Address:
34A Totleben Boulevard, 1606 Sofia,
Bulgaria
Phones: 359 29224700, 359 2 9224705
Fax: 359 2 9224755

Dear Readers,

Welcome to the 2019 CMDR COE Proceedings. It is a great pleasure to introduce it to you. I hope it will become a salutary tool to promote and facilitate "The Interagency Interaction in Crisis Management and Disaster Response". Herewith I would like to stress the importance CMDR COE pays on such cooperation through meeting opinions in the sphere of professional interests.

Over the past years, our organization participated, hosted and organized a number of key courses, seminars and conferences in the crisis management and disaster response domain. Among the leading events are the CMDR COE Annual conferences based on the themes of the importance of interagency interactions. Present book is a very good example of our efforts through the year 2019 to provide venue in support of mutual understanding and interaction in crisis management and disaster response. Therefore the present edition covers aspects from several authors and their thoughts on CMDR domain.

Welcome once again and thanks for reading.

Orlin NIKOLOV,
CMDR COE Director

TABLE OF CONTENT

TRACING RESILIENCE – A CONTEXT OF UNCERTAINTY, A TRAJECTORY OF MOTION

Gergana VAKLINOVA, (CMDR COE)

Abstract: Alongside a relative novelty, resilience has decisively turned into an objective necessity in international relations, and especially – in peace and security. Tracing its past, to understand its future, while (re)defining the present, requires to simultaneously set resilience, and its object of analysis, in context and in motion. The complexity and uncertainty of a connected and interdependent international system necessitates elaborating and clarifying resilience manifestations and expressions, which inform decision-making and activities aimed at tackling contemporary and future security threats, both from a civilian and a military perspective. Crisis and disaster management have become standard responses in situations, which defy, in varying degrees, established and accepted normality. The demands of changed, and changing, notions of peace and security, strain capabilities and preclude the capacity, and responsibility, of a single point of defence to withstand and tackle complexity, and dictate interaction on collaborative terms. Theatres of operation have firmly settled among societies shifting tasks from purely military to people-centred and seeking broader (political) realisation. Whether an ability, capacity, or a (relational) process, resilience potentially aims to increase chances for survival, as a first step, and then – to enable (continuous) adaptation. As a security and defence organisation NATO has taken important steps towards building a collective interpretation of resilience – one that positions societies' preparedness at the core of collaborative efforts at shared understanding of the imperatives of time.

Key words: resilience, complexity, manifestations, expressions, complex systems, societies, military, security, crisis management, disaster management, NATO.

Introduction

Resilience is a relative novelty to international relations and one that is decisively gaining traction in the fields of conflict, crisis, and disaster management, with a notable proliferation within the (Euro-Atlantic) body of research since the 2000s. It is, perhaps, all but a coincidence that this productivity runs in parallel with an increasing interconnectedness and interdependence within and between systems on a global scale. Complexity and uncertainty strain the capacity to calculate risks and respond to threats within a (fragile) balance between robustness and flexibility, elasticity and adaptation, and *normality* and transformation. Changes in the manner of perceiving hence "exercising" security – a focus steadily shifted from the whole (i.e. state) to the constitutive (i.e. people), have positioned societies at the forefront of defence, both in terms of prevention and protection. Therefore, tracing resilience in complex systems, through a preparedness perspective and within a crisis and disaster management context, begs the question(s): what is *that* which is to be *protected,* and better yet - what is *that* which should be *resilient*, thus enabling an effective and efficient (self) protection.

There exists no straightforward answer to the conundrums the latter questions foment, nor does or can resilience – either framed as an ability / capability, capacity, or as a relational process of (social) learning and exchange – provide *quick-fixes* awaiting to be downloaded wherever, and whenever, a system

might require an update on the imperatives of time. Crisis and disaster management have grown standard responses in situations which defy, with varying degrees, established and accepted normality. As imperfect as both underlying rationale and decision-making, and *on field* execution might be, the course of action is confined by the fact that the contemporary security strains capabilities and precludes the capacity, and responsibility, of a single *point of defence* to withstand and tackle complexity, dictating interaction on collaborative terms.

The concept of resilience, appearing "equally applicable to the individual, society, nature, and technical systems […] aspires to describe mechanisms for maintaining stability, survival, and safety" (Cavelty, et al. 2015, 4). In a context of dynamism, there also appears a tendency on a (comprehensive yet tailored) resilience trajectory from reaction (the ability to *bounce-back*) through pro-action (the processes of improving the capacities), to pre-emption (relational (networked) processes). This trajectory brings together civilians and military in an unprecedented way and therefore, necessitates flexibility and cooperation, to ensure a level of functional common understanding to the effect of ensuring security through crisis and disaster management.

Crisis[1] and resilience could be understood as the flip sides of one coin – when you have one, you do not have (see) the other.

[1] For the purpose of this article *crisis* is understood in broad *political* terms.

At current pace, however, a statement that crisis management rescinds resilience, and vice-versa, would, perhaps, remain a speculation until a detailed investigation into the mechanisms of both resilience and crisis and disaster management translates their applicability, separately or in a combination, to dynamic contexts and to specific objects of analysis.

The present research examines prevalent interpretations of resilience with the aim of opening a debate on how to understand (better tailor) societal and military resilience in terms of future crisis and disaster management, and to account for the (tendency of an ever growing) complexity and uncertainty in an interconnected and interdependent international (security) environment. Even though the scope of the present article is limited in time, literature studied and focus – setting the stage for a panel discussion on conceptualising resilience, its larger intent is to contribute and stimulate a larger debate on the modalities of "that which is / is not (and should / should not be) resilient" - from both a civilian and military perspective - and what implications the answer to this question would bear on planning and decision-making, and operationalisation and execution for crisis and disaster management, and particularly NATO crisis response operations – within and outside collective defence.

Tracing Resilience

Resilience is a relatively new, and quite demanding, concept in international relations while being more extensively studied in

other (core) disciplines such as engineering, psychology, economy/business, and ecology. Regardless of whether approached from an engineering or an ecologic perspective, what is engaging the interest of academics and practitioners alike is the quest to *know* resilience - what types (what does it look like); what sources (where does it come from); what resources (how to reveal /build it / at what cost), and hence *understand* how to *make* entities[2] resilient, be it civilian or military. The type of entities, or the unit of analysis[3], will further bear implications for the approach and mechanisms of causality used to describe what it is that is resilient and how resilience is *generated*. Therefore, in international relations, and in peace and security, the discussion inevitably invokes the need to simultaneously set resilience into a context and into motion to the effect of studying its mechanisms.

Within the contemporary security environment, characterised by unprecedented levels of connectivity and interdependence, widespread cascading effects from disruptive events occurring anywhere on the globe blur the lines between *internal* and *external*. System dynamics, with their inherent uncertainty, breeds complexity marked by a multiplicity of actors and their

[2] Entities, as well as subjects, objects, structures, systems, organisations will be hereafter used, interchangeably, in reference to resilience units of analysis without however, and in line with extant limitations upon this work, entering into a discussion on their detailed characteristics.

[3] Could be a subject or an object - agents (individuals), systems (society), organisations (state) - a structure, i.e. sub-system, within a given organisation, processes, and world-system (global).

respective, often competing, interests, objectives, and means involved in any given situation, including such that presents challenges to system (routine) functioning. Responding to these developments, peace and security have been changing and have been changed by the imperatives of the environment. In this context, some would argue that resilience enables analysis and common understanding of reality – uncertain and complex as it is (Roth 2019), while others would suggest that uncertainty reveals the limits of knowledge and prediction (Chandler 2014) without necessarily providing a ready-made solution for this realisation.

Crisis management[4] emerges as an answer to an increased focus on human security[5] and the need for civil-military cooperation premised on interaction and interoperability at times when the imperatives of the current, and, perhaps, even more so the future, environment largely outstrips the capacity and capability of any single entity to counter threats to peace and security. The urgency of reaction and the demands of a shifted focus from state to human security have triggered dramatic changes in military tasks – a transition from the pursuit of concrete military strategic objectives to the establishment of specific conditions from which political outcomes can be derived. Military resilience, however, does not dwell in isolation

[4] The article will mostly discuss crisis management in light of resilience.

[5] Human security encompasses ecological, functional (science, technology, and economic activity), and social dimensions – human societies and governance (politics) (Hamilton 2016).

from the preparedness and adaptation capacity of societies. As military activities become ever more people-centred involving, for instance, the protection of civilians (PoC), including humanitarian and diplomatic activities, the establishment of order, and the prevention of sexual and gender based violence, the pressure on long-term adaptation and capability development mounts and necessitating an improved framework, within which burden sharing and transformation translate into increased overall resilience. As much as this may be beneficial in peacetime, the connectivity and interdependence of societies and their functions at their current pace, carry a potential to transform into a destructive force during conflicts and crises, thereby necessitating adequate preparedness.

In such a security context, understanding the mechanisms of resilience, when applied to complex systems[6], such as societies

[6] Going beyond the scope of this article, complex systems warrant a rigorous analysis in relation to resilience. Some excellent reads include: McClelland, Charles A. "The Function of Theory in International Relations." The Journal of Conflict Resolution 4, no. 3 (1960): 303-36. http://www.jstor.org/stable/172856; Tanter, Raymond. "International System And Foreign Policy Approaches: Implications for Conflict Modelling and Management." In Theory and Policy in International Relations, edited by Tanter Raymond and Ullman Richard H., 7-39. Princeton University Press, 1972. http://www.jstor.org/stable/j.ctt13x143h.5; Weltman, John J. "Systems Theory in International Relations: A Critique." Polity 4, no. 3 (1972): 301-29. doi:10.2307/3233964; Harvey, David L., and Michael Reed. "Social Science as the Study of Complex Systems." In Chaos Theory in the Social Sciences: Foundations and Applications, edited by Kiel L. Douglas and Elliott Euel, 295-324. Ann Arbor: University of Michigan Press, 1996. http://www.jstor.org/stable/10.3998/mpub.14623.16.; Lansing, J. Stephen. "Complex Adaptive Systems." Annual Review of Anthropology 32 (2003): 183-204. http://www.jstor.org/stable/25064826.; Miller, John H., and Scott E. Page. "Social

and the military, “has significant implications for security policy and its development, and for the development of preparedness or mitigation strategies” (Prior and Hagmann 2012, 7). Therefore, delving into the *manifestations* and *expressions* (Prior and Herzog 2013) of resilience, i.e. attempting to conceptualise these system interactions - duly accounting for the specificities of the broader (security environment) and narrower (individual, community, society, state, group of states)[7] context - could, from a hindsight perspective, provide an insight into future crisis management.

The effects of major non-routine events or uncertainty, caused by either internal or external stressor factors, put to the test the *resilience* of a given system and its established procedures, which thereafter finds itself in a state of a *crisis*[8]. These effects could be measured on a continuum from changes, through transformation to serious or total disruption. The system itself ‘communicates’ with the external environment and with other systems. What makes the difference between its normal state and a state of crisis is the *overall level of resilience*. The latter

Science in Between." In Complex Adaptive Systems: An Introduction to Computational Models of Social Life, 213-26. Princeton University Press, 2007. http://www.jstor.org/stable/j.ctt7s3kx.17.; Spindler, Manuela. "Didactics and Method." In International Relations: A Self-Study Guide to Theory, 106-20. Opladen; Berlin; Toronto: Verlag Barbara Budrich, 2013. doi:10.2307/j.ctvdf09vd.7.

[7] Unit of analysis, which affects the method of analysis and the measurement metric. On measuring resilience see: Prior and Hagmann, Measuring Resilience: Benefits and Limitations of Resilience Indices 2012

[8] CMDR COE working definition.

prevents external factors from turning into external stressor factors. Crisis management entails specific expertise, skills and techniques for analysis and measures for defining routine (normality) and hence, identifying deviations from this routine, which could lead a system to a state of a crisis. Specific and tailored arrangements should be put in place guiding the work through all crisis phases – from prevention (before), through occurrence (during), to recovery (after), with a clear vision and strategy for a final outcome. And these arrangements should be informed by due consideration for that which makes the difference between crisis and routine.

Similarly to the CMDR COE interpretation of a crisis, the literature on resilience tends to revolve around, with differences in degree contingent upon the unit of analysis, a resilience *continuum* from *static* (engineering / physical) to *dynamic* (socio-ecological), whereby the transposing factor would be the realisation of resilience – as an ability, capacity, process (including a learning process), and relations. To set off, an investigation into the conditions under which resilience *manifests,* i.e. comes into play (Prior and Herzog 2013), crystallises the notion of a stressor factor, be it internal or external to the unit of analysis experiencing it. As Prior and Herzog explain "resilience 'happens' only in response to an event that disrupts *normality"* (Prior and Herzog 2013, 6, emphasis added), and Prior and Hagmann further add that it is

inherent in most entities, but evident post hoc (post stress / threat / shock) (Prior and Hagmann 2012).

With this, they frame resilience as a *latent (static) characteristic* of a given entity, which is only demonstrated when triggered by a disruptive event, that is - when necessary to go beyond standard routine[9]. In other words, resilience is understood as an *outcome* which confers a certain *state* to entities – i.e. being resilient. This state could be characterised as a set of attributes generally indicating the possession of (innate or *installed*[10]*)* abilities to "maintain critical operations" (McLeod, et al. 2016, 7). As Hollnagel elaborates, resilience is "[a]n *ability* to maintain

[9] A certain level of routine and subjective and material arrangements are required, also in anticipating, so as to enable shock tolerance for coping with emergencies (Lentzos and Rose 2009, 243 in O"Malley 2010), as a first step. Further delving into notions of what constitutes *normality* (in international relations – and peace and security) and thereby, deviations from it, for different levels and units of analysis, goes beyond the scope of this research. See, for instance: Berl, Ethel G. "Normality: An Historical and Comparative Analysis of the Concept." The Journal of Experimental Education 9, no. 1 (1940): 91-94. http://www.jstor.org/stable/20150641; Strößner, Corina. "Normality and Majority: Towards a Statistical Understanding of Normality Statements." Erkenntnis (1975-) 80, no. 4 (2015): 793-809. http://www.jstor.org/stable/24735072; Smart, Ian. "The Adopted Image: Assumptions about International Relations." International Journal 39, no. 2 (1984): 251-66. http://www.jstor.org/stable/40202333; Adler-Nissen, Rebecca. "Stigma Management in International Relations: Transgressive Identities, Norms, and Order in International Society." International Organization 68, no. 1 (2014): 143-76. http://www.jstor.org/stable/43282098; Mansbach, Richard W. "Integrating Normative Theory in Teaching International Relations." International Studies Perspectives 13, no. 1 (2012): 10-12. http://www.jstor.org/stable/44218673.

[10] Abilities which are not *natural* to entities but rather require dedicated actions (training / finance) to be developed. For instance, the ability to operate a tank.

equilibrium or "bounce back"[11], analogous to the (physical) ability of a material to "absorb energy when it is deformed elastically and then to recover" (Hollnagel et al. 2006, in Goldstein 2009, 5, emphasis added). Holling and Gunderson (2002) argue that in ecosystem resilience, which in their understanding also involves a stressor factor for initiation, the scale and intensity of *reaction* correlates with the magnitude of the disturbance. The higher the magnitude the closer the system structures become to "changing the variables and processes that control behaviour" (Holling and Gunderson, 2002, 28 in Gotts 2007, 2).

Complex systems bounce-back in order to maintain "critical operations in the face of *adverse disruptions*." (McLeod, et al. 2016, 7, emphasis added). Both the military and modern societies are characterised by an intricate dynamics of connectivity and interdependent of structures and processes – of vital services and sectors, and consist of an array of sub-systems, both "human and non-human" (Giroux and Prior 2012)[12]. Being open, complex systems communicate not only internally (sub-systems) but externally as well (with other complex systems), which requires (and renders) a certain level of *adaptability* in response to "disruptive events and regardless

[11] Quick return to stability, highly valued aspect of an entity in a context of disturbance, especially in engineering.

[12] Systems that include the following elements: technical or physical, individuals, business/economic interests and assets, ecological systems and environmental characteristics, and communities (Giroux and Prior 2012).

of the impact on individual systems and components" (K. S. Langeland, D. Manheim, et al. 2016, 6). Similarly to interpretations of adaptation in ecosystem resilience (Giroux and Prior 2012) *change* and *reorganisation* appear essential elements within human (social) systems as well (Kaufmann 2013) thereby marking a shift from a *static* understanding of resilience as a *bounce-back* ability to the more dynamic end of the afore-mentioned resilience continuum (Giroux & Prior, 2012).

Thus, in human systems, in contrast with technical – i.e. infrastructure, *reactive* (static) interpretations of resilience (robustness and elasticity) are supplemented with a focus on *proactive* (dynamic) processes, particularly in decision-making to ensure systemic flexibility (to adapt and transform) to withstand, rebuild, and re-organise. A key characteristic of societal resilience through adaptation is social *learning*[13] or the generation, preservation, and transfer of knowledge about (past) experience which then enables future planning, essentially expanding the scope of (potential) responses. Understanding resilience through the perspective of a *process* (i.e. becoming resilient) is further stimulating the change of focus away from "natural given to being a technique" (O"Malley 2010, 28), and further – applied in a degree corresponding to

[13] As Prior and Herzog argue, social learning (adaptive learning) is premised on strong associations (social cohesion) between members of the system (society) so as to enable cooperation and thereby the transfer and preservation of knowledge and practices (Prior and Herzog 2013)

the requirements of a specific situation. Adaptation through social learning is particularly applicable to crisis and disaster management, both in military and civilian terms, not only at individual and community but also institutional level[14], as ”experienced history” (Prior and Herzog 2013) improves / increases the capacity to anticipate, prepare for, react to, and recover from similar events in the future.

Resilience in an open, interdependent, and *learning* system, Hamilton (2016) argues, is *shared* for it goes beyond entities (i.e. individuals) and their needs and capacities. “Forward resilience” entails security of networks (across borders) and (their) critical functions (i.e. ensuring security) (Hamilton 2016). Such resilience aggregates and takes on a relational perspective, thereby becoming, what Chandler would argue - a *collective* responsibility (Chandler 2019). For instance, military mobility - moving equipment and personnel across (national) borders would require coordination of military and civilian functions and thereby would depend on the individual resilience of each function and relation. Societal resilience is premised on collaboration, collective sense making and social learning and offers “the conceptual means to understand society as a system that exists in a constantly shifting relationship with an unpredictable and radically changing environment” (Cavelty, et

[14] The importance of institutional memory to decision-making and planning processes.

al. 2015, 5). Resilient connections[15] link relations within, between, and across societies (Hamilton 2016), whereby resilience can potentially have a *domino effect* across the entire system in case of a disturbance. It is pertinent to inquire here whether the whole system i.e. *all* or *specific* systemic (core) functions and constitutive parts should be equally resilient, which receives an answer in the *core* – *periphery* concept of world systems[16], where preservation of the core is an imperative, even if necessitating sacrificing the periphery (support system) to ensure identity preservation, hence – system survival.

Resilience by and for the military – NATO

Resilience allows for a non-linear analysis capturing episodic change and continuity alike for it unfolds in a dynamic setting. Complexity and uncertainty require flexibility and simultaneously breed innovation and adaptation – hence, resilience could be understood as a result of this complexity – an innovation aimed at flexibility and progress, improving the understanding of its very mother category.

[15] Along the lines of Levin's (1999) argument that "ecosystems can become either less or more resilient as they become more connected" (Levin 1999 in Gotts 2007), depending on the details of the connection networks, a similar speculation could be made as to networked societies whereby the correlation between connectedness and resilience would depend on whether societies become *more* or *less* resilient as they become more or less connected.

[16] Wallerstein 1974, Denemark et al. 2000, Chase-Dunn and Hall 1997a, Hall 2000 in Gotts 2007.

Jan Sabiniarz notes that resilience could effectively be “a tool for two different toolboxes – military and civilian” (Sabiniarz 2019), and as such to have different mechanisms of expression. For instance, and from a military perspective, at a strategic level – i.e. decision-making, resilience serves as a “framework for capability development” (Ibid), one that accounts for increased civil-military interaction. NATO has adopted an “all-hazard” approach to building resilience, which involves “planning and preparedness that is relevant for all types of threats” (Roepke and Thankey 2019, 52), be it armed conflict, natural disaster, terrorism, complex emergency, “or anything in between” (Ibid). Translating strategic objectives into operational tasks requires a comprehensive situational awareness which can enable swift adaptation in a highly dynamic environment. Finally, dynamism dictates a resilient force which has “sufficient capability, capacity, and will to endure adversity over time, retain the ability to respond, and to recover quickly from strategic shocks or operational setbacks” (NATO - Strategic Plans and Policy 2018, 23). Evidently, the primary focus is placed on processes and procedures in support of military activities[17], however, with a recognition of the link between resilient forces and resilient societies. In other words, whether s*pecific* (i.e. the capability to maintain functions during and following a disruptive event) or

[17] For instance, maintaining critical operations in the event of a disruption, which, at the minimum requires: creating a common understanding of and identifying critical components / functions; improving existing or developing new (required) capabilities, and ensuring continuous assessment and evaluation.

*general (*the ability to maintain operations over a span of unanticipated events) (K. S. Langeland, D. Manheim, et al. 2016), a resilient force would be contingent upon a "resilient society" (HQ SACT Strategic Plans and Policy 2017).

NATO has recognised not only that *resilience* is an important element of *deterrence by denial*: "persuading an adversary not to attack by convincing it that an attack will not achieve its intended objectives" (Roepke and Thankey 2019, 51), but also, and critically, that "resilience of civil structures, resources and services is the *first line of defence* for today's modern societies" (Ibid, emphasis added). Resilient societies[18] establish the fundament of stability and security overall. Therefore, and minding that it is primarily a national responsibility, nevertheless – this has implications for collective security as enhancing societal resilience through civil preparedness strengthens NATO's deterrence and defence posture. The 7 Baseline Requirements for civil preparedness (2016)[19] establish a systematic cooperative approach to improve national and, by extension, NATO resilience in this domain, and to enable the exchange of information on good practices, progress made and

[18] Human resilience includes "mental health and survivability, enabling individuals to retain flexibility and cope with the physical and cognitive stressors of the Future Security Environment." (NATO - Strategic Plans and Policy 2018, 35).

[19] 1) Assured continuity of government and critical government services; 2) Resilient energy supplies; 3) Ability to deal effectively with uncontrolled movement of people; 4) Resilient food and water resources; 5) Ability to deal with mass casualties; 6) Resilient civil communications systems; 7) Resilient civil transportation systems (Roepke and Thankey 2019).

outstanding challenges[20], ultimately fed into overall efforts at fostering the Alliance's *transformation*.

Whatever resilience rationales inform strategy and policy, analysing key stakeholders, including their vulnerabilities and capabilities, and establishing collaborative interaction[21] is an essential element of operational effectiveness. Therefore, military leaders bear the responsibility of establishing contacts with key stakeholders (nations – transit and host) in setting conditions for the conduct of operations. Establishing working networks helps to create greater credibility, communication, awareness, and agility, and improves resilience by sharing resources (NATO - Strategic Plans and Policy 2018). NATO civil-military cooperation, or CIMIC, is critical when it comes to "coordinating resilience" with the aim to prevent overstretching support capabilities and infrastructure beyond a single structural limit. CIMIC serves as an interlocutor between a mission Commander and civil actors, including the private sector, on the ground, which could greatly vary in number, type, composition, mandate and functions[22]. Cooperation, in CIMIC, is understood as *engagement* and *interaction*, the level of interaction varying according to context - conflict or peace, and

[20] Regular assessments – both on national (individual country reports, the state of civil preparedness of a given Ally) and collective Alliance levels (aggregated State of Civil Preparedness) (Roepke and Thankey 2019).
[21] Collaborative interaction allows for increased mutual understanding – of roles, mandates, objectives, and thus - trust.
[22]Generally including population, national and local authorities, international and national non-governmental organisations, institutions, agencies.

on a continuum from, respectively, co-existence[23], awareness[24], de-confliction[25], cooperation[26], coherence, integration (Civil-Military Centre of Excellence - CCOE 2016). That said, it should be borne in mind that CIMIC is effectively a military concept, as such "linked to an operational objective" (Civil-Military Centre of Excellence - CCOE 2016, I-1-4). It is integrated in all NATO operations support function[27] to the effect of accomplishing a military mission within the context of a given mandate.

Vulnerabilities, Threats, and Risks

Hagmann defines vulnerability as "the tendency of a system to be damaged, when exposed to a hazard (or threat) […]" (Hagmann 2012 in Prior and Hagmann 2012, 2). The way *vulnerability* is defined, or the manner in which a tendency develops and unfolds, will have implications for how resilience is interpreted. Related as they are, resilience and vulnerability are, however, not interdependent (Giroux 2012), therefore, an increase in the former would not necessarily lead to a decrease

[23] Military and civilians being together at the same place, at the same time. Adapted from CIMIC Handbook 4th Edition, CCOE, 2016.
[24] Military and civilians sharing information hence increasing transparency and a level of common understanding of the engagement space. Adapted from CIMIC Handbook 4th Edition, CCOE, 2016.
[25] Shared information and common understanding elevated to improved understanding of separate mandates, activities, resources, and a level of self-synchronization. Adapted from CIMIC Handbook 4th Edition, CCOE, 2016.
[26] Improved mutual understanding of purpose and effort encourages common purpose and objective. Adapted from CIMIC Handbook 4th Edition, CCOE, 2016.
[27] In support of a mission Commander.

in the latter, and vice versa. An “interior perspective” – as Roth would argue (Roth 2019), vulnerability is largely a function of risks deriving from perceptions of threats, and this relation affects the way crisis and disaster management are planned and conducted. In a security mind-set, threats are “knowable” and predictable, whereas risks are ever-evolving, gravitating (beyond) the margins of calculability, especially in an environment imagined as “characterised by radical uncertainty” (O"Malley 2010, 29). Prudence here necessitates cautious reliance on past experience as a basis for calculating risks as projections might fall out of context, underestimating its dynamism and complexity. An organisation could adapt its behaviour to address a given threat, depending on the (perceived) risk posed either to the entire organisation or to its separate parts, only to find itself exposed to another threat. A certain level of vulnerability may well be constructive in that it allows for adaptation and flexibility rather than rigidly foreclosing any opportunity for transformation.

Vulnerability translates into societies lacking adequate capacities to respond to risks or threats[28] and this lack is not predestined but rather a consequence of prevailing social, economic, and political inequalities. Noteworthy here is that “risk is considered in light of culture, knowledge, beliefs and experiences (Prior and Herzog 2015, 8). The social construction

[28] For instance, the risk of a flood in an uninhabited area does not pose a direct threat to a community.

of risk posits that individual perceptions, determined by culture, tradition, and - not least - gender dynamics within a given society or community, shape (different) experiences of security, and respectively insecurity and calculations of what constitutes, or not, a risk / threat. For instance, an individual's gender will influence roles, hence vulnerabilities, in a crisis or disaster situations and respectively, experience, response to, and recovery from such situations. Therefore, due consideration, i.e. continuous contextual and situational awareness, is required as per what are the dominant social constructions of risk and what affects its generation and preservation.

State authorities and institutions do have an impact on the social construction of risk, specifically through communication (risk communication), which seeks to create a common understanding (unity of purpose) and hence – response (unity of effort), which and when translated into resilience terms, is what LTC Lazarov calls "organised resilience" – the sum total of individual levels of preparedness (basic resilience) and the level of institutionalised support[29] (Lazarov 2019). Importantly, resilience does inform security governance and hence, security policy and strategy, particularly with regards to crisis and disaster management in a way which aims at coping with uncertainty, which could be, and depending on the specificities of a given context and unit of analysis, either by accommodating

[29] In the sense of tailored and targeted activities aimed at boosting individual resilience. Further discussed under *Measuring Resilience* here-below.

risk to bounce back, or by pre-emption through preparedness and adaptation. Nevertheless, one should not expect resilience to fully control for uncertainty, as it rather provides a framework within which uncertainty becomes operationally manageable (Ries, in Hamilton 2016). Furthermore, some argue that uncertainty may actually serve more good (Cavelty, et al. 2015) than the potentiality of closing in a "rigidity trap" (Gunderson and Holling 2002 in Goldstein 2009), which prevents adaptive change, catalysed by disturbances, by *maintaining* (imposing resilience) system conditions, which might not be functional /operational in a post-shock environment (Allison and Hobbs 2004 in Goldstein 2009).

Prudent planning is greatly facilitated by accurate risk assessment. One of the key elements within the later assessment are *risk tolerance* and *cost of failure* (McLeod, et al. 2016). From a societal perspective, and in a dynamic environment, high impact / short term disturbance would change a society's *development velocity*, whereas low impact / long(er) term – its *direction* (Lazarov 2019). Whether an entity has a *low risk tolerance* (i.e. hazardous industries) and high cost of failure, therefore strives at *impact avoidance;* or an organisation is operating in a dynamic environment (i.e. NATO) thereby focusing on operational continuity through adaptation and flexibility in the face of disruptions – *accommodating and transforming impact*, or optimises recovery (i.e. natural disaster) *rapidly recovering* mission-critical capabilities – situational

awareness[30], dynamic assessment, rigorous reporting for continuous feedback and lessons-identified are all critical requirements for improving resilience.

Providing a measurement in science serves to prove the existence of *things*. Systematic attribution of value and discovering and exploring patterns through parameterisation makes phenomena observable, explainable, and ultimately – *knowable*.

The debate of whether quantifying or qualifying best serves the purpose of knowing things fully applies to gauging resilience. A word of caution – measuring invariably means simplifying yet without losing the intricacy and core meaning of that which is under scrutiny. One of the largely applied measurements for resilience relies on quantitative indicators, i.e. such pertaining to critical infrastructure, for instance Protective Measures Index (PMI), Resilience Index (RI) and Criticality Index (CI) (Prior and Hagmann 2012). With respect to the operational environment risk tolerance, scope of possible threats, and expected impact, these indexes help to indicate which metrics can provide workable solutions for assessing resilience (McLeod, et al. 2016).

