly strengthen their naval (and maritime) capabilities in order to preserve stability and order at sea, after several decades of reduced investments and a notable decline in the size of their navies[1]. With the publication of the U.S. Navy's new Naval Plan (henceforth NAVPLAN), which echoes the situation just described very clearly, this article seeks to analyze the contents of the document and the historical context in which it is framed. To do so, aside from the contents of the document, it also examines some aspects related to its recent past (the late stages of the Cold War) and the Navy's future projection in the medium term.

Strategic Context Overview

The U.S. Navy is publishing the NAVPLAN at a very delicate time at the strategic level, something that, as will be seen later on, is clearly reflected throughout the pages of the document.

Firstly, the strategic situation at sea has undergone a radical change with the return to great power competition. As the Cold War came to an end in 1990, Washington emerged as the only maritime power with global power projection capability, based on

[1] Vázquez, Gonzalo, Sailing Rough Seas: NATO's Maritime Posture, Opinion Paper, IEEE bulletin, 11 March 2024, 947-967. Available at: https://publicaciones.defensa.gob.es/media/downloadable/files/links/b/o/boletin_ieee_33_.pdf (Accessed 29 September 2024).

the Navy's ability to secure control of the sea wherever was needed. This was confirmed almost immediately, when Iraq decided to invade Kuwait in August 1990. Saddam Hussein's move prompted a massive deployment in response led by the US Navy, which began in the early hours of January 17, 1991, and in which the Spanish Navy (Armada) also made some contributions[2]. During the course of *Operation Desert Storm* (the second phase of the Gulf War that followed Operation Desert Shield), the Americans deployed six aircraft carriers in the waters of the Persian Gulf and the Red Sea, supported by the full range of U.S. and allied naval platforms –highlighting, once again, the inherent flexibility that naval power has.

While it is true that, as Vice Admiral Stan Arthur, then commander of the U.S. Naval Forces Central Command, would point out shortly afterwards, part of the resounding success was due to '*modern port infrastructures, large and numerous airfields, and an enemy whose army did not really believe in its mission*' [3], the massive deployment, which saw the debut of the Tomahawk land attack missiles (TLAMs), is certainly a relevant event in the history of joint aeronaval operations. Moreover, as the current crisis in the Red Sea has shown, it is something for which neither Washington nor its allies have the will or the capability to do today.

While Operation Prosperity Guardian has managed to escort a large number of merchant ships and Europe's Operation Aspides has done something similar, both interventions are far from resembling the 1991 deployment of force (which was eminently focused on achieving a certain result on land). The U.S. Navy has decreased considerably in size, as have the navies of most of its allies; at the same time, the 'democratization' of defensive capabilities gathered under the concept of Anti-Access/Area Denial (A2/AD), now deployed by groups such as the Houthis (supported by Tehran), has meant that control of the sea can no longer be taken for granted.

Almost simultaneously, the rapid growth of the Chinese navy in Southeast Asia, which is already the largest in the world in terms of number of platforms (something which,

---

[2] Enrech De Acedo, José Luís, Zippo Uno», Revista General de Marina, tomo 284, May 2023, 717-732. Available at: https://dialnet.unirioja.es/servlet/articulo?codigo=8947114&orden=0&info=link (Accessed 28 September 2024).

[3] Arthur, Stan & Pokrant, Marvin, The Storm at Sea, USNI Proceedings, Vol. 117/5/1,059, Mayo 1991. Available at: https://www.usni.org/magazines/proceedings/1991/may/storm-sea (Accessed 28 September 2024).

although far from being decisive, is a factor to be taken into account), has as its central objective seizing control of the sea in the region and, should this not be possible, deny access to it to the Americans and their allies as much as possible. Over the past twelve years, Beijing has made more than significant investments to equip its navy and coast guard (and maritime militia) with the appropriate means and the best training possible for high-intensity naval warfare. Although, for obvious reasons, China is still far from becoming a global maritime power (there is no consensus on whether this is the goal they are pursuing), it has the support of A2/AD capabilities to rely on and complement its firepower.

This development has been made possible by the complementary growth of another fundamental element of naval power: the industrial base needed to build ships and sustain them throughout their operational life. In this respect, the Southeast Asian region is already the leading naval industrial power –and will continue to be in the foreseeable future. Between China, Japan and South Korea, they account for a major part of the total tonnage launched annually, including both warships and merchant ships[4]. In contrast, the shipbuilding industry in NATO countries suffers from the lack of qualified personnel in the shipyards, which are, at the same time, not enough for the current strategic needs, and is thus lagging behind.

In the case of the Americans, in addition to the disappointment of the Littoral Combat Ship (LCS) program, of which several units have been already decommissioned after less than a decade in service, the case of the future Constellation-class frigates (a project that was finally awarded to BAE Systems to the detriment of Navantia's proposal) has received wider attention internationally. The new frigates were initially supposed to be based on the European FREMMs operated by France and Italy. However, successive changes in the design have turned the future class into a completely different platform, one which bears very little resemblance with the original design which was initially sought. At the same time, the lack of qualified personnel and sufficient shipyards in the United States has also prompted numerous delays in the

[4] Kang, Choi & Lee, Peter K. Why U.S. Naval Power needs Asian Allies, War on the Rocks, 12 January 2024. Available at: https://warontherocks.com/2024/01/why-u-s-naval-power-needs-asian-allies/ (Accessed 29 September 2024).

program, of which the first unit will not be commissioned before 2029 (three years later than initially expected)[5].

The submarine fleet is in a very similar position. As retired U.S. Navy Captain Jerry Hendrix underscored, only a single boat is scheduled to be delivered within budgets in 2025. '*Additionally, of the submarine force already in commission, sixteen of those forty-nine boats— or nearly a third of the Navy's premier offensive force—are in drydocks or tied to piers, lacking required dive certifications*', he ascertains[6]. Given that the U.S. submarine force is one of the Navy's most important tools, the poor state of the fleet and the lack of sufficient shipyards to provide adequate maintenance of the units in service means that the construction of the future Columbia-class (SSBN strategic submarines to replace the Ohio-class) and the program to replace the Virginia class attack submarines have also suffered delays.

In broad terms, these are some of the biggest challenges Admiral Lisa Franchetti has encountered since she took over as Chief of Naval Operations (CNO) in August 2023. The U.S. Navy faces a strategic landscape in which control of the sea is no longer guaranteed, and the possibility of conflict with its antagonist in Southeast Asia looms ever closer. More than ever, the United States needs a new push to strengthen its maritime power (which encompasses not only the navy, but also its merchant marine and auxiliary fleet, an industry capable of supporting them, and the logistical base necessary to coordinate all efforts). NAVPLAN 2024 is conceived under such premise.

NAVPLAN 2024

'*This Navigation Plan is my strategic guidance to the Navy, building on that vision and picking up where the 2022 Navigation Plan left off*', opens Admiral Lisa Franchetti, the U.S. Navy's current Chief of Naval Operations (CNO) in the 2024 NAVPLAN[7]. The

---

[5] Conte De Los Ríos, Augusto, Fragatas clase Constellation: Crónica de una Muerte Anunciada?, Revista Ejércitos, 5 June 2024. Available at: https://www.revistaejercitos.com/opinion/fragatas-clase-constellation-cronica-de-una-muerte-anunciada/ (Accessed 28 September 2024).

[6] Hendrix, Jerry, Sunk at Pier: Crisis in the American Submarine Industrial Base, American Affairs Journal, Vol. 8, No 2, 2024. Available at: https://americanaffairsjournal.org/2024/05/sunk-at-the-pier-crisis-in-the-american-submarine-industrial-base/ (Accessed 28 September 2024).

[7] Chief of Naval Operations Navigation Plan for America's Warfighting Navy 2024, September 2024, ii. Available at: https://www.navy.mil/Leadership/Chief-of-Naval-Operations/CNO-NAVPLAN-2024/ (Accessed 28 September 2024).

United States is faced with the need to take a step to the front in order to resolve the numerous issues that have been deteriorating its readiness over the past several decades, while preparing for the possibility of a conflict with China's navy in 2027. Although such a scenario has been talked about for many years, as highlighted by the concept of '*the Davidson Window*' coined a few years ago, we have not encountered many such direct statements of intent until now:

> *The Chairman of the People's Republic of China (PRC) has told his forces to be ready for war by 2027—we will be more ready. The challenge posed by the PRC to our Navy now goes well beyond just the size of the PLA Navy fleet […] The PRC's defense industrial base is on a wartime footing, including the world's largest shipbuilding capacity now at the hands of the PLA navy.*[8]

The NAVPLAN makes it clear that preparation for a hypothetical war scenario like that will be the center of gravity of the Navy's work from this moment on. The document, not very long, is structured in three different sections: "Why the Update"; "How we Fight"; and "How we Accelerate". The two main strategic ends defined by it are «readiness for the possibility of war with the People's Republic of China by 2027 and enhancing the Navy's long-term advantage». Both comprise what the plan describes as its «north star», upon which the rest is articulated: '*By 2027, the Navy will be more ready for sustained combat as part of a Joint and Combined force, prioritizing the People's Republic of China as the pacing challenge and focusing on enabling the Joint warfighting ecosystem*'[9].

To fulfill such vision, seven key objectives are established – the ways – to enhance the preparation of the naval force by 2027:

1. Ready our Platforms (achieve and sustain an 80 percent combat surge ready posture for ships, submarines, and aircraft);
2. Operationalize Robotic and Autonomous Systems (integrate proven robotic and autonomous systems for routine use by the commanders who will employ them);

[8] NAVPLAN, 6.
[9] Ibid, 6, 19.

3. Fight from the MOC (have ready MOCs certified and proficient in command and control, information, intelligence, fires, movement and maneuver, protection, and sustainment functions in all fleet headquarters);

4. Recruit and Retain Talent (achieve 100% rating fill for the Navy active and reserve components, man our deploying units to 95% of billets authorized, and fill 100% of strategic depth mobilization billets);

5. Deliver Quality of Service (eliminate involuntary living aboard ships in homeport);

6. Invest in Warfighter Competency (have reliable, realistic, relevant, and recordable LVC-enabled architectures to train Navy warfighters); and

7. Restore our Critical Infrastructure (generate, sustain, and posture the force for the fight).[10]

Overall, the document stresses a unitary vision for the entire service, one that provides a strong purpose to drive its efforts during the next few years. "*Why we fight has not changed, but how we fight has, which must inform what we fight with*"[11].

Also worthy of consideration is the acknowledgement that the Navy does not fight on its own, but rather, as part of an ecosystem in which the contribution of each part is vital for its overall success. As such, interoperability with other services and with their European and Asian allies also underlies the vision of the NAVPLAN. They U.S. Navy is no longer able to cope with the entire plethora of challenges on its own. Thus, while recognizing that the need to grow the fleet will take some years, and a «3-5% sustained budget growth above inflation» to do so, the role of their allies also plays a relevant part in the successful attainment of Project 33's goals.

On broad terms, the NAVPLAN has been well received in the naval circles of Washington. It underscores a series of objectives which are without a doubt ambitious, and evidently, will be hard to attain. Placing China as the main antagonist adds a higher sense of purpose to the document, something fundamental for any strategy. '*Trying to design a force without an antagonist in view, or without a war plan to vanquish that antagonist, was like 'trying to design a machine tool without knowing*

[10] Ibid, 19-23

[11] Ibid, 13

whether it is going to manufacture hair pins or locomotives", argues U.S. Naval War College Professor James Holmes quoting U.S. Navy Captain Harry Yarnell[12].

Especially significant is the document's emphasis on the fact that "asymmetric sea denial" is among the core capabilities that the Navy must hone for a hypothetical conflict by 2027. Traditionally, the Navy has not operated in the defensive, but has rather sough the offensive (particularly in decisive moments, as during the latter stages of the Cold War against the USSR). Thus, for Admiral Franchetti herself to underscore the need to seek an asymmetric sea denial remains quite a statement. 'T*he Navigation Plan, then, seems to admit the unsettling reality that the Navy will be weaker than its major foe at the outset of a Pacific contest of arms. It's jarring for America's top uniformed naval officer to confess that in writing*', Holmes continues.[13]

Although generally positive, the NAVPLAN still lacks more depth and detail in some of the aspects it discusses. In terms of logistics or the naval industrial base (which are mentioned later on in this article) the document fails to elaborate further on the precise needs derived. It mentions on several instances the paramount necessity of improving the maritime industry to support the Navy's general preparation, albeit it is still immersed in the construction of a fleet geared towards high-intensity naval warfare with big and expensive platforms and systems.[14] When it comes to seeking a positive balance between high-end and low-end capabilities, the development of platforms comprising the latter category seems like a good opportunity to reduce the high costs that the former entail, so that financial resources to the Navy can be used more efficiently.

It seems obvious, then, that while the ambition reflected in the plan is high, the efforts and dedication that will have to follow to make Project 33's vision a reality will have to be just as big, and will definitely put to the test Washington's willingness towards

---

[12] Holmes, James «The Navy's New NavPlan sets its sights on China, from a sea denial stance», USNI Proceedings, Vol. 150/9/1,459, September 2024. Available at: https://www.usni.org/magazines/proceedings/2024/september/navys-new-navplan-sets-its-sights-china-sea-denial-stance?check_logged_in=1 (Accessed 29 September 2024).

[13] Ibid.

[14] CMS Editorial Board, Assessing the 2024 Navigation Plan, Center for Maritime Strategy, 23 September 2024. Available at: https://centerformaritimestrategy.org/publications/assessing-the-2024-navigation-plan/ (Accessed 28 September 2024).

revamping its sea power. In spite of this, it is not the first time that they have had to do so, as the days of the Reagan administration (and several other instances) illustrate.

From the Cold War to DMO: The NAVPLAN in Perspective

The NAVPLAN must be understood as an element within a wider historical context. The very name Project 33 is precisely intended to frame the plan of Franchetti and his team in the historical trajectory of the navy, building on the work of her predecessors. Thus, at a time when it has already lost part of the capabilities that consolidated it as the great naval power immediately after the Cold War. Throughout the last three decades, a major part of those capabilities comes from the revolution that took place during the 1980s under Ronald Reagan's administration. But at the same time, as that heritage becomes increasingly diluted with the decommissioning of the platforms built back then, the U.S. Navy has been working for years to adapt its concept of operations to meet the threats posed by A2/AD systems and the prospects of increasingly challenging littorals. It is therefore useful to put the NAVPLAN in the context of its background, and the process of adaptation towards the new concept of Distributed Maritime Operations (DMO) on which the Navy has been working on for years.

The Maritime Strategy and the Reagan Administration

As we have highlighted, the publication of NAVPLAN seems, at least on paper, an important turning point after almost two decades of setbacks and major failures. In this sense, the change that seems to be sought for the coming years is reminiscent of the change of direction that President Ronald Reagan instituted with his arrival at the White House in 1981. During the 1970s, the Soviet Union's navy, under the command of Admiral Sergei Gorshkov since 1956, had embarked on an ambitious shipbuilding plan to convert a navy subservient to the Red Army and limited to near-water operations into a blue-water navy capable of operating simultaneously in different maritime theaters (something that is in itself an imperative for Russia given its geographic configuration). The Cuban missile crisis in 1962 had exposed the navy's serious shortcomings when it came to deploying 'far from home', and allowed

Gorshkov to forge ahead with his plan to rebuild the Soviet navy into a global force - which became a reality a decade later with the Okean-70 (Russian for 'ocean) large naval exercise.[15] This exercise would be repeated three more times over the following two decades, as well as several other large-scale exercise.

In response to the relatively little attention that the Nixon and Carter administrations had paid to the navy as a tool for defense against the USSR, the Reagan administration launched an ambitious plan to make the navy the spearhead of its policy against the Soviets. The culmination of its project was the so-called Maritime Strategy, which in turn served as the main argument for the Reagan administration's '600-ship navy'. Thus, during the 1980s, the navy devoted major efforts to establishing a solid schedule of large-scale naval exercises, involving its Pacific and NATO allies, and, above all, conducting deployments farther up the GIUK Gap in waters the Soviets considered almost theirs –something that had not been done until then.

Some of the most significant programs originated during these years were the Nimitz-class aircraft carriers, the Oliver Hazard-Perry-class frigates (upon which the Navy's F-80 Santa María-class were based), or the Arleigh Burke-class destroyers (of which 73 units have already been built in different flights). Thus, through major investments in the navy, which reached the 600-ship navy target over several years (including 15 aircraft carriers with their respective task forces), and guided by the requirements that had been established thanks to the Maritime Strategy, which defined the maritime theaters where they were to focus their efforts and the means necessary for each of them, the Reagan administration made a substantial turnaround in the navy's trajectory. Although it is beyond the scope of this article, the study of the Maritime Strategy deserves significant attention today; given the many lessons, it holds for helping to navigate the current strategic context at sea.

[15] OKEAN-70 was a naval exercise which took place during several months and in several maritime theaters simultaneously. It was the largest naval exercise in Soviet/Russian history until that point, and confirmed their ability to contest command of the sea to the U.S. Navy. The exercise had three additional iterations between then and 1985. Most recently, the Russian Navy conducted the first iteration of the exercise since the end of the Cold War, albeit with the participation of the PLA Navy and at a much smaller scale.

Concept for Distributed Maritime Operations (DMO)

On the other hand, the NAVPLAN comes at a time in which the U.S. Navy, faced with the evident proliferation of A2/AD capabilities mentioned above, needs to transform its concept of operations to meet the aforementioned threat. In particular, when thinking about a possible conflict in Southeast Asian waters against its antagonist in Beijing. To this end, the Navy, through entities such as the Center for Naval Analyses (CNA), has been working for years on the concept of distributed lethality.

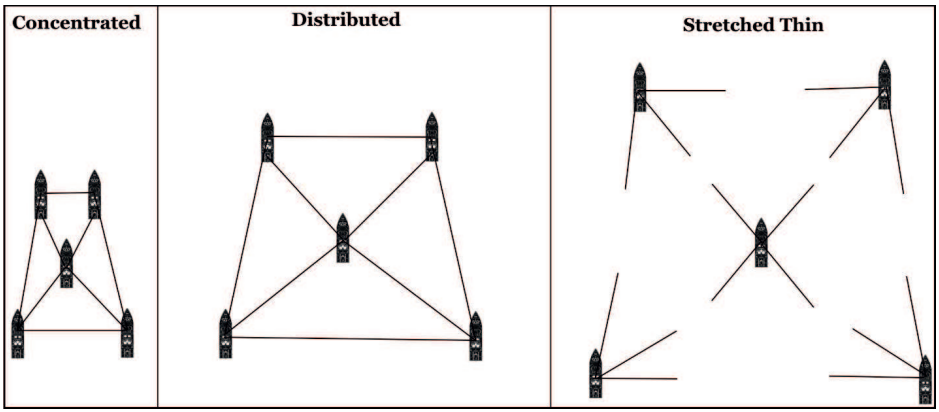


Figure 1: Difference between a concentrated, a distributed and a dispersed fleet (Source: Filipoff, 2023)

In essence, the aim is to complicate the adversary's ability to locate and attack targets in the fleet through a distribution of his units while maintaining the lethality of fire resulting from the combined capabilities of all of them. This has been embodied in its Distributed Maritime Operations concept. [16] Fundamentally, the DMO concept (illustrated in the figure below), arises 'partly as a defensive reaction and partly as an offensive evolution', and under the premise that distribution is understood as 'the ideal balance in the spread of capabilities'.[17] It pursues a higher level of distribution so as to complicate a potential enemy's ability to target the fleet by multiplying the number

[16] FILIPOFF, Dmitry «Fighting DMO, Pt. 1: Defining Distributed Maritime Operations and the Future of Naval Warfare», CIMSEC, 20 febrero 2023. Available at: https://cimsec.org/fighting-dmo-pt-1-defining-distributed-maritime-operations-and-the-future-of-naval-warfare/ (Accessed 28 September 2024).

[17] Ibid.

of targets, while the vessels retain the ability to combine their aggregated fires on the enemy.

DMO, however, brings with it several tactical and operational challenges for the U.S. Navy, which will take several years to fully resolve for the proper implementation of the concept. Firstly, given the number of weapon systems the Navy has and the different types of missiles that it fields, each with its own technical peculiarities, coordinating them in time and space to converge on the selected target and saturate the adversary's defenses is highly complicated. At present, Washington does not have a homogeneous missile arsenal, which makes coordination extremely difficult, and, at the same time,

> *US surface warships and submarines have very little anti-ship missile firepower. They only field a small number of short-range Harpoon missiles, which are inadequate for long-range, massed fires against warships. Their increase in firepower will come with the fielding of the Maritime Strike Tomahawk, which is compatible with their launch cells.* [18]

Secondly, because a distributed fleet brings along, at the same time, a great need for logistical support in order to work efficiently. As the situation in the Red Sea has shown, in high-intensity naval warfare, the ability to resupply ships once they have exhausted their onboard arsenal (which, in a real high-intensity conflict, could happen in a few hours) is fundamental. At present, no navy is capable of resupplying without having to return to port, although the way to do so has been under study for years.

Therefore, to ensure the resupply of missiles, fuel and any other material, the work of the auxiliary fleet and the merchant marine is fundamental –but also a need that has been significantly neglected. As of today, Washington and several of its allies have a greatly reduced auxiliary fleet, while continuing to decommission units due to a lack of personnel to fill out their crews.[19] This poses some obstacles for the successful implementation of the DMO concept moving forward. Such distributed lethality, on the

---

[18] Filipoff, Dmitry Distributed Maritime Operations: Solving what problems and seizing which opportunities?, Atlantic Council, July 2024, 5. Available at: https://www.atlanticcouncil.org/wp-content/uploads/2024/06/Distributed-Maritime-Operations-Solving-what-problems-and-seizing-which-opportunities.pdf.

[19] *US and UK are sidelining Fleet Auxiliary Ships because of crew shortages*, The Maritime Executive, 24 August 2024. Available at: https://maritime-executive.com/article/u-s-and-uk-are-sidelining-naval-auxiliary-ships-because-of-crew-shortages (Accessed 28 September 2024).

other hand, is not unique to the U.S. Navy. Many allied navies, aware of the challenges that the proliferation of anti-ship capabilities presents to their ships, will also need to explore new operational concepts that involve a greater degree of distribution of their fleets. One option to facilitate this is the incorporation of new technologies and autonomous systems that allow larger and more valuable ships to stay out of range of coastal artillery.[20] In that sense, the integration of unmanned vehicles into fleets (both UUVS, USVs and UAVs) is set to become one of the central tasks for many navies over the last few years, while exploring the appropriate ratio of manned to unmanned units to meet the particular needs of each navy.[21] Once again, the lack of material and human resources resulting from reduced investments in capabilities is an obstacle for many navies, and will create further problems in the future.

Final Considerations

In light of the several aspects outlined in this paper, it is worth underlining that the launch of Admiral Franchetti's NAVPLAN brings great promises for a Navy in search for reasserting its dominant status as the main maritime power with a real and serious global power projection ability. But just as the ambition and motivation that characterize Project 33, Washington has now an equally great challenge that will demand large investments sustained over a long period of time to be successfully implemented.

The plan is framed in a historical context of great changes for the Navy, which recognizes for the first time in a long time that in case of conflict against their Asian antagonist, they won't have the initial advantage. In fact, all the contrary: the Navy will have to first surpass the tyranny of distance to get to the main theater of operations, and once there, cope with an adversary which will enjoy the '*home team advantage*'.

---

[20] On the concept of distributed lethality, see also: Herráiz García, Fernando, Letalidad Distribuida, Revista General de Marina, December 2019, pp. 979-988. Available at: https://armada.defensa.gob.es/archivo/rgm/2019/12/rgmdic2019cap10.pdf (Accessed 29 September 2024).

[21] VV.AA. Vehículos Navales no Tripulados: A Modo de Introducción, Cuadernos de Pensamiento Naval, No. 37, 2024, 155-174. Available at: https://publicaciones.defensa.gob.es/media/downloadable/files/links/p/e/pensamiento_naval_37.pdf (Accessed 28 September 2024).

Thus, the implicit effort of such a massive mobilization calls for the strengthening of such vital aspects as the auxiliary fleet, which, as the plan outlines, doesn't have the size nor the capabilities necessary to provide the support needed.

Looking at the current situation, and assuming great difficulty of strengthening the Navy's capabilities based on the current state of its naval industrial base, Washington has a major endeavor ahead. To guide its efforts, the experience provided by the days of the Reagan Administration and the Maritime Strategy of the 1980s offers valuable lessons to observe. As former Navy Secretary John Lehman rightfully ascertained a few years ago:

> *Our situation now parallels that of 1980, and our adversaries are actively seeking to take advantage of our weakness […] The experience of the 1980s demonstrates that a restoration of American command of the seas could reap 90 percent of the deterrent benefits of naval supremacy almost immediately*.[22]

Thus, as Admiral Franchetti has instructed, the way forward is clear: all ahead flank. So it is for the rest of NATO navies.

[22] Lehman, John F. *Oceans Ventured: Winning Cold War at Sea* (W.W. Norton & Co., 2018), 283.

BUSINESS IMPACT ANALYSIS AND RISK ASSESSMENT IN THE MARITIME SHIPPING INDUSTRY

Gonzalo VÁZQUEZ ORBAICETA[1]

Abstract: Over the last decades, global maritime shipping has seen a gradual increase of threats to its security as a consequence of the deterioration of the international system. Non-state actors acting close to strategically important places within the main sea lines of communication (SLOCs) have been involved in illicit actions to disrupt commerce. Given the vital importance of maritime commerce for the security of European and NATO nations, addressing these threats and developing a set of mechanisms to protect the shipping industry is just as important.

As part of the wider discipline of business continuity management, business impact analysis and risk assessment constitute an important pillar to help address the major shortcomings of current businesses. In the field of maritime shipping, which is important for NATO's maritime security at a wider level, the shipping industry must find ways to address the existing problems.

Introduction

Over the last decades, global maritime shipping has seen a gradual increase of threats to its security as a consequence of the deterioration of the international system. Non-state actors acting close to strategically important places within the main sea lines of communication (SLOCs) have been involved in illicit actions to disrupt commerce.

The heightened disruptions to global maritime logistics observed over recent years have underscored the critical importance of risk management and emergency response preparedness and the need to build ever more agile and resilient maritime

[1] Gonzalo Vázquez holds a BA in International Relations from the University of Navarra (Spain) He had been an intern at the Education and Training Branch of the Crisis Management and Disaster Response Center of Excellence (CMDR COE) from September 2023 to February 2024 when he worked out the present article.

transportation systems.[2] Given the vital importance of maritime commerce for the security of European and NATO nations, addressing these threats and developing a set of mechanisms to protect the shipping industry is just as important.

As part of the wider discipline of business continuity management, business impact analysis and risk assessment constitute an important pillar to help address the major shortcomings of current businesses. In the field of maritime shipping, which is important for NATO's maritime security at a wider level, the shipping industry must find ways to address the existing problems.

The following paper examines the current and evolving situation of business continuity and risk assessment from the perspective of the shipping industry. It addresses the importance of resilient maritime connectivity for NATO's security, the various threats currently faced in the maritime sector including the business in general and ports in particular, as well as the current Red Sea Crisis, and provides several proposals to enhance the relation between NATO governments and the main actors in the maritime shipping industry.

Business Impact Analysis, Risk Assessment & Supply Chain Resilience

Both the notions of business impact analysis and risk assessment are important to understand the overall purpose of this work. Business impact analysis essentially predicts the consequences that would derive in case a given business suffered any kind of disruption. As its name suggests, it analyzes the impact of any potential disruption for a given business. As a complement to business impact analysis, the specific loss scenarios that may derive are identified through a risk assessment, with which it is often possible to understand how the different variables will affect the results of that business,

Aside from these two concepts, risk management is also a tool that is used together with them. The framework in which this paper understands the notion of risk management, and the one which must come to mind whenever addressing risk assessment is that provided by the OECD, by virtue of which "the overall objective of

[2] UNCTAD, 2023; 88.

the risk assessment is to prioritize development policy, programming and investments towards the particular 'layer' of risk being assessed: the individual, the community, or the government and its institutions."

According to their study, risk assessment needs to be comprehensive, and requires a robust governance framework with agreed definitions and rules, to ensure consistent and reliable outcomes. It also needs to be simple, and appropriate for whatever sector or discipline is being addressed.

As will be seen in the following sections, business impact analysis is paramount for the maritime shipping industry for two simple reasons. First, because it is a business that involves many other businesses, serving as a node that connects all industrial sectors by supplying them with the necessary resources. Most economic sectors, industries and businesses depend upon the proper functioning of maritime shipping to ensure they can work smoothly.

Secondly, and derived from the first fact, the impact of any disruption that may be suffered by the business, not only affects the maritime shipping industry itself, but it has the potential to cause many other disruptions across all sectors with different consequences; from the textile industry to oil supplies to the agriculture sector. In terms of maritime commerce and the shipping industry, which will be assessed over the following sections, UNCTAD indicates how:

"Difficulties faced as part of efforts to mainstream environmental sustainability principles into commercial and business practices illustrate the complexity of some of these issues and the magnitude of the challenge in resilience building efforts."[3]

As previously underlined, risk assessment guides the optimal allocation of scarce resources to building the resilience that is necessary to ensure the continuity and the strengthening of almost any project, initiative, or given industry. For the purposes of the study carried out in this paper, one of the fundamental definitions that must be addressed before entering into the details of the subject is the concept of risk culture.

According to the Institute for Risk Management, within the study of risk culture, the A-B-C (Attitude, Behavior and Culture) Model is often a useful tool to understand the functioning of risk dynamics. With their risk variants, risk attitude is understood as "the

[3] UNCTAD, 2023; 88.

chosen position adopted by an individual or group towards risk, influenced by risk perception"; risk behavior includes the "external observable risk-related actions, including risk-based decision-making, risk processes, risk communications etc."; and risk culture describes "the values, beliefs, knowledge, attitudes and understanding about risk shared by a group of people with a common purpose."[4]

Another aspect that is closely linked to risk assessment and resilience, strongly determining the outcome of any process for which that assessment may be required in the first place, is uncertainty. It is the fundamental element that truly gives meaning (or, we could say, is the reason for their existence) to both business impact analysis and risk assessment. Uncertainty is the challenges which can hamper the development of businesses and drive them towards a path of ineffectiveness and irrelevance.

In essence, as is described in the upcoming section, supply chain resilience is one of the main objectives for the work of the maritime shipping industry. Without a resilient and protected maritime shipping, many other businesses run the risk of suffering losses and damaging the national economies of many nations. NATO must therefore devote more efforts to ensuring the adequate level of connectivity and supply chain resilience, so that the maritime shipping industry is adequately protected against potential threats and disruptions.