[30] Organisations operating in a dynamic environment require a high level of situational awareness to enable pro-active preparedness and timely adaptation. For instance, NATO's focus on "left of bang" requirements, which essentially, involves continuously improved situational awareness, thereby – improves readiness prior to potential incidents or attacks (Roepke and Thankey 2019, 52).

Regardless of the method used, resilience should be measured to allow for better understanding of what should become or be resilient; how to become / develop/build/facilitate[31] resilience; what resources to what sort of resilience. First and foremost, for a measurement to be "fit for purpose", it requires a sound definition linked to the unit of analysis and the specific context (i.e. crisis or disaster management); an explicit policy linked to the definition with clearly articulated objectives, targets, and resources, and explicit articulation of scale and context. (Prior and Hagmann 2012, 19).

Lazarov (Lazarov 2019) suggests that resilience be understood in terms of *basic* (individual) resilience and *organised* (institutionalised)[32] resilience, both of which he defines as highly (resource) demanding. The relation between basic and organised resilience is inversely proportional, meaning that changes in the former, whether in the positive or negative, do not necessarily trigger changes in the latter, that is, when individual resilience is high, organised resilience may not require adjustments, and vice versa. Coordination and interaction within and between basic and organised resilience

[31] Roth argues that resilience cannot be enforced (Roth 2019) but rather facilitated and supported where individuals, specifically in societal resilience, have ownership and bear responsibility for individual levels of resilience. The idea of self-sufficiency and institutions, i.e. state institutions, intervening intermittently and whenever individual capacities are exhausted, or otherwise stretched beyond limits.

[32] Maintained, for instance, by state authorities via regulations, guidelines and support to basic resilience (Lazarov 2019).

increase coherence of action and synergies, thereby changing the direction of proportionality from inverse to direct.

Testing and experimenting with *things*, once proven extant, is what turns assumptions, predictions, and hypotheses into (actionable) *knowledge*. As with measurement, the lack of conceptual clarity is commonly cited as impairing systematic and effective training for resilience. However, interpreted through a relational perspective, as discussed here-earlier, resilience initiates and enables transfer of knowledge and improves learning capacity. Preparedness is a constantly recurring theme in the resilience discourse for it "involves the creation of routines and resources for coping with emergencies that are *imaginable*" (O"Malley 2010, 4, emphasis added), and not necessarily calculable. Training a "resilient muscle" should allow imagination to unfold and exercise and test, in a close-to-reality environment, not *to the* point of failure, but this *very point* of failure, would undoubtedly break some new ground in the study of resilience. Modelling and simulation provides an excellent opportunity for training responses and capabilities (both military and civilian) as it encapsulates physical, cognitive and human factors in an as close to reality as possible (replicated complex) environment. Cooperation, interoperability and complementarity could, and should, be pushed beyond current capacities to test imagination and foresight.

Building upon the understanding of overall (societal resilience) as the combination of its basic and organised elements,

Lazarov proposes an initial concept for a model based on statistical/historical data fed into a simple equation (Lazarov 2019):

$$F = k * \mathrm{c}$$

In the above, *k* is situational awareness and impact on society, varying impact depending on the specificities of individuals – women, men, boys and girls, and social groups (groupings). The *k* varies between 0 and 1, where 0 means that basic resilience would suffice in an event of disturbance, and 1 that survival is threatened for the lack of preparedness. The *C* stands for capabilities – both natural (and potentially latent) and installed (in-built) through targeted (institutional) actions such as, but not limited to, education and training, information campaigns, regulations (Standard Operating Procedures – SOPs). Lazarov takes on a naturalistic perspective looking at core-periphery symbiosis, where the core is bestowed flexibility and adaptability, and the periphery – robustness and elasticity (to bounce back). Speed and accuracy of data exchange, decision-making and capability development are critical.

Resilience really? A word of caution

It is tempting, if the only tool you have is a hammer, to treat everything as if it were a nail. (Abraham H. Maslow)

Discussing the contemporary security environment when deliberating on effectiveness and efficiency in crisis and disaster management, serves two purposes. One, is to point

that complexity and uncertainty, connectivity and interdependence largely exceed human capacity to anticipate, calculate and plan for the "unknown unknowns"[33], and second, to point at an emerging tendency, potentially a new type of governance (Chandler 2014). The limits of the former and the requirements of latter effectively lead to "a fundamental acceptance of contingency and conditions of insecurity" (Kaufmann 2013, 59). Contingency planning seeks to ensure maintenance of (core) functions, focusing on the ability to respond to, and in a short time span, the most *probable* disruptive events. Too much reliance on contingency could, arguably, be a bellwether of reality in which a state of security is neither reached nor attempted.

If resilience *thrives on chaos* (Cavelty, et al. 2015), and requires a disturbance to manifest, then, through its expressions, it could presumably form a particular kind of subject that "actively contributes to the expansion and production" of crises and conflict (Cavelty, et al. 2015, 11). By extension, resilience not only enables responses to but could also prolong crises. Assisted, or organised, resilience could also generate dependence and inertia, thereby a decrease in self-sufficiency (individual resilience), which to (further) strain (limited) capacities in the, arguably, wrongful attempt at applying resilience as a universal solution to every and all complex

[33] Donald Rumsfeld, US Secretary of Defence, at a US Department of Defense (DoD) news briefing on February 12, 2002.

(future) challenges. It puts the subject into the focus of security and suffocates transformation, with instability being defined, within such a paradigm, as a state of potential change. Therefore, to ensure stability would require eliminating change, be it positive or negative, which then opens up space for speculating that resilience could not be applicable to crisis and disaster management as the latter seeks to establish a state of security, whereas the former – to perpetuate crisis.

"Shifting relations", the inherent non-linearity and dynamism, is what prompts the argument that the relation between crisis management, understood in (traditional) terms of linearity rather than as a process with relational dimensions, and resilience is seriously strained with the latter, effectively, making visible the limitations of the former, thus calling for reinvigoration and reconsideration of what crisis management is and how it is performed (Chandler 2019).

Conclusion

Ensuring security in a dynamic, complex, and uncertain environment requires innovation and flexibility, and thus, calls for an investigation into *that* which could contribute to adapting, overcoming, and improving[34]. Resilience unfolds as a demanding yet enabling concept, allowing the resilient subject to look, and see, beyond challenges presented by insecurity, and seek and seize opportunities for a better future (O"Malley

[34] Adopted from the infamous "Ultimate Survivor" series hosted by Bear Grylls.

2010). Indeed, looking at the respective, and proposed, continua of *crisis* and *resilience* one could not but notice, that the far end of a crisis – *disruption*, marks the beginning of resilience. The effects and implications of the latter warrant further scrutiny, particularly in terms of military resilience and civil preparedness in crisis and disaster management contexts, which to consequently serve to inform decision-making and (policy) planning.

Another (sequenced) highly enterprising research avenue would be on measurement and metrics so as to *make* resilience visible, thus allowing for critical assessment and (re)evaluation. NATO has already recognised that the 7 Baseline Requirements require, and do provide space for, improvement so as to strengthen their capacity to indicate the level (and progress thereafter) of civil preparedness across the Alliance, and within individual Allies (Roepke and Thankey 2019).

The role of the private sector in resilience for crisis and disaster management remains largely under-researched, specifically in relation to crisis management in a military context. Control over and access to critical (civilian) infrastructure requires close cooperation and exchange of information between relevant civil and military stakeholders, which could prove a choking point if not well systematised and coordinated.

Acknowledgement

The CMDR COE is committed to its thematic work on *resilience*, specifically as part of the Centre's support to NATO's Collaborative Resilience (CoRe) Concept development process. We have been, therefore, exerting dedicated efforts at actively contributing to the concept elaboration, to currently developing a course on the topic, in close cooperation with the Civil-Military Centre of Excellence (CCOE), whose pilot iteration is scheduled for December 2019 in Sofia. Moreover, and as a means of enriching the knowledge on and expertise in the practice of resilience, the 7th edition of the CMDR COE Annual Conference on Interagency Interaction in Crisis Management and Disaster Response (CMDR) (5-6 JUN 2019, Sofia, Bulgaria) featured a panel dedicated to exploring the concept of resilience in light of future crisis management and disaster response (CMDR).

The present article is to be seen as both the input to and output from the panel discussion: *Conceptualising Resilience – Enabling Future CMDR*. It is premised on a cross-disciplinary investigation into the growing body of research on resilience in international relations examined through the lens of the role of the military in a changing security environment. Its fabric is woven by the invaluable contributions of the panel members (in alphabetic order): Professor David Chandler (Westminster University); Dr. Florian Roth (Centre for Security Studies, ETH Zurich), LTC Jan Sabiniarz (Civil-Military Centre of Excellence

(CCOE)), and LTC Kostadin Lazarov (CMDR COE), to whom I express sincere gratitude for their constructive editorial comments and remarks on the draft of the article.

The overall inspiration for this work, and the opportunity for organising and moderating the panel discussion, I owe to Colonel Plamen Milanov (CMDR COE), who generously placed his confidence in my ideas, providing his unconditional support to the organisation of the panel.

I extend my gratitude to Mrs Svilena Darova (CMDR COE) – the penholder for the panel discussion minutes, for dedicatedly summarizing our thoughts and skilfully extracting the essence of the discussion, as well as to all CMDR COE staff members involved in the organisation of the Conference for professionally managing various technical arrangements, and ensuring the comfort of both – the panellists and the audience alike. (*Gergana Vaklinova*)

Bibliography

Adler-Nissen, Rebecca. "Stigma Management in International Relations: Transgressive Identities, Norms, and Order in International Society." International Organization 68, no. 1 (2014): 143-76. http://www.jstor.org/stable/43282098.

Berl, Ethel G. "Normality: An Historical and Comparative Analysis of the Concept." The Journal of Experimental Education 9, no. 1 (1940): 91-94. http://www.jstor.org/stable/20150641.

Cavelty, Myriam Dunn, Mareile Kaufmann, Kristensen, and Kristian Søby. 2015. “Resilience and (in)security: Practices, subjects, temporalities.” *Security Dialogue* 46 (1): 3-14. doi:10.1177/0967010614559637.

Chandler, David. 2014. “Beyond neoliberalism: resilience, the new art of governing complexity.” *Resilience* 2 (1): 47-63. doi:10.1080/21693293.2013.878544.

Chandler, David, interview by Vaklinova. 2019. “Conceptualising Resilience - Enabling Future CMDR.” *CMDR COE Annual Conference 2019.* Sofia, (5 June).

Chandra, Anita, Joie Acosta, Stefanie Stern, Lori Uscher-Pines, Malcolm Williams V, Douglas Yeung, Jeffrey Garnett, and Lisa Meredith S. 2011. “Definition and Application of Community Resilience.” In *Building Community Resilience to Disasters: A Way Forward to Enhance National Health Security*. RAND Corporation. https://www.jstor.org/stable/10.7249/tr915dhhs.10.

Civil-Military Centre of Excellence - CCOE. 2016. “CIMIC FIELD HANDBOOK 4th Edition.” Accessed 2019. https://www.cimic-coe.org/wp-content/uploads/2014/06/CFHB-4-0-CONTENT-1-5-E-Book-2.pdf.

Giroux, Jennifer. 2012. *Trends in Resilience: Spotlight on Teaching & Learning.* Factsheet No. 9, Center for Security Studies (CSS),, Zurich: ETH Zurich.

Giroux, Jennifer, and Tim Prior. 2012. *Expressions of Resilience: From ‘Bounce Back’ to Adaptation.* Risk and Resilience Research Group, Center for Security Studies (CSS), ETH Zürich.

Giroux, Jennifer, and Tim Prior. 2012. *Expressions of Resilience: From ‘Bounce Back’ to Adaptation.* Risk and Resilience Research Group, Center for Security Studies (CSS), ETH Zürich.

Goldstein, Evan Bruce. 2009. “Resilience to Surprises through Communicative Planning.” *Resilience Alliance Inc.* 14 (2). https://www.jstor.org/stable/26268334.

Gotts, Nicholas M. 2007. “Resilience, Panarchy, and World-Systems Analysis.” *Ecology and Society* (Resilience Alliance Inc.) 12 (1). https://www.jstor.org/stable/26267856.

Hamilton, S. Daniel. 2016. *Forward Resilience: Protecting Society in an Interconnected World.* Washington, DC: Centre for Transatlantic Relations.

Harvey, David L., and Michael Reed. "Social Science as the Study of Complex Systems." In Chaos Theory in the Social Sciences: Foundations and Applications, edited by Kiel L. Douglas and Elliott Euel, 295-324. Ann Arbor: University of Michigan Press, 1996. http://www.jstor.org/stable/10.3998/mpub.14623.16.

HQ SACT Strategic Plans and Policy. 2017. *Strategic Foresight Analysis.* NATO. Accessed 2018.

Kaufmann, Mareile. 2013. “Emergent self-organisation in emergencies: resilience rationales in interconnected societies.” *Resilience* 1 (1): 53-68. doi:10.1080/21693293.2013.765742.

Langeland, Krista S., David Manheim, Gary McLeod, and George Nacouzi. 2016. “Definitions, Characteristics, and Assessments of Resilience.” In *How Civil Institutions Build Resilience: Organizational Practices Derived from Academic Literature and Case Studies*. RAND Corporation. https://www.jstor.org/stable/10.7249/j.ctt1btc0m7.8.

Langeland, Krista S., David Manheim, Gary McLeod, and George Nacouzi. 2016. “Recover: Disaster Response and Recovery-Oriented Resilience.” In *How Civil Institutions Build Resilience*, 27-32. RAND Corporation. https://www.jstor.org/stable/10.7249/j.ctt1btc0m7.11.

Langeland, Krista S., David Manheim, McLeod, Gary, and George Nacouzi. 2016. “Summary of Themes and Methods for Building Resilience.” In *How Civil Institutions Build Resilience*, 33-38. RAND Corporation. https://www.jstor.org/stable/10.7249/j.ctt1btc0m7.12.

Lansing, J. Stephen. "Complex Adaptive Systems." Annual Review of Anthropology 32 (2003): 183-204. http://www.jstor.org/stable/25064826.

Lazarov, Kostadin, interview by Gergana Vaklinova. 2019. “Conceptualising Resilience - Enabling Future CMDR.” *CMDR COE Annual Conference .* Sofia, (5 July).

Mansbach, Richard W. "Integrating Normative Theory in Teaching International Relations." International Studies Perspectives 13, no. 1 (2012): 10-12. http://www.jstor.org/stable/44218673.

McClelland, Charles A. "The Function of Theory in International Relations." The Journal of Conflict Resolution 4, no. 3 (1960): 303-36. http://www.jstor.org/stable/172856.

McLeod, Gary, George Nacouzi, Paul Dreyer, Mel Eisman, Myron Hura, S Krista Langeland, Mayhem Manheim, and Geoffrey Torrington. 2016. “Resilience and Civil Institutions.” In *Enhancing Space Resilience Through Non-Materiel Means*, 7-14. Rand Corporation. https://www.jstor.org/stable/10.7249/j.ctt1btc13z.10.

Miller, John H., and Scott E. Page. "Social Science in Between." In Complex Adaptive Systems: An Introduction to Computational Models of Social Life, 213-26. Princeton University Press, 2007. http://www.jstor.org/stable/j.ctt7s3kx.17.

NATO - Strategic Plans and Policy. 2018. *Framework for Future Alliance Operations.* Norfolk: HQ Supreme Allied Commander Transformation.

O"Malley, Pat. 2010. “Resilient Subjects: Uncertainty, Warfare and Liberalism.” *Social Science Research Network Electronic Library.* http://ssrn.com/abstract=1600437.

Prior, Tim, and Jonas Hagmann. 2012. *Measuring Resilience: Benefits and Limitations of Resilience Indices.* SKI Focus Report 8, Zurich: Center for Security Studies (CSS), ETH Zurich. Accessed 2019.

Prior, Tim, and Michel Herzog. 2015. *Public interpretation of risk information: decisions and action.* Report 10, Center for Security Studies (CSS), Zurich: ETH Zurich.

Prior, Tom, and Michael Herzog. 2013. *The Practical Application of Resilience: Resilience Manifestation and Expression.* Center for Security Studies (CSS), ETH Zurich.

Roepke, Wolf-Diether, and Hasit Thankey. 2019. “Resilience - first line of defense.” *The Three Swords Magazine,* 50-53. http://www.jwc.nato.int/images/stories/_news_items_/2019/three-swords/ResilienceTotalDef.pdf.

Roth, Florian, interview by Gergana Vaklinova. 2019. “Conceptualising Resilience- Enabling Future CMDR.” *CMDR COE Annual Conference 2019.* Sofia, (5 June).

Sabiniarz, Jan, interview by Gergana Vaklinova. 2019. “Conceptualising Resilience - Enabling Future CMDR.” *CMDR COE Annual Conference 2019.* Sofia, (5 June).

Smart, Ian. "The Adopted Image: Assumptions about International Relations." International Journal 39, no. 2 (1984): 251-66. http://www.jstor.org/stable/40202333.

Spindler, Manuela. "Didactics and Method." In International Relations: A Self-Study Guide to Theory, 106-20. Opladen; Berlin; Toronto: Verlag Barbara Budrich, 2013. doi:10.2307/j.ctvdf09vd.7.

Strößner, Corina. "Normality and Majority: Towards a Statistical Understanding of Normality Statements." Erkenntnis (1975-) 80, no. 4 (2015): 793-809. http://www.jstor.org/stable/24735072;

Tanter, Raymond. "International System And Foreign Policy Approaches: Implications for Conflict Modelling and Management." In Theory and Policy in International Relations, edited by Tanter Raymond and Ullman Richard H., 7-39. Princeton University Press, 1972. http://www.jstor.org/stable/j.ctt13x143h.5.

Weltman, John J. "Systems Theory in International Relations: A Critique." Polity 4, no. 3 (1972): 301-29. doi:10.2307/3233964.

MANAGING RISK IN A MULTI-AGENCY, ALL-HAZARD ENVIRONMENT

Dr. Joseph GREEN, (Pacific Disaster Center, Kihei, Maui, Hawaii, USA)

Dr. Benjamin RYAN, (Daniel K. Inouye Asia-Pacific Center for Security Studies, Honolulu, USA)

Dr. Richard FRANKLIN, (College of Public Health, Medical and Veterinary Sciences, James Cook University, Townsville, Australia)

Prof. Deon CANYON, (Daniel K. Inouye Asia-Pacific Center for Security Studies, Honolulu, USA)

Prof. Frederick M. BURKLE, (Harvard Humanitarian Initiative, Harvard School of Public Health, Cambridge, USA)

Abstract: Application of national and sub-national indicators to rank and prioritize needs of people with life threatening conditions and chronic diseases before, during and after a disaster. This paper complements the presentation by Dr. Joseph Green at the 7th CMDR COE Annual Conference, June 6th, 2019. The methodology described in the subsequent pages addresses the presentation theme, Managing Risk in a Multi-Agency, All-Hazard Environment.

Key words: indicators, life threatening condition, chronic disease, disaster.

Introduction

The United Nations (UN) has recognized the risk disasters pose to people with life threatening conditions and chronic diseases in the *Sendai Framework for Disaster Risk Reduction: 2015-*

2030 (Sendai Framework) (UNISDR, 2015a). Item 30(k) of the Framework recommends people with life threatening and chronic diseases be included in the design of policies and plans to manage their risks before, during and after disasters (UNISDR, 2015a). This builds on the World Health Organization (WHO) *Global Action Plan for the Prevention and Control of Noncommunicable Diseases – 2013-2020* (Action Plan) (WHO, 2013). The World Economic Forum (WEF) also recognizes increasing "chronic diseases" as a global trend that could lead to rising costs of health care and threaten societal gains in life expectancy and quality (World Economic Forum, 2018).

Chronic diseases, also known as non-communicable diseases (NCD), are rarely cured prolonged illnesses that are not passed from person to person and include diabetes, cancer, cardiovascular diseases, respiratory conditions and renal diseases (WHO, 2018). Life threatening conditions require prompt health care (within 30 minutes) and can be the result of acute exacerbation of a chronic disease (Hirshon et al., 2013, NSW Government, 2017). Examples of life threatening conditions include: severe respiratory problems requiring endotracheal intubation, patients with seizures caused by cerebral malaria, bleeding that cannot be stopped, myocardial infarctions and acute cerebrovascular accidents (Hirshon et al., 2013).

The chronic disease burden is a global challenge. Chronic diseases account for 71% of deaths globally with almost three quarters occurring in low and middle-income countries (WHO, 2016a, WHO, 2018, Ryan et al., 2018). There are four major disease groupings that account for over 80% of premature deaths (before reaching 70 years of age): cardiovascular diseases (heart attack and stroke); cancers; respiratory diseases (chronic obstructive pulmonary disease and asthma); and diabetes (WHO, 2018). In low and middle-income countries, chronic diseases are responsible for 85% of premature deaths (WHO, 2018). Also, in low-resource settings there is reduced capacity for chronic disease treatment and care, meanwhile, people in high-income settings are almost four times more likely to have the required services covered by health insurance (WHO, 2018). The global chronic disease burden is impeding poverty reduction initiatives (WHO, 2018). The exorbitant costs of chronic diseases, including often lengthy and expensive treatment and loss of breadwinners is forcing millions of people into poverty annually, stifling development and increasing the population with poorly managed conditions (WHO, 2018).

While disasters can cause significant direct mortality and morbidity, they also result in widespread damage to public health infrastructure (PHI) required to maintain treatment and care for people with life threatening conditions and chronic diseases. This contributes to indirect mortality and morbidity,

primarily due to population displacement, disruption to supplies and damage to health facilities and systems (Burkle and Greenough, 2008). For example, post-Hurricane Katrina (2005; New Orleans) the mortality rate for the first six months of 2006 was 47% higher compared to the baseline (pre-Hurricane Katrina) and post Hurricane Maria (2017; Puerto Rico) there was a 62% increase in the mortality rate from September 20 through December 31 in 2017 compared with the same period in 2016 (Stephens et al., 2007, Kishore et al., 2018).

When the PHI required to maintain treatment and care (e.g. hospital, primary health care services, medications and safe water) is not recovered or rehabilitated in a timely manner a major and sustained “public health emergency” may occur (Burkle, 2014). People with chronic diseases at greatest risk are those with underlying cardiovascular and respiratory diseases, undergoing cancer treatment, unstable diabetes and renal diseases (Llewellyn, 2006, CDC, 2005, Evans, 2010, Demaio et al., 2013, Crook et al., 2010, Rath et al., 2007, Howe et al., 2008, Ryan et al., 2015b). This risk is anticipated to continue, if not increase, due to an increasing chronic disease burden combined with a changing climate, increasing frequency and intensity of disasters and rapid unsustainable urbanisation in flood plains and storm-prone coastal zones (COAG, 2011, McMichael et al., 2006, UNISDR, 2015a, CRED, 2015).

Traditionally the health focus before, during and after a disaster has been on communicable diseases. However, the actual risk of a disease outbreak after a disaster is low, particularly in developed countries, and there has been a “disease transition” in recent years to chronic diseases (Watson et al., 2007). This “disease transition” is due to combination of population aging, rapid unplanned urbanization, unhealthy diets, increasing obesity, decreasing physical activity, environmental change and reduction in communicable diseases (The Sphere Project, 2011, WHO, 2011b, WHO, 2015, Demaio et al., 2013).

Reducing the impact of disasters on people with life threatening conditions and chronic diseases is a complex challenge for disaster management and health systems. Heart attacks and strokes may be up to 2–3 times more likely in an emergency (a time when there are reduced resources) (WHO, 2016b). During the USA preparations and response to Hurricane Katrina, 33% of people presented to emergency shelters with chronic disease exacerbation (Evans, 2010). Following Hurricane Sandy, cardiac incidence increased by 22% and mortality of people with chronic diseases by 31% (Ryan et al., 2015b), (Swerdel et al., 2014). Cancer related deaths increased by 19% in the 12 months after Hurricane Iniki (1992) and in the weeks after Florida’s four hurricanes in 2004 (Hendrickson et al., 1997, McKinney et al., 2011). In addition, cardiac incidence increased by 22% and mortality by 31% in the 30 days after Hurricane Sandy (2012) (Swerdel et al., 2014),

The risk disasters pose to people with life threatening conditions and chronic diseases was further demonstrated by the indirect mortality in the three months after the 2011 Great East Japan Earthquake (Uchimura et al., 2014). The mortality rate for people over 60 years of age increased by 54% for those with Chronic Obstructive Pulmonary Disease (COPD), 48% for those with endocrine, nutritional and metabolic diseases, 41% if on dialysis, 37% with heart diseases (excluding hypertension), and 33% with cerebrovascular diseases (Uchimura et al., 2014). There was a decrease in the mortality rate for this cohort in the second month, however, there was a 143% increase in mortality in the 60-69 age group (Uchimura et al., 2014).

In conflict ridden complex humanitarian emergencies, chronic diseases are also a concern. For example, a survey of Syrian refugee households in Jordan found 50% had a person with a chronic disease (Doocy et al., 2013). The same study found 85% of people with chronic diseases sought treatment and care (Doocy et al., 2013). Meanwhile, of the Syrian refugees over 60 years in Lebanon, 60% had hypertension, 47% diabetes, 30% heart disease, 11% lung disease, 6% renal disease and 74% were dependent on humanitarian assistance for treatment and care (Strong et al., 2015).

Chronic diseases now make up a considerable proportion of hospital attendances following disasters (Aitken et al., 2015, Mitchell et al., 2014). For example, there was a 40% increase

in emergency department presentations at The Townsville Hospital, Australia, in the five days following Severe Tropical Cyclone Yasi (2011) due to disrupted access to treatment and care (Aitken et al., 2015). When the roads after Hurricane Harvey (2017; Houston, USA) became passable, the number of patients attending the Houston Methodist's Emergency Department's was between two and three times above average with many suffering chronic disease exacerbation due little to no access to medication (Huff, 2018). There is a developing evidence-base describing the risk of disaster-related exacerbation of chronic diseases with mitigation strategies recommended (ADEA, 2015, Ryan et al., 2016, Ryan et al., 2015b, Ryan et al., 2015a, Gnanapragasam et al., 2016, WHO, 2011a, Ryan et al., 2018, WHO, 2016b). For example, WHO published *Noncommunicable diseases in emergencies*; Emergency Management Australia *Disaster Health Handbook*; Australian Diabetes Educators Association (ADEA) *The needs of people with chronic diseases in natural disasters – A guide for state and local governments, emergency management services and the not-for-profit sector*; and Ryan et al (2018) a paper titled "Ranking and prioritizing strategies for reducing mortality and morbidity from noncommunicable diseases post disaster: an Australian perspective" (Ryan et al., 2018). However, there is little detail on how to systematically identify treatment and care needs of people with life threatening conditions and chronic diseases before, during and after a

disaster (Jobanputra et al., 2016, Commonwealth of Australia, 2011, WHO, 2016b).

To address this gap, this paper describes how a composite indicator approach using DisasterAWARE™ (All-hazard Warnings, Analysis, and Risk Evaluation) could systematically rank and prioritize the needs of people with life threatening and chronic diseases at national and sub-national levels. This includes discussing a composite indicator approach, describing DisasterAWARE™, outlining a systematic method for ranking and prioritizing needs, proposing a composite indicator for life threatening and chronic diseases, and an implementation strategy.

Composite indicator approach

This approach aims to acknowledge the multidimensional nature of risk and vulnerability while providing a necessary level of information for decision support. In addition, indicator-based disaster risk assessments can be useful hypothesis generation tools and method for increasing participation, and the interaction of stakeholders within and across disciplines (Nardo et al., 2005). Even with their drawbacks, the use of indicator-based approaches may have the effect of initiating an interest in the process of risk evaluation and the search for better data and models (Saisana, 2004, International Federation of Red Cross and Red Crescent Societies, 2006). The overarching goal of the composite-indicator approach should be to develop, as

stated by Saltelli: "…*a robust culture of evaluation of policies based on information*" (Saltelli, 2007).

Assessing and prioritizing the needs of people with life threatening and chronic diseases before, during and after disasters can facilitate the implementation of efforts to reduce indirect mortality and morbidity associated with natural disasters. Indicatorbased approaches, such as DisasterAWARE™, are particularly useful in this context due to the inclusion of variables representing the broader concepts of risk and vulnerability.

Thoughtful construction of a composite index can provide a quick overview of risk and its spatial and temporal distribution as well as a tool for benchmarking progress. This can facilitate the prioritization of populations in need or at risk and evidence-based allocation of resources. Indicators utilized for assessing multi-hazard risk are often conceptualized based on their relationship solely to "natural disaster" risk. However, factors contributing to disaster vulnerability also considerably overlap with the social determinants of health (Gray, 2017, Lindsay, 2003). Linking assessments of disaster risk reduction (DRR) and health provides an opportunity to decrease risk and vulnerability while minimizing the impact disasters pose to people with life threatening conditions and chronic diseases (Banwell et al., 2018).

There is no universally agreed approach to assessing and communicating risk. As a result, many indicator-based

approaches have been developed to rank, prioritize, and better understand disaster risk (for example, INFORM, City Resilience Index, WRR and PDC's RVA). Indicator-based approaches have also been leveraged for health system performance (Murray, et al 2000, WHO 2000) and human development (HDI) (Jāhāna, 2016). Many of the currently available disaster risk composite indicators attempt to operationalize the theoretical framework of disaster vulnerability as it has been outlined in the literature (Cardona and Carreño, 2011, Turner et al., 2003, Birkmann, 2007). Disaster vulnerability is a central and important component in aggregate disaster risk indices due to its representation of the human component. None, however, directly assess the impact disaster exposure may have on those with life threatening conditions and chronic diseases. A more thorough inclusion of indicators directly related to health could improve the understanding of the intersection of disaster vulnerability and health-related outcomes.