The Maritime Shipping Industry & its Importance for NATO

Maritime commerce/maritime trade is one of the most important pillars upon which the global economy is sustained and supported. As highlighted in one of the latest reports published by the United Nations Conference on Trade and Development (UNCTAD):

"Maritime transport underpins world economic interdependency and global supply chain linkages. Shipping and ports handle over 80 per cent of global merchandise trade by volume, and more than 70 per cent of its value. Supply chain disruptions caused by stressors spanning economic crises, political events, natural disasters, cybersecurity incidents and the COVID-19 pandemic, and more recently the conflict in

[4] Institute of Risk Management, 2012;

the Black Sea region, underscore the role of maritime transport as an important transmission channel – one which can send shockwaves across supply chains and bring world trade and business to a halt."[5]

Furthermore, according to UNCTAD, maritime trade volume is projected to grow in 2023 a 2.4% in comparison to 2022, thereby showcasing that the maritime industry remains resilient and with a positive balance. [6] Furthermore, even though containerized trade experiences a gradual period of recession after the COVID-19 crisis, figures from 2023 have confirmed a marginal increase.[7]

Year	Total seaborne trade	Containerized trade
2024	2.1	3.2
2025	2.2	3.2
2026	2.2	3.2
2027	2.1	3.0
2028	2.1	2.9

Figure 1: International maritime trade development forecast, 2024–2028 (Annual percentage change)

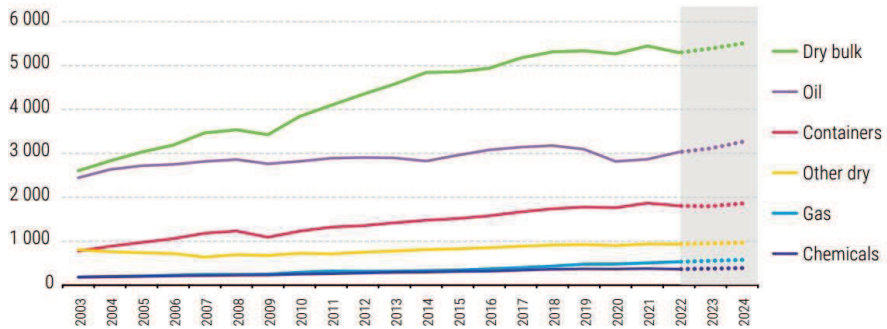


Figure 2: International maritime trade, 2003–2024 (Million tons loaded) (*Source: UNCTAD, 2022*).

[5] UNCTAD, 2022.

[6] UNCTAD, 2023.

[7] Ibid.

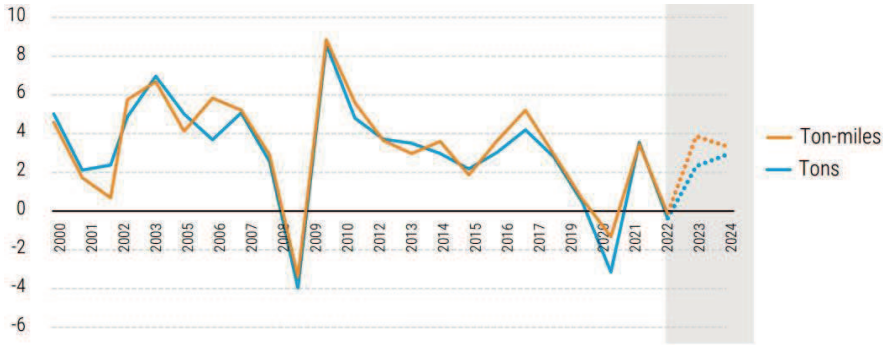


Figure 3: Seaborne trade growth, tons and ton-miles, 2000–2024 (Annual percentage change) (*Source: UNCTAD, 2022*).

Essentially, maritime commerce (and thus, the shipping industry) constitutes a pivotal element for the proper functioning in which security, risk assessment, resilience and business continuity (among other elements) meet. The logic of their interconnectedness within the maritime industry is consequential, or causal.

Maritime commerce, as said, accounts for almost 85% of the world's total commercial flow, which is responsible of ensuring human security and the sustainment of most economies in the world. Most businesses in the world rely heavily on the proper functioning of the maritime shipping industry, as a result of the increased interconnectedness in our global supply chains. In case any disruption occurs within, as was the case with the Ever-Given crisis in 2021 or the ongoing crisis in the Red Sea, many sectors across the global economy are affected. In contrast, the way to prevent these incidents from happening is ensuring a resilient maritime industry, which is partly attained through proper risk assessment measures which ensure its business continuity altogether.

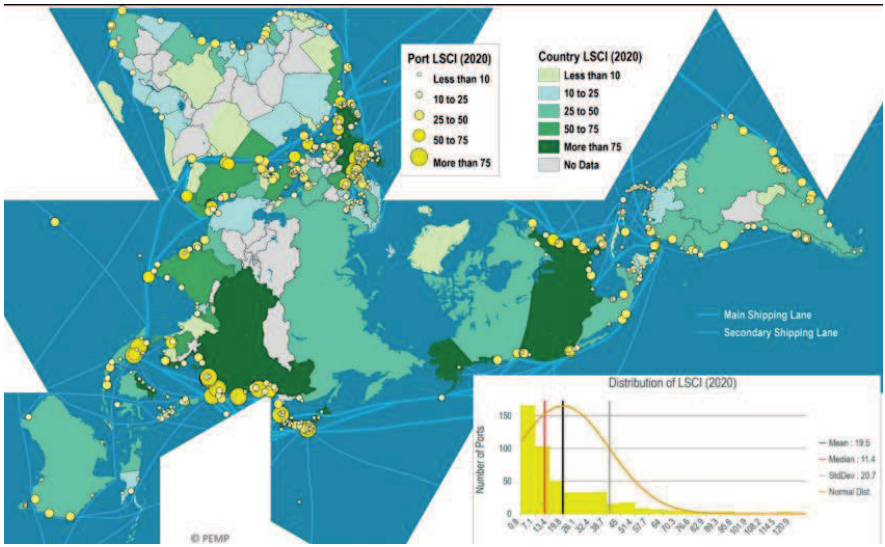


Figure 4: Maritime Contained Shipping Connectivity (*Source: UNCTAD, 2022*).

NATO' security relies on robust and resilient maritime supply chains. Many of the industries in its territory are dependent upon the goods that are supplied by sea. Thus, protecting its maritime commerce with a view to secure the economies of its members, as well as their wealth and economic growth, is one of the main tasks for the naval forces – their navies. As has been highlighted before by many naval thinkers, one of the main reasons for the existence of navies altogether is to provide protection for national commerce and prevent any enemy or hostile actor from causing a disruption.

In the following sections, these relations are explored more thoroughly, examining the current landscape of risks and threats to maritime commerce (Section 5); the importance of having strong and resilient ports (Section 6); the ongoing situation in the Red Sea, with its most immediate consequences for the global economy, as an example of the influence of geopolitics in the continuity of the industry (Section 7); the way in which the risks and threats described in the previous sections can be addressed and mitigated (Section 8); and some brief conclusions and recommendations based on the insights provided throughout the paper.

Risks and Threats to Maritime Commerce

During the past decades, maritime commerce has become increasingly vulnerable to external shocks and threats to entire connectivity. The main reasons for such deterioration at an international level are derived from a worsened geopolitical situation at sea, and aggravated by the rising number of threats (most of which originating from non-state actors) which could potentially disrupt the flow of maritime shipping.

The war in Ukraine, for example, has had an important impact on trade patterns. According to the UNCTAD,

"In the context of the war in Ukraine, the United Kingdom, the United States and the European Union, have applied restrictive economic measures to the trade of Russian crude oil, refined petroleum products and gas, such as import bans, pipeline transport restrictions and a cap on the price of the oil barrel, impacting underwriting for insurance-related processes. These measures have induced changes in the trading patterns of these products."[8]

A prominent example of resilience in the maritime trade sector has been the Black Sea Initiative, launched shortly after the outbreak of the conflict in Ukraine to prevent a major disruption of grain trade (and thus, of food and energy security in some parts of the world). More precisely,

"Since its signature and up until 20 July 2023, the Black Sea Initiative facilitated exports of 32.9 million metric tons of various food commodities encompassing corn, wheat, sunflower products, barley, soya and rapeseed and 725,000 metric tons of humanitarian food assistance exports to regions facing acute food insecurity. Around 57 percent of shipments went to developing countries. Considering World Bank income categories, 20 per cent of exports went to low-income and lower-middle income groups."[9]

All this data denotes the importance of the maritime shipping industry for economic prosperity (not only of NATO members, but for the entire world) and the importance of ensuring a resilient and stable service of maritime commerce. As has been

[8] UNCTAD, 2023; 12-13.

[9] UNCTAD, 2023; 15.

demonstrated in multiple occasions in the past, threats to maritime trade go far beyond the immediate disruption in the shipping routes.

Their ripple effect often permeates the entire supply chain, which then sustains damages to manufacturers, retailers, and consumers in general. Some of the challenges that they will bring as a consequence, are, for example, delays in cargo delivery, potential damage to goods, or increased insurance premiums (all of which are featuring right now as a result of the Red Sea Crisis). As a result of this, finding a comprehensive crisis management solution becomes of crucial importance to mitigate these risks and ensure business continuity.[10]

Another aspect which tends to be particularly vulnerable to malpractices aboard the ships and subject to a wide spectrum of risks is container safety. Goods are loaded into containers which are then loaded on the ships. In many instances, accidents or unforeseen incidents may occur which lead to the damaging of the container or even its loss. The graph below in Figure 5 shows the number of containers lost at sea over the past 16 years. On average, the graph shows a total of 1,566 containers lost at sea each year, although there was a notable spike in 2013.[11]

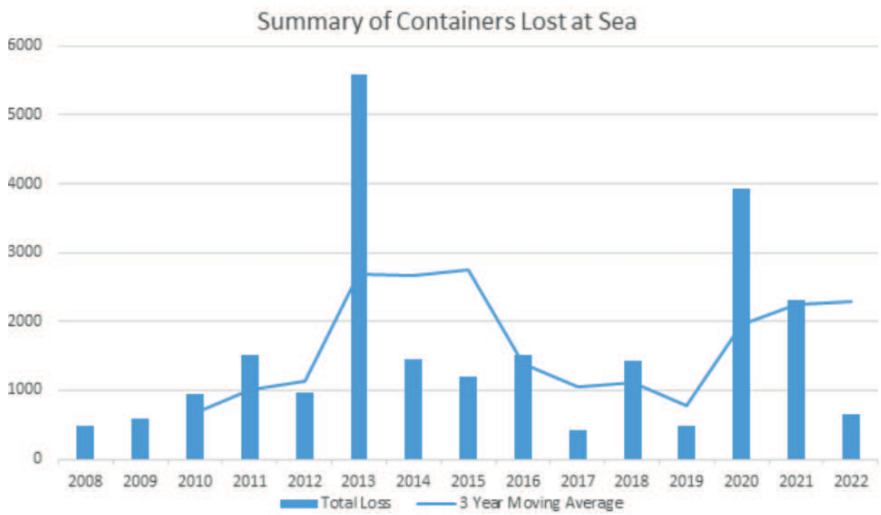


Figure 5: Summary of Containers lost at Sea (2008-2022) (Source: IMO, 2023).

[10] CRISES CONTROL, 2024.

[11] IMO, 2023.

From the perspective of the shipping liners and the companies, every transit must be done ensuring a strong level of safety for all containers. Owners and crew in each ship must ensure that the container is clean, in good condition, and properly secured in its position in order to prevent it is lost at sea. In this regard, the main code regulating the storage and packing of goods and cargo into the containers is the IMO/UNECE Code of Practice for Packing Cargo Transit Units (often referred to as CTU Code). Aside from the code, further measures and initiatives of risk management for containers' security are detailed in Section 8.

In concluding this section, one additional aspect which must be highlighted is that most successful maritime businesses have, at least to some extent, planned how they might recover from or mitigate particular setbacks, ranging from higher costs to fire. Some planning is imposed from outside. Insurance companies often require insurers to develop plans for mitigating losses.[12] This is further developed in section 7 of the paper.

Resilience and Protection of Ports

Ports are part of the broad category of critical maritime infrastructure, which also encompasses undersea infrastructures such as cables and pipelines. The role of ports is of paramount importance for global connectivity and the resilience of the supply chains, as they are the primary hubs that link commercial activity both at sea and on land. As a result of this, protecting ports within the broader effort of protecting global shipping is an important interest of most governments which rely on such commerce for their economic prosperity.

[12] BRYANT, 2023.

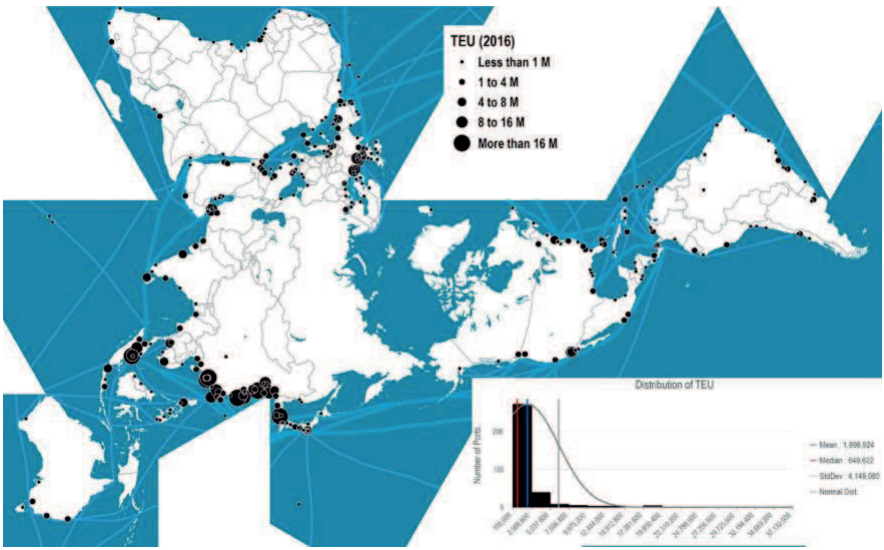


Figure 6: Container Port Traffic based on data from 2016 (*Source: UNCTAD, 2022*)

In this sense port resilience is a prominent element in the quest to make global shipping and the maritime shipping industry stronger. According to the UNCTAD, port resilience can be defined as the ability to maintain an acceptable level of service in the face of disruptions (e.g. pandemics, natural disasters and cyber or terrorist attacks)",[13] which varies with port size, location and type of operations. Most notably,

"Port resilience is not only an imperative for supply chains, but also for the national economies they support. Safeguarding the integrity of the maritime transport chain is a sustainable development imperative, particularly as developing countries have become major players in maritime transport and trade. Ensuring the integrity and the well-functioning of maritime transportation is critical for all economies, developed and developing alike."

Their adequate functioning is largely determined by the ability of keeping them operational and able to offer services and infrastructure to commercial vessels and other interested parties. Thus, its resilience (showcased in the graph below of Figure 7) is closely related to its capacity and capability to manage activity and maritime traffic through them.

[13] UNCTAD, 2022; 4.

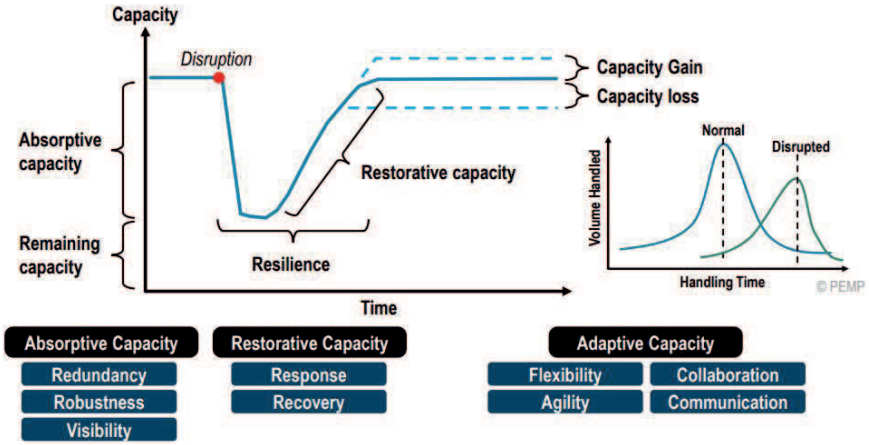


Figure 7: The Concept of Port Resilience (*Source: UNCTAD, 2022*).

In spite of their importance and the emphasis on their protection, ports are exposed to a wide plethora of risks that in turn endanger the overall resilience of the maritime shipping industry. Some of those threats are external factors, relate to the forces that generally affect the demand for maritime transport and therefore impact the volumes handled by shipping and port services. Other disruptive events that can be internal, and under the control or influence of stakeholders, such as shipping lines, port authorities and inland carriers.[14]

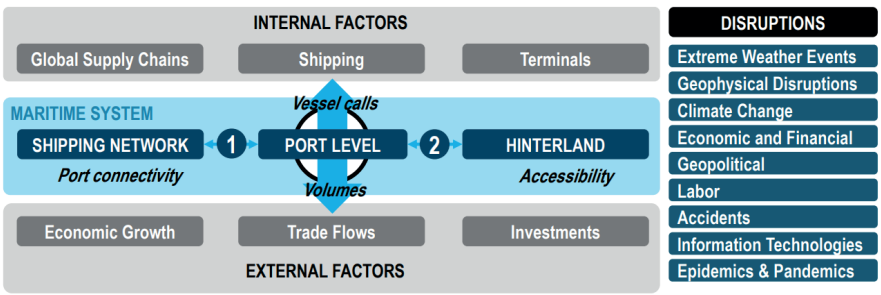


Figure 8: Ports in the maritime supply chain resilience landscape (*Source: UNCTAD, 2022*)

[14] UNCTAD, 2022; 2.

Although most disruptions tend to be local in scale and scope, there are several instances when these can become wide-ranging and affect an entire region. Some of the most prominent threats to ports' resilience, and thus, to the delivery of goods and services by the maritime shipping industry are the following:

Shipping Network: A change in a ship's routing, scheduling and service configuration can result in a decline or rise in volumes, which can negatively affect ports. A simple change in scheduling involves operational adjustments in terminal work hours and gate traffic. A port's capability to handle these changes can reflect its operational resilience.[15]

Port Level: Governance could be ineffective at the port authority, or terminal level, and could lead to delayed decision-making and responses to disruptions, particularly if the hierarchical structure of the port authority relies on only a few key managers. There could also be a lack of regulatory oversight, implying that rules and regulations are not sufficiently monitored and enforced.[16]

Cybersecurity: Maritime supply chains are increasingly relying on IT to manage operations and to transfer documentation. Such reliance increases the vulnerability of the industry to potential cyberattacks and the resulting disruptions.[17]

Environmental Impacts: Environmental conditions, such as pollutants, water contamination and noise that impair port activities and the health of the workforce. Efforts that aim to mitigate impacts or provide remedy can also result in additional burden.[18]

Safety: Theft, piracy and terrorism have come into sharp focus in recent years, especially after the events of 11 September 2001. These activities are prevalent in many ports throughout the globe, including in Europe, and can negatively impact the resilience of ports.[19]

---

[15] UNCTAD, 2022; 12.

[16] Ibid,

[17] Ibid. 13.

[18] Ibid.

[19] Ibid.

Geopolitical Events: Although this factor is addressed in the following section, which examines the Red Sea crisis in detail and its consequences for global shipping, geopolitics is also a factor to be considered in protecting ports. As the crisis in the Black Sea (also ongoing) has shown, a simple disruption in the flow of commercial activity in the ports of Ukraine threatened food security in many countries of Africa which depend on the fertilizers and the cereal exported from the region.

In sum, ports are avital element in the logistics chain of global maritime shipping, and have to be adequately protected from the wide number of threats to their proper functioning and use. Ensuring resilience of ports and providing with a solid assessment of all different risks involved is crucial to withhold both the continuity of the maritime business and global connectivity.

Implications of the Red Sea Crisis

The latest episode of maritime instability, adding to the ongoing situation in the Black Sea as a consequence of the conflict in Ukraine (which has also put at risk maritime connectivity for the last two years), is the crisis in the Red Sea following the numerous attacks by Houthi rebels in Yemen against global shipping lanes transiting through the Bab El-Mandeb Strait.

Since October 19th, 2023, and with a higher degree of intensity since December 2023, the Houthis, a military group supported by the government of Iran in the latter's efforts to attack Israel, have been engaging in unlawful attacks against commercial vessels around their coast. Yemen, astride one of the most commercially-relevant regions in the world (the maritime route that connects the Mediterranean Sea and the Indian Ocean through the Red Sea), has provided a perfect launch platform for their attacks, which have included anti-ship ballistic and cruise missiles, UAVs and USVs, and the hijacking of several vessels.[20]

Since November, the Houthis have targeted commercial vessels passing through the strait of Bab al-Mandeb, a 20 mile (32km) wide channel, while they claim to be targeting vessels with connections to Israel following the start of the war in the Gaza

[20] ALI & ZHDANNIKOV, 2024.

Strip. For all the seafarers that have been caught up in the chaos, it is not a desired experience. A tanker, for example, could carry around one million barrels of highly flammable oil, and an attack which implies an explosion onboard the ship could have disastrous effects for the crew (as well as destroying the cargo).

The interventions of three NATO countries' warships, the U.S, France and the UK (arguably the strongest navies in the Alliance at the moment), have contributed to the protection of many vessels from missile and drone attacks, with more than a hundred intercepted since October 2023. These successful interventions, however, have highlighted the acute shortfalls in NATO's anti-air warfare (AAW) capabilities.[21] Not only have the number of large surface combatants designed for AAW declined significantly since the 1990s, but more importantly, launching heavily expensive missiles to intercept the much cheaper drones will not be sustainable in the long-term.[22]

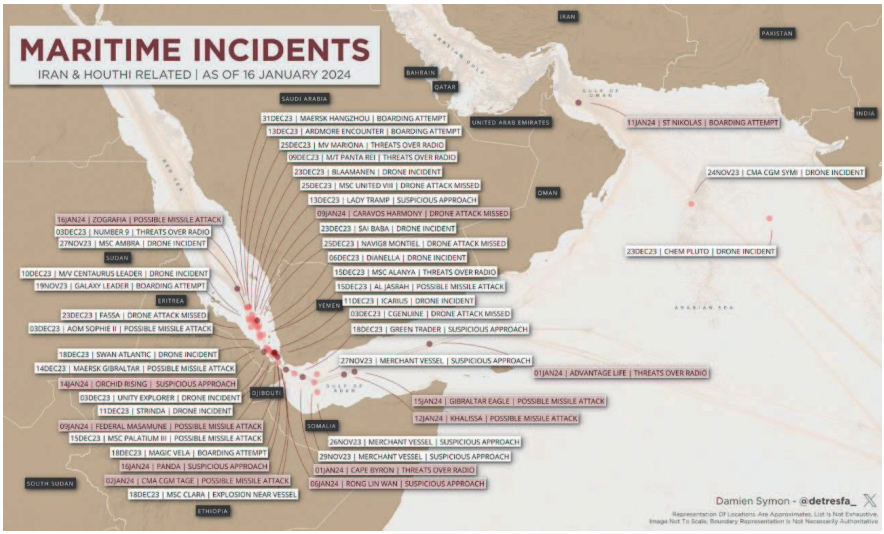


Figure 9: Summary of all maritime incidents during the Red Sea Crisis until January 16, 2024. (*Source: Damien Symon*).

These shortfalls suffered by many NATO navies could also endanger the maritime shipping industry, as the latter relies on the protection that navies provide to sea lines

[21] VÁZQUEZ, 2023.

[22] CHILDS, 2023.

of communication all over the globe. If non-state actors such as the Houthis in Yemen or any others feel that they can inflict some level of damage to maritime connectivity and the flow of maritime commerce without fearing a response against them, the number of incidents and attacks is bound to increase.

Thus, NATO navies are faced with the twofold challenge of putting additional AAW-capable surface combatants in service while finding more effective solutions to address asymmetric threats such as that of the Houthis. This could open potential avenues for development and cooperation between the private sector and the navies of the alliance for future weapon systems and security measures that can maximize the employment of naval forces against threats to Allied maritime security. As is described in the following section, one potential avenue to address these problems is to strengthen the cooperation between the maritime industry (especially the main companies such as Hapag Lloyd, Moller Maersk, MSC and others) and the navies.

As of February 2024, the main risks that have materialized with the ongoing situation in the region are the redirection of many merchant vessels to avoid transiting through the region and getting exposed to the threat of attack. These redirections imply longer routes, which translate into longer times in the delivery of cargo, and therefore, higher prices. In the case of tankers, which also comprise an important part of the shipping industry, the consequences for them can also lead to problems with the delivery of supplies, which will then affect the prices of energy in many regions.

A prominent example just prior of the delivery of this paper happened when Qatar notified the Spanish services about several LNG (liquified natural gas) shipping delays. Qatar Energy decided to take a longer route via the Cape of Good Hope (around the African continent instead of the Red Sea) due to the conflict, and informed in January to buyers in Europe, as well as some British terminals where it has long-term capacity, that it would delay or reschedule shipments.[23]

The crisis has been further aggravated by the reemergence of piracy in the Indian Ocean, around the Horn of Africa where the European Union has Operation Atalanta working to protect maritime trade. Throughout the last decades, piracy has been a major factor impacting maritime commerce around the African continent, most of which

[23] RASHAD & LOMBARDI, 2024.

delivers food and other goods in many countries of the region. This threat, combined with the consequences of the Red Sea Crisis, has the potential of causing major disruptions if not properly addressed.

They main implications of the Red Sea Crisis, which is still ongoing at the moment of finishing this paper (February 2024), will require a careful assessment on the side of the maritime companies and the national governments, extracting as many lessons learned as possible which will then have to be implemented accordingly. Section 8 reviews some of the most common ways through which risk assessment can be best leveraged, and provides with several risk management measures to help improve resilience in the maritime shipping industry in particular, and maritime connectivity in general.

Addressing the Risks and Enhancing Resilience

General Considerations

All the above discussed threats and challenges for the maritime industry and the shipping businesses require an effective avenue to address the risks involved, with a view to make them stronger and resilient into the future. The current situation of the international order suggests that more challenges lie ahead, which will further complicate the protection of maritime businesses. Thus, it behooves NATO members and any partner association involved in the sector to address these risks or at least attempt to mitigate them as much as possible.

As highlighted by Bråfelt & Larsson, the best source of knowledge and instrument to help address and prevent risks at sea is experience. In their view,

“Actual accident prevention has to be exercised hands on, at location or in designing or constructing the physical or socio-technical conditions. It comes into existence when the preventor is supplied with the relevant information, motivation and resources.”[24]

Their views suggest that a stronger emphasis should be placed upon gathering all the knowledge derived from such experiences, so that it can be then transformed into lessons learned and distributed to all companies involved in the maritime shipping industry. An initiative as such would require of a wide spectrum of experiences, in

[24] BRÅFELT & LARSSON, 2000; 3.

order to ensure that all different sectors are represented in such collection. They also suggest the establishment of an expert system for prevention on reported incident data, arguing that

“The difficulties of local accident prevention can be overcome with the linking of the local field to the national or industrial overview; if tools for local assessment are structured in the same way as collected data on national or industry level, comparisons will be possible. If tools for local risk assessment are implemented, they could also be used for local storing of information about injuries/claims.”[25]

Cargo and Container Protection

For the protection of cargo and containers aboard the ships during transits, with a view to minimize as much as possible the amount of goods that are lost at sea, there are several measures which have been put in place, and should be further developed.

The first is MARIN Top Tier Study, a project based on scientific analyses, studies and real-life measurements put in place with the aim to develop actionable and effective recommendations to increase container safety. Essentially, it has developed three types of tools that are employed to reduce prospects of future incidents:[26]

A Notice to Mariners describing the ways in which these risks can be assessed and prevented;

A series of videos that spread awareness on how the vessel may behave under several conditions, and how will the containers react in each situation; and

A Roll Risk Estimator tool, which enables the crews of the ship to make a calculation with the estimate risk of parametric rolling, based on the weather conditions that influence the sea.

The second is the revision of the IMO Guidelines for the implementation of inspection programs for cargo transport units, including containers, with the purpose of clarifying that the scope of application extends to all types of cargos (not just those classified as

[25] BRÅFELT & LARSSON, 2000; 4.

[26] IMO, 2023; 4.

dangerous), and allowing for inspection reports from non-governmental organizations to be included.[27]

Port management and protection

When it comes to ports, the other vital link in the chain of maritime connectivity and the shipping industry, risk assessment must draw a distinction among the causes of the risks (as has been discussed above noting the difference between internal or external factors, and disruptions). For external factors, which are often the hardest to influence due to the inability to affect their sources of origin (in many cases related to natural disasters or climate change), it is generally recommended to establish monitoring mechanisms and scenario analysis to inform planning and preparedness action.[28]

As was shown in Figure 8, some of the factors which can contribute to disruptions in ports include: extreme weather events, geophysical disruptions, climate change, economic and financial problems, labor, accidents, or epidemics/pandemics (as was the case with COVID-19). Thus, there are five steps which have been proposed by UNCTAD based on the analyses of past incidents and lessons learned from case studies, which have proven to be effective in the efforts of risk management and enhancing resilience:

Identification of the hazards through a list of the most likely ones;

Assessment of the vulnerability and impact of each of the hazards identified;

Elaboration of response and mitigation measures, focused on risk management, setting response strategies once a particular incident occurs;

Evaluating the costs and benefits of the selected mitigation measures, including the potential costs of inaction and their opportunity costs; and

Exercising a regular cycle of implementation, monitoring and reviewing, taking advantage of each incident happening to improve common knowledge.[29]

---

[27] Ibid, 5.

[28] UNCTAD, 2022; 3.

[29] UNCTAD, 2023; 90.

Geopolitical factors affecting trade

Lastly, geopolitical factors affecting connectivity and resilience of trade are among the hardest to address due to their unpredictability. Nevertheless, both the cases of piracy over the last decades and the ongoing situation in the Red Sea and the Gulf of Aden have left several insights as to how to better manage their potential adverse effects.

In spite of the ongoing efforts to suppress piracy in the Horn of Africa (and in the Gulf of Guinea), experience has shown that the missions deployed were not focused on treating the illness, but rather an isolated symptom (the reported cases). Thus, the first important, long-term task for protecting maritime trade in the region is to work on the issue of Somalia and other failed states around. Piracy is a consequence of Somalia being a failed state, and thus, the most important efforts are in addressing the issue of governance in Somalia.

Additionally, another potential tool which has been extensively studied but not quite as implemented has been enhancing security aboard merchant vessels. Experience has shown that many vessels do not have crews with a lot of experience when it comes to dealing with potential aggressors. Thus, many have suggested that security onboard the ships should be strengthened so as to ensure that any attempt of hijacking is more likely to be suppressed.