There is a substantial literature devoted to the construction, applications, and drawbacks of indicator-based approaches (Saisana, 2004, Metge et al., 2009, Nardo et al., 2005). Indicator-based approaches allow for the examination of complex, multidimensional concepts and often provide a single, composite measure. This approach promotes the use of baseline data for prioritization and decision making while facilitating the communication of complex ideas. The benefit of a composite index is the ability to summarize complex

phenomena while providing a starting point for ongoing discussion and evaluation (Metge et al., 2009, Nardo et al., 2005).

Composite indicators can be misleading if the user is not aware of the decisions made for the inclusion/exclusion of certain data, if certain potentially unmeasurable dimensions are not included, and if data of poor quality are used. An indicator-based approach is an oversimplification by nature. Therefore, an often-cited criticism levied against indicator-based approaches is that they provide the end user with an oversimplification of reality on which decisions are to be based (Saisana and Tarantola, 2002). One method for addressing these potential shortfalls is to provide a platform for the presentation of results whereby the data can be examined by the end user and broader contextual information is also readily available. The production of a comprehensive, technical report is a useful first step. However, end users at the decision making level do not often have the time or inclination to read lengthy reports. Therefore, an alternative presentation is often warranted. Web-based applications where each data set feeding into indicator and composite indicators as well as metadata including decisions and calculation steps can serve as a useful decision-support tool. Once such tool is Pacific Disaster Center's (PDC) DisasterAWARE™ platform.

DisasterAWARE™

DisasterAWARE™ is an integrated platform providing situational awareness, decision support, and information exchange capabilities to disaster management decision-makers. DisasterAWARE™ is made available in free-access (public) and limited access (password-protected) versions around the world to support early warning and humanitarian assistance activities in the realm of disaster management and risk reduction. The interactive system allows users to access actionable information based on user driven questions. Not only does this method and tool proved a richer context to risk information, it also seeks to address Target 7 of the Sendai Framework to "*substantially increase the availability of and access to multi-hazard early warning systems and disaster risk information and assessments to people by 2030*". (UNISDR, 2015a)

The DisasterAWARE™ platform incorporates international best-practice methodologies and technologies for data acquisition, hazard modeling, risk and vulnerability assessment, mapping, visualization, and communications into one system while continually monitoring information feeds from reliable meteorological and geological agencies around the world ensuring accurate, real-time reporting of hazard events. Hazard data are put into context for responders in an easy-to-use, but sophisticated geospatial information environment. Collaborating experts can instantly share analyses and

situational reports through a simple process, supported (where appropriate) by a mobile application interface, thereby enriching the knowledge base for all stakeholders.

Method to systematically rank and prioritize needs

Using a composite indicator-based approach, a new method to systematically rank and prioritize the needs of populations with life threatening conditions and chronic diseases is proposed. The indicator-based approach has four (4) main purposes:

1. To systematically rank and prioritize the needs of people with life threatening and chronic disease before, during and after a disaster.
2. To establish a baseline to measure progress in addressing the disaster vulnerabilities of those with life threatening conditions and chronic diseases.
3. To better understand the complex relationship between life threatening conditions, chronic diseases, and disaster risk.
4. To better communicate the complex relationship between life threatening conditions, chronic diseases, and disaster risk.

Indicator selection and rationale

The selection of health indicators to be used and the structure of a composite index are determined by their ability to approximate the vulnerabilities, needs and abilities of those with life threatening diseases and chronic conditions have in

preparing for, responding to, and recovering from disasters (CDC, 2017). The inclusion of multiple indicators may represent domains which are proxy measures for more complex phenomena. For example, indicators suited for the assessment of population health can be grouped into one of four general domains: health status, risk factors, service coverage, and health systems. (Stevens et al., 2016, WHO, 2014).

Existing composite indicators such as PDC's Risk and Vulnerability Assessment (IHME, 2017) and the JRC's INFORM (De Groeve et al., 2016) attempt to assess health status as a vulnerability. PDC's assessment includes a vulnerability sub-domain of vulnerable health status. The indicators aggregated to approximate vulnerable health status are included to reflect the population's general health. The rationale for inclusion is that poor health contributes to increased susceptibility to injury, disease, and stress associated with disasters and may necessitate special accommodations for activities such as evacuation. The indicators that comprise this sub-domain of disaster vulnerability are:

- Life Expectancy (UNDP-HDI, World Bank)
- Infant Mortality (World Bank)
- Maternal mortality (World Bank)
- Prevalence Undernourished (World Bank)

As the assessment is designed to rank, assess and establish a baseline measure for natural disaster risk at the country-level the indicators chosen are often a composite that measure broader concepts like exiting mortality patterns (life expectancy

at birth), gender-based access to care (maternal mortality), risk factors for further morbidity and mortality (prevalence undernourished). Together, these provide a country-level measure of potential disaster vulnerability due to existing forces of morbidity and mortality as well as access to care.

The INFORM index (De Groeve et al., 2016) by contrast includes health measures as part of the “Vulnerable Groups” sub-domain of vulnerability to humanitarian crisis. Within the “Other Vulnerable groups/Health conditions” component, INFORM includes variables measuring:

- HIV Prevalence
- Tuberculosis prevalence
- Malaria Mortality Rate
- INFORM also includes the HDI and Multidimensional Poverty Index (MPI) as part of the vulnerability domain. These include measures of life expectancy. Maternal Mortality Ratio is included as part of the access to health care index.

Both the PDC and INFORM indicators include some measures of health to assess the increase in vulnerability due to intrinsic internal qualities of individual[s] (De Groeve et al., 2016). Neither directly addresses the unique, intrinsic qualities of those living with the life threatening conditions and chronic diseases when facing natural hazard exposure(s).

A composite indicator of Health-related Sustainable Development Goals (SDG) Indicators has been developed by the Global Burden of Disease Collaborative Network (Fullman et al., 2017). This composite indicator was developed as a measure of health related SDG attainment for the country level. The Health-Related Sustainable Development Goals Indicators assess 37 indicators, with some addressing chronic disease risk factors. This index however, it is not a comprehensive assessment of chronic disease as a vulnerability to natural disasters.

There appears to be a gap between health-related assessments and disaster vulnerability assessments focusing on health status. To address this gap a composite indicator of disaster vulnerability tailored for those with life threatening conditions and chronic diseases is proposed. Indicator selection is driven by conceptual match to domains and sub-domains, data availability, and data quality. The composite indicator example given here is for a country to country comparison. The same framework can be applied to sub-national level assessments as well. The difference in a global, country to country assessment and a sub-national assessment lies in the implementation. The implementation of a sub-national assessment should include extensive input from vested stakeholders. Disease patterns, capacities and vulnerabilities as well as data availability differ from country to country and, as such, planned assessments

should account for these to best describe the distribution of vulnerability within a country.

Composite indicator for life threatening conditions and chronic diseases

The purpose of the proposed indicator-based approach is to provide a measure of disaster vulnerability among those with life threatening conditions and chronic diseases. Using PDC's Multi-Hazard Risk and Vulnerability Assessment as a guide, the proposed composite indicator envisages disaster risk as the product of population-level hazard exposure and chronic disease-based vulnerability. This equation is consistent with the disaster literature (De Groeve et al., 2016, Cardona and Carreño, 2011). To represent the multiplicative nature of the disaster risk model in a composite indicator form, the geometric mean of multi-hazard exposure and vulnerability are calculated (Equation 1).

$$Multi\text{-}Hazard\ Disaster\ Risk = (Multi - Hazard\ Exposure)^{½} (Vulnerability)^{½}$$

Equation 1. Multi- Hazard Disaster Risk

Domain: Multi-hazard exposure

Exposure considers four hazard types: tropical cyclone winds (Categories 1-4), tsunamis, earthquakes (MMI 7 and above), and floods. For each of the four hazard types, exposure is calculated based on the estimated average annual occurrence of hazard events equal to or greater than a given magnitude and

the estimated population or Grod Domestic Product (GDP) that falls within the modeled spatial extent of those events. Probabilities and spatial extents are estimated based on historical events and a variety of modeling approaches. While other hazards may be of critical importance in certain regions, these four hazards were included in the analysis because they are widespread, cause the most damage globally, are easily compared, and because input data and modeling techniques tend to be more advanced or appropriate for global analysis than for some other hazards (e.g., drought, landslides). All data sets were derived using data from the *2015 Global Assessment Report on Disaster Risk Reduction* (UNISDR, 2015b) except for riverine flood exposure. Riverine flood exposure was obtained from the 2015 World Resources Institute (Luo et al., 2015). Multi-Hazard Exposure is the arithmetic mean of raw exposure and relative exposure (Equation 2).

$$Multi\text{-}Hazard\ Exposure = \frac{Raw\ Exposure + Relative\ Exposure}{2}$$

Equation 2

Raw exposure is designed to provide an indication of "how many or how much" of the population or economic stock is exposed. This can assist in planning and give an idea of the raw scale of potential activities. Raw exposure is the geometric mean of total population exposed to hazards and the total economic exposure to hazards (Equation 3).

$$Raw\ Exposure = (Raw\ Population\ Exposure)\ ½\ (Raw\ Economic\ Exposure)\ ½$$

Equation 3

Relative exposure represents exposure as the geometric mean of the proportion of the base population exposed to hazards and the economic stock exposed as a proportion of the GDP. This indicator (Equation 4) provides information on *how important* an event may be thereby assisting with prioritization of resources.

$$Relative\ Exposure = (Relative\ Population\ Exposure)\ ½\ (Relative\ Economic\ Exposure)\ ½$$

Equation 4

Domain: Vulnerability

The domain of chronic disease-based vulnerability is the geometric mean of population-level vulnerable health status and one minus public health infrastructure (Equation 5). Public health infrastructure is conceptualized as a capacity to deal with chronic disease burdens and risk factors. In this case, infrastructure is a positive attribute of the population and serves to counterbalance the vulnerable health status. Therefore, to provide a measure in a direction consistent with risk (higher values representing a higher risk), public health infrastructure is presented as a *1-public health infrastructure.*

$$Vulnerability = (Vulnerable\ Health\ Status)\ ½\ (1 - Public\ Health\ Infrastructure)\ ½$$

Equation 5

Sub-domain: Vulnerable health status

Vulnerable health status reflects the population's health as it relates to life threatening conditions and chronic diseases. People with these conditions are at an increased risk for indirect mortality following a natural disaster. [23,32-36] Therefore, it is essential that any indicator-based approach assess the current chronic disease burden within a population. Vulnerable health status (Equation 6) is assessed as the geometric mean of the chronic disease burden and the prevalence of risk factors within the population under study.

$$Vulnerable\ Health\ Status = (Chronic\ disease\ burden)\ ½\ (Chronic\ disease\ risk\ factors)\ ½$$

Equation 6

Chronic disease burden

Chronic diseases are not passed from person to person, are long-lasting and place a great burden on patients, health services and fiscal systems (WHO, 2018, Queensland Health, 2016). The bulk of ill health, disability and premature death around the globe now generates from chronic diseases (Murray et al., 2013, WHO, 2013). This assessment considers four main groupings: cardiovascular diseases; cancers; chronic respiratory diseases; and diabetes (AIHW, 2014, WHO, 2018).

These conditions have common behavioural risk factors (smoking, physical inactivity, poor nutrition and harmful use of alcohol) and account for 79% of chronic disease deaths globally (AIHW, 2014, WHO, 2018). Those are greatest risk post disaster are patients undergoing cancer treatment, with underlying cardiovascular and respiratory diseases, unstable diabetes and renal diseases, especially if receiving dialysis, and mental health conditions (Ryan et al., 2015b). For this reason, the chronic disease terms used as indicators for this methodology were: cardiovascular disease, cerebrovascular disease, cancers, diabetes, renal diseases, and respiratory conditions. Table 1 is a compilation of indicators included in the NDC burden.

Table 1. Indicators included in the chronic disease burden.

Indicator	Associate Measure(s)	Data Source
Cardiovascular Disease	Cardiovascular Disease Prevalence	GBD 2016 (IHME, 2017)
Cerebrovascular Disease	Cerebrovascular Disease Prevalence	GBD 2016 (IHME, 2017)
Cancers	Neoplasm Prevalence	GBD 2016 (IHME, 2017)
Diabetes	Diabetes Prevalence	GBD 2016 (IHME, 2017)
Renal Disease	Chronic Kidney Disease Prevalence	GBD 2016 (IHME, 2017)
Respiratory diseases	Chronic Respiratory Disease Prevalence	GBD 2016 (IHME, 2017)

Chronic disease risk factors

Although the current disease burden is an essential element of any assessment of disaster vulnerability among those with life threatening conditions and chronic diseases, risk factors are an important consideration as well. Socio-economic components of vulnerability are conceptualized as the modifiable risk factors present at the societal level that affect health risks and outcomes (Gray, 2017, CDC, 2017). These elements are largely thought to represent the underlying conditions associated with health inequalities (AIHW, 2016). The multidimensional poverty index (MPI) is included as an indicator of these inequalities (Jāhāna, 2016). These will allow for the identification of groups that suffer disproportionate health consequences. Populations with high prevalence of risk factors will likely give rise to incident cases of chronic disease thus increasing the vulnerability of the population beyond the current level. Moreover, chronic disease risk factors may increase disaster vulnerability (CDC, 2014, Department of Health, 2014, AIHW, 2014). For example, people with severe or morbid obesity (a risk factor for other chronic diseases) have been negatively impacted by natural disasters (Gray, 2017). Social determinants of health significantly overlap with components of poverty and disaster vulnerability (Lindsay, 2003). Identifying the spatial and temporal pattern of these components can guide efforts to reduce incident disease and strengthen DRR activities. This subdomain is the arithmetic mean of the included

indicators. Table 2 is a compilation of included indicators of chronic disease risk factors.

Indicator	Associate Measure(s)	Data Source
Poverty	Multidimensional Poverty Index	UNDP (Jāhāna, 2016)
Tobacco Consumption	Number of cigarettes smoked per person per year: age ≥ 15	GBD 2016 (IHME, 2017)
Alcohol Consumption	Risk-weighted prevalence of alcohol consumption, as measured by the summary exposure value (SEV) for alcohol use (%)	GBD 2016 (IHME, 2017)
Elevated fasting blood glucose	Raised fasting blood glucose (≥ 7.00 mmol/L or on medication) (age standardized)	WHO Global Health Observatory data
Elevated Blood Pressure	Raised blood pressure (SBP ≥ 140 or DBP ≥ 90), age standardized (%)	WHO Global Health Observatory data
Ambient Air Pollution	Population-weighted mean PM2.5 levels	GBD 2016 (IHME, 2017)
Overweight/Obesity	Prevalence of overweight among adults, BMI ≥ 25, age standardized	WHO Global Health Observatory data
Physical Inactivity	Prevalence of insufficient physical activity among adults, age standardized	WHO Global Health Observatory data

Table 2 Indicators included in chronic disease risk factors

Sub-domain: Public health infrastructure

This domain attempts to capture the presence, strength and availability of a national public health system. This indicator is based on the definition developed by Ryan et al (2016, p.10):

"The workforce, equipment, supplies, and protection services required to maintain the health and wellbeing of individuals and the community"

This measure includes the presence of a functioning system of health care delivery and a measure of service access and quality. The indicator is the arithmetic average of health service access and quality and health system infrastructure (Equation7).

$$Public\ Health\ Infrastructure = \frac{(Health\ Service\ Access\ and\ Quality) + (Health\ System\ Infrastructure)}{2}$$

Equation 7 Healthcare Service Access and Quality

Healthcare Service Access and Quality (Table 3) is assessed by the Healthcare Access and Quality Index constructed by the GBD 2016 Healthcare Access and Quality Collaborators. This index provides a comparison measure of mortality based healthcare access and quality at the national level (Barber et al., 2017).

Indicator	Associate Measure(s)	Data Source
Healthcare access and quality	Healthcare Access and Quality Index	GBD 2017 (Barber et al., 2017)

Table 3. Indicators included in Healthcare access and quality

Health System Infrastructure

Health system infrastructure is the arithmetic average of all included indicators. Indictors are measures of workforce density, vaccination coverage, funding, and statistical capacity. Table 4 is a summary of indicators included in health system infrastructure.

Table 4. Indicators included in health system infrastructure

Indicator	Associate Measure(s)	Data Source
Workforce Density	Physicians Per 1000* Nurses and Midwives per 1000 Pharmaceutical personnel per 1000	WHO Global Health Observatory
Vaccination Coverage	Diphtheria tetanus toxoid and pertussis (DTP3) Coverage Measles (MCV2) Coverage	WHO Global Health Observatory
System Funding	Per Capita Public and Private expenditure on healthcare	WHO Global Health Observatory

Statistical Capacity	Percentage of well-certified deaths by a vital registration (VR) system among a country's total population	GBD 2016 (IHME, 2017)

Implementation strategy

Implementation of the composite indicator for life threatening conditions and chronic disease will require expansion of the traditional health focus of disaster management beyond immediate trauma and communicable diseases. This facilitation of change can occur system-wide though a collaborative governance approach and integration of a composite indicator into performance monitoring requirements. The type of change required aligns with Promoting Action on Research Implementation in Health Services framework (Kitson et al., 1998). PARIHS has been successfully applied in the field of health to implement evidence into practice (Harvey and Kitson, 2015). It includes three elements, evidence base (demonstrated in this paper (Ryan et al., 2015a, Ryan et al., 2015b, Ryan et al., 2017, Ryan et al., 2016, Ryan et al., 2018), context (life threatening conditions, chronic disease burden, increasing disaster risks and the Sendai Framework) and facilitation of change (the next step) (Rabin et al., 2008). Recommendations on how the final element (facilitation) can be achieved is described in the following.

System-wide change

Implementation of the composite indicator, through a system such as DisasterAWARE^{TM}, will help ensure disaster and health systems expand their focus to include indirect mortality and morbidity. This is required because disasters are often measured in terms of direct consequences; however, the majority of losses (as high as 70%–90%) are indirect deaths that would not have occurred without the breakdown of infrastructure (Burkle and Greenough, 2008). The composite indicator described provides a repeatable methodology to systematically rank and prioritize needs of people with life threatening conditions and chronic diseases. Application across disaster preparedness, response and recovery would allow treatment and care needs for vulnerable populations to be better identified and understood across agencies at national and sub-national levels. Ultimately, leading to a system-wide change by ensuring all aspects of health risks associated with disasters are systematically ranked and prioritized.

The methodology proposed would also provide an integrated and effective information sharing system about life threatening conditions and chronic diseases. This overcomes ethical and community willingness considerations, which are often a barrier to ensure accurate and effective disaster planning and response (Ryan et al., 2016). For example, registers of vulnerable populations in Australia (includes people with life threatening conditions and chronic diseases) are maintained by

local governments and are voluntary (Department of Health and Human Services, 2015). This results in an underestimate of the vulnerable population, for example, in Victoria, Australia, there is less than 1,350 people registered from a population of around six million (ABS, 2016, Garlick, 2015). Using a composite indicator-based approach would overcome this challenge by leveraging existing data and systems used at sub-national and national levels to share information across agencies.

Collaborative governance

Due to the range of sectors, organizations and disciplines involved in disaster management, a collaborative governance approach is required to facilitate change (Aitsi-Selmi and Murray, 2015). This is due to the range of infrastructure and services required to treat and care for people with life threatening conditions and chronic diseases. Also, the risk disasters pose to life threatening conditions and chronic diseases may not be seen as a priority for those outside the health sector. Demonstrating the need for cross and intra sectoral planning at a whole of government level (the foundation of collaborative governance) (Aitsi-Selmi and Murray, 2015).

Implementation should be led by national disaster management offices and include non-government and private sector organizations. This would need to include: engagement in comprehensive and shared planning; formal communication across multiple levels; and pooling and jointly acquiring

resources to implement and sustain the composite indicator (O'Flynn and Wanna, 2008).

Integration into performance and monitoring

To sustainably implement composite indicator method described, it should be integrated into performance and monitoring of the disaster and health sectors during non-disaster periods (Ryan et al., 2016). This could be achieved by integrating this as a requirement in strategic plans, business operations and where applicable accreditation/certification process at sub-national levels. This could include, for example, requirements to demonstrate its use and how the data collected is applied to disaster planning and response. This would help ensure the needs of people with life threatening conditions and chronic diseases are integrated into system-wide activities, budgets, policies, programs and plans.

Conclusion

The increasing global burden of life threatening conditions and chronic disease, changing climate, and rapid unsustainable urbanisation in disaster prone areas highlights the need to systematically rank and prioritize the needs of vulnerable populations. The composite indicator approach and its use in DisasterAWARE™ (All-hazard Warnings, Analysis, and Risk Evaluation) presented in this paper acknowledges the multidimensional nature of risk and vulnerability while providing a necessary level of information for decision support. This is

achieved by: providing a repeatable and systematic process to rank and prioritize the needs of people with life threatening and chronic disease before, during and after a disaster; establishing a baseline to measure progress in addressing disaster vulnerabilities; better understanding the complex relationship between health conditions and disaster risk; and enhancing communication across disciplines and agencies. Ultimately, implementation of the composite indicator will support the Sendai Framework by providing disaster and health systems with reliable information to accurately develop plans and strategies for reducing indirect disaster-related mortality and morbidity.

Bibliography

ABS. 2016. Australian demographic statistics, Sep 2015, catalogue no. 3101.0 [Online]. Canberra, ACT: Australian Bureau of Statistics. Available: http://www.abs.gov.au/ausstats/abs@.nsf/mf/3101.0 [Accessed 12 April 2016].

ADEA 2015. THE NEEDS OF PEOPLE WITH DIABETES AND OTHER CHRONIC

CONDITIONS IN NATURAL DISASTERS: A Guide for Emergency Services, Local Councils and the Not-for-Profit Sector. In: Health, D. o. (ed.). Canberra, Australia: Diabetes Australia and the Australian Diabetes Educators Association.

AIHW 2014. Australia's health 2014. Canberra, Australlia: Australian Institute of Health and Welfare.

AIHW. 2016. Australia's Health - Social Determinants of Health [Online]. Available: http://www.aihw.gov.au/australias-health/2016/determinants/ [Accessed].

Aitken, P., Franklin, R. C., Lawlor, J., Mitchell, R., Watt, K., Furyk, J., Small, N., Lovegrove, L. & Leggat, P. 2015. Emergency Department Presentations following Tropical Cyclone Yasi. PloS one, 10, e0131196.

Aitsi-Selmi, A. & Murray, V. 2015. The Sendai framework: disaster risk reduction through a health lens. Bulletin of the World Health Organization, 93, 362-362.

Banwell, N., Rutherford, S., Mackey, B. & Chu, C. 2018. Towards Improved Linkage of Disaster Risk Reduction and Climate Change Adaptation in Health: A Review. International journal of environmental research and public health, 15, 793.

Barber, R. M., Fullman, N., Sorensen, R. J., Bollyky, T., McKee, M., Nolte, E., Abajobir, A. A., Abate, K. H., Abbafati, C. & Abbas, K. M. 2017. Healthcare Access and Quality Index based on mortality from causes amenable to personal health care in 195 countries and territories, 1990–2015: a novel analysis from the Global Burden of Disease Study 2015.

The Lancet, 390, 231-266.

Birkmann, J. 2007. Risk and vulnerability indicators at different scales: Applicability, usefulness and policy implications. Environmental hazards, 7, 20-31.

Burkle, F. M. 2014. Public Health Issues in Disaster Management. The Wiley Blackwell Encyclopedia of Health, Illness, Behavior, and Society. John Wiley & Sons, Ltd.

Burkle, F. M. & Greenough, P. G. 2008. Impact of public health emergencies on modern disaster taxonomy, planning, and response. Disaster medicine and public health preparedness, 2, 192-199.

Cardona, O. D. & Carreño, M. L. 2011. Updating the indicators of disaster risk and risk management for the Americas. IDRiM Journal, 1, 27-47.

CDC 2005. Epidemiologic assessment of the impact of four hurricanes--Florida, 2004. MMWR: Morbidity and Mortality Weekly Report, 54, 693-697.

CDC. 2014. Chronic Diseases and Health Promotion [Online]. Centers for Disease Control and Prevention. Available: http://www.cdc.gov/chronicdisease/overview/index.htm [Accessed 25 October 2014].

CDC 2017. Social determinants of health: Know what affects health, Center for Disease Control and Prevention.

COAG 2011. National Strategy for Disaster Resilience – Building the resilience of our nation to disasters, Barton, ACT, Commonwealth of Australia.

Commonwealth of Australia 2011. Disaster Health Handbook In: Department, A.-G. s. (ed.). Barton.

CRED 2015. The Human Cost of Natural Disasters - A Global Perspective, Centre for Research on the Epidemiology of Disasters.

Crook, E. D., Arrieta, M. I. & Foreman, R. D. 2010. Management of Hypertension Following Hurricane Katrina: A Review of Issues in Management of Chronic Health Conditions

Following a Disaster. Current Cardiovascular Risk Reports, 4, 195-201.

De Groeve, T., Poljansek, K. & Vernaccini, L. 2016. Index For Risk Management - INFORM Concept and Methodology Version 2016. Luxembourg: European Commission Joint Research Centre Institute for the Protection and Security of the Citizen.

Demaio, A., Jamieson, J., Horn, R., de Courten, M. & Tellier, S. 2013. Non-communicable diseases in emergencies: a call to action. PLoS currents, 5.

Department of Health. 2014. Chronic Disease [Online]. Australian Government. Available: http://www.health.gov.au/internet/main/publishing.nsf/Content/chronic-disease [Accessed 24 June 2015].

Department of Health and Human Services 2015. Vulnerable people in emergencies - Guideline 1 - Planning and screening. Melbourne, Australia: Victoria Government.

Doocy, S., Dick, A., Daniels, A. & Kirsch, T. D. 2013. The Human Impact of Tropical Cyclones: a Historical Review of Events 1980-2009 and Systematic Literature Review. PLoS Currents, 5.

Evans, J. 2010. Mapping the vulnerability of older persons to disasters. International Journal of Older People Nursing, 5, 63-70.

Fullman, N., Barber, R. M., Abajobir, A. A., Abate, K. H., Abbafati, C., Abbas, K. M., Abd-Allah, F., Abdulkader, R. S., Abdulle, A. M. & Abera, S. F. 2017. Measuring progress and projecting attainment on the basis of past trends of the health-related Sustainable Development Goals in 188 countries: an analysis from the Global Burden of Disease Study 2016. The Lancet, 390, 1423-1459.

Garlick, D. 2015. The vulnerable people in emergencies policy: hiding vulnerable people in plain sight. Australian Journal of Emergency Management, 30, 31.

Gnanapragasam, S., Aitsi-Selmi, A., Rashbrook, E. & Murray, V. 2016. Addressing noncommunicable diseases in disaster risk reduction–an issue of equity. Journal of epidemiology and global health, 6, 119-121.

Gray, L. 2017. Social Determinants of Health, Disaster Vulnerability, Severe and Morbid Obesity in Adults: Triple Jeopardy? International Journal of Environmental Research and Public Health, 10.

Harvey, G. & Kitson, A. 2015. Implementing evidence-based practice in healthcare, London, Routledge.

Hendrickson, L. A., Vogt, R. L., Goebert, D. & Pon, E. 1997. Morbidity on Kauai before and after Hurricane Iniki. Preventive Medicine, 26, 711-716.

Hirshon, J. M., Risko, N., Calvello, E. J., Ramirez, S. S. d., Narayan, M., Theodosis, C. & O'Neill, J. 2013. Health systems and services: the role of acute care. Bulletin of the World Health Organization, 91, 386-388.

Howe, E., Victor, D. & Price, E. G. 2008. Chief complaints, diagnoses, and medications prescribed seven weeks post-Katrina in New Orleans. Prehospital and Disaster Medicine, 23, 41-47.

Huff, C. 2018. Lessons From an Extreme Hurricane Season: Staffing, Logistics Strain Safety Net. Elsevier.

IHME 2017. Global Burden of Disease Study 2016 (GBD 2016) Population Estimates 19502016, Seatle, Institute for Health Metrics and Evaluation (IHME).

International Federation of Red Cross and Red Crescent Societies. 2006. What is VCA? An introduction to vulnerability and capacity assessment [Online]. Geneva: International

Federation of Red Cross and Red Crescent Societies. Available: http://www.ifrc.org/Global/Publications/disasters/vca/whats-vca-en.pdf [Accessed 28 July 2017].

Jāhāna, S. 2016. Human development report 2016: human development for everyone, United Nations Publications.

Jobanputra, K., Boulle, P., Roberts, B. & Perel, P. 2016. Three Steps to Improve Management of Noncommunicable Diseases in Humanitarian Crises. PLoS Med, 13, e1002180.

Kishore, N., Marqués, D., Mahmud, A., Kiang, M. V., Rodriguez, I., Fuller, A., Ebner, P., Sorensen, C., Racy, F. & Lemery, J. 2018. Mortality in Puerto Rico after Hurricane Maria. New England journal of medicine.

Kitson, A., Harvey, G. & McCormack, B. 1998. Enabling the implementation of evidence based practice: a conceptual framework. Quality in Health care, 7, 149-158.

Lindsay, J. R. 2003. The determinants of disaster vulnerability: Acheiving sustainable mitigation through population health. Natural Hazards, 13.

Llewellyn, M. 2006. Floods and Tsunamis. Surgical Clinics of North America, 86, 557-578.

Luo, T., Winsemius, H. & Ward, P. 2015. Aqueduct Global Flood Risk Country Rankings. Washington D.C: World Resoureces Institute.

McKinney, N., Houser, C. & Meyer-Arendt, K. 2011. Direct and indirect mortality in Florida during the 2004 hurricane season. International journal of biometeorology, 55, 533-546. McMichael, A.