Conclusions & Recommendations

The maritime shipping industry is one of the most important pillars of the current global order, with most of the global commerce transiting via the sea through the global sea lines of communication (SLOCs). Shipping and ports are essential for global trade and supply chain continuity both during and outside of global/regional crises. In spite of its importance, the shipping industry remains relatively unprotected and vulnerable to several kinds of threats, the most important and prevailing of them being disruption in the flow of trade – which in turn affects many other businesses across different sectors. As has been described, maritime commerce is of particular interest as a case study of business impact analysis, as it is a business in itself, but one that depends upon many other businesses, one that connects many other businesses, and one without which the global economy would be severely constrained.

However, the causes for disruptions can come as a result of man-made activity, such as piracy or hostile attacks with the deliberate intention of damaging the vessels, or can come as a result of natural causes. The latter is, in most cases related to climate change, which can take the form of droughts, destruction of infrastructure and other damages to vital components such as ports.

When addressing the problems that may arise for the maritime industry, particularly if these can threaten the continuity of businesses involved, it is important that the solution that is found comes as a result of involving all the stakeholders: representatives of the shipping lines, ports and terminal operators, inland waterways, supply chain logistics, ship owners, vessel manufacturers and owners, custom agents. Otherwise, any measure adopted or solution that is reached will not guarantee a complete effectiveness for the entire industry.

The different attacks that have taken place over the last months of 2023 and early 2024 have affected a vast number of business sectors, as a consequence of the great reliance that most economies in the world have on maritime commerce and shipping. From car carriers to oilers to bulk carriers, more than 80% of the total volume of trade in the world travels by sea, as it is the most effective medium of transport. Yet, aside from the attacks taking place, which comprise the human side in the total amount of threats to seaborne shipping, there are also natural sources of threats which are not man-made, but are a consequence of climate change and the evolution of the natural environment.

The most prominent example of the second category is the droughts that have affected the Panama Canal almost at the same time as the crisis of the Red Sea was unfolding. Thus, some useful recommendations moving forward which should be considered are listed below.

First, national government need to be more aware about the importance of the sea in today's global geopolitics. With the drastic change that the international order has made, towards great power competition, the seas have become one of the primary arenas for their confrontation. Most great powers and relevant international actors are expanding their naval capabilities and are relying more on their sea for their economic prosperity. Thus, NATO governments must increase their awareness about the vital role of the seas for them and act accordingly to protect their maritime interests.

Secondly, once the governments are mindful about this and allocate the necessary resources to enhance the protection of their maritime interests, one of the measures to be adopted is the cooperation of its naval forces with the main shipping companies and other businesses related to the sea. Providing them with stronger lines of communication to work together could help prevent any potential incident caused by external actors, and could facilitate a faster and more effective response by the security efforts that react to the crisis.

Thirdly, on a more global scale, international organizations such as the IMO and other bodies that work with the maritime industry must extract the appropriate lessons from the Red Sea crisis and other problems that have taken place during 2023. The analysis of many of these incidents suggests that security teams aboard commercial vessels instead of just training the ships' crews to defend in case of attacks will become a more common feature for the maritime industry. The risk assessment derived from the ongoing incidents shows that many of the attempts of hijacking (both the failed and the successful ones have come as a result of a lack of protection in the vessels, making them easy targets.

Fourth, ports are a vital link in the chain of maritime connectivity, but are still vulnerable to risks. Measures such as the one proposed in this article would bring positive results if properly studied and applied. There is extensive literature describing the role they play as links that ensure connectivity and resilience in the global economy. Factors to pay special attention to are the proper handling of cargo and containers, and the strengthening of security measures to prevent smuggling and other kinds of illicit activity.

Bibliography

1. Bloch, Mark, “Building Capacity to Manage Risks and Enhance Resilience: A Guidebook for Ports”, UNCTAD, 2022. Available at: https://resilientmaritimelogistics.unctad.org/sites/resilientmaritimelogistics/files/2022-08/UNCTAD_TCS_DTL_INF_2022_3%20WEB_23%20August.pdf
2. “The Role of Business Continuity Software in Maritime Crisis Management”, https://www.crises-control.com/blogs/business-continuity-software/
3. “Maritime Crisis Management and Business Continuity”, https://maritimecyprus.com/2019/09/30/maritime-crisis-management-and-business-continuity/
4. “The Importance of Risk Assessment in Marine Operations”, Ship Mate, https://sbntech.com/marine-operations-risk-assessment/
5. IMO, “Any Other Business: Estimate of Containers lost at sea – 2023 update”, World Shipping Council, Sub-Committee on Carriage of Cargoes and Containers, CCC 9/13, 24 May 2023. Available at: https://wwwcdn.imo.org/localresources/en/MediaCentre/Documents/CCC%209-13%20-%20Estimate%20of%20containers%20lost%20at%20sea%20-%202023%20update%20(World%20Shipping%20Council%20(W...).pdf
6. “Shipping minister discusses business continuity plan with maritime industry leaders”, Hellenic Shipping News, https://www.hellenicshippingnews.com/shipping-minister-discusses-business-continuity-plan-with-maritime-industry-leaders/
7. “Risk in the Maritime Sector: Dealing skillfully with the Risk”, ClassNK Technical Journal, No. 6, 2022, https://www.classnk.or.jp/hp/pdf/research/rd/2022/06_e02.pdf
8. “Risk Assessment in the Maritime Industry”, Engineering, Technology and Applied Science Research, Vol. 7, No. 1, 2017, 1377-1381.
9. “Risk Control in the Shipping Industry: Relevant Applications for the Prevention of Accidents”, Safety Science Monitor, Vol. 4, Issue 1, Art. 3, 2000. https://www.diva-portal.org/smash/get/diva2:429881/FULLTEXT01.pdf
10. “Risk Assessment in the Shipping Industry: An Analysis of Standardized Approaches”, University of Oslo, 2009, https://www.duo.uio.no/bitstream/handle/10852/17891/Leveringsinstruks_og_forsidemal_ESST_avsluttende_merged.pdf?sequence=1&isAllowed=y
11. ALI, Idrees & Zhdannikov, Dmitry “Red Sea Attacks continue to disrupt global trade”, GCaptain, 16 January 2024. Available at: https://gcaptain.com/another-bulk-carrier-hit-in-the-red-sea/ (Accessed 20 January 2024).
12. Vázquez, Gonzalo “NATO Must be Ready for High-Intensity Naval Conflict”, CEPA, 11 December 2023. Available at: https://cepa.org/article/nato-must-be-ready-for-high-intensity-naval-conflict/ (Accessed 20 January 2024).

13. Childs, Nick “Global implications of the shipping attacks in the Red Sea”, IISS, 19 December 2023. Available at: https://www.iiss.org/online-analysis/online-analysis/2023/12/global-implications-of-the-shipping-attacks-in-the-red-sea/ (Accessed 20 January 2024).

14. “Red Sea crisis: What it takes to reroute the world's biggest cargo ships on a 4,000-mile detour”, BBC, 19 January 2024. Available at: https://www.bbc.com/future/article/20240119-red-sea-crisis-how-global-shipping-is-being-rerouted-out-of-danger
15. Rashad, Marwa & LOMBARDI, Pietro “Qatar notifies Spanish Utility of LNG Shipping Delay”, GCaptain, 25 January 2024. Available at: https://gcaptain.com/qatar-notifies-spanish-utility-of-lng-shipping-delay/
16. Bryant, Dennis Resilience and the Maritime Industry, Maritime Reporter, 2023. Available at: https://magazines.marinelink.com/Magazines/MaritimeReporter/201503/content/resilience-maritime-industry-488266

RESILIENCE AND STRATEGIC COMMUNICATIONS

Tsveti MONOVA

Abstract: Resilience and strategic communication are vital for effectively facing challenges. This research contributes to the discourse on resilience by unveiling a foundational framework for products aimed at practical implementation. Focused on fostering resilience, the study underscores the importance of objective logic, a thorough comprehension of the subject matter, and the incorporation of standardized operating procedures (SOP). Through an exploration of these key elements, the research seeks to provide a nuanced understanding of the multifaceted nature of resilience and to offer insights that can guide the development and application of products.

Introduction

Communication, in its multifaced forms, serves as the heart of organizations, societies, and nations. In an age marked by the dynamic changes, unpredictability, turbulence, and rapid transformation, the ability of communication strategies to withstand and adapt to unforeseen challenges has become paramount. Resilience, the capacity to anticipate, withstand, recover from, and adapt to adversity, emerges as a fundamental attribute within this dynamic landscape of strategic communications.

This research embarks on a comprehensive exploration of the intricate interplay between resilience and strategic communications. It delves deep into the fabric of existing procedures and practices prevalent in the realms of public relations, corporate communication, crisis management, and beyond. The primary objective has the task to identify the current state of affairs in communication strategies and to critically analyze these practices through the lens of resilience.

The urgency of this inquiry lies in the realization that conventional approaches to communication, while robust in structured environments, often lose strength in the face of unforeseen disruptions. A global crisis altering market landscapes, a social media storm igniting controversies, or a sudden technological advancement transforming communication paradigms, the fragility of static strategies becomes starkly evident.

By taking a close look at the current situation and circumstances procedures, this study seeks to uncover that what was not easily noticeable such as nuances, intricacies, and potential vulnerabilities within existing communication frameworks. It aims to take apart and closely inspect each element such as strategies, tools, methodologies, and underlying philosophies guiding current practices, thus illuminating the strengths and limitations inherent in their ability to pivot amidst the circumstances.

Moreover, this research endeavors not merely to diagnose but to prescribe. It endeavors to synthesize the findings into actionable insights, crafting a roadmap for bolstering resilience within strategic communications. Through the identification of gaps, discrepancies, and areas ripe for improvement, this project aims to generate innovative proposals poised to fortify communication strategies against the unpredictable tides of the contemporary landscape.

The significance of this endeavor lies not solely in its academic or theoretical implications but in its real-world impact. The insights garnered from this research endeavor hold the potential to reshape how organizations, governments, and entities across diverse sectors approach communication. The resulting recommendations aspire to empower practitioners with adaptive, agile, and resilient communication strategies fit for navigating the intricate web of modern challenges.

- In essence, this research project serves as a clarion call to rethink, reimagine, and revolutionize the paradigms governing strategic communications. It seeks to elevate resilience from a mere theoretical construct to a practical cornerstone upon which robust, agile, and future-proof communication strategies are built.

Through meticulous inquiry, critical analysis, and innovative propositions, this research endeavors to usher in a new era where communication is not just a conduit of information but a resilient bastion that fortifies entities against the turbulent currents of an ever-evolving world.

Where does Resilience come from?

Resilience, as defined by the American Psychological Association (APA), encompasses the dynamic process and positive result of effectively navigating and adapting to life's tough or demanding situations. According to the APA, it involves

possessing the mental, emotional, and behavioral flexibility required to cope with challenges arising from both internal and external sources[1].

In simpler terms, resilience is your capability to endure and rebound from adversity, fostering personal growth despite the setbacks that life may throw at you. As explained by Dr. Amit Sood, the executive director of the Global Center for Resiliency and Well-Being – Resilience it's the ability to withstand life's hardships and emerge stronger, displaying adaptability and growth in the face of difficulties[2].

- The journey toward resilience is a dynamic one, where individuals learn and grow through experiences, adapting to challenges and building strength along the way.

Resilience theory explores how individuals are impacted by and adapt to adversity, change, loss, and risk. This theory has been examined in various fields, including psychiatry, human development, and management[3]. It emphasizes that resilience is not a fixed trait - individuals can cultivate and expand their capacity for resilience over time. An individual may demonstrate considerable resilience in one situation but struggle more in another[4].

Flexibility, adaptability, and perseverance play key roles in resilience by influencing thoughts and behaviors. Research indicates that people who believe in the potential for the development and improvement of both intellectual abilities and social attributes demonstrate increased resilience. This belief system leads to lower stress responses in the face of adversity and improved overall performance[5]. In essence, resilience is not only about enduring challenges but also about actively developing the skills and attitudes that contribute to facing life's difficulties with strength and adaptability[6].

---

[1] American Psychological Association, n.d. Resilience. [online] Available at: https://www.apa.org/topics/resilience

[2] Sood, A., 2021. The Science of Resilience. Global Center for Resiliency and Well-Being. [online] Available at: https://www.resiliencycenter.com

[3] Masten, A.S., 2014. Global perspectives on resilience in children and youth. Child Development, 85(1), pp.6-16.

[4] Reich, J.W., 2006. Theoretical perspectives on resilience. In: M.C. Masten, ed., Resilience in Children, Families, and Communities. Cambridge University Press, pp.1-30.

[5] Dweck, C.S., 2006. Mindset: The New Psychology of Success. Random House.

[6] Dweck, C.S., 2006. Mindset: The New Psychology of Success. Random House.

Resilience comes in various forms, addressing different aspects of an individual's or community's ability to face challenges:

- Psychological Resilience:

Psychological resilience refers to the mental ability to cope with uncertainty, challenges, and adversity. Individuals with psychological resilience develop coping strategies that help them stay calm and focused during crises, avoiding long-term negative consequences like distress and anxiety. It's often referred to as "mental fortitude"[7].

- Emotional Resilience:

Emotional resilience involves how individuals cope with stress and adversity on an emotional level. It varies among individuals, with some naturally more or less sensitive to change. Emotionally resilient people understand their feelings, use realistic optimism during crises, and proactively tap into both internal and external resources to manage stressors positively[8].

- Physical Resilience:

Physical resilience is the body's ability to adapt to challenges, maintain stamina and strength, and recover efficiently. It encompasses the capacity to function effectively and recover from illness, accidents, or other physical demands. Healthy lifestyle choices, social connections, relaxation techniques, and engaging in enjoyable activities contribute to physical resilience, playing a crucial role in healthy aging[9].

- Community Resilience:

Community resilience refers to the collective ability of groups of people to respond to and recover from adverse situations that impact the community as a whole. It is demonstrated in the collective response to challenges like natural disasters, acts of

---

[7] American Psychological Association, n.d. Resilience. [online] Available at: https://www.apa.org/topics/resilience

[8] Masten, A.S., 2014. Global perspectives on resilience in children and youth. Child Development, 85(1), pp.6-16.

[9] Sieber, J.E., 2006. The Role of Physical Resilience in Health and Well-Being. Academic Press.

violence, economic hardship, and other crises. Real-life examples include the resilience of communities such as New York City after 9/11 and New Orleans following Hurricane Katrina. Community resilience is essential for the survival and recovery of communities facing significant challenges[10].

As the world faces unprecedented events, like the COVID-19 pandemic, understanding and developing these different forms of resilience become crucial. Individuals need psychological, emotional, and physical coping mechanisms, while communities must demonstrate collective strength in the face of adversity[11].

Resilience defined by NATO:

NATO's focus on resilience has evolved over time, but it gained significant prominence and became an active procedure in the aftermath of various global events that highlighted the importance of adaptability and preparedness against diverse threats. The concept of resilience within NATO has been increasingly emphasized and actively integrated into strategies, doctrines, and exercises, particularly in the last decade[12].

The alliance started to formally address resilience as a critical aspect of security following events like, the stated earlier in this project, 9/11 terrorist attacks and subsequent security challenges that highlighted the need for a comprehensive approach beyond traditional defense strategies. However, the exact timeline of when resilience became an active procedure within NATO's operations can be traced to more recent years, notably after the Wales Summit in 2014 and subsequent summits[13].

The Wales Summit Declaration in 2014 marked a significant shift for NATO, where member states acknowledged the importance of resilience as a key component of collective defense. This declaration emphasized the necessity for member nations to

---

[10] Norris, F.H., Stevens, S.P., Pfefferbaum, B., Wyche, K.F., and Pfefferbaum, R.L., 2008. Community resilience as a metaphor, theory, set of capacities, and strategy for disaster readiness. American Journal of Community Psychology, 41(1-2), pp.127-150.

[11] Bonanno, G.A., 2004. Loss, trauma, and human resilience. American Psychologist, 59(1), pp.20-28.

[12] NATO, 2014. Wales Summit Declaration. [online] Available at: https://www.nato.int/cps/en/natolive/official_texts_112956.htm

[13] NATO, 2018. Brussels Summit Declaration. [online] Available at: https://www.nato.int/cps/en/natolive/official_texts_156624.htm

enhance their resilience capacities, particularly in areas such as cybersecurity, energy security, critical infrastructure protection, and civil preparedness[14].

Since then, NATO has progressively integrated resilience into its strategic thinking, policy frameworks, and exercises. Subsequent summits and strategic initiatives, such as the Brussels Summit in 2018, further underscored the importance of resilience in countering hybrid threats, strengthening civil preparedness, and enhancing alliance-wide capabilities[15].

Therefore, while the concept of resilience has been part of NATO's considerations for some time, its formal recognition and active integration into procedures and policies have notably intensified in the past decade, responding to a rapidly evolving security landscape and the emergence of new and multifaceted threats[16][17][18].

NATO defines resilience as a comprehensive and dynamic capability essential for anticipating, preparing for, responding to, and recovering from an extensive spectrum of challenges and disruptions. It embodies the agility to adapt swiftly to evolving and multifaceted threats, acknowledging the interconnectedness of vulnerabilities across various domains[19].

Resilience within NATO's paradigm extends beyond the mere anticipation of potential risks; it entails proactive measures to fortify critical infrastructure, enhance societal resilience, and foster collaboration between civilian and military entities. This approach aims to establish robust backup systems, ensuring the continuity of essential services

---

[14] NATO, 2018. Brussels Summit Declaration. [online] Available at: https://www.nato.int/cps/en/natolive/official_texts_156624.htm

[15] NATO, 2021. NATO's Resilience Framework. [online] Available at: https://www.nato.int/cps/en/natolive/topics_82734.htm

[16]NATO, 2014. Wales Summit Declaration. [online] Available at: https://www.nato.int/cps/en/natolive/official_texts_112956.htm

[17] NATO, 2018. Brussels Summit Declaration. [online] Available at: https://www.nato.int/cps/en/natolive/official_texts_156624.htm

[18] NATO, 2021. NATO's Resilience Framework. [online] Available at: https://www.nato.int/cps/en/natolive/topics_82734.htm.

[19] NATO, 2020. Resilience in NATO. [online] Available at: https://www.nato.int/cps/en/natolive/topics_156604.htm

and governmental functions even amid the most demanding and unpredictable circumstances[20].

Integral to this resilience framework is a strategic emphasis on comprehensive risk management strategies, encompassing proactive measures to mitigate vulnerabilities and potential impacts. Such a proactive stance not only safeguards against systemic risks but also enables swift response and recovery, minimizing disruptions to essential services[21].

Moreover, NATO places a significant premium on solidarity and cooperation among member states and partner nations. Recognizing the collective strength derived from shared resilience efforts, the alliance fosters collaboration, resource sharing, and mutual support to collectively strengthen the security posture of all participating nations. This collaborative approach enhances readiness, responsiveness, and adaptability, aligning with the evolving challenges of today's complex security landscape[22].

In essence, NATO's resilience framework embodies a proactive and interconnected approach, emphasizing not just preparedness but also adaptability and collective strength to confront and overcome multifaceted challenges and disruptions.

As of last information in January 2022, the North Atlantic Treaty Organization has been actively involved in enhancing its resilience procedures and practices, particularly in response to evolving security challenges and the changing nature of threats. These are NATO’s key resilience baseline requirements:

- assured continuity of government and critical government services;
- resilient energy supplies;
- ability to deal effectively with uncontrolled movement of people;
- resilient food and water resources;
- ability to deal with mass casualties;

---

[20] NATO, 2022. Strategic Concepts and Resilience. [online] Available at: https://www.nato.int/cps/en/natolive/topics_82732.htm

[21] NATO, 2021. Comprehensive Risk Management in NATO. [online] Available at: https://www.nato.int/cps/en/natolive/topics_82731.htm.

[22] NATO, 2022. Solidarity and Cooperation among Member States. [online] Available at: https://www.nato.int/cps/en/natolive/topics_82730.htm

- resilient civil communications systems;
- resilient civil transportation systems[23].

NATO's commitment to resilience extends across diverse domains, reflecting a comprehensive strategy to address emerging challenges, foster cooperation, and ensure the security and stability of member nations and partner countries alike[24].

Baseline requirements grouped into services and abilities are outlined as:

SERVICES:

- Assured Continuity of Government and Critical Government *Services*: This involves the capacity to make crucial decisions and maintain communication with citizens during a crisis, ensuring governance functions persist even under challenging conditions[25].
- Resilient Energy Supplies *Service*: Ensuring a continuous and secure energy supply, including contingency plans to manage disruptions, safeguarding against potential energy-related threats[26].
- Resilient Food and Water Resources *Service*: Establishing resilient supply chains for food and water, safeguarding these essential resources from disruptions or sabotage to ensure the population's sustenance and safety[27].
- Resilient Civil Communications Systems *Service*: Guaranteeing that telecommunications and cyber networks remain operational during crises, including the provision of backup capacities. This encompasses robust systems such as 5G,

[23] NATO, 2022. Baseline Resilience Requirements. [online] Available at: https://www.nato.int/cps/en/natolive/topics_82729.htm

[24] NATO, 2022. Baseline Resilience Requirements. [online] Available at: https://www.nato.int/cps/en/natolive/topics_82729.htm

[25] NATO, 2022. *Resilience and Article 3*. [online] Available at: https://www.nato.int/cps/en/natolive/topics_132722.htm

[26] NATO Parliamentary Assembly, 2021. *Report on Enhancing NATO's Resilience*. [pdf] Available at: https://www.nato-pa.int/document/2021-report-enhancing-natos-resilience

[27] Bailey, R., 2019. The Role of Strategic Communications in NATO's Hybrid Warfare. *NATO Review*, [online] Available at: https://www.nato.int/docu/review/articles/2019/06/20/the-role-of-strategic-communications-in-natos-hybrid-warfare/index.html

restoration plans, priority access for national authorities during emergencies, and comprehensive risk assessments for communication systems[28][29].

- Resilient Transport Systems *Service*: Ensuring reliable transportation networks for both NATO forces' rapid movement across Alliance territories and civilian services, even in crisis scenarios[30].

ABILITIES:

- *Ability* to Deal Effectively with Uncontrolled Movement of People: Developing capabilities to manage and control unanticipated movements of individuals, segregating these movements from NATO's military deployments to maintain operational integrity[31].
- *Ability* to Manage Mass Casualties and Disruptive Health Crises: Equipping civilian health systems to effectively handle mass casualties and disruptive health crises, ensuring sufficient medical supplies, readiness, and security of healthcare resources[32].

These services and abilities collectively form the baseline requirements, emphasizing the necessity of continuity, resilience, and effective management across critical areas to ensure the maintenance of essential functions, services, and safety even in the most challenging circumstances[33][34].

---

[28] Department of Homeland Security (DHS), 2020. National Critical Functions and Resilience Requirements. [online] Available at: https://www.dhs.gov/national-critical-functions

[29] NATO Communications and Information Agency, 2021. Cyber Resilience and NATO. [online] Available at: https://www.nato.int/cps/en/natolive/topics_128390.htm

[30] NATO, 2020. Transport and Logistics in NATO Operations. [online] Available at: https://www.nato.int/cps/en/natolive/topics_82742.htm

[31] NATO, 2019. Managing Migration and Humanitarian Crises. [online] Available at: https://www.nato.int/cps/en/natolive/topics_84325.htm

[32] NATO, 2018. Medical Support and Mass Casualty Management. [online] Available at: https://www.nato.int/cps/en/natolive/topics_149026.htm

[33] NATO, 2014. Wales Summit Declaration. [online] Available at: https://www.nato.int/cps/en/natohq/official_texts_112964.htm

[34] NATO, 2018. Brussels Summit Declaration. [online] Available at: https://www.nato.int/cps/en/natohq/official_texts_156624.htm

Grouping the baseline requirements into services and abilities offers several advantages:

- **Clarity and Organization:** Grouping these requirements helps in categorizing and organizing complex elements into distinct service-oriented and ability-focused clusters. This aids in understanding and visualizing the critical areas that need attention[35].
- **Strategic Focus:** By organizing them into services and abilities, it helps in directing strategic attention to specific functional areas rather than treating them as isolated entities[36].
- **Interconnectedness Recognition:** Highlighting the interconnection among these requirements becomes clearer when grouped. It emphasizes how a deficiency or impact in one area might affect or compromise another, enabling a more comprehensive approach to resilience planning[37].
- **Prioritization and Resource Allocation:** Grouping allows for better prioritization and resource allocation based on the criticality of services and abilities. It aids in identifying where resources, investments, and efforts need to be concentrated for optimal resilience building.
- **Comprehensive Assessment:** This categorization facilitates a more comprehensive assessment of each service or ability area. It allows for a detailed analysis of vulnerabilities, risk assessments, and readiness levels within each category[38].
- **Strategic Planning and Preparedness:** It aids in devising strategic plans and preparedness measures specific to each service or ability area. This approach ensures a more tailored and focused response in enhancing resilience across critical sectors[39].

---

[35] Boin, A., 2019. Resilience and Governance: A Research Agenda. International Review of Administrative Sciences, 85(1), pp.191-205.

[36] Tierney, K., 2014. The Social Roots of Risk: Producing Disasters, Promoting Resilience. Stanford University Press

[37] Adger, W.N., 2000. Social and ecological resilience: are they related? Progress in Human Geography, 24(3), pp.347-364.

[38] Wildavsky, A., 1988. Searching for Safety. Transaction Publishers.

[39] Bonanno, G.A., 2004. Loss, trauma, and human resilience. American Psychologist, 59(1), pp.20-28.

- **Communication and Collaboration:** Using these groupings can facilitate clearer communication and collaboration among various stakeholders, allowing for a shared understanding and coordinated efforts in addressing resilience needs within each category[40].

Grouping the baseline requirements into services and abilities provides a structured framework for resilience planning, ensuring a more systematic, focused, and interconnected approach to addressing critical functions and capabilities in challenging circumstances.

Strategic Communications in NATO Resilience

Strategic communications within NATO's resilience framework encompass a multifaceted approach aimed at bolstering the alliance's ability to anticipate, withstand, and recover from diverse challenges and threats. This involves countering disinformation, fostering public confidence, crisis communication, coordinated messaging, information sharing, adaptive strategies, and civil-military cooperation[41]. Within this framework:

- Countering Disinformation involves proactive messaging, debunking false narratives, and promoting accurate information to combat attempts at sowing discord or manipulating public opinion.
- Fostering Public Confidence aims to maintain trust in the alliance's capabilities and decisions by transparent communication, engagement, and providing accurate information during crises.
- Crisis Communication becomes vital during high-stress situations, ensuring rapid, clear, and coordinated messaging to member states, partners, and the public to manage perceptions and reduce uncertainty.

---

[40] NATO, 2022. Resilience and Article 3. [online] Available at: https://www.nato.int/cps/en/natolive/topics_132722.htm

[41] Bailey, R., 2019. The Role of Strategic Communications in NATO's Hybrid Warfare. NATO Review, [online] Available at: https://www.nato.int/docu/review/articles/2019/06/20/the-role-of-strategic-communications-in-natos-hybrid-warfare/index.html

- Coordinated Messaging emphasizes alignment among member states to convey consistent narratives, goals, and responses, avoiding conflicting or confusing messages.
- Information Sharing strengthens collective resilience by facilitating collaboration, sharing best practices, intelligence, and lessons learned against emerging threats.
- Adaptive Strategies involve continually evolving communication approaches leveraging innovative technologies to effectively engage diverse audiences.
- Civil-Military Cooperation ensures a unified approach, leveraging military and civilian expertise for effective communication strategies.

This holistic approach to strategic communications serves as a critical component of NATO's resilience framework, enhancing its ability to respond effectively to multifaceted challenges while fostering unity, trust, and informed decision-making across member states and partners.

Gaps:

Identifying specific gaps in NATO's strategic communications within its resilience framework might involve areas where improvements or enhancements could further strengthen the alliance's capabilities. Some potential gaps could include:

- The need for more agile and adaptive communication strategies to respond effectively to rapidly evolving and multifaceted threats, including emerging technologies used in hybrid warfare or cyberattacks.
- Ensuring seamless coordination and consistency in messaging across member states, avoiding conflicting narratives or information gaps during crises or high-stress situations.
- Strengthening engagement and trust-building efforts, especially in reaching diverse audiences, countering disinformation, and enhancing public understanding of NATO's objectives and values.
- Enhancing the utilization of innovative communication technologies and tools for monitoring and engaging across various digital platforms and media channels to effectively reach and influence target audiences.

- Strengthening crisis preparedness and rapid response mechanisms, ensuring timely and coordinated communication during emergencies to manage perceptions, reduce uncertainty, and disseminate accurate information.
- Instituting robust evaluation mechanisms to assess the effectiveness of communication strategies, incorporating feedback loops, and adapting strategies based on lessons learned and best practices.

Identifying and addressing these gaps would contribute to enhancing NATO's strategic communications within its resilience framework, ensuring a more comprehensive, adaptive, and effective approach to communication in the face of diverse and evolving security challenges.

Proposals of improvement

Addressing gaps in NATO's strategic communications within its resilience framework requires targeted strategies and proposals for improvement:

Implement agile communication frameworks that allow for quick adjustments in response to emerging threats. Regularly assess and update communication strategies based on real-time threat intelligence.

Establish a centralized communication hub to coordinate messaging across member states. Develop communication protocols and guidelines for consistent narratives during crises.

Enhance public engagement through interactive platforms, town halls, and targeted campaigns. Collaborate with civil society, media, and academia to amplify authentic narratives and build trust.

Conduct joint exercises and training programs involving both civilian and military communicators. Foster a culture of collaboration and mutual understanding across these sectors.

Invest in cutting-edge communication tools and analytics to monitor and engage across digital platforms. Develop tailored content for different demographics and regions.

Create predefined crisis communication protocols and dedicated response teams. Conduct regular drills to test communication strategies and response mechanisms.

Establish a continuous evaluation framework to measure the impact of communication strategies. Use feedback mechanisms to iterate and refine approaches based on lessons learned.

Implementing these proposals would enhance NATO's strategic communications by fostering adaptability, coherence, engagement, and effectiveness in addressing identified gaps within its resilience framework. Regular assessment, collaboration, and innovation are essential for continually improving communication strategies and ensuring the alliance's readiness in a rapidly evolving security landscape.

Resilience in NATO can be enhanced by addressing gaps in areas such as cybersecurity, infrastructure protection, and rapid response capabilities. Strengthening cooperation with non-NATO partners and improving intelligence-sharing mechanisms can also bolster resilience. Additionally, investing in cutting-edge technologies and conducting regular joint exercises can help NATO adapt to evolving threats and challenges.