J., Woodruff, R. E. & Hales, S. 2006. Climate change and human health: present and future risks. The Lancet, 367, 859-869.

Metge, C., Chateau, D., Prior, H., Soodeen, R., De Coster, C. & Barre, L. 2009. Composite measures/indices of health and health system performance. Winnipeg, MB: Manitoba Centre for Health Policy.

Mitchell, R. D., Aitken, P. & Franklin, R. C. 2014. The physical health impacts of tropical cyclones. Annals of the ACTM: An International Journal of Tropical and Travel Medicine, 15, 2.

Murray, C. J., Vos, T., Lozano, R., Naghavi, M., Flaxman, A. D., Michaud, C., Ezzati, M.,

Shibuya, K., Salomon, J. A. & Abdalla, S. 2013. Disability-adjusted life years (DALYs) for 291 diseases and injuries in 21 regions, 1990–2010: a systematic analysis for the Global Burden of Disease Study 2010. The Lancet, 380, 2197-2223.

Nardo, M., Saisana, M., Saltelli, A. & Tarantola, S. 2005. Tools for Composite Indicators Building Ispra, Italy, Joint Research Centre

NSW Government. 2017. Hospital triage [Online]. NSW Health. Available: http://www.health.nsw.gov.au/Hospitals/Going_To_hospital/Pages/triage.aspx [Accessed 3 August 2018].

O'Flynn, J. & Wanna, J. 2008. Collaborative Governance: A new era of public policy in Australia?, ANU Press.

Queensland Health. 2016. The Health of Queenslanders 2016 [Online]. Brisbane, Australia:

Queensland Government. Available: https://www.health.qld.gov.au/__data/assets/pdf_file/0017/537101/cho-reportcomplete.pdf [Accessed 1 April 2017].

Rabin, B. A., Brownson, R. C., Haire-Joshu, D., Kreuter, M. W. & Weaver, N. L. 2008. A glossary for dissemination and implementation research in health. Journal of Public Health Management and Practice, 14, 117-123.

Rath, B., Donato, J., Duggan, A., Perrin, K., Bronfin, D. R., Ratard, R., VanDyke, R. & Magnus, M. 2007. Adverse health outcomes after Hurricane Katrina among children and adolescents with chronic conditions. Journal of Health Care for the Poor & Underserved, 18, 405-417.

Ryan, B. J., Franklin, R. C., Burkle, F. M., Watt, K., Aitken, P., Smith, E. C. & Leggat, P. 2015a. Analyzing the impact of severe tropical Cyclone Yasi on public health infrastructure and the management of noncommunicable diseases. Prehospital and disaster medicine, 1-10.

Ryan, B. J., Franklin, R. C., Burkle, F. M., Watt, K., Aitken, P., Smith, E. C. & Leggat, P. 2015b.

Identifying and Describing the Impact of Cyclone, Storm and Flood Related Disasters on Treatment Management, Care and Exacerbations of Non-communicable Diseases and the Implications for Public Health. PLOS Currents: Disasters.

Ryan, B. J., Franklin, R. C., Burkle, F. M., Watt, K., Smith, E. C., Aitken, P. & Leggat, P. 2017. The role of environmental health in understanding and mitigating post-disaster noncommunicable diseases: The critical need for improved multidisciplinary solutions Journal of Environmental Health.

Ryan, B. J., Franklin, R. C., Burkle Jr, F. M., Aitken, P., Smith, E., Watt, K. & Leggat, P. 2016.

Reducing Disaster Exacerbated Non-communicable Diseases Through Public Health Infrastructure Resilience: Perspectives of Australian Disaster Service Providers. PLOS Currents Disasters.

Ryan, B. J., Franklin, R. C., Burkle Jr, F. M., Aitken, P., Smith, E., Watt, K. & Leggat, P. 2018. Ranking and prioritizing strategies for reducing mortality and morbidity from noncommunicable diseases post disaster: an Australian perspective. International Journal of Disaster Risk Reduction 27, 223-238.

Saisana, M. Composite Indicators - A review. Second Workshop on Composite Indicators of Countnry Performance, 2004 Paris. Organisation for Economic Co-operation and Development (OECD), 29.

Saisana, M. & Tarantola, S. 2002. State-of-the-art report on current methodologies and practices for composite indicator development. Ispra: European Commision-Joint Research Centre.

Saltelli, A. 2007. Composite Indicators Between Analysis and Advocacy. Social Indicators Research, 65-77.

Stephens, K. U., Grew, D., Chin, K., Kadetz, P., Greenough, P. G., Burkle, F. M., Robinson, S. L. & Franklin, E. R. 2007. Excess mortality in the aftermath of Hurricane Katrina: a preliminary report. Disaster Medicine and Public Health Preparedness, 1, 15-20.

Stevens, G. A., Alkema, L., Black, R. E., Boerma, J. T., Collins, G. S., Ezzati, M., Grove, J. T., Hogan, D. R., Hogan, M. C., Horton, R., Lawn, J. E., Marusic, A., Mathers, C. D., Murray, C. J. L., Rudan, I., Salomon, J., Simpson, P. J., Vos, T. & Welch, V. 2016. Guidlines for Accurate and Transparent Health Estimates Reporting: The GATHER Statement. PLOS Medicine, 1-8.

Strong, J., Varady, C., Chahda, N., Doocy, S. & Burnham, G. 2015. Health status and health needs of older refugees from Syria in Lebanon. Conflict and health, 9, 12.

Swerdel, J. N., Janevic, T. M., Cosgrove, N. M. & Kostis, J. B. 2014. The Effect of Hurricane Sandy on Cardiovascular Events in New Jersey. Journal of the American Heart Association, 3, e001354.

The Sphere Project (ed.) 2011. The Sphere Handbook: Humanitarian Charter and Minimum Standards in Humanitarian Response, Geneva: The Sphere Project.

Turner, B. L., Kasperson, R. E., Matson, P. A., McCarthy, J. J., Corell, R. W., Christensen, L., Eckley, N., Kasperson, J. X., Luers, A. & Martello, M. L. 2003. A framework for vulnerability analysis in sustainability science. Proceedings of the national academy of sciences, 100, 8074-8079.

Uchimura, M., Kizuki, M., Takano, T., Morita, A. & Seino, K. 2014. Impact of the 2011 Great East Japan Earthquake on community health: ecological time series on transient increase in indirect mortality and recovery of health and long-term-care system. Journal of epidemiology and community health, jech-2014-204063.

UNISDR 2015a. Sendai Framework for Disaster Risk Reduction 2015-2030. Sendai, Japan.

UNISDR 2015b. UNISDR Global Risk Assessment, Brussels, UNISDR.

Watson, J. T., Gayer, M. & Connolly, M. A. 2007. Epidemics after natural disasters.

Emerging Infectious Diseases, 13, 1.

WHO. 2011a. Disaster Risk Management for Health - non-communicable diseases [Online]. Available: http://www.who.int/hac/events/drm_fact_sheet_non_communicable_diseases.pdf [Accessed 21 May 2015].

WHO. 2011b. Global health and ageing [Online]. Geneva: World Health Organization. Available:

http://www.who.int/ageing/publications/global_health/en/ [Accessed 12 December 2014].

WHO 2013. Global action plan for the prevention and control of noncommunicable diseases 2013-2020.

WHO 2014. Global reference list of 100 core health indicators: working version, Geneva, World Health Organization.

WHO. 2015. Noncommunicable diseases - fact sheet [Online]. Available: http://www.who.int/mediacentre/factsheets/fs355/en/ [Accessed 16 September 2016].

WHO. 2016a. Major NCDs and their risk factors [Online]. Available: http://www.who.int/ncds/introduction/en/ [Accessed].

WHO. 2016b. Noncommunicable diseases in emergencies [Online]. Geneva: World Health Organization. Available: http://www.who.int/news-room/fact-sheets/detail/noncommunicable-diseases [Accessed 2 August 2018].

WHO. 2018. Noncommunicable diseases [Online]. Geneva: World Health Organization. Available: http://www.who.int/news-room/fact-sheets/detail/noncommunicable-diseases [Accessed 3 August 2018].

World Economic Forum 2018. The Global Risks Report 2018 Geneva, World Economic Forum.

QUANTIFYING RESILIENCE: A CASE STUDY ON CRITICAL INFRASTRUCTURE RESILIENCE IN THE REPUBLIC OF BULGARIA

Nikolay Pavlov and Stefan Hadjitodorov[1],
Centre for National Security and Defence Research - Bulgarian Academy of Sciences

Abstract: This paper presents a method for quantifying resilience which is exemplified by a case study on critical infrastructure resilience in the Republic of Bulgaria. The research links quantitative research methods for measuring critical infrastructure resilience with qualitative legal, strategic and sector research. The main research results are policy recommendations for enhancing the legal framework and improving the process of critical infrastructures' identification at the national level by the application of an innovative quantification method.

Keywords: critical infrastructure protection and resilience; quantitative research methods

Introduction

The principal objectives of this paper are 1) to elaborate a method for quantifying resilience; and 2) to exemplify the method by a case study on critical infrastructure resilience in the Republic

[1] Nikolay Pavlov, PhD is Senior Expert at the Centre for National Security and Defence Research at the Bulgarian Academy of Sciences (BAS). Prof. Dr. Stefan Hadjitodorov is Director of the Centre for National Security and Defence Research and Corresponding Member of BAS. This work has been carried out in the framework of the National Science Programme "Environmental Protection and Reduction of Risks of Adverse Events and Natural Disasters", approved by the Resolution of Council of Ministers No.577/17.08.2018 and supported by the Ministry of Education and Science (MES) of the Republic of Bulgaria (Agreement No.D01-230/06-12-2018).

of Bulgaria. The quantitative research method is seen as a preliminary step to the development of a methodology for quantification of critical infrastructure resilience. The qualitative research case study will focus on analysis of the legal framework of critical infrastructure (CI) resilience in the Republic of Bulgaria with a view to enhancing the process of CI sectors and assets identification at the national level. The research contributes to the conceptualization of resilience as a security concept in the area of critical infrastructure protection which has implications for both the security sector and the citizens. In this context the resilience of critical infrastructures is interpreted as a daily practice of both 'high' and 'low' security and public policy which may range from counter-terrorism measures to the adequate everyday provision of utility services.

In the last years the concept of resilience has triumphantly pervaded various domains such as disaster risk management, most of the social sciences - in terms of societal resilience - and the European Union's Foreign and Security Policy. For example, the EU's Global Strategy adopted in 2016 puts special emphasis on the concept of resilience which has been interpreted as the new EU foreign policy paradigm.[2] In some respects resilience has superseded the notion of 'stability' which has gone out of fashion. Being overused by policy-makers over the years the concept of resilience has been gradually overburdened with

[2] Ana E. Juncos, 'Resilience as the New EU Foreign Policy Paradigm: A Pragmatist Turn?', *European Security* Vol.26, Iss.1, pp.1-7 (2017).

expectations and it is difficult to predict what the practical implications of the new resilience policies would be. Nevertheless, resilience arguably serves well as an analytical framework for understanding and explaining the behavior of a wide variety of phenomena in the natural and social world.

As argued by Chandler, discourses of resilience have ideological nature.[3] The shift to resilience follows disillusionment with liberal internationalist understandings that Western or international actors could resolve problems of development, democracy and peace through the export of liberal institutions. Resilience as an ideological understanding of the limits of international state-building sees the objects of state-building as producing the barriers to sustainable peace and development. The ideological power of resilience is driven by the understanding that 'we' cannot fix 'their' problems but, equally, that 'they' cannot be expected to break out of the reproduction of these problems without external assistance. Despite the focus on state-building these conclusions have broader implications in terms of the comprehensive 'ideology of resilience'. Thinking resilience as an ideology facilitates a realistic approach to the study and quantification of critical infrastructure resilience. Critical infrastructures have predominantly technical features, yet they are embedded in social structures and by default are ideologically imbued. Being the product of an ideologically

[3] David Chandler, 'International Statebuilding and the Ideology of Resilience', *Politics* Vol. 33(4), pp.276-286 (2013).

defined national or international political order, critical infrastructures have an ideological dimension too. For example, a nuclear facility as a critical infrastructure asset is not simply a technological facility with certain technical parameters, it has also a non-technical, social-political and, ultimately, ideological dimension related to national power. In this context the quantification of resilience should take into account this ideological dimension of critical infrastructures which is certainly difficult to measure, yet it has great practical implications.

Developing a Quantification Method

Taking into account the wider resilience-related ideological and conceptual framework this paper will focus on the development of a method for quantification of resilience in the specific, quantifiable area of critical infrastructure protection at the national level. In contrast to other social science subareas the field of critical infrastructure protection presents fertile soil for quantitative research. Critical infrastructure sectors and their assets are the products of engineer sciences and work. They are comparatively easy to measure and to quantify as they have quantifiable features which can be described in meaningful metrics. For example, the resilience of an industrial plant or an energy grid could be described, measured and quantified with the help of metrics. Since the separate unit (CI asset) can be measured, so can the whole critical infrastructure sector albeit with the respective difficulties regarding inter-relations, inter-connectivity and mutual impact. Quantifiability is one of critical

infrastructures' advantages in scientific terms compared with other social domains.

The proposed quantification method draws upon research methods which have been developed recently in the area of applied ecology and in the area of critical infrastructure resilience. The first category of methods summarized by Angeler and Allen[4] is informed by the classical definition of resilience as the amount of disturbance that a system can withstand before it shifts into an alternative stable state.[5] As noted by Angeler and Allen, the term 'resilience' has in many cases lost the clarity of the original definition and in fact is frequently used in a manner in direct opposition to the original definition. Many current uses of the concept are loose and incorrect. The term is becoming increasingly used in a normative sense, as if resilience were a desirable quality of systems. In this context to progress towards quantification of resilience, it is necessary to have a common vocabulary. In this paper resilience refers explicitly to the capacity of a system (critical infrastructure sector or assets) to return to its initial state following disturbance. More specifically, critical infrastructure resilience is policy-relevant as it has both material and ideational relations with the political public order. As a rule critical infrastructure protection – even in the case of

[4] David Angeler and Craig Allen, 'Quantifying resilience', *Journal of Applied Ecology* Vol.53, pp.617-624 (2016).
[5] C. Holling, 'Resilience and stability of ecological systems', *Annual Review of Ecology and Systematics* Vol.4, pp.1-23 (1973).

privately owned assets - is highly securitized and subject to public order-related and public law regulations.

One of the main approaches for quantifying resilience is the rapid assessment approach which focuses on surveys and stakeholder knowledge of the systems they inhabit.[6] This type of approach provides metrics which can be used to assess uncertainty, relative resilience among similar systems, and quantitatively assess trade-offs among social, economic and ecological components of complex systems. Spatial approaches focus on geometric relationships among spatial attributes of systems. Assessments of functional diversity and response diversity have been fruitful and have led to recommendations for assessing relative resilience. Discontinuity approaches, often combined with functional assessments, specifically assess scale-specific and cross-scale structure. Resilience assessment methods also focus on the identification of thresholds, including early warning indicators that aim at identifying impending regime shifts. One of the major knowledge gaps in resilience theory is the limited ability to integrate between the ecological and social sciences (including legal and policy dimensions) and to advance our understanding and management of combined social-ecological systems.[7] This knowledge gap is very relevant for critical infrastructure resilience with its specific policy / ideological dimension. A major distinction between social and ecological

[6] Angeler and Allen, *Ibid.*, p.621.
[7] Angeler and Allen, *Ibid.*, p.622.

resilience research is the explicit application of quantitative tools for measuring resilience. Significant methodological advances have been made in recent years in ecology, allowing for quantifying attributes of resilience. Much of the social resilience research remains qualitative, and the implementation of quantitative approaches is partly limited because of skepticism of scholars about abilities to make complex system dynamics tractable.

Another approach for quantitative assessment of resilience has been developed within the frameworks of the EU Horizon 2020 research project Smart Resilience (*Smart Resilience Indicators for Smart Critical Infrastructures*).[8] In the project the term 'resilience' of an infrastructure describes its ability to cope with possible adverse scenarios / events that can potentially lead to significant disruptions in its operation / functionality. Modern critical infrastructures are becoming increasingly 'smarter' and more efficient by means of smart technologies such as sensors, gateways, processors etc.[9] The project seeks to provide a quantitative assessment of resilience based on indicators, resulting in an aggregated resilience level number. The project's methodology aims at calculating the total resilience score for an infrastructure, aggregated bottom-up from diverse indicators to the issues that make up the assessed infrastructure / scenario.

[8] Web-site: http://www.smartresilience.eu-vri.eu/

[9] Alexander Jovanovic, Knut Oien and Amrita Choudhary, 'An Indicator-based approach to assessing resilience of smart critical infrastructures' – In: Urban Disaster Resilience and Security. Addressing Risks in Societies., pp.285-311 (2018).

The resilience indicators provide a quantifiable value in the methodology, providing a baseline for benchmarking and visualization.

Drawing upon the rapid assessment approach and the Smart Resilience methodology this paper makes the case for an innovative, integrative quantification method which entails three main components: 1) Expert assessments; 2) Scenario development & software tools; and 3) Public perception surveys. Expert assessments are a traditional approach for informed and knowledge-based evaluation of complex systems, including critical infrastructure assets. Some of the key requirements in the assessment process are the choice of independent experts, high level of competence and lack of conflict of interest. Scenario development is widely used both in the military and civilian sphere to support training and education but also testing and validation of concepts. A typical example thereof are Computer-assisted exercises (CAX). Scenarios are played with the support of software tools in virtual environments such as the integrated environment developed at the NATO Crisis Management and Disaster Response Centre of Excellence (CMDR COE). The most suitable software tools for critical infrastructure resilience scenarios are tools for Modelling & simulation (M&S); Serious gaming; and Concept development and experimentation (CD&E). Presently, there are plenty commercial-off-the-shelf tools which could be used for playing resilience scenarios – some of them being rather costly.

The third component of the quantification method should be public perception surveys. In keeping with the 'local turn' in academic literature[10] the method must take into account the perceptions of local populations living close by critical infrastructure assets. Of course, local perceptions might differ from expert assessments in some respects. It is exactly the integration of three different approaches and perspectives that lends originality and scientific reliability to the proposed quantification method. So far, the different approaches have been applied in isolation which leads to methodological reductionism and research results that do not fit reality. The proposed integrative method will seek to understand critical infrastructure resilience from three different perspectives and to integrate the research results into coherent policy-relevant recommendations. The quantification method will be implemented as a two level assessment. At the first level expert assessments, scenario development and public perception surveys will be carried out independently from each other. At the next level the research results from the three components will be aggregated. Depending on the CI sector and the competent authority involved the results from the first level components could be given either equal or different weight coefficients.

[10] On the 'local turn', see, for example: Roger Mac Ginty and Oliver P Richmond, 'The local turn in peace-building: a critical agenda for peace', *Third World Quarterly,* 34 (5), 2013.

Legal and Sector Analysis of Critical Infrastructure Resilience in the Republic of Bulgaria

Starting from 2006 the legal and strategic framework for the protection of European and national critical infrastructures in the Republic of Bulgaria has undergone significant transformation. In 2006 a new Disaster Protection Act was adopted to regulate the protection of the population and critical infrastructures against natural and man-made disasters.[11] At the European level a Directive on the identification and designation of European Critical Infrastructures and an assessment of the need to improve their protection was adopted in 2008[12]. The Directive gives legal definitions of basic concepts such as 'critical infrastructure, 'European critical infrastructures', 'risk analysis' and etc. Very importantly, the Directive establishes the list of European critical infrastructure sub-sectors in the energy and transport sectors.

In 2012 in Bulgaria a special Ordinance was adopted on the order, the way and the competent authorities for establishing critical infrastructures and their sites and risk assessment.[13] The Ordinance deals with national critical infrastructures. A comprehensive list of 19 sectors of critical infrastructures in the Republic of Bulgaria has been officially adopted to include: the

[11] Disaster Protection Act (State Gazette no.102, 19/12/2006).
[12] Council Directive 2008/114 / EC on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union, L345 / 75 of 23.12.2008
[13] Ordinance (Regulation) on the procedure, the way and the competent authorities for establishing the critical infrastructures and their sites and risk assessment for them, adopted by Decree of the Council of Ministers № 256 of 17.10.2012. SG. No. 81 of 23 October 2012, amend. SG. issue 19 of February 26, 2013

energy sector; the transport sector; information and communication technologies (ICT); post and courier services; the environment sector; agriculture and food sector; the health sector; finance, economy, sports facilities; education, science and technology; natural resources; tourism, regional and urban development; defence; justice, public order and security; government and social governance; disaster protection and cultural heritage. A competent authority (ministry or agency) has been assigned to 'protect' the respective critical infrastructure sector.

In keeping with the 2012 Ordinance several lists of critical infrastructure assets in the different sectors have been drafted by the relevant ministries. For example, in the ICT sector a Cyber Security Strategy was adopted by the Council of Ministers in 2016. It should be noted that in Bulgarian legal acts the term 'protection' of critical infrastructures is commonly used, whereas 'resilience' is seen as a more abstract and academic term.

In parallel to the legal acts the strategic framework for critical infrastructure protection in the Republic of Bulgaria is developed on three hierarchical levels as follows:

- Strategy for disaster risk reduction 2014 – 2020
- National Programme for the protection against disasters 2014 – 2018
- Annual Plans for the implementation of the National Programme for the protection against disasters

As a positive aspect the strategic framework clearly defines the policy objectives, priorities, the classification of disasters and measures for the protection of the population. On the other hand, the strategic framework has certain shortcomings. Overall, the protection of critical infrastructures is not sufficiently elaborated in all the three strategic documents. As a matter of fact the Strategy and the National Programme are not fully coherent and they have differing life spans. The issue of formalism in strategic planning and coordination is not adequately addressed. The focus on prevention is widely declared but it is not substantiated, especially with regard to the protection of critical infrastructures. The financial assurance of the Plans for protection has not been sufficiently provided. In addition, the role of local authorities in the protection of critical infrastructures is underestimated. To great extent the strategic documents are dominated by wishful thinking. In this context the implementation of the strategic framework in the Republic of Bulgaria is still an unfinished business.

Exemplifying the Quantification method in Critical Infrastructure Resilience in the Republic of Bulgaria

An example of the proposed quantification method with regard to critical infrastructure resilience in the Republic of Bulgaria is shown in Table 1.

CI Sector/ Quantification method	Energy sector	Transport sector	ICT sector
Expert assessments	Expert assessment of the vulnerability of energy subsectors: electricity; oil and gas. Expert assessment of a major energy CI asset, for example the largest oil refining enterprise in Bulgaria LUKOIL Neftohim.	Expert assessment of the vulnerability of transport subsectors: road transport, rail transport, air transport, inland waterways transport, sea shipping and ports. Expert assessment of a major transport CI asset, for example the transport infrastructure in the capital city of Sofia.	Expert assessment of the vulnerability of ICT subsectors: manufacturing, software and computer services; communications services and ICT wholesaling. Expert assessment of a major public communication service, e.g. the communications services supporting the issue of documents (passports, ID and driver cards) by the Ministry of the Interior.

Scenario / software tools	Scenario for a terrorist attack in the largest oil refining enterprise in Bulgaria to be played by M&S software.	Scenario for an earthquake in Sofia and its disastrous impact on the transport infrastructure to be played by M&S software.	Scenario for cyber- attack against the communication systems of the Ministry of the Interior and the implications for the citizens and public order. To be played by Serious gaming software.
Public perception surveys	Public perception survey in the town of Burgas regarding the vulnerability of the nearby oil refining enterprise with representative sample ~ 1000 persons.	Public perception survey in the capital city of Sofia regarding the vulnerability of transport critical infrastructure with representative sample ~ 1000 persons.	Public perception surveys in three major cities regarding the vulnerability of communications services provided by the Ministry of the Interior. Overall representative sample ~ 1000 persons.

Table 1: *Example of the quantification method in three critical infrastructure sectors in the Republic of Bulgaria*

Conclusion

This paper contributes to the development of state-of-the-art quantitative research methods for measuring critical infrastructure resilience and forges links with qualitative legal, strategic and sector analysis in a case study on the Republic of Bulgaria. The qualitative legal research clearly defines the Disaster Protection Act, the European CI Directive and the Ordinance on establishing CIs as the main legal acts regulating the protection of critical infrastructures in the Republic of Bulgaria. These acts can be assessed as a satisfactory administrative law framework which could be further developed in areas such as preventive measures for the protection of critical infrastructures and civil society involvement. One of the greatest challenges remains the real-life implementation of legal acts and strategic documents. Hence, changes and amendments in documents per se would hardly lead to enhancement of critical infrastructure resilience in the Republic of Bulgaria. This conclusion can further be developed into two specific policy recommendations.

First, the number of critical infrastructure sectors which are legally defined should be reduced. Under the present approach almost everything is interpreted as a critical infrastructure which in practice hampers the protection of critical infrastructures which are of crucial societal importance. In this re-assessment of criticality the involvement of local communities and citizens should be encouraged. Focusing on a few critical sectors such

as energy, transport and the ICT sector will make it possible for policy-makers to prioritize resilience measures and to provide adequate funding. Secondly, quantification methods for defining and assessing critical infrastructure sectors and assets should be applied. The proposed quantification method entails three main components: expert assessments; scenario development & software tools; and public perception surveys. The employment of this integrative method and overall quantification of the sector analysis will provide smart and evidence-based policy for critical infrastructure resilience in the Republic of Bulgaria.

RESILIENCE TO DISASTER – PSYCHOLOGICAL PERSPECTIVE

Margarita KUMANOVA,
Rakovski National Defense College

Abstract: The paper presents a review of conceptualization the psychology of disaster and resilience. The author outlines the main approaches to building, evaluating, and measuring community resilience. Here are analyzed key predictors to psychological resilience after disaster and their relationship to emotional recovery and well-being.

Key words: resilience, disaster, post-disaster psychological care, coping, emotional and social rebuilding.

Introduction

Industrial activities, population growth, urbanization, pollution, poverty, climate changes, local political instability, information overloading are just little part of banner-words of our century which sign how fragile the world is.

Increased frequency and scale of crisis events in world – natural, industrial, military, humanitarian – require adequate activities before, during and after disaster in order to prevent and to be ready for most of the potential environmental and personal consequences.

Most of us learn about disasters through News blocks and TV footages and not direct experience. We can see destroyed environment, first impression and influence the event over the

people and society, but all of these presented pictures are just simple excerpts of the huge reality. There is any place in News to show us the long-term impact of disasters on wildlife, psychology, culture, environment or finance. Reestablishing the life is longer than a News block. Disasters at all can influence enormous life, physical and psychological well-being of the affected people.

To deal with after effects of a crisis event we must have information and knowledge, skills and training, individual and community resources, awareness what people affected expect from government and institutions. Despite available knowledge on crisis management, the spontaneous and chaotic nature of disasters is challenge to build psychological resilience to disaster, to address complex psychosocial problems and to provide psychological care immediately and long termly.

Background

Some disasters are predictable, like foods. In such kind of situation, there is time to supply and store emergency food, water and medicine. There is opportunity to secure homes, hospitals, schools, and if it is necessary leave the vulnerable area. For others, the alert is extremely short or absent altogether. Earthquakes fall into that category, especially if they coming in the night.

Technological disasters like radiation or chemicals leaks can contaminate air, soil and waterways. Depending on leak's type

and quantity, it can kill immediately wildlife and humans in disaster area, and have invisible slow impact on life in unpredictable ways and radius. Some disaster interfere each other and diminish or enlarge their influence and affected area.

Disaster characteristics are relevant to perception process. This relation can be explained based on the informational approach. The more well known the parameters of disaster and existing resources are, the more predictable and organized the human behavior is.

More common in Bulgaria are natural disasters like earthquakes, fires, floods. On the National Statistical Institutes official web site are provided data for natural crisis events, damages' and rescues' costs in Bulgaria[1] since 2004.

Table I: Floods for the period 2010 - 2017 – total

Floods in Bulgaria							
2010	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**
651	382	692	547	360	266	184	159
Funds for recovery - thousand BGN							
2010	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**
16375	201136	9855	7338	51773	22665	5778	12227
Expenditures on rescue and emergency work - thousand BGN							
2010	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**
4524	3289	5819	1941	18003	5204	2215	3980

[1]http://www.nsi.bg/en/content/13266/crisis-events

Table II: Fires for the period 2010 - 2017 – total

Fires in Bulgaria							
2010	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**
1630	2185	3010	764	2245	2474	2448	741
Funds for recovery - thousand BGN							
2010	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**
479	192	47	308	10	-	11	707
Expenditures on rescue and emergency work - thousand BGN							
2010	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**
911	113	70	231	4	1	6	108

There are any official data about injured and died people in this statistic data. Nevertheless, Google[2] and News web sites[3] provide some sufficiently indicative examples:

1) **Floods:** 2014, Asparuhovo, Varna – 13 people died, four of them were children; Vinevo – 4 people died, one of them was child; 2016, Mizia – 2 people died; 2017, Burgas – 4 people died etc;

2) **Earthquakes:** During the years we have experience in earthquakes and post-earthquakes recovery – Svistov (over 130 people died), Strajica, Velingrad, Sofia are just little part of a long list;

3) **Fires** are not an exception: in 2003 we lost a helicopter Mi-17 with 4 persons on board nearby Razlog[4].

[2]https://www.google.com/search?ei=0P7sXKywHeeGrwS23LbADQ&q=наводнения+в+България+жертви&oq

[3]http://www.vesti.bg/incidenti/nameriha-tialoto-i-na-chetvyrtiia-udaven-ot-vinevo-6011061

[4] http://www.aircrashconsult.info/240703Mi17.html

Along with natural disasters, we have to mention other types of crisis events – human-created or technological. Sample excerpts: railway accidents (2014, 10 people died in train Sofia-Kardam[5]), cars and bus accidents (2004 – Lim, 12 children died[6]; 2018 – Svoge, 16 people died[7]), social event accidents (2001 – Sofia, Disco Club Indigo, 7 children died[8]), terroristic attacks (Sarafovo), radiation or chemical leaks, exsplosion (2016 – Hitrino, 7 people died[9]) etc.