To enhance NATO's resilience effectively, consider the following strategies:

Establish a Joint Cybersecurity Task Force:

Create a dedicated task force focused on cybersecurity, composed of experts from member states. This team can collaborate on developing and implementing advanced cybersecurity measures, sharing threat intelligence, and conducting joint exercises to test and improve defences.

Implement Resilience Standards for Critical Infrastructure:

Develop and enforce standardized resilience criteria for critical infrastructure across NATO member states. This can involve creating guidelines, providing resources for infrastructure upgrades, and establishing a monitoring system to ensure compliance.

Enhance Rapid Response Coordination:

Improve rapid response capabilities by establishing a centralized coordination centre for quick decision-making and deployment. This could involve regular joint training

exercises, sharing best practices, and investing in technologies that enable swift communication and mobilization.

Enhance Strategic Communication and Public Awareness: Strengthen strategic communication by establishing a centralized information hub to counter disinformation. Develop public awareness campaigns to educate citizens about NATO's role, fostering support and resilience against external influence.

Facilitate Interoperability Programs: Implement programs to enhance interoperability among member states. This includes joint training exercises, standardizing communication protocols, and investing in technologies that facilitate seamless coordination during military operations.

Conduct Hybrid Warfare Training and Simulation: Develop comprehensive training programs to prepare NATO forces for hybrid warfare scenarios. Simulate various combinations of conventional and unconventional threats to improve readiness and adaptability.

Promote Information Sharing with Allies and Partners: Strengthen information-sharing mechanisms with allies and partners, extending NATO's resilience network. This collaborative approach can enhance collective security and ensure a more comprehensive response to emerging challenges.

Establish Innovation Hubs for Emerging Technologies: Create innovation hubs to explore and adopt emerging technologies. Encourage collaboration with private industries and academia to stay at the forefront of technological advancements, ensuring NATO remains adaptive to evolving threats.

* To successfully implement the strategies for enhancing NATO's resilience, a diverse range of experts and staff members for effective collaboration and communication are needed.

To apply a power tool in this dynamic new and modern world where technologies are used let's conceptualize Resilience in NATO as an IT system using elements arranged in a circular system.

Desired State (Goal): At the core of the system is the Desired State, representing NATO's ideal state of resilience. This could include aspects like robust

cybersecurity, rapid response capabilities, and effective communication channels.

Control: The Control element surrounds the Desired State, symbolizing the mechanisms and protocols in place to maintain and safeguard the resilience of NATO. This includes policies, regulations, and strategic planning.

Actor (Doer): The Actor is positioned outside the Control layer, representing the entities responsible for maintaining and enhancing resilience. This includes NATO member countries, military units, and relevant agencies.

Object (Internal Impact): Moving outward, the Object layer signifies the areas within NATO that might be impacted internally. This could range from cyber threats to logistical challenges or geopolitical shifts.

Essential Needs: Beyond the Object layer, we have the Essential Needs, representing the fundamental requirements for resilience. This might encompass technology, intelligence sharing, cooperation among member nations, and adaptability.

Sensors: Positioned on the outer edge, Sensors symbolize the monitoring and early warning systems in place. These could include cyber threat detection tools, intelligence gathering mechanisms, and other surveillance systems.

Current State: The Current State completes the circle, depicting NATO's present level of resilience. This is influenced by the feedback loop from the Sensors, the effectiveness of the Essential Needs being met, and the actions taken by the Actors.

In this circular system, information flows both ways. The Sensors provide real-time data on the Current State, which informs the Actors about potential threats or vulnerabilities. The Actors then take actions within the framework of the Control layer to bring the system closer to the Desired State. This circular model emphasizes the dynamic and continuous nature of resilience in NATO, highlighting the need for constant monitoring, adaptation, and collaboration.

In the dynamic system of Resilience within NATO as an IT framework, a continuous loop unfolds, fostering learning and progress with each iteration.

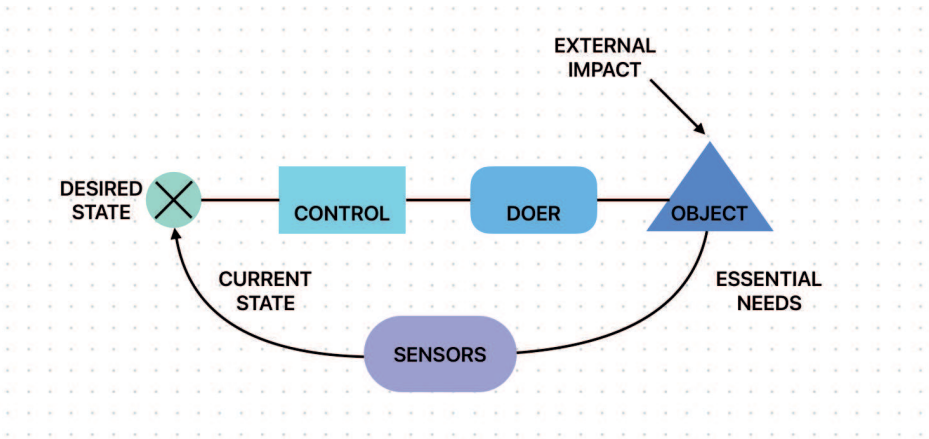


Figure 1

At its core, the Desired State encapsulates NATO's ideal resilience – a state of robust cybersecurity, swift response capabilities, and seamless communication channels. Surrounding this core is the Control layer, representing the mechanisms and protocols preserving and enhancing resilience.

Beyond this, the Actor – comprising NATO member countries, military units, and relevant agencies – takes on the role of implementing actions. External to this layer lies the Object, signifying the internal impact areas, ranging from cyber threats to logistical challenges.

Further out, the Essential Needs layer embodies the fundamental requirements for resilience, including technology, intelligence sharing, cooperation among member nations, and adaptability. The outer layer, Sensors, symbolizes monitoring and early warning systems like cyber threat detection tools and surveillance mechanisms.

Completing the circle, the Current State reflects NATO's present resilience level, influenced by the feedback loop from Sensors, Essential Needs fulfillment, and Actor actions. This cyclical operation creates a continuous learning process:

Data collected by Sensors undergoes analysis through advanced analytics and machine learning, identifying patterns and trends. The system autonomously adapts its strategies within the Control layer based on this analysis.

Decisions and interventions by the Actors lead to changes, shaping a new Current State that represents an evolved system. Essential Needs are optimized based on the effectiveness of various components, reflecting the system's learning.

Actors, whether human or automated, become more adaptive and responsive, learning from past experiences. This iterative learning cycle ensures the system becomes progressively more adept at anticipating, preventing, and mitigating challenges.

Knowledge gained from each iteration is transferred, creating a repository that informs subsequent cycles. This iterative learning process transforms the system into a dynamic, adaptive entity, evolving in response to changing circumstances.

* The implementation of such a comprehensive system is imperative to bolster and address the gaps in NATO's resilience. This integrated framework, encapsulating Desired State, Control mechanisms, Actor actions, Object impacts, Essential Needs, Sensors, and Current State, serves as a critical support structure. It serves as a Strategic Asset!

To sum up by adopting this system, NATO can proactively monitor and adapt to emerging threats, fostering a continuous learning cycle. The Control layer ensures robust governance and strategic planning, allowing for agile responses to evolving challenges. Actors, including member countries and agencies, operate within a well-defined framework, enhancing coordination and collaboration.

The system's focus on internal impacts (Object) and fulfillment of Essential Needs helps identify and rectify vulnerabilities, addressing gaps that may compromise resilience. Sensors provide real-time data, enabling early detection and response to potential threats.

As the system iterates, machine learning and analytics drive continuous improvement. Adaptive Actors learn from past experiences, refining strategies and actions. The optimization of Essential Needs reflects an evolving understanding of what is most effective in maintaining resilience.

In essence, this system becomes a vital tool for NATO to not only fortify its resilience but also to actively learn, adapt, and progress in the face of dynamic and multifaceted

challenges. It fills critical gaps, ensuring a comprehensive and evolving approach to maintaining the desired level of resilience within the alliance.

Why is it necessary to give people a certain direction?

Guiding people on resilience is crucial for several reasons:

- Empowerment: Offering practical strategies empowers individuals, fostering a sense of control over responses to adversity.
- Education and Awareness: Many may not be familiar with resilience, so guidance raises awareness and educates on its importance.
- Crisis Preparation: Resilience guidance prepares individuals for potential crises, equipping them with the mindset and skills to cope effectively.
- Community Building: Guidance on resilience helps communities come together, organize resources, and respond collectively to challenges.
- Adaptability to Change: Resilience guidance helps individuals and communities adapt more effectively to life's changes.
    * Providing guidance on resilience is essential for empowering individuals, raising awareness, preparing for crises, building community strength and fostering adaptability in the face of change. It serves as a roadmap for individuals and communities to navigate the complexities of life with greater strength and resilience.
    * To show the path to resilient way of living while dealing with challenges NATO needs standard which Resilience committee to approve and look forward to a more effective dealing with this yet again called – dynamically changing world in which we are living.

Simulation in resilience for individuals from the society

Simulation stands as a proactive tool in building resilience, offering a controlled space for individuals and communities to develop skills, practice responses, and navigate challenging scenarios. This approach, through repeated practice, aids in skill refinement, stress tolerance, crisis preparedness, and team building. Simulations

provide valuable feedback, fostering continuous improvement, and act as catalysts for positive behavioral changes. Moreover, they empower participants with a sense of confidence, contributing to overall psychological resilience. In essence, simulations serve as dynamic, adaptive platforms for individuals and communities to fortify themselves against the uncertainties of real-life challenges.

Simulation for NATO

NATO's reliance on simulation extends beyond routine training; it serves as a cornerstone in the alliance's resilience strategy. Simulations offer a realistic and controlled environment for military and allied forces to practice responses to various security challenges, fostering preparedness and coordination. They play a pivotal role in crisis management, allowing NATO to refine strategies and evaluate its ability to respond effectively. Interoperability testing ensures seamless collaboration among member states, enhancing the alliance's overall effectiveness. As security threats evolve, simulations enable NATO to adapt strategies and identify vulnerabilities. In the complex landscape of hybrid warfare, simulations assess and fortify NATO's resilience against multifaceted challenges. Ultimately, these simulations contribute significantly to NATO's strategic readiness and decision-making capabilities in an ever-changing global security landscape.

A reactive approach becomes crucial when faced with the immediate effects of a crisis or threat, necessitating swift response, damage control, and stabilization of the situation. On the other hand, a proactive approach involves preparing for potential future challenges by identifying risks, implementing preventive measures, and developing strategies for early intervention. Models and simulations play a vital role in both approaches, aiding in the preparation of personnel and testing response plans for immediate crisis management. Simultaneously, they contribute to strategic planning by allowing organizations to model potential scenarios, assess risks, and refine strategies for future challenges, fostering a culture of adaptive learning.

* We will react more rapidly to the challenges when SIMULATION is given as a tool of learning how to be more resilient.

Before delving into building resilience through skills and measures, it is imperative to have a precise and well-defined understanding of what resilience truly means. Without a clear definition, strategic communication efforts may lack effectiveness as they hinge on a shared understanding of the concept. A precise definition of resilience forms the foundation for strategic planning, communication, and the development of targeted measures, ensuring that efforts are aligned with a common understanding and goal.

To summarize, clarity in defining resilience is fundamental for laying the groundwork necessary for effective communication and subsequent resilience-building initiatives.

To synthesize, recognizing the diverse types of resilience is crucial, but for NATO, the effective integration of technology and simulation tools is paramount. The dynamic and multifaceted nature of modern challenges necessitates a proactive approach, and these tools provide a controlled environment for training, planning, and adapting strategies. Moreover, the clear definition and understanding of the seven basic requirements for resilience are fundamental. Without a shared comprehension of the concept, effective management and the achievement of excellent, rapid results become elusive. Therefore, the synergy of well-defined resilience requirements, technology, simulation, and a comprehensive understanding of resilience is indispensable for NATO's ability to navigate the complexities of contemporary security challenges.

Conclusion

The study has laid the foundation for the practical implementation of resilience by highlighting key areas where improvements are necessary. Effective resilience management requires a clear understanding of objective logic, standardized operating procedures (SOPs), and a comprehensive framework for addressing various needs. This is reflected in the three pie charts—recent, , service-oriented and ability-based — each crucial for daily resilience needs *(Figure 2,3,4).* While one component might be available, others need to be activated to fully utilize existing procedures and management systems on a broader scale.

It is essential to distinguish between services and systems, as they are not interchangeable and need to be defined accordingly. This distinction is crucial for determining whether we adequately cover all necessary sectors to achieve resilience.

Currently, there seems to be a gap in covering all sectors comprehensively, with no established standards to guide this process. The seven Baseline Requirements (7BR) may not be sufficient as they stand, revealing a need for further work in standardization, definition, and objective understanding, particularly within the NATO framework.

Systems remain vulnerable and require enhanced capabilities to meet the needs of the population. The existing 7BR, while foundational, exhibit gaps in adaptability and practical application. There is a pressing need for more robust and objective input to refine these requirements. As they are currently developed intuitively by experts, there is a need for more structured and evidence-based approaches to resilience management.

Moving forward, it is essential to focus on standardizing and defining resilience metrics and practices through NATO and other frameworks. By addressing these gaps and developing more comprehensive and adaptive systems, we can better meet the challenges of resilience management and improve our ability to respond effectively to future adversities.

Bibliography

1. Adger, W.N., 2000. Social and ecological resilience: are they related? Progress in Human Geography, 24(3), pp.347-364.
2. American Psychological Association, n.d. Resilience. [online] Available at: https://www.apa.org/topics/resilience.
3. Bailey, R., 2019. The Role of Strategic Communications in NATO's Hybrid Warfare. NATO Review. [online] Available at: https://www.nato.int/docu/review/articles/2019/06/20/the-role-of-strategic-communications-in-natos-hybrid-warfare/index.html
4. Boin, A., 2019. Resilience and Governance: A Research Agenda. International Review of Administrative Sciences, 85(1), pp.191-205.
5. Bonanno, G.A., 2004. Loss, trauma, and human resilience. American Psychologist, 59(1), pp.20-28.
6. Department of Homeland Security (DHS), 2020. National Critical Functions and Resilience Requirements. [online] Available at: https://www.dhs.gov/national-critical-functions.
7. Masten, A.S., 2014. Global perspectives on resilience in children and youth. Child Development, 85(1), pp.6-16.
8. NATO, 2014. Wales Summit Declaration. [online] Available at: https://www.nato.int/cps/en/natolive/official_texts_112956.htm.
9. NATO, 2018. Brussels Summit Declaration. [online] Available at: https://www.nato.int/cps/en/natolive/official_texts_156624.htm.
10. NATO, 2019. Managing Migration and Humanitarian Crises. [online] Available at: https://www.nato.int/cps/en/natolive/topics_84325.htm.
11. NATO, 2020. Transport and Logistics in NATO Operations. [online] Available at: https://www.nato.int/cps/en/natolive/topics_82742.htm.
12. NATO, 2021. Resilience and Article 3. [online] Available at: https://www.nato.int/cps/en/natolive/topics_132722.htm.
13. NATO, 2022. Baseline Resilience Requirements. [online] Available at: https://www.nato.int/cps/en/natolive/topics_82729.htm .
14. NATO Communications and Information Agency, 2021. Cyber Resilience and NATO. [online] Available at: https://www.nato.int/cps/en/natolive/topics_128390.htm .
15. NATO Parliamentary Assembly, 2021. Report on Enhancing NATO’s Resilience. [pdf] Available at: https://www.nato-pa.int/document/2021-report-enhancing-natos-resilience.
16. Sieber, J.E., 2006. The Role of Physical Resilience in Health and Well-Being. Academic Press.
17. Tierney, K., 2014. The Social Roots of Risk: Producing Disasters, Promoting Resilience. Stanford University Press.
18. Wildavsky, A., 1988. Searching for Safety. Transaction Publishers

ADAPTING TO EMERGING RISKS

Anelia ATIPOVA[1]

Abstract: The article presents a reading of the concept of emerging risks, in the context of shared resilience. The nature and critical impact of these risks require them to be addressed in a structured, systematic and consistent manner, with the full participation of all stakeholders. Since these are cross-border, complex and poorly predictable risks, the collaboration of all stakeholders within the organization, as well as with those outside the organization, is highlighted as mandatory. Emerging risk management is most efficient and effective through its implementation in existing approaches and strategies for managing organizational risk, taking into account its nature and context of occurrence.

Introduction

Emerging risks put the organization in a state of imbalance, directly confronting the challenges of uncertainty with organizational resilience.

Counteracting emerging risks does not cancel the counteraction to traditional risks, on the contrary. A learning organization striving to achieve its goals and develop should develop flexible strategies for managing various types of risk, including emerging ones. This is related to creating an organizational rhythm of identifying, analyzing, prioritizing risks and properly allocating resources for their management. Traditional and emerging risks must be managed, observing the following conditions:

1. Adherence to established risk management standards, due to the high dependence of the organization on other organizations.
2. Incorporating emerging risks into risk management strategies applicable to traditional risks for the organization.
3. Using a flexible approach, with established techniques for analyzing and assessing emerging risks.

[1] Assistant Professor, Rakovski National Defence College

The surest way to be fundamentally prepared to respond to (emerging) risks is to build organizational resilience.

The Concept of Emerging Risks

Emerging risks appear in areas where there is insufficient knowledge about their management and are realized in ways that go beyond the known approaches and methods for risk response. They have characteristics that distinguish them from known risks, such as - ambiguity, chaos, complexity, uncertainty, variability, uncontrollability.

Such a type of risk is difficult to define, changes continuously, in conditions of difficult to predict time horizon, affects multiple aspects and is completely beyond the control of the organization. That is, it appears external to the organization and requires adaptation mechanisms rather than management mechanisms.

The nature of emerging risk requires that it be considered outside the standard concept of risk, as simply "the effect of uncertainty on goals". Thus, if by definition, risk management means "guiding the organization in conditions of uncertainty", the main way to manage emerging risks is to manage uncertainty itself.

Examples of emerging risks are climate change, cyber-attacks, collapses of international stock markets or pandemics, such as the latest pandemic with global consequences – COVID 19.

Some of them are critical, by virtue of their consequences and probability, and have a sudden, creeping or permanent nature. Therefore, they can arise from "suddenly occurring events (e.g. earthquakes, industrial accidents, terrorist attacks), gradually occurring events (e.g. pandemics) and steady-state risks (in particular those related to illegal trade or organised crime)".

By emerging risk we should understand both a known risk that is developing very quickly and a sudden and rapidly developing risk that is completely unexpected and unknown until now.

In general, emerging risks can be categorised as follows:

1. New risk in a known context.

2. This is a risk that arises outside the organisation but has an impact on the activities and. and has an impact on the existing activities of the organisation.
3. Known risk in a new context.
4. This requires a change in the way an existing risk is managed when it is transferred to a new subject area (or activity).
5. New risk in a new context.

This category includes a risk that is completely new to the organisation and has never been managed.

Emerging risks have long-term consequences, often occur in parallel with other risks and affect the entire society. Therefore, they must be managed systematically and comprehensively. In addition, they are the result of some structural change and often have a cross-border nature, therefore, confronting them is possible only by achieving sustainability - both at the organizational and clusteral (collective) level.

The difficulties in managing emerging risks also arise from the fact that it is almost impossible to indicate the owner of the risk. In view of the practically zero predictability and the enormous resources required to manage emerging risks, organizations often implement emerging risk management strategies in the daily process of managing already existing low-order risks.

The most common approach to managing such a risk is to reduce it (translate) to a risk known to the organization, with clearly defined owners and worked out response approaches.

Managing emerging risks for organizational prosperity

Emerging risks rarely affect short-term goals, which is why the organization often decides not to invest in their management. However, as an element of strategic uncertainty, they need to be imposed as a mandatory aspect of the organizational risk culture.

If standard risk management is aimed at allowing the organization to achieve its goals, then the management of emerging risks, on the contrary, is aimed at the survival of the organization, which will increase its resilience and allow it to undergo positive development in conditions of uncertainty.

Resilience is the ability of an organization to anticipate, prepare for and respond to changes in the security environment in order to survive and prosper. Developing resilience helps organizations anticipate possible adverse scenarios or events, prepare for and adapt to them, as well as recover after a disruption or impact.

The risk landscape is dynamic, due to the high connectivity of modern societies, economies, markets and new technologies. In order to effectively manage emerging risks, it is necessary to assess their transgenicity, low predictability and systemic, polycrisis nature.

As specific risks, with "low probability and high impact", translating them into a known risk can be effective. However, the lack of the ability to determine the probability and extent of impact with a high degree of confidence hinders timely decision-making.

This requires the development and testing of emerging risk management approaches that take into account the natural risk management cycle, adapting it both to the nature of the emerging risks and to the specific needs of the organization.

Possible approaches to managing emerging risks

The classic emerging risk management cycle is based on the International Risk Management Standard ISO 31000:2018 and includes the steps: identification, assessment, sharing information and offering strategic directions to be validated over time. Validation is achieved by integrating emerging risks into daily risk management processes, while increasing resilience to current and future challenges.

The process includes two possible approaches, based on the resources of the respective organization:

First approach: An iterative process of anticipating, assessing and classifying emerging risks, with the aim of situational and strategic awareness and incorporating the process of managing them, into the organization's risk management framework.

Second approach: Creating a common strategy for managing emerging risks, by building organizational and supra-organizational (cluster, collective, etc.) resilience to recover from unexpected shocks.

The steps in both approaches are the same.

Step One: Identify the Emerging Risk

This step involves using the horizon scanning method to explore potential changes in the security environment. The identified risks are subject to subsequent analysis. The goal of the scan is to explore plausible future developments that could change the risk management context. The result of this stage is:

1. Creating a risk management framework that takes into account future changes in the security environment.
2. Creating possible scenarios for the development of future risks, taking into account the influences (combinations) of already existing risks.
3. Prioritizing risks to create a framework for their management. The organization must first determine whether it has sufficient information to manage emerging risks by integrating them into existing risk management processes. Second, it must understand what changes it needs to make to manage emerging risks effectively.

Step Two: Assessing Emerging Risks and Communicating to Stakeholders

During this step, risks are assessed in a structured manner and the results are communicated to key stakeholders. The stage relies on a structured methodology for conducting the analysis that is consistent and universal in nature (i.e., applicable to all types of risk).

The methodology should include: a description of the characteristics of the risk before it occurs, the potential conditions necessary for the risk to occur, the characteristics of the risk after it has occurred (including systemic impacts that may require a reformulation of the management approach), necessary changes in the organization to manage the risk, and to achieve a sufficient level of understanding of the risk.

Sharing the emerging risk assessment with stakeholders is necessary to achieve situational awareness and informed decision-making.

During this stage, awareness, responsibility, authority and capabilities for the identified risks are assessed, based on which the organization is able to manage emerging risks. Existing deficits in organizational capabilities are also assessed.

Awareness shows how much stakeholders understand the emerging risk and its likely impacts on them. When necessary, a more in-depth risk study is carried out.

Allocation of responsibilities and their acceptance (awareness) is another important element of the management process. The last aspect assesses how much the organization is able to manage risks.

The result of this step should be a list of existing gaps in certain areas, which should be prioritized and addressed subsequently.

Step Three: Formulate Risk Management Recommendations

This stage involves developing recommendations for building preparedness for all hazards and managing specific identified risks or groups of risks. The recommendations address both the individual stages of the assessment and management cycle and the response to specific identified deficiencies.

Again, they are aligned with one of the two chosen risk management approaches – responding to specific emerging risks or improving overall resilience to respond to future, as yet unknown, emerging risks.

Such measures may include:

- Developing specific risk controls.
- Reducing vulnerability to a broad range (or all) of hazards.
- Developing incident response mechanisms.
- Developing crisis recovery mechanisms.

The most effective are the measures related to the management of more than one risk (emerging or emerging, in the same way as traditional risk).

The recommendations made for risk management have the character of a strategic document and should be incorporated into a strategy and strategic plans for risk management, including emerging risks. These plans take into account the time horizons and stages of risk development, as well as the nature of the various risks.

Regardless of how the plan is structured, it should be a living document that adapts to changing conditions.

Often, in order to achieve management effectiveness, the organization collaborates with partners at each stage of the risk management process.

To ensure continuity of the process and adequacy of the measures applied, the organization, as a learning organism, should integrate lessons learned from practice - both in its activities and in the risk management processes.

Techniques for Identifying Emerging Risks

Methods, applicable to identifying emerging risks include PESTLE, SWOT, and Horizon Scanning. They can be used alone or in combination.

The PESTLE analysis

The PESTLE analysis method identifies external factors in the categories:

- P - Political
- E - Economic
- S - Social
- T - Technological
- L - Legal
- E - Environmental

The information obtained can shape the structure for horizon scanning.

The method allows an organization to think about potential emerging risks within categories. This structures information, increases understanding, and focuses risk response efforts.

The steps in implementing the method are outlined in Table 1.

Table 1.The steps in implementing the PESTLE analysis

Step	Process
Identify key stakeholders	Gather relevant people to work together who have insights to make from a political, economic, social, technological, legal and/or environmental perspective.
Brief team	Explain the context of the work, your strategic and project objectives so they can prepare for the Review Meeting.
Review meeting	Share, gather and review insights under each heading considering both internal and external risks.
Meeting output	Document the insights in terms of themes, issues and risks, e.g. using a table with the PESTLE factors as headings. This is the current list of potential emerging risks to monitor.

Rfelect and review	After a suitable period of reflection, bring the group back together to review and confirm the emerging risks identified.

The PESTEL Analysis includes all stakeholders with competencies and interests in the specified subject areas (political, economic, social, technological, legal and environmental).

The SWOT Analysis

Another applicable method for identifying emerging risks is SWOT analysis. SWOT analysis is a method that can help an organization understand its strengths, weaknesses, opportunities and threats.

It is an easy to implement and recognizable approach that can be a useful framework for thinking about the PESTLE factors. SWOT supports the identification of risks by providing a broader perspective on the factors that may affect the strategy or implementation of activities.

The technique increases understanding of the impact and what can be done to minimize adverse effects and maximize potential opportunities.

An example of a SWOT analysis is shown in Table 2.

Table 2 SWOT Analysis Quadrants

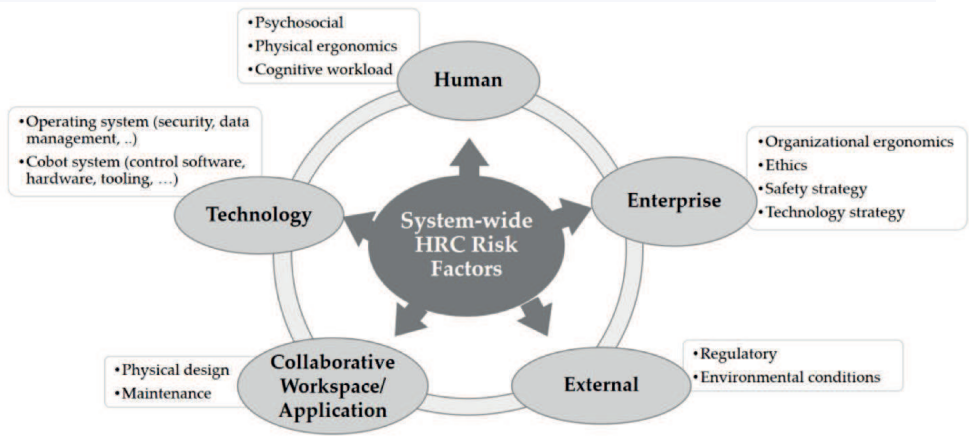
Strengths	**Weaknesses**
Trustee board has recently appointed a trustee champion for risk and compliance issues.	Our poor record on compliance with existing regulations and lack of governance and assurance systems.
Opportunities	**Threats**
Use the upcoming regulatory change to improve our compliance with all relevant regulations by setting up an assurance system, which could be used for all other rules that apply to our activities.	Stricter future regulations with increased fines for non-compliance and negative media coverage.

The third method mentioned is Horizon Scanning.

The method is used across a wide range of sectors to identify potential problems and risks facing an organization in the future. It is a systematic examination of information to identify potential threats, risks, emerging issues and opportunities. Based on the Horizon scanning, risks can be time-framed and analyzed.

The application of Horizon Scanning is shown in Figure 1.

Figure 1 Horizon Scanning Example



Just like PESTLE and SWOT, Horizon scanning should involve key stakeholders.

Conclusion

The article presents an overview of a more specific category of risks – emerging risks, which accompany traditional risks but have a fundamental impact on organizational activities. The two approaches highlighted – preparing for a response to specific emerging risks and preparing through resilience – provide a framework for managing not only risk but also uncertainty.

The presented cycle represents an interpretation of the classical understandings of risk management – such as ISO 31000:2018 postulates them, but through the prism of the need for collective and comprehensive resilience.

Each step in risk management is significant, from understanding to mitigation, but the most essential for the targeted management of emerging risk is the ability to apply the achieved understanding in the strategic concept of the organization.

Bibliography

1. ISO 31000:2018: Risk management – Guidelines, provides principles
2. ISO Guide 73:2009: Risk Management – Vocabulary
3. ISO 22316:2017: Organizational resilience – Principles and attributes
4. RECOMMENDATION OF THE COUNCIL ON THE GOVERNANCE OF CRITICAL RISKS (Adopted by the Council at Ministerial Level on 6 May 2014), Microsoft Word - CMIN(2014)8-FINAL-EN-GOV-Recommendation Governance Critical Risks.docx
5. An introduction to emerging risks and how to identify them, Institute of Risk Management, IRM Charities Special Interest Group Report
6. Hopkin, P. (2018) Fundamentals of Risk Management: Understanding, evaluating and implementing effective risk management. 5th edition. IRM. Kogan Page: New York
7. Hardy, C. & Maguire, S. (2020) Organizations, risk translation, and the ecology of risks: the discursive construction of a novel risk. Academy of Management, Vol. 63(3)
8. SWOT Analysis A framework to understand and analyze a company's Strengths, Weaknesses, Opportunities, and Threats, SWOT - Definition, Examples, Process, Uses
9. What is PESTLE Analysis?, Jim Makos,What is PESTLE Analysis? (Free Template)
10. Horizon Scanning: A Practitioner's Guide Produced by the Innovation Special Interest Group of the Institute of Risk Management, horizon-scanning_final2-1.pdf

The Crisis Management and Disaster Response Centre of Excellence

thanks all authors and contributors who helped to accomplish the present issue.

Sincerest appreciation for their time and willingness to share information and opinions.

The CMDR COE also thanks all organisations and individuals

who engaged in the Centre's events

held during the year of 2024.

ISSN 2367-766X