The presented sheets and data show how much this disaster cost in financial way. In open information, sources we can find enough information about environment, infrastructure and life recovering but there are meager data about social and community reestablishment, though we have good practices in psychological assistance after extreme situation.

Psychology to Disaster/ Crisis

The Bulgarian psychological experience in crises intervention researches starts many years ago. There are scientists like professor Georgi Yolov[10], professor Ivan Paspalanov, professor

[5]https://dariknews.bg/novini/bylgariia/osem-izgorqha-vyv-vlaka-sofiq-kardam-229474
[6]https://news.bg/bulgaria/avtobus-s-nashi-detsa-padna-v-srabska-reka. html
[7]https://btvnovinite.bg/bulgaria/katastrofa-s-avtobus-zatrudnjava-dvizhenieto-po-patja-sofija-svoge.html
[8]https://www.dnevnik.bg/bulgaria/2001/12/22/123083_tragediia_v_diskoteka_indigo_otne_jivota_na_sedem_deca/
[9]https://news.bg/topic/eksploziya-i-tragediya-v-hitrino
[10]Йолов Г., Критичните ситуации и масовата психика, Sofia, 1973

Doncho Gradev etc.[11] who have examined the group psychological processes at all, group dynamic, pop ups of crowds and crowds phenomena, positive and negative psychological activities in face of danger or due disaster and post-disaster period. They have had the opportunity to conduct a research after the earthquake in Svishtov, 1977. This extreme situation is a "natural experiment"[12] which presents the specifics in the psychical regulation on behavior on all levels, and are great basis to start researches in disaster psychology.

Nowadays the Bulgarian society of psychologist provides a classification to the crisis events (for Bulgarian purposes only) in order to manage better the post-crisis psychological care. According this classification:

1) event with up to five people affected is small spread crisis;
2) event with 5 to 15 people affected is middle spread crisis;
3) event with more than 15 people affected is big spread crisis;
4) event with more than 100 people affected is mass crisis.

If there is injured or died child, the event is always classified as big or more (remember the examples above) by reporting.

In fact, the behavior of human (individual and mass phenomena) in non-standard situation is one of the most topical problems for psychology in our unstable world and life. Tempted to psychology of disaster scientists collect data on the specific psychical acting

[11]Колектив, под редакцията на Йолов, Г., Земетресението и амплитудите на психиката, Sofia, 1977
[12] Ibid.

under paramount stress, danger, lack of information, deprivation of time for decision; analyze that; extend lessons learn and evaluate training and assistance programs. The main goals are to maintain predictable behavior of individuals and groups under huge stress, to provide efficient post-care, faster and stable recovery and rebuilding of self-confidence, relationships, and values.

Contemporary disaster psychology shifts the focus from illnesses and disorders' researches to exploring proactive approaches, resilience and the diminishing or absence of adverse lasting mental health effects following a disaster.

Resilience – The Psychology Perspective

The word resilience origins from Latin, where ‘resiliō’ had the meaning of springing back; recoiling; rebounding[13]. Typical physics' term "resilience" becomes its wide usage outside physic in last century.

Garmezy (1973) first introduce resilience in psychology[14] by publishing him research on children who are grown by parents with psychological disability and their unexpected ability to cope. The term "resilience" evaluated during the years. To the 2006 when Reich[15] provides a psychological perspective on natural

[13] Babylon Online Dictionary, 2011

[14] Ponis, S.T., "Supply Chain Resilience: Definition Of Concept And Its Formative Elements", The Journal of Applied Business Research – September/October 2012 Volume 28, Number 5, pp. 921-929

[15] Reich, J.W. (2006) "Three psychological principles of resilience in natural disasters", Disaster Prevention and Management, Vol. 15 Iss: 5, pp.793 – 798.

and human-created disasters. He introduces three basic principles of human resilience, which are called by him "3Cs". The principles are:

1) control, by making possible for people to restore control of their lives – goals, decisions;
2) coherence, by reducing the uncertainty the disaster imposes by enhancing meaning, understanding;
3) connectedness, by providing the necessary informational and emotional support.

The main idea here is that in psychology resilience has a developmental nature. It means accumulating internal and external resources, developing skills for successfully resolve stressing issues, reestablishing stable bonds with other people. In this point of view, resilience is not a superhero-trait. It is nothing for granted. Resilience is nurtured by society, it is achievable, and it is something to reach after.

Resilience is the process of adapting well in the face of adversity, trauma, tragedy, threats or significant sources of ***stress*** – such as family and relationship problems, serious health problems or ***workplace*** and financial stressors. It means 'bouncing back' from difficult experiences[16].

While resilience stays in focus, we have to pay attention and to make difference among individual resilience, organizational

[16] https://www.apa.org/helpcenter/road-resilience?fbclid=IwAR1JAUnARhda2DvUzZlzx0rQnOAvstr97YvmhQjeskc-yZVNZJgiDvGFJqc

resilience and community resilience. Each of these phenomenons has specific manifestation and predictors, which means that each one requires different skills and type training.

Table III presents the common definitions of organizational resilience shared by Stavros Ponis[17].

Table III: Definitions of Organizational Resilience

	Definitions of Organizational Resilience
Wildavsky (1988)	Resilience is the dynamic capacity of organizational adaptability that grows and develops over time
Horne & Orre (1998)	Resilience is a fundamental quality of individuals, groups, organisations, and systems as a whole to respond productively to significant change that disrupts the expected pattern of events without engaging in an extended period of regressive behavior
Mallak (1998)	Resilience is the ability of an individual or organisation to expeditiously design and implement positive adaptive behaviors matched to the immediate situation, while enduring minimal stress'
Coutu (2002)	The ability of an organization to face reality with staunchness, make meaning of hardship and improvise solutions from thin air.
Sutcliffe & Vogus (2003) & Vogus & Sutcliffe (2007)	Organizational resilience is the maintenance of positive adjustment under challenging conditions such that the organization emerges from those conditions strengthened and more resourceful.
Hamel & Valikangas (2003)	Organizational Resilience refers to a capacity for continuous reconstruction. It requires innovation with respect to those organizational values, processes, and behaviors that systematically favor perpetuation over innovation.
Fiksel (2006)	The capacity of an enterprise to survive, adapt, and grow in the face of turbulent change
Lengnick-Hall et al. (2011)	The firm's ability to effectively absorb, develop situation-specific responses to, and ultimately engage in transformative activities to capitalize on disruptive surprises that potentially threaten organization survival

Since risk and demands realization, resilience has become a top priority for many organizations that work in humanitarian action and development.

In Road map to community, resilience[18] is written this definition of Community resilience: The ability of communities (and their

[17] Ponis, S.T., "Supply Chain Resilience: Definition Of Concept And Its Formative Elements", The Journal of Applied Business Research – September/October 2012 Volume 28, Number 5, pp. 921-929

[18] https://www.preparecenter.org/sites/default/files/1310403-road_map_to_community_resilience-en-04.pdf

members) exposed to disasters, crises and underlying vulnerabilities to anticipate, prepare for, reduce the impact of, cope with and recover from the effects of shocks and stresses without compromising their long-term prospects.

There are pinpointed six core characteristics identified in the Framework for Community Resilience:

1) knowledge, health, basic needs do not suffer;
2) social cohesion;
3) economic opportunities;
4) well-maintained and accessible infrastructures and services;
5) managing natural assets;
6) connection.

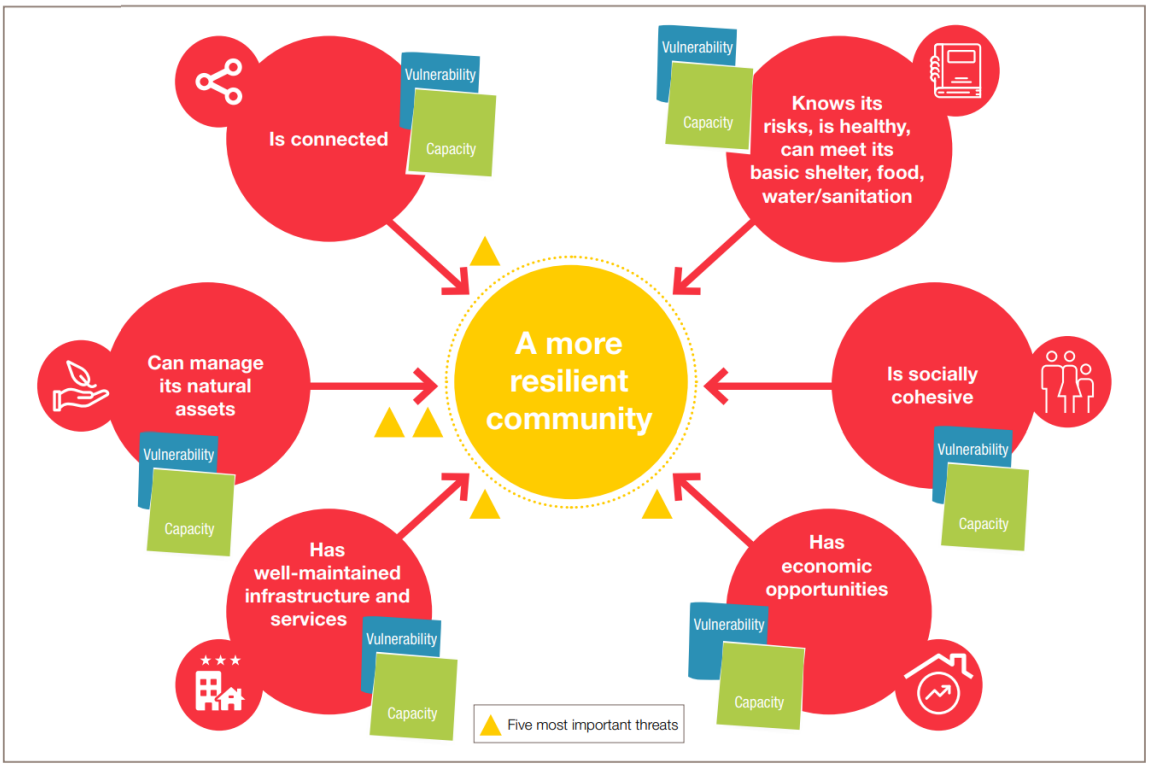
When we place the six core characteristics in a star chart (pic. 1), we are able to see the most important threats, to use the star as a tool of analysis, to brainstorm each relation to each characteristic in order to find capacities that help in building resilience.

There are any psychological bullets in this characteristics list or in the star, but all of these are not just related, moreover these are results of national culture, traits, attitudes and archetypes. The more proper culture, values, religion, social structure known and assessed are, the more resilience training programs and psychological post-care structured and efficient are.

When we work on phenomena of a group dynamic next before, during and after a crisis event with high psycho-emotional tension, we cannot exclude these types of informal, formed by chance groups (passengers in a bus, spectators in a theatre etc.), which are high unpredictable not only in a crisis, but also in everyday life. Professor Yolov call these "*accidentally mass*"[19]. He outlines some of main characteristics of these ‘accidentally mass’ – people in have not external moral imperative. No one in area can judge and comment. The remarks from other become irrelevant.

[19] Йолов Г., Критичните ситуации и масовата психика, Sofia, 1973

Picture 1: A Resilience Star[20]



Such kinds of groups' acts are impetuous, turbulent and careless. For the purpose of exploration and research in disaster psychology is necessary to know how "accidentally mass" come into being and what power drives it. Moreover, analyzing the resilient star, an 'accidentally mass' can be a serious vulnerability to social cohesion. By developing resilience training program (psychological point of view), we have to pay attention to some main points: to raise the society cohesion, to extend interpersonal and institutional basis trust, educate empathy and

[20] https://www.preparecenter.org/sites/default/files/1310403-road_map_to_community_resilience-en-04.pdf

emotional intelligence. These are a little set of tools to overcome the collateral obstacles in a crises event.

Conclusion

No one wants to consider the possibility of bad things happening. But they do. A Bulgarian proverb says that we must always expect the worst things that may happen, if something good comes, it does... and it is welcome. This is a great example how national domestic attitudes work as individual psychological prevention. Is it enough?

The aim of the paper is to uncover a little bit the curtain how versatile and deep the reasons for humans and crowds behavior after disaster are. It outlines how multilayer the concept of resilience is, where we are at the line of conceptualization and building psychological resilience after disaster. In my opinion, this paper is just a step from my intention to explore the validity of conceptual constructs and to design a structured questionnaire about community resilience.

Bibliography

http://www.nsi.bg/en/content/13266/crisis-events (last access, 28 May 2019)

https://www.google.com/search?ei=0P7sXKywHeeGrwS23LbADQ&q=наводнения+в+българия+жертви&oq (last access, 28 May 2019)
http://www.vesti.bg/incidenti/nameriha-tialoto-i-na-chetvyrtiia-udaven-ot-vinevo-6011061 (last access, 28 May 2019)
http://www.aircrashconsult.info/240703Mi17.html (last access, 28 May 2019)

https://dariknews.bg/novini/bylgariia/osem-izgorqha-vyv-vlaka-sofiq-kardam-229474 (last access, 28 May 2019)

https://news.bg/bulgaria/avtobus-s-nashi-detsa-padna-v-srabska-reka.html (last access, 28 May 2019)

https://btvnovinite.bg/bulgaria/katastrofa-s-avtobus-zatrudnjava-dvizhenieto-po-patja-sofija-svoge.html (last access, 28 May 2019)
https://www.dnevnik.bg/bulgaria/2001/12/22/123083_tragediia_v_diskoteka_indigo_otne_jivota_na_sedem_deca/ (last access, 28 May 2019)

https://news.bg/topic/eksploziya-i-tragediya-v-hitrino (last access, 28 May 2019)

Йолов Г., Критичните ситуации и масовата психика, Наука и изкуство, София, 1973

Babylon Online Dictionary, 2011 (last access, 28 May 2019)

Ponis, S.T., "Supply Chain Resilience: Definition Of Concept And Its Formative Elements", The Journal of Applied Business Research – September/October 2012 Volume 28, Number 5, pp. 921-929

Reich, J.W. (2006) "Three psychological principles of resilience in natural disasters", Disaster Prevention and Management, Vol. 15 Iss: 5, pp.793 – 798.

https://www.apa.org/helpcenter/road-resilience?fbclid=IwAR1JAUnARhda2DvUzZlzx0rQnOAvstr97YvmhQjeskc-yZVNZJgiDvGFJqc (last access, 28 May 2019)

https://www.preparecenter.org/sites/default/files/1310403-road_map_to_community_resilience-en-04.pdf (last access, 28 May 2019)

CLIMATE CHANGE AND SECURITY

Ralitsa BAKALOVA, Svetozar BOSSILKOV
CMDR COE

Abstract: International organizations and governments deliberating the topic concerning climate change unambiguously acknowledged that some tipping points are passed and the humanity is on a threshold of dramatic environmental changes. Unfortunately, unified world adaptation strategy is missing so far and because of the different impact climate change would have the common strategies wouldn't be able to cope with the consequences reciprocally. At the same time Global warming and Climate change are becoming more and more a global commercial trends, while the humanity is suffering from the real outcomes of the real warming and changes whereas the time for reaction dramatically running out. The article is focusing on the real physical manifestation as consequences of climate change. It also explains the linkage between anthropogenic influence over the climate system, severe weather events and security environment. Underlining the role of NATO as a pillar of security and how the Alliance implement climate change, how adapt to them and how to anticipate the future challenges emanating from climate change.

Keywords: adaption, climate change; mitigation, national-international security; risk; threat.

Introduction

Since human society rests on certain environmental conditions, a changing climate that significantly alters these conditions is expected to have an impact on human life, society and security. Understanding the complexity of interactions between climate stress factors, their human and societal impacts and responses, is a crucial element to the assessment of implications to security and conflict.

Climate change – a global issue

The Earth system consists of three coupled subsystems: the climate system, the natural system, and the human system. Each of these systems affects the others directly and indirectly, creating a complex (and highly uncertain) socio-environmental system. For that reason, it is essential to consider the relationship between climate and security as there is only one global climate system and problems within it have wide international repercussions quickly transcending distance between the origin and affected place.

Despite being a natural phenomenon, rising global temperatures is propelled by human activities and as result it leads to inducing environmental changes in many parts of the world. The main consequences are sea-level rise excessive droughts, high magnitude floods and storms, water scarcity, soil and ecosystems degradation, reduced food production, loss of biodiversity and spread of diseases and large-scale climate disruption.

In its 2007 Fourth Assessment Report, the Intergovernmental Panel on Climate Change (IPCC) addressed serious risks associated with climate change that could undermine the living conditions of people all over the world. Vulnerable systems include water resources, agriculture, forestry, human health, human settlements, energy systems, and the economy. According to the IPCC, the economic, social and security costs of severe weather events, as tropical cyclones, tornadoes,

severe thunderstorms, squalls, etc. will increase, and climate change impacts will "*spread from directly impacted areas and sectors to other areas and sectors through extensive and complex linkages*".

The international community seeks to tackle the issue. To this end, the Climate change agenda is framed by some critical documents, as follows:

- The United Nations Framework Convention on Climate Change (UNFCCC) – international environmental treaty adopted in 1992 with main objective is to "*stabilize greenhouse gas concentrations in the atmosphere at a level that would prevent dangerous anthropogenic (human) interference with the climate system*".
- The Kyoto Protocol (1997) – sets greenhouse emissions targets for developed countries which are binding under international law.
- IPCC Fifth Assessment Report (2014) - says that the warming of the atmosphere and ocean system is a fact and counts the clear influence of the humanity on climate.
- The Paris agreement (PA) – In 2015, all the parties to UNFCCC came together for the UN Climate Change Conference and adopted by consensus the Paris Agreement, aimed at limiting global warming to less than two degrees Celsius, and pursue efforts to limit the rise to 1.5 degrees Celsius.

- IPCC special report: global warming of 1.5 °C (2018) – prepared as a response to invitation contained in the Decision of the 21st Conference of Parties of the UNFCCC to adopt PA. This special report represents the impact of global warming of 1.5 °C above pre-industrial levels and related global greenhouse gas emission pathways.

Moreover G20 Osaka Leaders' Declaration from June 2019, admits the importance of international "efforts to support actions and cooperation in adaptation and disaster risk reduction, in particular, for the most vulnerable communities." It also emphasize the importance of "clean technologies and approaches, including smart cities, ecosystem and community based approaches" in order to be reached sustainable development.

A joint report by the European Commission and the High Representative for the Common Foreign and Security Policy concluded that climate change is already having serious consequences for regional and hence - international security that directly influence European and respectively NATO's interests.

Human induced climate change and real consequences

Nowadays the main stakeholders involved in the policies connected with climate change put huge efforts to reduce the consequences of the dramatically fast changing natural environment. The industrial revolution made irreparable impact over the ecosystem, the atmosphere and the whole Planet Earth.

From now on the people will experience these dynamic changes in the climate in very untypical and difficult to adapt way. Humanity has to deal with all the weather events that are becoming more unusual, severe and devastating. The main stakeholders and the governments should know the real threat emanating from the irreversible climate change. Pointing the real menace and consequences in the field of climate change should be a cornerstone for future policy making in the area of adaptation and resilience.

Even without the influence of humans, the Earth has natural cycles that drive the climate changing. Climate is a synthesis of weather conditions in a given area, characterized by long-term statistics (mean values, variances, probabilities of extreme values, etc.) of the meteorological elements in that area. Climate change is something natural for the Planet Earth, it refers to a change in the state of the climate that can be identified (e.g., by using statistical tests) by changes in the mean and/or the variability of its properties, and that persists for an extended period, typically decades or longer. Climate change may be due to natural internal processes or external forcing such as modulations of the solar cycles, volcanic eruptions. The difference between Natural and Anthropogenic climate change is that the natural changes are very slow, but the Anthropogenic are very fast, severe and untypical.

Without the Natural Green House effect, there will be no life on Earth. This is the perfect balance between solar radiation and

energy. Having greenhouse gases in the atmosphere is natural, their heat-trapping abilities keep Earth from being extremely cold. But the Human influenced Green House effect keeps that heat trapped in the lower atmosphere, which leads to increased surface and atmosphere temperature.

The changes in the temperature can cause changes in a lot of weather elements, but the global climate change is actually much more complicated than the scientist thought 20 years ago. Nowadays there is enough data and knowledge to point the exact consequences of the Global warming that leads to Climate change and severe weather events. It is possible to identify the human fingerprint in certain types of extreme weather events. Human-induced climate change has already increased the number and strength of some of these extreme events.

The consequences of global warming and human induced aerosols over the atmosphere

Some of the particular results of the human action on the climate changing system are the Anthropogenic Green House effect and the Global warming. They influence on the thermal structure of the atmosphere and warm the levels of clouds formation. This changes the usual physical and chemical process in the atmosphere, and is one of the reasons for more extreme and severe weather events.

Rising global temperature accelerates evaporation rates worldwide. More evaporation leads to more rainfall. Global

Warming change the magnitude and scale frequency of the extreme weather events, increase their power and duration, they become more unusual and unseasonal. The extra moisture in the atmosphere becomes available to storm systems, because water vapour is the fuel for storms, the result is heavier rainfalls. As temperatures continue to rise, the atmosphere is more loaded with humidity and every normal storm will have a greater potential to develop into an intense, severe and devastating one. Cyclones are the primary producer of heavy rainfall. Hurricanes or typhoons are strong types of cyclones, with severe consequences due to extremely high wind speeds, storm surges, and heavy rainfall.

The Cloud condensation nucleis are small particles on which water vapour condenses. The atmosphere is seeded with them and without them there will be no rain. Where do cloud condensation nuclei come from? They are the atmospheric aerosols natural and anthropogenic. Due to the pollution the atmosphere is crowded with them. That is how aerosols effect on severe weather events. The storms as well as clouds formation are sensitive to any small change in atmospheric thermodynamics and dynamics, so effects of aerosols are dramatically influencing these processes. Aerosol effects lightning, thunderstorms and cloud electrification. They also effect the power and severity of cyclones, hurricanes, typhoons and tornadoes .The amount of aerosols ingested into hurricanes could partially explain the deviations in storms' observed

maximum wind speeds from their predicted values. Aerosol effects hail formation, hail forms and allows fast growth into large hailstones. The role of aerosols in modifying clouds and precipitation has been one of the most intriguing questions in cloud physics and in the study of climate change.

The structure of the atmosphere, its physical and chemical processes have been stable for centuries. Unfortunately due to human activity the structure is no longer stable. Because of the increasing temperature the layers of the atmosphere start to move. There are several factors that will determine how tall a thunderstorm will get. One of them is the height of the tropopause. The tropopause is the boundary in the Earth's atmosphere between the troposphere and the stratosphere. The tropopause acts as a giant cap to cloud formation. This is a stable layer and behaves like a wall. There is observational evidence that shows that tropopause folds and makes more space than usual for cloud formation. Tropopause is very sensitive of cyclones, hurricanes, typhoon and other clouds formations.

'The Arctic invasion! Not a military invasion, but a human one'

The sea ice is melting and the trend is to continue as the Arctic region goes ice free. The increased temperature in the Arctic changes not only the ecosystem but makes the cold polar air masses unstable. So the result of this "human invasion" leads to instability in the atmospheric arctic air masses and this allows for an increased transport of heat into the upper atmosphere, which disturbs the stratospheric polar vortex. A polar vortex is an upper-

level low-pressure area lying near one of the Earth's poles. If the polar vortex is unstable, the frequency and intensity of the extreme weather events observed in the middle latitudes will increase dramatically. There is a scientific connection between climate change, Arctic Sea ice melt and severe weather events, like disastrous flooding, cold spells, heat wave, severe tornadoes, typhoons, cyclones, hurricanes, because of a warming climate.

The last report of IPCC shows that the temperature has raised with 1,5 degree Celsius. But rising the temperature with 1,5 degree, rises the energy of the of the atmosphere many times, thus leading to instability and increasing the number and the strength of the severe weather events. The results are more water, more space and energy for the extreme weather events.

Climate change in security environment and NATO

NATO with its Strategic concept for the Defence and Security admits that the climate change is one of the factors that will shape the future security environment. Put in a row with resource constraints, health risks, water scarcity and increasing energy needs, climate change will further 'have the potential to significantly affect NATO planning and operations' necessitating ever more credible, networked, aware, agile, and resilient forces.

In the process of developing the afore-mentioned Strategic concept, the NATO Secretary General Anders Fogh Rasmussen, was assisted by a group of experts who prepared analysis and

recommendations emphasizing the ‘unconventional’ character of future security threats, and the growing importance of addressing current and potential climate change implications to security. Equally important is the focus on new capabilities, including climate change capabilities, which are and will be required to grapple with the uncertainty of unconventional threats.

NATO as a political-military organization is not a primary actor with respect to climate change policy. The efforts were mostly directed at maintaining basic awareness of the issue, sponsorship and participation in events, or providing assistance to partnership countries. But NATO leaders have started to implement the idea about climate change, despite very modest and slow efforts about examination of the role, posture and adaptation on NATO to this change. Throughout the past decade, great deals of efforts have been made to examine the potential consequences of climate change on the security environment and NATO has recognized the indirect influence of climate on security .The international security community is becoming more aware of the necessity to anticipate and cope with potential and future climate issues, and to understand the demands climate change would place on international / regional organizations and even to examine how NATO can address with this issue. High level expert concludes:

As an Alliance, NATO does not have a formal role in regulating the greenhouse gas emissions that experts believe lead to global warming. NATO could, however, be called upon to help cope with

security challenges stemming from such consequences of climate change as a melting polar ice cap or an increase in catastrophic storms and other natural disasters. The Alliance should keep this possibility in mind when preparing for future contingencies.

Special expertise in the field of climate change by two of the NATO Secretary General – Mr. Anders Rasmussen and Mr. Jens Stoltenberg – is a strong posture concerning the importance of the topic. As a Prime Minister of Denmark, Mr. Rasmussen initiated hosting the 15th Conference of the Parties to UNFCCC and the 5th Meeting of the Parties to the Kyoto Protocol. Mr. Stoltenberg is former UN Special Envoy for Climate. Alongside with this, all 29 NATO States are members of the IPCC. All these serve as enablers for constructive deliberation on climate change implications to security, thereafter – NATO Allies and Partners.

NATO addresses climate change and its impact and influence on future security environment through its Long-Term Military Transformation programme. It is the Allied Command Transformation (ACT) process for anticipating and preparing for the ambiguous, complex and rapidly changing future security environment. The programme has two components: Strategic Foresight Analysis (SFA) and Framework for Future Alliance Operations (FFAO).SFA report describes the future trends and defense and security implications, and defines that "*climate change is drawing unprecedented international attention because it impacts nearly all domains and is a compounding*

factor for other existing issues". The FFAO describes the development of the Future Security Environment and Instability Situations. Future Security Environment is described as complex and "*the effects of climate change are more evident and pervasive than ever before*". Instability situations depend on climate change, because "*climate change will likely increase the frequency and impact of natural disasters*".

A conclusion after analyzing SFA and FFAO reports is that the most serious concerns for NATO as consequences of climate change derive from worsened security due to climate-induced social stress. The latter goes far beyond the damage of the physical environment. The potential outcomes of the impact of this worsened security depends on the nature of the impact, the type of climate event and last but not least how resilient is that state. Indeed, states' resilience will determine whether it will be only weakened or could face dramatic crisis. It becomes apparent that "*the most serious climate risks and conflicts are expected in poor countries*" because of their vulnerability to climate change, but "*more wealthy countries are not immune*".

The comprehensive approach is critical to the process of coping with future security challenges. As the former U.S. Secretary of State Madeleine Albright addressed 'new' security issues, saying that "*the boundary between military and non-military threats is becoming blurred*." Climate change is defined as "*threats that cross the divide between the military and the civilian spheres*" and together with energy security, cyber security and asymmetric

terrorist attacks they defined the abovementioned ‘new’ security issues. That’s why civil-military cooperation is in the basis in managing the climate change challenges.

NATO current Secretary General Jens Stoltenberg admits that NATO “*has recognised that climate change is a security challenge and that’s also the reason why we have expressed concern about climate change*”, underlines the most common future threats, makes the crossing point between climate change and security and emphasizes on the responsibilities different organisation would have to have, by saying:

> “NATO is a military alliance, so NATO doesn’t have the tools to address climate change. Having said that, climate change is important for our security, meaning that climate change will most likely lead to that people will start to move, it may lead to new conflicts about water, about agriculture, and it may also, you know, change for instance transport routes.(…) So, climate change has security consequences and NATO has recognised that in what we call the Strategic Concept.(...) It's important that NATO Allies engage in that, but it's not for NATO to in a way develop windmills or clean energy, because we have other institutions and organisations for that.”

Climate change and NATO's infrastructure

The Alliance first recognised the natural environmental challenges facing the international community in 1969, when it established the Committee on the Challenges of Modern Society (CCMS), which provide a unique forum for NATO and its partner countries to share knowledge and experience on social, health and environmental matters, both in the civilian and military sectors. In 2006 CCMS merged with the NATO Science for Peace and Security (SPS) Programme. Nowadays one of the NATO's current activities related to the natural environment addressing the impact of climate change. The Alliance is looking closely at how to best address environmental risks to security in general as well as those that directly impact military activities. For example, environmental factors can affect energy supplies to both populations and military operations, making energy security a major topic of concern. Currently, NATO conducting this through its SPS Programme EADRCC and Partnership for Peace Trust Fund projects. It is considering enhancing its efforts in this area, with a focus on civil emergencies, energy efficiency and renewable power, and on consulting with relevant international organisations and experts on NATO's stake in climate change.

In order to better coordinate its activities, NATO joined in 2004 in Environment and Security (ENVSEC) Initiative. The main purpose is to address environmental issues that threaten security.

NATO's Military Committee Working Group on Meteorology and Oceanography helps NATO members and partner countries understand how, with national civil or military capabilities or within a collective capability, to assess and prepare for climate change and related national security threats.

NATO's Civil Emerging Planning Committee (CEPC) provides NATO with civilian expertise in consequence management, humanitarian and disaster response, and protection of critical infrastructure. The CEPC also oversees EADRCC which coordinates disaster relief efforts among NATO and partner countries, and in countries where NATO operates.

In line with NATO Secretary General's confirmation that climate change is a security challenge, and with the founding principle of collective defence, NATO has taken measure to adapt to potential climate implications to security by incorporating the topic in its policies, procedures and structure. The leading structure is NATO Parliamentary Assembly (PA) which serves as the consultative interparlamentary organisation for NATO and provides a link between NATO and the parliaments of its member nations. PA repeatedly insists inclusion of climate change in NATO's political agenda and "*has been consistent in its support for a concerted global response to the challenge of climate change*".

Follows a short timeline of the events:

1. In 2005 the NATO PA released reports that focused on the relevance of climate change for NATO- “Climate Change in the Arctic: Challenges for the North Atlantic Community”.
2. In 2007 the NATO PA released reports that focused on the relevance of climate change for NATO – “Climate Change: Thinking Beyond Kyoto”.
3. In 2009 the NATO PA released report on the potential security consequences of climate change “Climate Change and Global Security”.
4. In 2010 the NATO PA released reports that focused on the relevance of climate change for NATO - “Security at the Top of the World: Is There a NATO Role in the High North?”.
5. In 2014, the NATO PA’s Science and Technology Committee visited the IPCC Secretariat in Geneva, Switzerland to discuss the IPCC Fifth Assessment Report.
6. Finally NATO Parliamentary Assembly released “Climate Change, International Security and the Way to Paris (2015 Draft Special Report)” to draw attention to the security consequences of climate change, and to encourage NATO member states to support a climate agreement during the 21st Conference of the Parties to the United Nations Framework Convention on Climate Change in Paris.

Way ahead

Starting to facilitate discussion amongst climate scientists in 1980s, NATO admitted the importance of climate-related security implications. Almost 40 years later NATO’s former Secretary General Rasmussen highlighted that, with the growing impact of

climate change, the demand over the military as “first responder to natural disasters” is likely to grow and how to optimize the Alliance’s contribution in that area is of high importance.

Currently the dialogue with other international organisations has been enhanced with a focus on how NATO and its armed forces could better adapt to the challenge of an increasing number of natural disasters. Allies with their well-developed political and economic institutions are largely anticipated to have the resilience and adaptive capacity to adjust to a new climatological environment without internal civil strife or breakdown. This new security environment calls for new ideas, concepts, and response types. Recognizing that climate change will have security implications, national governments and international and non-governmental organisations have struggled to identify a way forward, through: scientific assessment on how NATO would have military capabilities required for this new circumstance; distribution of political and military resources from Euro-Atlantic countries to assist or intervene in less fortunate regions; early-warning infrastructure and regulations; raising awareness and information-sharing concerning climate change and security implications; avoiding duplication of roles already undertaken by other organisations; cooperation with world leaders with deep expertise in climate change such as UN, IPCC, EU etc.; building resilience; mitigation and adaptation.

Conclusion

NATO recognized that climate-induced social stress will negatively impact security, and that the Alliance should adapt and prepare accordingly. Moreover, today we are on a threshold of general change of the security environment coming from the Arctic and the melting ice there which will affect the North Atlantic region directly and will fundamentally change the environment.

The security implications of environmental issues to political leaders and decision-makers are area where the Alliance has to play a major role as a security pillar. The first step is to ensure that members and partners alike have the knowledge and ability needed to mitigate climate change and adapt to its effects. Furthermore a preventive climate policy have to seek strengthen institutions and interaction between countries to build globally coordinated climate policy against climate change.

The anticipated complex dynamics of the future security environment places a serious strain on structures in terms of adaptation and capability development. To preserve peace and security, NATO leaders and decision-makers have to be precise enough to find the crossing point between what forces need to be, what forces need to do and the characteristics of new security environment with its most important consequences to the society: conflicts, instability, unrests, capacity, poverty, migration, countries´ collapse and dependency.

Bibliography

Maximilian Auffhammer, Detection and Attribution of Observed Impacts in Climate Change 2014: Impacts, Adaptation, and Vulnerability.

Climate Change 2007, Synthesis Report.

IPCC Fourth Assessment Report: Climate Change 2007, Climate Change 2007: Working Group II: Impacts, Adaptation and Vulnerability.

Climate change and international security, Paper from the High Representative and the European Commission to the European Council, 2008.

Strategic concept for the Defence and Security of the Members of the North Atlantic Treaty Organization 2010.

Framework For Future Alliance Operations 2018 Report.

Strategic Foresight Analysis 2017 Report.

NATO 2020: Assured Security; Dynamic Engagement, Analysis and Recommendations of the group of experts on a new Strategic Concept for NATO.

Scheffran and Battaglini, Climate and Conflicts: The Security Risks of Global Warming, 2010

Zhanqing Li, Daniel Rosenfeld, and Jiwen Fan, Aerosols and Their Impact on Radiation, Clouds, Precipitation, and Severe Weather Events, Sep 2017.

Effects of microphysical drop size distribution on tornadogenesis in supercell thunderstorms Nathan Snook1 and Ming Xue1 Received 31 August 2008; revised 9 November 2008; accepted 18 November 2008; published 20 December 2008.

Daniel Rosenfeld, Michal Clavner, Ronit Nirel, Pollution and Dust Aerosols Modulating Tropical Cyclones Intensities, 2011

Eyal Ilotoviz and Alexander P. Khain, Effect of Aerosols on Freezing Drops, Hail, and Precipitation in a Midlatitude Storm.

S.Twomey, P.Squires, The Influence of Cloud Nucleus Population on the Microstructure and Stability of Convective Clouds, November 1959;

Masato Mori, Yu Kosaka, Masahiro Watanabe, Hisashi Nakamura, Masahide Kimoto and Warm Arctic, Cold Continents: A Common Pattern Related to Arctic Sea Ice Melt, Snow Advance, and Extreme Winter Weather, Judah Cohen,Justin Jones, Jason C. Furtado, Eli

Tziperman, A reconciled estimate of the influence of Arctic sea-ice loss on recent Eurasian cooling. October 2, 2015

Geoffrey Giller, Arctic Invasion, 2015

CLIMATE CHANGE AND SECURITY IMPLICATIONS

Siana MIRCHEVA, Orlin NIKOLOV, Anastasios VASILEIOU, Svetozar BOSSILKOV
CMDR COE

Abstract: Climate change is a significant change in weather pattern. Even though not a novelty, the scale of climate change is threatening the sustainable human development. Human influence is the dominant cause of the observed warming impacting the socio-economic conditions of millions of people and degrading the entire global ecosystem. But can we view the unequivocal climate change as a threat to national or international security? The paper explores the links between climate and security providing insights into how climate change – induced threats affect the political and socio-economic security. Finally, the article provides recommendations in terms adaptation and mitigation of this phenomenon.

Keywords: adaption, climate change; mitigation, national-international security; risk; threat.

Introduction

In this rapidly changing world, the global security context is redefining by interaction between political, social, technological and environmental trends and states are facing several security challenges. The Earth's climate is changing and by that environmental issues are dominated by this change. The climate has always changed but in the past these alterations developed slowly and lasted for thousands of years. This slow pace of climate change gave flora and fauna enough time to adapt and

evolve. But nowadays climate change is rapid and leads dynamic and ambiguous outcomes for the planet.

Climate change is one of the greatest challenges of our time and its adverse impacts undermine the ability of all countries to achieve sustainable development[1]. Changes to the climate impose stresses on current ways of life, on individuals' ability to subsist and on governments' abilities to keep pace and provide for the needs of their populations. It may also lead to increasing incidences of natural disasters which will have an increasing impact, particularly in those areas unaccustomed to such events. The overwhelming consensus is that our planet is facing a massive risk that undermines the national and international security. The intersection of climate change and the national security will be a reality in the years ahead. Climate change is the new modern war that can have several direct or indirect consequences. **Conflict, instability, unrest, capacity, poverty, migration, countries´ collapse, dependency** are some of them. **Mitigation and adaptation** are the desiderata and where we should focus our efforts on.

Conflict

There is growing recognition of the interrelationship between climate change and conflict. Research and field experience are demonstrating that these dynamics are often particularly acute in

[1] Transforming our world: the 2030 Agenda for Sustainable Development", UN outcome document, 2015

countries that are fragile or conflict-affected. Fragility and conflicts always emerge through the interaction of different shocks, pressures and structural factors. Inequality has become a major emerging urban challenge. A history of conflict or marginalization increases conflict potential. The climate changes serve as a catalyst that agitates a tense situation to become a conflict. It impacts the basic resources which are necessary for humans to survive and nations to go on.

The risks of climate change impact on every asset of national and international security. They can act as a 'multiplier' that exacerbates existing environmental stressors and increases resulting tensions. The demand for resources will increase with population and economic growth particularly in developing countries. Transboundary waters are frequently a source of tension; as demand grows and climate impacts affect availability and quality, competition over water use will likely increase the pressure on existing governance structures. The World Bank estimates that by 2025 2.4 billion people will face absolute water scarcity. Similarly, climate change might exacerbate problems such as government instability, the spread of disease, the strengthening of terrorism, and widespread migration[2]. All of these climate change-related factors significantly increase the likelihood of conflict escalation.

[2] World Bank Group, "At a glance: Water," 2016, http://water.worldbank.org/node/84122

Understanding the vulnerability of people, infrastructure, and ecosystems to climate variability and change can illuminate the potential for existing social tensions to be exacerbated, or for new tensions to emerge. A **better understanding of how will climate change impact economic, environmental, social and political drivers of fragility and conflict would be the first step to tackle it.**

Instability

Instability is a state of likely change while 'Instability drivers' are defined as any conditions, events, or circumstances that increase the tendency for the security environment to be unpredictable.

Environmental pressures have shaped human migration and settlement patterns for millennia. However, two features make the current era unique in human history. First, the process of climate change in the modern period stems partly from human-induced changes in the environment. Industrialization and mass consumption have led to a dramatic increase in pollutants which have long-term consequences for the Earth and exacerbating health problems.

Secondly, **nationalism** and the compartmentalization of territory into exclusive **political jurisdictions** (i.e. states) places limits on human mobility as societies place a greater emphasis on who is to be included within the polity.

There still is no consensus as to the specific implications of climate change or other such pressures for human security. Due to climate changes sea-level rise caused by a reduction in glacial coverage will lead to the flooding of coastal areas; low-lying, coastal regions will be evacuated as water encroaches upon human habitats; desertification will cause people to migrate out of unproductive and water-scarce areas; greater variability in weather patterns will lead to dramatic climate events such as hurricanes, typhoons, and extreme cold which will disrupt human settlements; unpredictable rainfall will lead to periods of flooding and drought, making certain areas uninhabitable. That may exceed national civil response capacity.

The **scarcity of resources** such as water, farmland, and timber may lead to Malthusian conflict between people competing over the same limited supply goods. This may result in increased internal tension between government and populace, immigrants or between different subnational groups. Many risks of climate change are concentrated in urban areas.

Climate change is able to accelerate instability and exacerbate other drivers of insecurity that will simultaneously affect the environmental, economic, social, and political fabric of any modern society. **It undermines the pillars of stability: food, water and other resources,** especially for countries suffering from political instability and ethnic tensions. Overall, the risks to the stability of states and societies will increase. And that would

become an **accelerant to national and international instability.**

Unrest

As a consequence of climate change, heat waves and drought have strong impact over the people way of live. It affects simultaneously every person, despite his economic, educational, societal or age status and every state big or small, developed or developing. It concerns especially crop production. Climate change has strong influence over countries which rely on food growing. High temperatures and reduced rainfall lead to crop devastation, poverty and migration. Climate change and globalization of food market have direct influence over the price of the grain all over the world and in countries with volatile political situation. In 2012, Oxfam estimated that the average price of staple foods such as maize could more than double by 2030[3].

Climate-induced food insecurity and volatile food prices coupled with lack of trust in governments in some countries may spur social unrest, protests, rioting, democratic breakdown or even civil conflict social unrest are possible. Effects very by affected groups of society. **Social unrest could include mob violence, post-conflict revenge, insurgency, predatory violence,**

[3]https://www.oxfam.org/sites/www.oxfam.org/fles/20120905-ib-extremeweather-extreme-prices-en.pdf

communal conflict, sexual and gender-based violence, government repression.

Change in the climate will have future effect over almost every aspect of human life including interdependency between climates, economic and politic would be in the basis for future social unrest.

Capacity

The capacity represents the ability of an institution/organization to do something in particular. Each state must have the capacity in completing its core goals. Climate change is drawing unprecedented international attention because it impacts nearly all domains and is a compounding factor for other existing issues. They present challenges to the capacity of individual states to manage a mounting set of interconnected problems. Extreme weather phenomena worldwide, such as droughts, floods, severe storms, heat waves, and sea level raise the specter of significant impacts of changing climate in the near term. The higher severity undermines the states and NATO capacity to react in a proper extent in order to be efficient enough. The capacity depends on the ability of using of the technics, infrastructure condition and recourses availability. Climate change and following sea-level rising, storm surges and rain rates increase, lead to limitations in technics usage, infrastructure disruption and recourses restrictions. The greatest insecurity will likely occur in states or regions that are already recognized as fragile, with low economic, social, or

political capacity to absorb the effects of climate change and adapt effectively.

NATO identified the Artic, natural disasters worldwide, and potential instability due to migration as 'Instability Situation'[4]. Civilian and military authorities must have capability to respond to instability situations. Climate impacts will directly affect military facilities, personnel, and hardware. NATO cannot ignore the effects of extreme weather events and rising temperatures on military training, operations, acquisitions, and infrastructure. The military installations' vulnerability to global warming impacts and directed military planners to incorporate climate change considerations into certain installation planning efforts; a faster process of sharing climate change-related knowledge between member states and the Alliance is indispensable. This encompasses learning from capacities that exist on the member state level and upgrading them to work on the Alliance level.

The main question concerning the CAPACITY is "How adequate the states or even NATO would be if in some occasion some instability situations happening in the same time and simultaneous reaction is needed?"

[4] NATO defines " Instability Situations" as generic descriptions of possible future events of critical significance that could reach the threshold requiring the Alliance to use military forces

Poverty

The increased frequency and intensity of extreme weather events like hurricanes, floods, wildfires and droughts threaten food supplies, drive people from their homes, separate families and jeopardize livelihoods. Meanwhile oceans are already suffering from elevated acidity and lower levels of oxygen as a result of climate change. One prognostic model shows marine fisheries would lose 3m tons if the average temperature will be increased at 2C", twice the decline at 1.5C".And all of these effects increase the risk of conflict, hunger and poverty.

Furthermore, gradual changes brought on by deforestation, overgrazing and drought slowly transform pastures to dust, destroy crops and kill livestock, effectively challenging the livelihoods of millions of farmers. These families are forced to leave their homes behind in search of basic necessities and new work. **All aspects of food security are potentially affected.**

Pre-existing poverty multiplies the chances of failure when a state or region is faced with a massive flood or long drought. Climate-related hazards exacerbate other stressors, often with negative outcomes for livelihoods, especially for people living in poverty. The majority of low-income countries are situated in tropical zones closer to the equator. On average they are hotter, which has traditionally limited their agricultural outputs, and as temperatures increase, the amount of agricultural output decreases further. Slow down economic growth, make poverty

reduction more difficult. Effects vary by region and global economic impacts are difficult to be estimated**.**

Climate change threatens the cleanliness of our air and depletes our water sources. It disrupts livelihoods, forces families from their homes and pushes people into poverty and as a consequence of that to migrate.

Migration

Climate-driven environmental change is anticipated to influence some, if not all, of the factors that threaten security. It can undermine livelihoods, increase migration, create political instability or other forms of insecurity, and weaken the resilience and ability of states to respond appropriately. Even today, the flow of refugees has reached a level that is unprecedented in recent history. The collective inability to recognize and mitigate rapidly deteriorating circumstances in a specific region, and to prevent a crisis from occurring, might lead to a mass migration. Uncontrolled migration on this scale exacerbates security risks for the country of origin as well as for transit and receiving countries. Migration and unrelated population growth have added supplementary stress to already unstable relations between ethnic groups in the Muslim north and Christian south.

As climate change causes shifts in accessibility to water, we observe large movements of refugees and emigration. Also, rising sea levels, extreme weather events and prolonged drought force millions of people to move away from home every year in

search of food, water and jobs. Extreme weather displacement can be national, international; permanent, circular, temporary; voluntary or forced.

Lack of effective governance may allow other state and non-state actors to exploit the power vacuum. Under-governed or un-governed areas due to newly inhospitable local climates or in the aftermath of pandemic could provide refuge or safe havens to potential adversaries.

Collapse

Linear thinking underlines that if we face a change of a certain magnitude we can predict the change of its output. Similarly, the non-linear thinking suggests that relatively small changes can lead to significant and unpredictable circumstances on the output. Assuming that the rate of how the climate is changing is not linear but is depicted as a curve, it is very likely that things are happening faster and with greater magnitude that we might expect and as result all our projections and predictions might turn to be excessively conservative. **It is indisputable that climate change is a long term process.** If the sea level continues to rise in the upcoming years, a proportion of the land is going to disappear under the sea. A remarkable proportion of the population dwells along the coastline. All these people will flee their homes seeking new places to live. The same result will take place in rural areas due to crop degradation. That can lead to a large climate change refugee population who is going to move within the stricken country or towards neighboring ones. **The**

humanitarian crises could take epic dimensions. How the stricken or the receive country will absorb them? Some countries maybe build fences to stop the migrants exacerbating the crises. Others will accept them deliberately or not. Depending on the immigrant´s number the consequences might be dramatic. **No factor of the state could be excluded from the impacts. The consequences might be multiple.** Overwhelmed medical sector, deteriorated sanitization conditions, food and water scarcity, energy inadequacy, failure of physical and critical infrastructures, urbanization, social unrest, criminality, terrorism, diseases, economic and educational degradation and inflation are only some of them. Each government should meet at least the basic needs of the population. The state especially if is characterized by poor governance, corruption, political instability and economic vulnerability might fail adapt the emerging situation by coping with the stresses and looking after the population.

In such case the state is likely to collapse destabilizing not only the specific country but also affecting the regional and international stability. The reality is that the world is globalized. It is very difficult in this world to isolate a country. It is clear that threats emanating from global warming will exceed national and regional scopes. As result, **it is very likely, that the collapse of a country may have a domino effect. Against this backdrop, our predictions regarding the impacts in such a case could be refuted by the events**.

Dependency

Our entire way of living is based on fossil fuels. Everything we touch in our daily life is moved back to us by using a simple source. **There is absolutely a link between the way we use energy and the security.** Oil and gas are global trade commodities. Events around the world impact the supplies and the prices at home affecting the daily life. Moreover ties and relationships between countries have been based on fossil fuels supplies and transactions. The international community spends a huge amount of money and human resources to ensure the uninterrupted flow of these supplies through sea or land, protecting and defending strategic oil and gas share points. A possible disruption could have devastating consequences for national and international economies. Energy as a natural resource creates a new arena for conflicts. Climate change is in that mix of causes. In some cases climate change can change the map itself. Melting icebergs in the Arctic can drive a military build-up. It is believed that Arctic Cycle contains 30% and the 50% of the world´s undiscovered reserves of natural gas and oil respectively. While the ice is melting new opportunities and challenges are opening. As the Arctic ice continues to retreat, trade routes will remain open for longer periods of time, increasing annual traffic of ships carrying goods and resources in the North making the Arctic more and more accessible. That is related to new resources, routes and wealth. But at the same time shapes land claims, powers´ competition and disputes. At

present, no one owns the Arctic, but Canada, Denmark, Norway, Russia, and the United States have all laid different claims to territories on it. These stressors are in turn likely to disrupt the lives of millions of people leading to regional resource conflicts.

Climate change propels the current energy system to an uncertainty rendering it unsustainable and cascading risks and impacts around the globe. By amplifying existing environmental, social, political and economic challenges, climate change increases the likelihood of competition and conflict over resources

Mitigation/Adaptation

Mitigation are actions to limit the magnitude or rate of long term climate change while **adaptation** aims to increase society's resilience to climate change.

The fundamental issue over climate change is whether we can foresee what need to be done in order to mitigate the emerging risk timely. We cannot ignore the cost of inaction leaving the massive security concern to the next generations. Nowadays we face severe with high probability risks due to climate change. Climate change is a threat multiplier. It threatens national and international security aspects. Even super powers cannot handle this security issue with the strong military force they have. **Limiting climate change will require substantial and sustained reductions of greenhouse gas emissions.** A

toolbox with politic, economic, technological, environmental and risk reduction tools must be encapsulated into our arsenal.

Prevention and prediction are the first steps. Scientific advances and increasing computing power mean that weather and climate prediction and early warning will become increasingly long-range, more accurate and available. Employing this knowledge with intelligent application of risk based methodologies will allow governments and authorities to take positive steps to plan, prepare and respond to events that are related to climate, environment or natural disasters. New data for improved climate and weather forecasting can be used. The accuracy of predictions enhances the effectiveness of strategic planning, modeling and gaming. If we can make the right predictions we can perceive what we have to do to mitigate the climate change impact. Of course this is a very hard work because weather and climate are chaotic. It takes a lot of scientific research. **The analysis of the problem in order to define the most vulnerable parts, to address and reduce the risk is also fundamental.**

Policy is the first decisive component. Politicians have to believe that climate change is reality. Unfortunately, in contrast to the scientific mainstreaming some of them are still highly skeptical regarding this issue. They must be the catalysts in a manner of cooperation within a system in which many countries take part, especially the industrialized ones which are the vast polluters. We need to brink the world together for a common

target, a common action. Steps that build resilience and enable sustainable development can accelerate successful climate-change adaptation globally otherwise the costs of adaptation and mitigation can be extremely high and fall disproportionately across the globe, such that some of the world's poorest nations, which contributed very little to creating the crisis, will face some of the greatest challenges. To tackle the problem we need a whole governmental and societal approach. Adaptation planning and implementation can be enhanced through complementary actions across levels, from individuals to governments. Nations will need to improve resilience by addressing climate adaptation measures for their infrastructure and equipment. Governments must start developing adaptation plans and policies based on multilateral environmental agreements and protocols, adopting domestic environmental legislation, cooperate in international environmental organizations and institutions and integrating climate-change considerations into broader development plans. An overarching step towards adaptation to future climate change is reducing the carbon dioxide emissions. The Paris agreement must be implemented and strengthen goal to "well below 2C" and efforts to reach 1.5C". Governments must be better prepared acting drastically. They have to consider mitigation of and adaptation to climate change as one of their most crucial national security priorities. Our course of action must be very fast. In any strategic system time is the most precious recourse. It is maybe the only one thing that cannot be replenished. Even if the targets concerning greenhouse gas were met today, any mitigation

efforts would not have impact for at least two decades, and so climate change will continue along its current trajectory through 2035 and beyond.

There is also a **military role in it**. Military plays a significant role in conflicts, prevention, protection and in building capacity and stability overseas. Since military is one of the greater oil consumers it has a huge margin to reduce carbon dioxide emissions by minimizing its energy footprint, for instance by charging its batteries by using solar systems. Besides it can provide the satellite and reconnaissance systems for helping the scientific research and the response in humanitarian assistance. **Private sector** can contribute by providing technological assistance, creating job and funding.

Technology is an overarching tool. New challenges need new means and initiatives to tackle them. The response on climate change involves a type of an industrial revolution. We need to live behind the technology based on fossil fuels and shift towards a clean technological resonance. The rate that technology is improving constitutes a economic boom. Technological means are enhanced. Oceans can provide with water, energy and food. **Renewable energy is the solution.** Adoption of new, efficient or renewable energy technology may save our lives and Earth´s existence. It is given that good progress has been made in the adoption of renewable energy. Though, the Earth needs more clean energy.

Science maps out different pathways to limit our planet´s warming using different combinations of land use and technological change. **Reforestation** is essential to all of them as are **shifts to electric transport systems and greater adoption of carbon capture technology.**

Responding to climate-related risks involves decision making in a continuous changing world.

Conclusion

The Earth system consists of three coupled subsystems: the climate system, the natural system, and the human system. Each of these systems affects the others directly and indirectly, creating a complex socio-environmental system. The changes in climate have **caused impacts on natural and human systems on all continents and across the oceans, but in very short geological time scale**. Exactly this shortness is the main issue. Climate change exacerbates existing trends, tensions and instability that's why can be classified as a threat multiplier which does not discriminate between borders, but is more a concern with global implications. It is significant threat to security operating on a planetary scale simultaneously activating multiple security challenges. Hence, it is expected to shape the security environment in the twenty first century.

Scientists agree that humans are causing climate change. Currently, the main action is the need for urgency to mitigate the threat. Mitigation of climate change can only be achieved through

extensive global cooperation and action. Local governments and the main international actors such as regional-international organisations. States and civil society must be integral part and helper to that direction if we are still interested in human´s being survival. Current efforts are not adequate to meet future security challenges.

The overall risks of climate change impacts can be reduced by limiting the rate and magnitude of climate change. The international community must pay increase attention implementing a stronger and more coherent approach to dealing with the problem. Our future relies on our hands.

Bibliography

Amar Causevic, “Facing an Unpredictable Threat: Is NATO Ideally Placed to Manage Climate Change as a Non-Traditional Threat Multiplier?”, 2017

UN Intergovernmental Panel on Climate Change (IPCC) Assessment report, AR5-2014, https://www.ipcc.ch/site/assets/uploads/2018/03/WGIIAR5_SPM_Top_Level_Findings-1.pdf

“Climate change and security,” Bulletin of the Atomic Scientists 64, no. 2 (2008)
NATO SACT, Strategic Foresight Analysis Report, 2017

NATO SACT, Framework for Future Alliance Operations Report, 2018

OXFAM “Extreme weather, extreme prices. The costs of feeding a warming world”, 2012

UN outcome document, Transforming our world: the 2030 Agenda for Sustainable Development”, 2015.

World Bank Group, “At a glance: Water,” 2016, http://water.worldbank.org/node/84122

https://www.theguardian.com/environment/2018/oct/08/global-warming-must-not-exceed-15c-warns-landmark-un-report

https://www.unenvironment.org/explore-topics/disasters-conflicts/what-we-do/risk-reduction/climate-change-and-security-risks

NATO IN THE ANTHROPOCENE: EMERGENCE OF THE TIPPING POINTS AND ASSOCIATED SECURITY CHALLENGES

Amar CAUSEVIC,
Royal Swedish Academy of Sciences

Abstract: The Anthropocene defines Earth's current geologic era in which human activities have been the dominant factor in influencing the Earth system processes such as climate and the environment. This paper will briefly introduce the Anthropocene, and its main characteristics emphasizing important role humankind represents in this geological era. Then, the paper will provide a general definition, classify per estimated threshold temperature, and explain the phenomenon of self-reinforcing feedbacks of Earth system tipping points. In the third section, the paper will outline a brief risk analysis of impacts originating from the emergence of selected tipping points. For example, what will be security risks of continuous melting of the Alpine glaciers in the near future on individual NATO member states? Furthermore, how will sea-level rise caused by the melting of the Greenland Ice Sheet and Arctic summer sea-ice impact coastal cities in NATO member states and Alliance's vital military infrastructure? The last section will examine the Alliance's ability to addressing emerging and non-traditional security challenges, the focus being on the threat multiplier effect of climate change.

Key words: NATO, Anthropocene, tipping points, threat multiplier, non-traditional security challenges.

Introduction

Climate change is evident, and from year to year, it is becoming more and more critical. In 2016, atmospheric carbon dioxide (CO_2) concentrations rose past 400 parts per million (ppm), a stunning figure given that pre-industrial era levels were 280 ppm

(Thompson, 2017). Extreme weather events are becoming more frequent and devastating. In 2018, 13 federal agencies in the United States issued a major report stating that climate change is a threat to national health and economic well-being costing the country US$3.5 trillion since 2008 (United States Global Change Research Program, 2018). Climate change claimed its first mammal extinction, tiny Australian rodent called Bramble Cay melomys, when the rise in sea-level over the years destroyed coastal vegetation which was the only source of food on the island it inhabited (Platt, 2019).

Climate change is a threat to security. Climate change is also a severe threat to militaries since it tests their readiness to respond to national security emergencies. Correspondingly, environmental risks emanating from climate change directly threaten military installations. Raging wildfire made the Marine Corps Mountain Warfare Training Center evacuate its staff in September 2018 (Navy Times, 2018). According to the Union of Concerned Scientists report from 2016, rising oceans threaten to submerge 128 United States military bases by 2050 (Union of Concerned Scientists, 2016).

This paper conducts an analysis of climate change as a threat by investigating the role of Earth system tipping points. The paper will introduce the Anthropocene epoch and explain how are climate change and tipping points an integral part of our current geological age. The analysis will continue with a brief definition of tipping points, explanation of their interconnectivity, and

tendency to operate as a cascading system. Then the paper will focus on looking at potential future security risks of tipping points that will activate with the average global temperature increase of 1 degrees Celsius (°C) to 3°C. This section will be followed by a short discussion on the problematic nature of integrating tipping points and the Anthropocene in North Atlantic Treaty Organization's (NATO) security mechanism as well as discuss current efforts of the Alliance aimed at addressing environment-related security concerns.

The Anthropocene: The age of humans

The concept of the Anthropocene derives its name from Ancient Greek words *anthropo*, which stands for 'human' and *cene*, which stands for 'new'. The Anthropocene presents a newly proposed geological epoch, not yet officially approved the term as a recognized subdivision of geological time that marks a time point in planet's history in which human-induced activities started to have a significant global impact on Earth's geology and ecosystems. Unofficially the era started with James Watt's invention of the steam engine in the late 18th century (Crutzen, 2002). This means that human actions radically define changes in the Earth system, instead of previously led traditional factors such as Earth geology itself (e.g. volcanos) or cosmic forces (e.g., meteorites).

People have been trying to control nature since the outset of the human civilization. With the advance in technological, economic,

and social developments, human influence on the planet has become more and more significant. The origins of the Anthropocene stem from research done by the American diplomat and philologist George Perkins Marsh who in his books *The Earth as Modified by Human Action* and *Man and Nature* provided first scientific observations summarizing destructive power of industrial societies on the environment (Marsh, 1862, 1874). In the 20th century Marsh's idea will be taken further by scientists such as R. L. Sherlock, W. L. Thomas, Pierre Teilhard de Chardin, Aleksei Pavlov and Vladimir Vernadsky who all in their respective scientific work observed surprising speed in the growth of mankind's geochemical impact on the Earth (Steffen *et al.*, 2011; Lewis and Maslin, 2015). In the year 2000 Eugene F. Stoermer and Paul J. Crutzen officially introduced the idea of the Anthropocene in the newsletter of the International Geosphere-Biosphere Programme defining it as an epoch in which human activities are exerting increasing impacts on the environment on all scales (e.g., population growth, resource extraction, greenhouse gases emissions, etc.) and in many ways outcompeting natural processes and their ability to regenerate (Trischler, 2016).

Even though the epoch originated with steam engine invention in 1784, it was not until post-1945 that the human influence radically increased. The imprint of human activity on the Earth system was present and visible before the end of the Second World War. Nevertheless, its magnitude and speed radically increased after

1950. This trend was referred to as the Great Acceleration (see Figure 1), characterizing current phase of the Anthropocene (Costanza, Graumlich and Steffen, 2007). The human population more than doubled, and economic growth rates increased over 15 times (Steffen, Broadgate, *et al.*, 2015). The growth was also evident in other indicators such as primary energy use, fertilizer consumption, water use, and transportation. At the same time, the Earth system's indicators such as surface temperature, ocean acidification, tropical forests loss, and several others experienced an increase as well. Global Footprint Network estimated in 2012 that human ecological footprint of consumption is overshooting the planet's capacity to provide enough resources to sustain it; for example, if we consumed resources like Emiraties we would need over five planets, like Americans around four and as Ugandans little bit above the half of the Earth (McDonald, 2015).

The Anthropocene is changing the Earth's geology, atmosphere, and biosphere, and these actions have a long term effect on future trajectories of natural systems. Scientist at Intergovernmental Panel on Climate Change that until temperatures 2100 are going to rise between 2°C and 4°C and in order to keep up with the projected changes for 2100 the species would 'require rates of niche evolution that are > 10,000 times faster than rates typically observed among species, for most variables and clades' (Quintero and Wiens, 2013, p. 1095). Human influence on the Earth started when our societies

organized in primitive hunting, farming and animal husbandry communities several thousand years ago. However, human activity through a primarily modern economic system is transforming planet's physical, chemical and biological processes from their current know state and behavior to future unknown and potentially dangerous states for the survival of civilization as we know it (Steffen *et al.*, 2018). Humans are slowly crossing environmental limits within which humanity can safely operate (Steffen, Richardson, *et al.*, 2015). This means that reasonably stable current environmental conditions will become more unstable and unpredictable in the decades and centuries to come. The planet will react to the actions humans conduct on it.

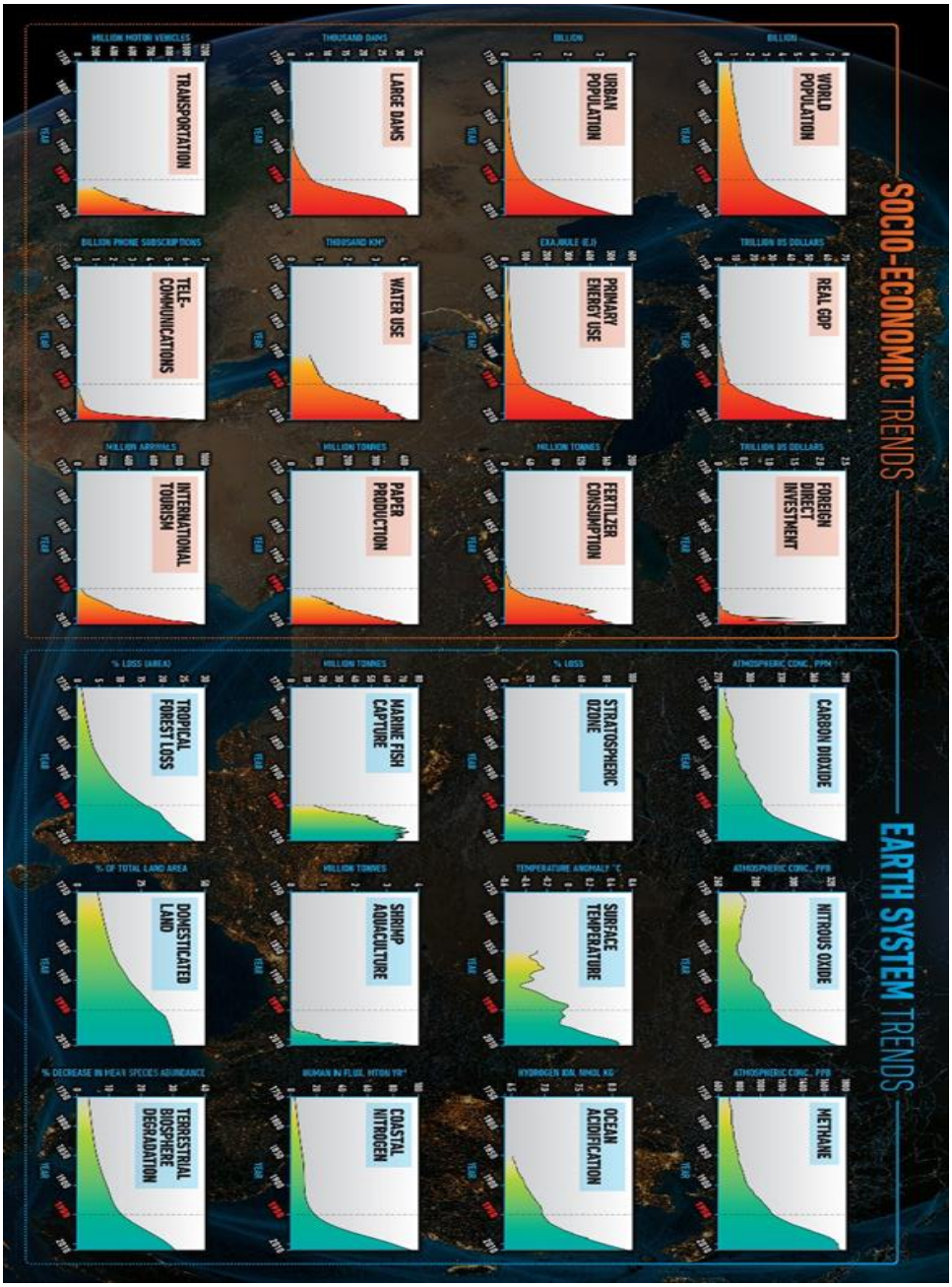


Figure 1: *The Great Acceleration in Socio-Economic and Earth System Trends (Steffen, Broadgate, et al., 2015).*

Tipping points in the Earth's climate system: definition and modus operandi

A tipping point in the climate system is defined as a climate system's stability threshold, which if surpassed, can lead to substantial changes in the state of the system. Tipping points in the Earth's climate system can be both classified as the physical climate system and impacted large-scale ecosystems. Tipping points have been studied more intensively since the 2000s (Lindsay and Zhang, 2005; Russill and Nyssa, 2009; Nuttall, 2012; Milkoreit *et al.*, 2018). Lenton et al. (2008) identified and evaluated tipping points that focused explicitly on large-scale components of the Earth system that are under anthropogenic forcing (see Figure 2).

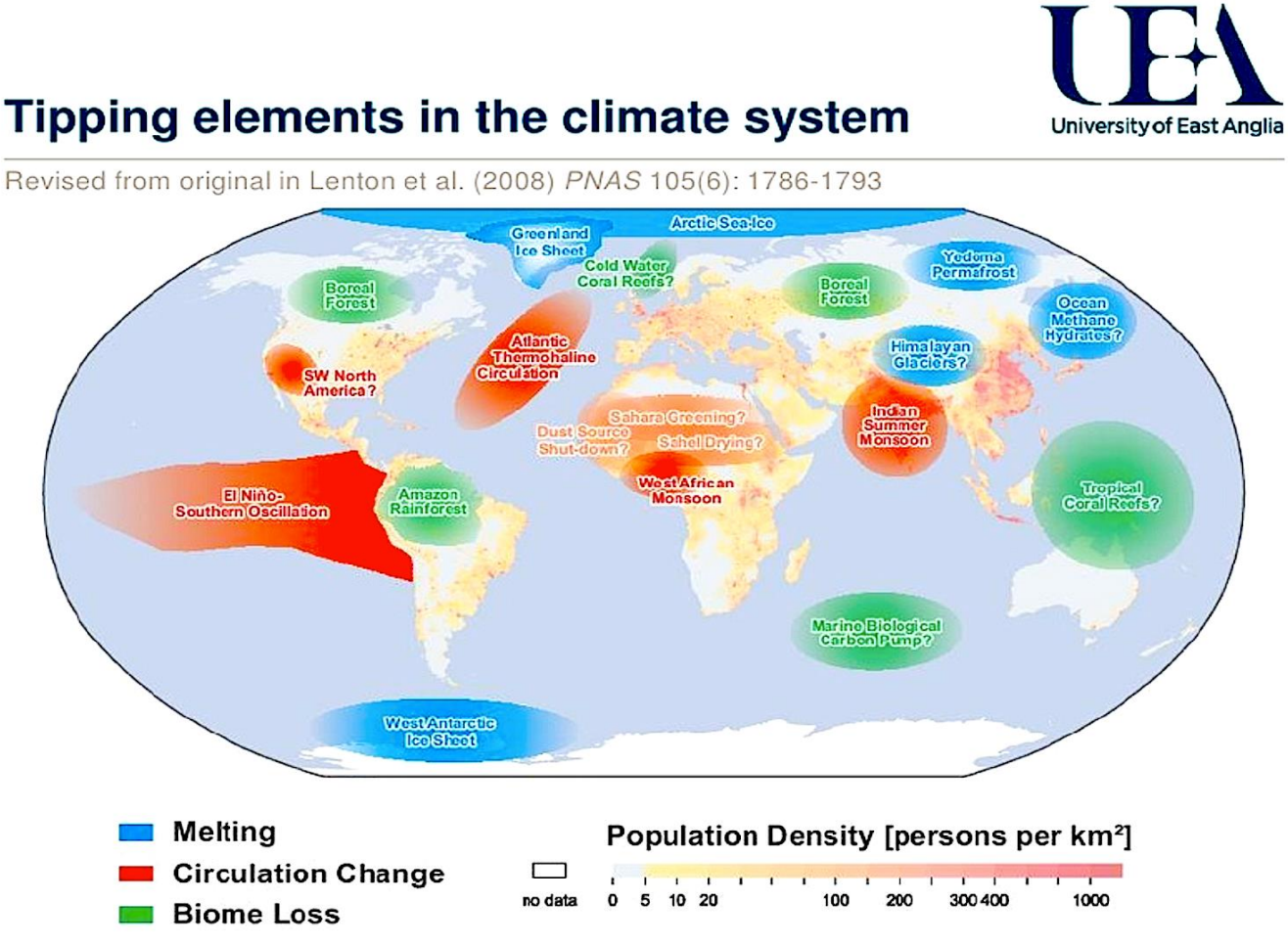


Figure 2: *Map of potential policy-relevant tipping elements in the climate system (Lenton et al., 2008)*

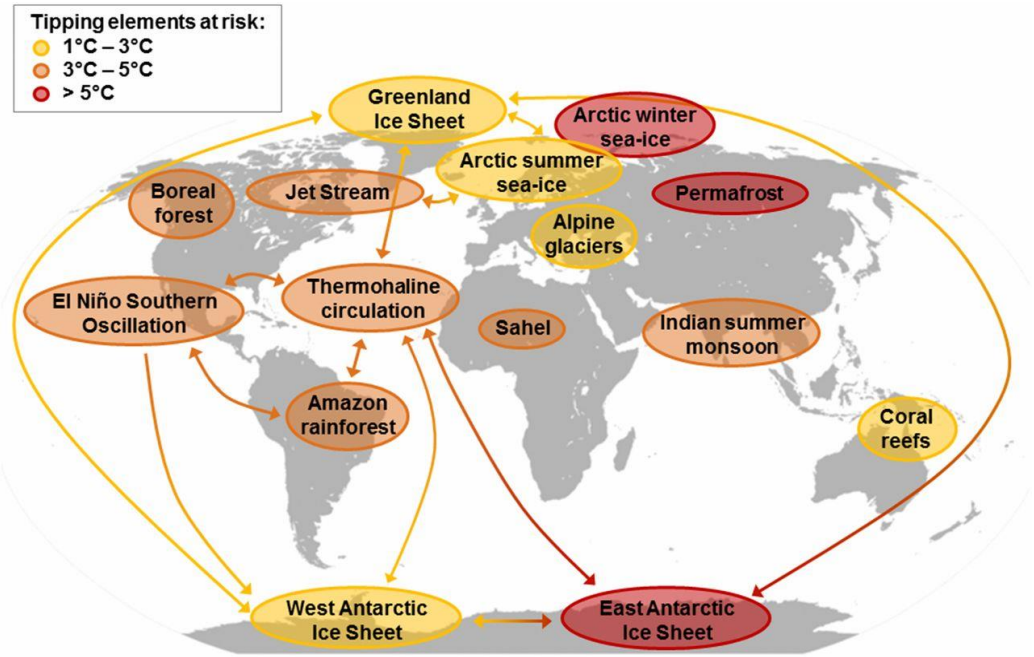
Milkoreit et al. (2018) defined tipping points as:

> ‘threshold at which small quantitative changes in the system trigger a non-linear change process that is driven by system-internal feedback mechanisms and inevitably leads to a qualitatively different state of the system, which is often irreversible.’ (p. 9)

The common denominator to all identified Earth’s climate system tipping points is the fact that, in our case of study, human-induced stress they incur can lead to unexpected system changes that are difficult, or even impossible to reverse. The level of unexpected system changes depends on the tipping point that is changing; some experience more while others tend to have less dramatic change and impact on the climate system.

Earth system is a cascading system; a type of dynamic system characterized by the transfer both positive and negative feedbacks along a chain of component subsystems and in the end this feedback will affect the condition of the entire system. A recent study examined more than 300 case studies and 30 types of regime shifts finding out ‘that 45% of regime shift pairwise combinations present at least one plausible structural interdependence’ (Rocha *et al.*, 2018, p. 1379). This means that the tipping point in one ecosystem can trigger or increase the risk of tipping points in other ecosystems; sometimes, this can happen over far distances.

Figure 3: *The individual tipping elements and their estimated global average surface temperature thresholds (Steffen et al., 2018).*



The idea of cascading effects can be easily applied to the tipping points as well. One feature of the tipping points is their interconnectivity operating in a domino effect pattern (Hu *et al.*, 2009; Boers *et al.*, 2017). For example, the rapid melting of the Greenland Ice Sheet will increase the amount of fresh water in the North Atlantic Ocean. This increased influx of fresh water could reduce the surface salinity and density disrupting the Atlantic Thermohaline Circulation (Rahmstorf *et al.*, 2015). Worst case scenario is a shutdown of the thermohaline circulation, which if this happens will have cataclysmic consequences. There are currently no accurate predictions when specific tipping points might be triggered, how fast it will unfold, and what will be exact

damage to the global political, ecological, and economic systems. However, scientists were able, based on exhaustive previous research and data, to approximately identify temperature thresholds (see Figure 3) which if crossed can lead to the tipping of the planetary climate system's elements causing severe disruption (Steffen *et al.*, 2018).

When tipping points cross their threshold, they can increase the speed of the average global temperature rise. This increases the risk that self-reinforcing feedbacks could push the planet towards a pathway which in the end 'could prevent stabilization of the climate at intermediate temperature rises and cause continued warming' (Steffen *et al.*, 2018, p. 8252). Past and current evidence gathered through tipping points observation research indicated that human activities are quickly changing the internal dynamics and driving feedbacks affecting the long-term stability of the Earth's climate system as a whole (Lenton *et al.*, 2008; Lenton and Williams, 2013).

Tipping points and potential future security risks

During the United Nations' 24th Conference of the Parties in 2018, it was announced that after two years of plateauing anthropogenic CO_2 emissions have been on the rise again. Increase in emissions stands in complete contrast to the Paris Agreement from 2014 in which international community agreed that humanity would need to reduce CO_2 emissions in order to limit global average temperature increase between 1.5°C and

2°C in the 21st century. The rise in the emissions is evident in all major economies; in China up 4.7%, in the United States by 2.5% and in India by 6.3% (Carrington, 2018). Many experts are a skeptic that the humanity will be able to reorganize its socio-economic system and emission generation patterns anytime soon and that this would lead to a global average temperature increase up to 4°C until 2010 which well beyond potentially safe 1.5°C−2°C increase (Brown and Caldeira, 2017). As presented in Figure 3, tipping points will be affected by any increase, even 1°C, of the global average temperature. Nevertheless, the higher the increase of the temperature, the more radical effect and potential cascading consequence of the particular tipping point.

Due to the length and the format of this paper, the analysis of the potential future security risks originating from global average temperature increase stress on the Earth climate system's tipping points will be limited at looking at the security risks of 1°C−3°C temperature increase (as depicted in Figure 3). The paragraphs below will examine potential future security risks that can emerge as North and South Poles (Greenland, Arctic, and the Antarctic) ice sheets melt, as mountain glaciers diminish and as corals face massive die-off.

Melting ice will raise sea-level. If wholly melted, the Greenland ice sheet will raise sea-level for 6 meters (VPRO Tegenlicht, 2017). Raising sea-level is a direct threat to human habitat alongside the coastlines. In 2013 a group of experts from the World Bank published a paper that estimated future flood losses

in major coastal cities across the world. They found out that average global flood losses in 2005 were estimated to be approximately US$6 billion per annum, but due to projected future sea-level rise, these costs are expected to spike to US$52 billion per year by 2050 (Hallegatte *et al.*, 2013, p. 802). Cities from cultural hubs such as Venice to financial powerhouses such as New York will be seriously endangered.

Rising sea-levels can contaminate freshwater sources used by the coastal communities. With the increase in its level, sea water will leak into the freshwater sources in the ground that many coastal areas rely on for their drinking water. Furthermore, as rising salty water moves inland by penetrating farmland close to river estuaries and the coasts. Nicholls and Leatherman (1995) estimated that 1-meter sea-level rise would affect 6 million people, 12%−15% of agricultural land lost in Egypt, and 16% of national rice production lost alongside 13 million people in Bangladesh. Dutch agriculture, an industry worth billions of dollars, has very high economic sensitivity in the agricultural sector and impact associated with sea-level rise (Schuttenhelm, 2019). Besides creating millions of climate refugees, the devastation of infrastructure and disturbance in global food production, the sea-level rise would upsurge the price of different food commodities.

Melting ice can unfreeze diseases and microbes that had not circulated in the air for millions of years in some cases, probably before humans walked on the Earth (Fox-Skelly, 2017).

Greenland receding ice cap slowly started to reduce the ice cover above the United States Army's Project Iceworm site, which was a secret base sought to deploy up to 600 medium-range ballistic missiles during the 1960s. According to recent research, the base was:

> '*eventually abandoned with minimal decommissioning, under the explicit assumption that perpetual snowfall would entomb them in perpetuity, leaving large quantities of waste buried in the ice sheet*' (Colgan, 2018, p. 35).

Lastly, sea-ice reflects most of the sunlight it receives, and as sea ice melts, it exposes the dark ocean surface. Dark ocean surface does the opposite, and it absorbs most of the sunlight it receives. As a result, the oceans will heat up, leading to further warming of the ocean surface. Direct sunlight in dark ocean surface has a direct impact on ocean acidification, ocean currents, tides, and weather as well trigger several changes in ocean bio-geochemistry which can have severe replications for the societies at large (Balmaseda, Trenberth and Källén, 2013; Mora *et al.*, 2013).

World Glacier Monitoring Service recently warned that mountain glaciers around the world are retreating at alarming rates (World Glacier Monitoring Service, 2019). The disappearance of the mountain glaciers will cause several problems. Alpine glaciers provide large quantities of drinking water and water for agricultural use. Italian River Po Basin accounts for more than

30% of the total agricultural production in the country, and it's surface water is predominantly coming from the Alpine glaciers (European Commission, 2012). After a hot summer in 2018 one of Europe's most important rivers, the Rhine, experienced one of the shallowest water levels which led to the grounding of the river traffic for nearly a month (Wilkes, Dezem and Parkin, 2019). The river traffic on the Rhine is of extreme economic significance since it links German and Swiss industry with Europe's biggest port, Rotterdam.

Melting of glacial ice will affect hydropower generation. Bettina Schaefli (2019) estimated that Switzerland, which produces over 50% of its electricity from hydropower, will for the period 2070–2090 experience a production reduction of about one terawatt-hour per year due to glacier retreat. Melting glaciers can harm tourism because skiing is slowly becoming scarcer at lower altitudes. For example, several European Banks have begun refusing loans to ski resorts under 1,500 meters, and by 2030 Swiss skiing region Bernese Oberland will incur an annual turnover loss of US$58.7 million (Hartman, 2007).

Coral reefs are a vital component that contributes to the health of the ocean and the planetary ecosystem in general. They are areas with the most vibrant and most diverse biodiversity in the oceans providing breeding and nurturing grounds for thousands of different species, supporting 25% of marine life (Witschge, 2018). Coral reefs also prevent strong waves from crashing into the coastline, protecting humans and fragile coastal ecosystem

from strong waves. Nevertheless, these marine ecosystems are at considerable risk. According to World Wide Fund for Nature, tropical reefs have lost more than 50% of their reef-building corals since the mid-1980s and if the global average temperature continues to rise the reefs will disappear from global oceans by 2050 (World Wide Fund for Nature, 2015). Besides coral mining, different types of human-caused pollution, overfishing, blast fishing, the digging of canals and access into islands and bays coral reefs are experiencing massive bleaching due to raising of average water temperature across the oceans (Hughes *et al.*, 2017). If reefs continue to degrade further, they will harm the economies of different countries as well as disturbing way of life of their populations. In 2018, the global annual value of goods and services provided by coral reefs was US$30 billion, and economic value of coral reefs derived from tourism and recreation was around US$9.5 billion (Witschge, 2018).

NATO and tipping points-related security risks

Climate change is a non-traditional security challenge that has an active threat multiplier component (Causevic, 2017). It is a concept that cannot be easily integrated into political thinking and the security apparatus, since it strong foundation in both international relations and securitization theories which are used to addressing more traditional and human-centered security challenges (Lonergran, 1999; Donnelly, 2000; Trombetta, 2008; Smith *et al.*, 2014; Byrne and Maslin, 2015). Climate security, as a concept, represents a big challenge for politicians and the

security sector. For less than 12,000 years, humanity has been living in the geological epoch called Holocene, which was characterized by the stability of the climate, unlike during earlier epochs (Walker *et al.*, 2009). Human species utilized this period to thrive and develop major civilizations resulting in industrialization, which has led to the Anthropocene and the Great Acceleration in the mid-20th century. Security in the Anthropocene does not focus on the individual parts of the international system (i.e., states), but rather the system's (i.e., planet) capacity to develop a response to disturbance and adapt so it can preserve its identity and function (Walker and Salt, 2012).

> '*The complex inter-connections and feedback loops that comprise the Anthropocene's emergent spatiality generate non-linear changes that cannot be predicted from either past experiences or a given arrangement of things in the present.*' (Grove and Chandler, 2017, p. 83)

The Anthropocene undermines the sense of security that is familiar to modern society. This means that the notion of safe, confined, predictable space (i.e., national territory) that can be protected from outside influences which can be predicted does not stand. The Anthropocene functions through a set of dynamic interconnections, on a planetary scale, that is hard to recognize and comprehend through traditional securitization approaches.

Environmental security challenges have been recognized at NATO since the late 1960s, and the Alliance has officially acknowledged climate change as a threat in 2010 (Causevic, 2017). NATO disposes with institutional components such as the Emerging Security Challenges Division (established to respond to a growing range of non-traditional risks and challenges) and Green Defense framework (aimed at increasing operational effectiveness through resource resilience) all focusing on integrating climate change risk and threats to NATO's *modus operandi*. Member states such as France, Spain, the Netherlands, Denmark, and the United States formed units to respond to climate disasters and integrated climate risk in defense strategy policies (Youngs, 2014).

Through its Science for Peace and Security (SPS) Program the Alliance has cooperated with Environment and Security Cooperation Initiative the Alliance has been working on integrated water resource management, partially caused by the melting mountain glaciers in Central Asia, to restore wetlands in the Aral Sea basin (North Atlantic Treaty Organization, 2010). Also, NATO Research Vessel 'Alliance' shipped in the Atlantic Ocean in 2008 to execute research looking how military ships can operate without harming whales and dolphins as a part of Marine Mammal Risk Mitigation Project (North Atlantic Treaty Organization, 2008). SPS Program also has a Joint Working Group on Scientific and Environmental Cooperation (in existence since the early 2000s) as a part of NATO efforts to build a

partnership with Ukraine (North Atlantic Treaty Organization, 2019).

Tipping elements are part of the Earth System and will most likely be triggered by the further anthropogenic impact on the plant. However, tipping points are a problem on a planetary scale that causes threat multiplier effects across global ecosystems. Their cascading probabilities, the economic, environmental and political effects and the costs of mitigation will influence the extent to which tipping points will be securitized, as a part of a broader climate change debate (Rasmussen and Birk, 2012). In NATO's Strategic Foresight Analysis 2015 climate change is viewed as a catalyst that will further intensify political, social, and economic risks rather than the main risk itself (North Atlantic Treaty Organization, 2017). Consequently, if the Alliance wants to be better prepared to understand risks from the tipping elements, it will need better comprehension of the climate change in general and tipping points specifically.

Conclusion

The prevalence of short-sightedness makes climate change a problematic challenge, which is not the only case for the security sector but could be easily applied in politics and business. Still, climate change is happening. Indeed, one can argue that if CO_2 emissions continue to increase at the current level, they will create more direct and indirect security threats. British geologist Phil Gibbard recently said in an interview: 'We are not in control

of the Anthropocene, we are playing Russian roulette with this planet (VPRO Tegenlicht, 2017).' In the past when there were very few of us the activities of humans were negligible, but as our numbers increased together with our capacity to extract and use resources so did our impact which became as clearly as large. Earth system tipping points stimulated by changing climate are collateral damage of humankind's actions in the Anthropocene. They are a complex system, and this makes them extremely hard to label as a direct risk for the Alliance's security. To begin with their better understanding, they first need to be recognized as a risk. In order for this to happen, we need to see better integration of the climate change at large in NATO's *modus operandi*.

Bibliography

Balmaseda, M. A., Trenberth, K. E. and Källén, E. (2013) 'Distinctive climate signals in reanalysis of global ocean heat content', Geophysical Research Letters. John Wiley & Sons, Ltd, 40(9), pp. 1754–1759. doi: 10.1002/grl.50382.

Boers, N. et al. (2017) 'A deforestation-induced tipping point for the South American monsoon system', Scientific Reports, 7, p. 41489. doi: 10.1038/srep41489.

Brown, P. T. and Caldeira, K. (2017) 'Greater future global warming inferred from Earth's recent energy budget', Nature. Nature Publishing Group, 552(7683), pp. 45–50. doi: 10.1038/nature24672.

Byrne, A. and Maslin, M. (2015) 'Negotiating failure: Understanding the geopolitics of climate change', Geographical Journal, pp. 1–5. doi: 10.1111/geoj.12105.

Carrington, D. (2018) '"Brutal news": global carbon emissions jump to all-time high in 2018', The Guardian, 5 December. Available at: https://www.theguardian.com/environment/2018/dec/05/brutal-news-global-carbon-emissions-jump-to-all-time-high-in-2018.

Causevic, A. (2017) 'Facing an Unpredictable Threat: Is NATO Ideally Placed to Manage Climate Change as a Non-Traditional Threat Multiplier?', Connections: The Quarterly Journal, 16(2), pp. 59–80. doi: https://doi.org/10.11610/Connections.16.2.04.

Colgan, J. D. (2018) 'Climate Change and the Politics of Military Bases', Global Environmental Politics. MIT PressOne Rogers Street, Cambridge, MA 02142-1209USAjournals-info@mit.edu, 18(1), pp. 33–51. doi: 10.1162/GLEP_a_00443.

Costanza, R., Graumlich, L. J. and Steffen, W. (eds) (2007) Sustainability or collapse?: An integrated history and future of people on Earth. Cambridge, MA: MIT Press.

Crutzen, P. J. (2002) 'Geology of mankind', Nature, 415(6867), p. 23. doi: 10.1038/415023a.

Donnelly, J. (2000) Realism and International Relations. New York: Cambridge University Press. doi: 10.1017/CBO9780511612510.

European Commission (2012) Water saving potential in agriculture in Europe. Brussels. Available at:

http://ec.europa.eu/environment/water/quantity/pdf/BIO_Water savings in agiculture_Final report.pdf.

Fox-Skelly, J. (2017) There are diseases hidden in the ice, and they are waking up, British Broadcasting Corporation. Available at: http://www.bbc.com/earth/story/20170504-there-are-diseases-hidden-in-ice-and-they-are-waking-up (Accessed: 20 May 2019).

Grove, K. and Chandler, D. (2017) 'Introduction: resilience and the Anthropocene: the stakes of "renaturalising" politics', Resilience. Routledge, 5(2), pp. 79–91. doi: 10.1080/21693293.2016.1241476.

Hallegatte, S. et al. (2013) 'Future flood losses in major coastal cities', Nature Climate Change. Nature Publishing Group, 3(9), pp. 802–806. doi: 10.1038/nclimate1979.

Hartman, T. (2007) Alpine Tourism's Melting Prospects, Deutsche Welle. Available at: https://www.dw.com/en/alpine-tourisms-melting-prospects/a-2997649 (Accessed: 20 May 2019).

Hu, A. et al. (2009) 'Transient response of the MOC and climate to potential melting of the Greenland Ice Sheet in the 21st century', Geophysical Research Letters, 36(10). doi: 10.1029/2009GL037998.

Hughes, T. P. et al. (2017) 'Global warming and recurrent mass bleaching of corals', Nature. Nature Publishing Group, 543(7645), pp. 373–377. doi: 10.1038/nature21707.

Lenton, T. M. et al. (2008) 'Tipping elements in the Earth's climate system.', Proceedings of the National Academy of Sciences of the United States of America. National Academy of Sciences, 105(6), pp. 1786–93. doi: 10.1073/pnas.0705414105.

Lenton, T. M. and Williams, H. T. P. (2013) 'On the origin of planetary-scale tipping points', Trends in Ecology & Evolution, 28(7), pp. 380–382. doi: 10.1016/j.tree.2013.06.001.

Lewis, S. L. and Maslin, M. A. (2015) 'Defining the Anthropocene', Nature. Nature Publishing Group, 519(7542), pp. 171–180. doi: 10.1038/nature14258.

Lindsay, R. W. and Zhang, J. (2005) 'The Thinning of Arctic Sea Ice, 1988–2003: Have We Passed a Tipping Point?', Journal of Climate, 18(22), pp. 4879–4894. doi: 10.1175/JCLI3587.1.

Lonergran, S. C. (ed.) (1999) Environmental Change, Adaptation, and Security. Springer. doi: 10.1007/978-94-011-4219-9.

Marsh, G. P. (1862) Man and Nature: Or, Physical Geography as Modified by Human Action. New York, NY: Charles Scribners.

Marsh, G. P. (1874) The Earth as Modified by Human Action. New York, NY: Scribner, Armstrong & Co.

McDonald, C. (2015) 'How many Earths do we need?', British Broadcasting Corporation News. Available at: https://www.bbc.com/news/magazine-33133712.

Milkoreit, M. et al. (2018) 'Defining tipping points for social-ecological systems scholarship—an interdisciplinary literature review', Environmental Research Letters, 13(3), p. 033005. doi: 10.1088/1748-9326/aaaa75.

Mora, C. et al. (2013) 'Biotic and human vulnerability to projected changes in ocean biogeochemistry over the 21st century.', PLoS biology. Public Library of Science, 11(10), p. e1001682. doi: 10.1371/journal.pbio.1001682.

Navy Times (2018) Rampant wildfire closes military base. Available at: https://www.navytimes.com/news/your-navy/2018/09/06/rampant-wildfire-closes-military-base/ (Accessed: 21 May 2019).

Nicholls, R. J. and Leatherman, S. P. (1995) 'The Implications of Accelerated Sea-Level Rise for Developing Countries: A Discussion', Journal of Coastal Research. Coastal Education & Research Foundation, Inc., (14), pp. 303–323. doi: 10.2307/25735714.

North Atlantic Treaty Organization (2008) NATO Undersea Research Centre Human Diver and Marine Mammal Risk Mitigation Rules and Procedures (second edition). Brussels. Available at: https://www.cmre.nato.int/research/publications/latest-publications-list/87-nato-undersea-research-centre-human-diver-and-marine-mammal-risk-mitigation-rules-and-procedures-second-edition/file.

North Atlantic Treaty Organization (2010) NATO agrees to extend Environment and Security cooperation initiative. Available at: https://www.nato.int/cps/en/natohq/news_64466.htm (Accessed: 21 May 2019).

North Atlantic Treaty Organization (2017) The Strategic Foresight Analysis (SFA) 2017 Report. Brussels. Available at: https://www.act.nato.int/images/stories/media/doclibrary/171004_sfa_2017_report_hr.pdf.

North Atlantic Treaty Organization (2019) Interview with NATO Assistant Secretary General for Emerging Security Challenges Missiroli at the occasion of the 60th Anniversary of the SPS programme. Available at: https://www.nato.int/cps/en/natohq/opinions_161482.htm?selectedLocale=en (Accessed: 21 May 2019).

Nuttall, M. (2012) 'Tipping points and the human world: living with change and thinking about the future', Ambio, 41(1), pp. 96–105. doi: 10.1007/s13280-011-0228-3.

Platt, J. R. (2019) Climate Change Claims Its First Mammal Extinction, Scientific American. Available at: https://blogs.scientificamerican.com/extinction-countdown/climate-change-claims-its-first-mammal-extinction/?redirect=1 (Accessed: 21 May 2019).

Quintero, I. and Wiens, J. J. (2013) 'Rates of projected climate change dramatically exceed past rates of climatic niche evolution among vertebrate species', Ecology Letters. Edited by L. Harmon. John Wiley & Sons, Ltd (10.1111), 16(8), pp. 1095–1103. doi: 10.1111/ele.12144.

Rahmstorf, S. et al. (2015) 'Exceptional twentieth-century slowdown in Atlantic Ocean overturning circulation', Nature Climate Change. Nature Publishing Group, 5(5), pp. 475–480. doi: 10.1038/nclimate2554.

Rasmussen, K. and Birk, T. (2012) 'Climate Change, Tipping Elements and Security', in Fernando, H. J. S., Klaic, Z. B., and McCulley, J. L. (eds) National Security and Human Health Implications of Climate Change. Dordrecht: Springer, pp. 39–48. doi: 10.1007/978-94-007-2430-3_4.

Rocha, J. C. et al. (2018) 'Cascading regime shifts within and across scales', Science (New York, N.Y.). American Association for the Advancement of Science, 362(6421), pp. 1379–1383. doi: 10.1126/science.aat7850.

Russill, C. and Nyssa, Z. (2009) 'The tipping point trend in climate change communication', Global Environmental Change, 19(3), pp. 336–344. doi: 10.1016/j.gloenvcha.2009.04.001.

Schaefli, B. et al. (2019) 'The role of glacier retreat for Swiss hydropower production', Renewable Energy. Pergamon, 132, pp. 615–627. doi: 10.1016/J.RENENE.2018.07.104.

Schuttenhelm, R. (2019) In face of rising sea levels the Netherlands 'must consider controlled withdrawal', Vrij Nederland. Available at:

https://www.vn.nl/rising-sea-levels-netherlands/ (Accessed: 20 May 2019).

Smith, S. et al. (2014) Foreign Policy: Theories, Actors, Cases. 2nd Editio. New York: Oxford University Press.

Steffen, W. et al. (2011) 'The Anthropocene: conceptual and historical perspectives', Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences. The Royal Society Publishing, 369(1938), pp. 842–867. doi: 10.1098/rsta.2010.0327.

Steffen, W., Richardson, K., et al. (2015) 'Planetary boundaries: Guiding human development on a changing planet', Science, 347(6223), p. 1259855. doi: 10.1126/science.1259855.

Steffen, W., Broadgate, W., et al. (2015) 'The trajectory of the Anthropocene: The great acceleration', Anthropocene Review, 2(1), pp. 81–98. doi: 10.1177/2053019614564785.

Steffen, W. et al. (2018) 'Trajectories of the Earth System in the Anthropocene', Proceedings of the National Academy of Sciences of the United States of America. National Academy of Sciences, 115(33), pp. 8252–8259. doi: 10.1073/pnas.1810141115.

Thompson, A. (2017) '2016 Was the Hottest Year on Record', Scientific American, 18 January. Available at: https://www.scientificamerican.com/article/2016-was-the-hottest-year-on-record/.

Trischler, H. (2016) 'The Anthropocene: Challenge for the History of Science, Technology, and the Environment', NTM Zeitschrift für Geschichte der Wissenschaften, Technik und Medizin, 24(3), pp. 309–335. doi: 10.1007/s00048-016-0146-3.

Trombetta, M. J. (2008) 'Environmental security and climate change: analysing the discourse', Cambridge Review of International Affairs, 21(4), pp. 585–602. doi: 10.1080/09557570802452920.

Union of Concerned Scientists (2016) The US Military on the Front Lines of Rising Seas (2016). Cambridge, MA. Available at: https://www.ucsusa.org/global-warming/science-and-impacts/impacts/sea-level-rise-flooding-us-military-bases#.V5oer_krLb1.

United States Global Change Research Program (2018) Fourth National Climate Assessment Volume II. Washington, D.C. Available at: https://nca2018.globalchange.gov/.

VPRO Tegenlicht (2017) The Anthropocene: The age of mankind. The Netherlands. Available at: https://www.youtube.com/watch?v=AW138ZTKioM.

Walker, B. and Salt, D. (2012) Resilience practice: Building capacity to absorb disturbance and maintain function. Washington, DC: Island Press.

Walker, M. et al. (2009) 'Formal definition and dating of the GSSP (Global Stratotype Section and Point) for the base of the Holocene using the Greenland NGRIP ice core, and selected auxiliary records', Journal of Quaternary Science, 24(1), pp. 3–17. doi: 10.1002/jqs.1227.

Wilkes, W., Dezem, V. and Parkin, B. (2019) Europe's Most Important River Is Running Dry as Glaciers Shrink, Bloomberg. Available at: https://www.bloomberg.com/news/articles/2019-01-18/europe-s-most-important-river-is-running-dry (Accessed: 20 May 2019).

Witschge, L. (2018) Why are coral reefs important, and why are they dying?, Al Jazeera. Available at: https://www.aljazeera.com/indepth/features/coral-reefs-important-dying-180128135520949.html (Accessed: 21 May 2019).

World Glacier Monitoring Service (2019) Latest glacier mass balance data. Available at: https://wgms.ch/latest-glacier-mass-balance-data/ (Accessed: 20 May 2019).

World Wide Fund for Nature (2015) Living Blue Planet Report. Gland. Available at: http://ocean.panda.org/media/Living_Blue_Planet_Report_2015_Final_LR.pdf.

Youngs, R. (2014) Climate Change and European Security. New York: Routledge.

EU-NATO RELATIONS IN THE CONTEXT OF FORESIGHT SCENARIOS DEVELOPMENT

Plamena KARAIVANOVA[1],

Abstract: The current article explores the future of EU-NATO relations through the prism of foresight analysis. The relevance of such an analytic approach as well as the driving factors that it uses to draw certain perspectives for the future are presented. The author pays particular attention to the issues of strategic environment and its influence, further NATO and EU enlargement, burden-sharing and strategic autonomy. Four different foresight analyses, which have elaborated scenarios on the prospects of EU-NATO partnership, are compared in order to draw the most favorable, the most dangerous and the most likely development of EU-NATO cooperation in the short- to medium-term.

Key words: EU-NATO relations, scenarios development, co-operation, driving factors, burden-sharing, strategic autonomy, enlargement.

In an unpredictable world, NATO and the EU need to work even more closely together.
Jens Stoltenberg

Strengthening the European Union defence goes together with strengthening the EU-NATO partnership and cooperation.
Federica Mogherini

---

[1] Plamena Karaivanova is the Head of EU and International Organizations Department within the Defence Policy and Planning Directorate of the Ministry of Defence of the Republic of Bulgaria. She holds master degrees in International Relations and Law from Sofia University and a PhD degree in Private International Law from the Bulgarian Academy of Science. Her studies also include courses and programmes of the Command Academy of the Bundeswher in Hamburg, the Hague Academy of International Law, the NATO College in Rome and the College of Defence Studies in Beijing. Dr Karaivanova's particual research interests are related to Europen and Euroatlantic Dr Karaivanova is the author of numerous articles and a monography dedicated to international relations, international law and international security.

Foresight analysis and scenario development

EU-NATO relations are a topic largely explored by experts, academics and politicians. They are certainly an issue of great interest especially in the last years, when the EU has undertaken significant steps in strengthening its defense capacity and the US has repetitively raised the question of fair burden sharing in NATO. A lot of effort has been put in explaining why the two structures need to cooperate in a complementary manner without duplicating each other. Even more energy has been invested in emphasizing the unprecedented level of interaction that has been achieved recently. Two joint declarations in 2016 and 2018 (Joint Declaration, 2016; Joint Declaration, 2018), seven areas of enhanced cooperation, seventy four specific measures and regular progress reports form the institutional skeleton of this narrative. Practical steps have also been made at all levels in order to fuel the positive trend.

However, the vigorous and insisting way of underlining the achievements in EU-NATO cooperation can barely conceal the long-lasting issues of concern hampering the opportunities to make use of its full potential. One notorious example are the specific positions of Turkey in NATO and Cyprus in the EU resulting from their bilateral disputes, which block the exchange of classified information, the enactment of the Berlin Plus Agreement and other common undertakings, thus leading to the necessity for undesirable duplication of some tasks, capabilities and structures. There are no public indications that solutions to

these issues are pursuantly sought although problems have been existing and well-known for many years now.

The ambivalence between positive trends and existing unresolved issues poses uncertainty over the future of EU-NATO relations. Additional factors also exert influence on them and make it impossible to predict their development by simple linear extrapolation of current tendencies. This is where other methods of analysis could be applied with more efficiency, one of them being the foresight scenario development.

Such an approach is a rather complex and resource consuming endeavour, which can have useful outcomes if executed in a proper way following the stages of a clear methodology[2]. A key element in the pre-foresight phase is to form the core project team, which will perform the analysis, and to recruit as many specialists from different institutions, think-tanks, academia and NGOs in order to ensure the depth and variability of expertise needed. Consequently, it is obvious that the quality and credibility of a foresight analysis depend to a great extent on the interagency interaction of different actors. This specific

[2]One way to define the phases of a foresight analysis could be the following. The Pre-foresight phase includes the setting of objectives, project team and methods of work. During the Recruitment phase additional experts and specialists are sought for the purposes of the project. The Generation phase is characterized by exploration of existing data, its analysis and anticipation of specific developments. In the Action phase analysts outline priorities for the decision-making process. Strategies, technologies and policy instruments are also elaborated in this phase. The Renewal phase as the last one in the process follows the development of success indicators, which are used to check the credibility of the identified trends. See (Georghiu et al, 2008, pp 45-49).

characteristic of the foresight analysis is to be deliberately emphasized in the context of the current conference since centres of excellence are often asked to produce different analytic research and to give recommendations on future courses of action. It is to be reiterated that interagency interaction in science is just as important as in politics, economy and other fields of social life especially when the scientific effort is expected to generate guidance with the purpose to assist a decision-making process.

According to researcher Monika Sus, who was a participant in the Dahrendorf Forum's Project *European Union in the World 2025: Scenarios for EU Relations with its neighbours and strategic partners*, there are three main indicators to measure the value of scenario generation for foreign policy analyses:

First, they widen the perspective to cover a range of unexpected yet plausible outcomes based on various pairings of key drivers; thus scenarios break the assumption that the future will resemble the past and that change is only gradual. Second, scenario methodology facilitates contrarian thinking and undermines the groupthink that often occurs in homogeneous environments; and foreign policy elites of the past have shown that they are not immune to its sometimes fatal consequences. Third, foresight methodology in general and scenario approaches in particular offer a viable tool to bridge the growing gap between academia and policy making (Sus, 2017, p 116).

Driving factors used in the foresight analysis of EU - NATO partnership

Attempts to analyze the future of EU or NATO in the context of foresight scenarios, although made by different researchers with different aims and means, have one thing in common. They all use a selection of key assumptions and driving factors having an impact on them. Scenarios are constructed by exploring the deviations of these factors and their combinations. This of course results in numerous variations and choosing the most valuable scenarios is quite a challenge.

In the most limited case it would be useful for the end-users or the decision-makers to have the most favourable, the most likely and the most dangerous scenario. In a case when the most likely scenario is either the most favourable or the most dangerous, two elaborated options will be the minimum to rely on. Going to the other extreme and presenting too many scenarios would probably lead to overlaps, confusions and inability to effectively support the decision-making process. That is why a candid analysis of all options should be performed and the most representative for certain trends and required courses of engagement should be set out. Even so, it should always be taken into account that a scenario constructed by the use of foresight analysis cannot grasp all aspects of a certain topic and there could always be fluctuations in the real life situation in comparison with what has been previously sketched by the researchers.

Getting back to the driving factors, the influence and pairing of which is decisive for the elaboration of a certain scenario, it should be noted that when analyzing EU's or NATO's perspectives for future development, the set of drivers chosen by different analysts is almost identical.

The drivers of Europe's future as pointed out in the *White Paper on the Future of Europe*, issued by the European Commission in 2017, are: the development of new technologies and their impact on jobs and industry; climate change requiring new economic solutions; protection of borders against illegal migration together with freedom of movement in Europe; security challenges coming from East, Middle East and Africa; negative demographic trends such as ageing and shrinking of population, which pose difficulties to labour force and social welfare; long-term unemployment and high public and private debt; rise of populist and nationalist movements (European Commission, 2017, pp 8-13).

NATO ACT's *Strategic Foresight Analysis 2017 Report* is focused on the characteristics of the security environment that are expected to unfold to 2035 and beyond. The factors are classified in several dimensions: political, human, technology, economics/resources and environment (NATO Allied Command Transformation, 2017, pp 7-9). Each of these dimensions is described by several trends and their implications for NATO are also presented.

Besides the fact that this document is much more detailed than the White Paper, it is evident that it captures either the same or very similar driving factors, which comes to demonstrate that the assessment of future challenges, which will influence the development of NATO and EU is very close. The two EU-NATO Joint Declarations from 2016 and 2018 actually prove this statement (Smith and Gebhard, 2017, p 306). It would be added that this comes as no surprise, because the geographic areas of the two structures considerably overlap due to the fact that twenty two of their member states coincide. Even those member states, which differ, share the same democratic values and are confronted with the same political, social, technological, economic and environmental challenges.

A question rises whether this almost identical set of driving factors affecting the two structures could be applied when investigating the development of the relations **between** them and whether additional or more specific factors could be identified in this realm.

The answer to the first question is positive for several reasons. To begin with, while shaping the development of each structure, these drivers also affect the way they form their policies towards each other. Secondly, it is worth mentioning that one and the same driving factor could produce behaviours in NATO and the EU, which are incoherent and incompatible due to the fact that they are different by nature (NATO is a classic international organization specialized in the field of security and defence while

the EU is an integration community with supranational institutions and policies in various fields only one of them being CSDP[3]). This innate distinction determines difference in their raison d'être as well as the possession of specific functioning procedures and instruments for reaction.

Thirdly, the same driving factors could provoke antagonistic reactions by some of the leading member states in NATO and EU. Each of the two structures has its own centres of gravity. For the Alliance the leading role so far has been played by the United States. For the European Union there have been three leading members – the United Kingdom, France and Germany. The UK has been the strongest proponent of the transatlantic bond in the EU. Now that it is about to leave the Union, the positions of France and Germany, which currently stay very close together, will be more easily upheld. There are views already outspoken that the Common Security and Defence Policy of the European Union will develop in a more ambitious way without the UK. At the same time Churchill's thought that there are no lasting friends and enemies, only lasting interests suggests that the existing Franko-German harmony may not be taken as an absolute stability constant.

Turkey, being the biggest European Ally in NATO, has one of a kind and controversial relations with the European Union. Turkey's position has been an impediment to NATO-EU

[3] Common Security and Defence Policy of the European Union

cooperation for quite a long time. Recent inclinations toward Russia, “free-riding” in Syria and Iraq as well as periodic attempts to extort the EU on the issue of migration make its behavior a factor of consideration.

Although newer member states from Central and Eastern Europe rarely break the consensus of common decisions in NATO and the EU, their perception of the threat coming from East could also be a source of stronger NATO-centric stance in the EU calling for the preservation of the transatlantic bond and opposing the isolationistic voices from the two sides of the Atlantic.

Differences in policies towards the Middle East and North Africa as well as towards Iran may also affect NATO-EU relations. Some signs for that are already visible. The European Union more easily reaches agreement on common positions concerning these regions, which seems impossible for NATO. One could even doubt that this is a symptom of cracking unity in the Alliance. At the same time NATO has a clear and strong position on the INF Treaty, while discussions in the EU did not result in a loudly outspoken statement.

For all these reasons it is clear that factors of the strategic environment – being they internal for either of the two structures (functions, status, members, political trends), external to both of them (states, regions, conflicts, threats outside of EU and NATO) or invoked by globalization (economy, climate, technology, demography) should be analyzed not only when the future of

each of them is explored, but also in the context of their mutual relations.

Additionally, three specificities, which are intertwined with the aforementioned drivers, should be underscored in order to depict the full complexity of NATO-EU affiliations.

Prospects for enlargement

To begin with, this is the issue of further enlargement for both organizations. On the one hand it could bring new states and peculiarities to the puzzle of complicated connections and dependencies already existing. On the other, it might be construed by external actors as an attempt for power redistribution and as a result to provoke internal frictions between members of NATO and EU or by the two structures themselves.

An analysis of Fitch Solutions shows that after accepting Montenegro and extending an invitation to North Macedonia, other expansions of the Alliance on the Balkans are not very likely in the near future. NATO would also be reluctant to integrate Georgia, Ukraine and Moldova, because any such idea could trigger further Russian military action. Finland and Sweden are neutral countries, which have established deep cooperation with the Alliance, but internally there is a limited support for acceding it in addition to the fact that this again would be viewed as a great threat by Russia (Fitch Solutions, 2018).

As for the European Union enlargement perspectives are quite vague as well. The EU's strategy for the Western Balkans does

not entail new members in the short-term despite of the fact that such integration is anticipated upon the fulfillment of certain conditions (European Commission, 2018). The White Paper clearly states that the starting point for each scenario in it until 2025 is that the **twenty seven** Member States move forward together as a Union (European Commission, 2017, p 15), obviously excluding UK and not including any new members.

Burden-sharing

Second issue to be discussed is the problem with burden-sharing of US and European allies for the security of Europe and to what extent it is pivotal for the future of the transatlantic link. Much has been said and written on that issue. The Wales Summit in 2014 set a target for all allies to spend as a minimum 2% of their DGP on defence (NATO, 2014, para 14), but more visible engagement with the effort to reverse the trend of declining military budgets came only after the persistent calls of the United States for a more fair distribution of expenses for European defence and the offensive rhetoric of President Trump during the summits held after the beginning of his term of office in Brussels in 2017 and 2018.[4]

National plans to raise defence spending up to 2 % of GDP were adopted by the allies in 2017 and according to them by 2024-25

[4] The 2% target for defence spending was set as a collective goal in the European Union much earlier that in NATO. Annual reporting on the individual aspirations of the participating Member States is included under the National Implementations Plans on the fulfilment of the PESCO more binding commitments.

eighteen of them will have completed the target. Ten other NATO member states will not have reached the 2% of GDP by 2025 for their defence expenditures although their defence budgets will be increased.

What does it mean in terms of real money? Based on the NATO 2018 defence data, implementation of the 2% norm by all European allies would imply an annual increase of just over $100 billion or almost €90 billion (+35%). Taking into account the available data of the group of ten allies not realizing the 2% norm, the overall annual increase will be almost $70 billion or slightly more than €60 billion. The conclusion is that the total of defence budgets of European NATO-countries will show a significant increase in the period up to 2024 (Zandee, 2018).

For the burden-sharing assessment it is worthwhile looking at what the US is factually spending on its contribution to Europe's defence. All their efforts amount to approximately $100 billion annually. This represents less than 15% of the US defence budget. The US-Europe burden-sharing ratio would be 25-75 % (Zandee, 2018).

The new initiatives of the European Union - the Permanent Structured Cooperation, the European Defence Fund and the Coordinated Annual Review on Defence present another aspect of burden-sharing. They are also a political demonstration of a stronger will to make the first steps towards integration in the field of defence and to do more in that field, partially as a response to US appeals and aggressive Russian behavior and partially due

to an increased internal appetite in the leading EU nations such as France, Germany, Italy and Spain.

The European Commission for the first time included defence-related matters in its work programme with the elaboration of the European Defence Action Plan (European Commission, 2016). The next EU Multiannual Financial Framework (MFF) 2021-2027 envisages €13 billion to be invested in innovative defence capability projects, which will be developed and realized by the defence industry of the European Union member states. The two-fold effect should be strengthening of the European Defence Technological and Industrial Base together with a consolidation of the European defence market as well as delivery of modern defence capabilities for the EU Member States. The multiplication effect of that investment is expected to be five times bigger due to the fact that under the current European Defence Industrial Development Programme 2019-2020 the European Commission co-finances 20% (30% if they are also PESCO projects) of the capability projects and the rest of the expenses are supposed to be covered by the participating member states and their industry (European Parliament, 2018). This ratio is to be kept under EDF for 2021-2027. EDF will also invest in research and development projects, the level of which is currently unsatisfactory and substantially lacking behind in comparison to US and other countries.

Another € 6,5 billion are envisaged in the new MFF in support of the Military Mobility project. They will be invested in the

construction and rehabilitation of dual-use infrastructure from the Trans-European transport network. Additional € 6,5 billion have to be spent by the Member States as the projects will again involve co-financing.

Based on that, a rising trend in EU's defence spending could be traced. At the same time this positive tendency should not be overestimated since most of the new initiatives are at a very early stage of their development and the new MFF is not yet finally approved, which will be done by the newly elected European Parliament. In a mid to long-term perspective a factor of negative influence over defence spending will also be the ageing and shrinking of population. These unfavourable demographic expectations will lead to smaller labour force and bigger social welfare expenses (Zandee, 2018).

EU's strategic autonomy

The third specific problem impacting EU-NATO relations could be defined as a conceptual one. Back in 1998 the Saint Malo Declaration spoke about the need of the European Union to "have the capacity for autonomous action" (Joint Declaration, 1998). At that time British Prime Minister Tony Blair insisted that the newly established CSDP would not compete with NATO and that a European Army would not be created (Howorth, 2018, p 7). The 2016 European Union Global Strategy revived this debate stating:

While NATO exists to defend its members – most of which are European – from external attack, Europeans must be better equipped, trained and organized to contribute decisively to such collective efforts, as well as to act autonomously if and when necessary. (European External Action Service, 2016, p 19)

[…] European security and defence efforts should enable the EU to act autonomously while also contributing to and undertaking actions in cooperation with NATO (European External Action Service, 2016, p 20).

A more credible European defence is essential also for the sake of healthy transatlantic partnership with the United States (European External Action Service, 2016, p 20).

The question what the concept of the strategic autonomy of the European Union should entail was raised again. The new Defence Package of the EU proposed after the official presentation of EUGS had to be accepted as good news by the US. Instead, US officials made comments perceived as critical of European defense. Among the reported concerns were that the EU's efforts could shift attention or divert precious resources away from NATO and exclude non-EU countries. There were also concerns that closer European integration on defense might lead to more protectionism of defense industries in Europe (Brattberg and Fly, 2018).

The reason for these fears was the announcement of the European Defence Industrial Development Programme

(European Parliament, 2018) as a capability window of the European Defence Fund. The strict rules for the participation of third party entities into the projects led to the conclusion that Brussels wished to routinely shut out US and UK companies from a €13 billion defence programme in order to develop the EU's "strategic autonomy" (Barker, 2018).

At the time when these concerns have been rising, French President Macron gave his contribution to the heated debate over the essence of the European strategic autonomy:

We will not protect the Europeans unless we decide to have a true European army. […] We need a Europe which defends itself better alone, without just depending on the United States, in a more sovereign manner (Stone, 2018).

The speech of Macron also hinted that the European Army might be used to protect the Union against the United States, which provoked a couple of insulting tweets on the side of President Trump (Pilkington and Chrisafis, 2018). European Commission President Junker and German Chancellor Merkel gave a shoulder to the French President in this friendly fire over the Atlantic (Rankin, 2018).

As of 2019 it seems that the clarity over the concept of EU's strategic autonomy is not much bigger. There is rarely a ministerial level meeting in NATO or EU, which has no dedicated session on NATO and EU relations. The repetition of same theses by EU High Representative Mogherini and NATO

Secretary General Stoltenberg on how important it is for the two structures to co-operate in a manner of complementarity without duplication became a well-known narrative. Still, the doubts in the US about the real intentions of the European Union have not been rejected. One of the reasons for that is a lack of decision on the rules of third party participation in PESCO projects. It was decided that “third states could exceptionally be invited to participate in individual projects” (Council of EU, 2018), but PESCO nations have not yet agreed on the meaning of this wording. France and Germany believe that third parties should be able to be project participants on the basis of very restrictive rules while a bigger group of nations, led by the Netherlands, has a more liberal position.

Washington's latest shot against the EU's defense plans came in the form of a letter in early May 2019 from Pentagon acquisition chief Ellen Lord and Under Secretary of State for Arms Control and International Security Andrea Thompson. The two complained to EU High Representative Federica Mogherini that draft rules for allowing non-Europeans into the bloc's programs were too restrictive, amounting to a “dramatic reversal of the last three decades of increased integration of the trans-Atlantic defense sector” (Sprenger, 2019).

Which route will the European Union take – that of a strategic autonomy perceived as an ability to act alone when needed and if NATO does not wish to intervene (suggesting division of labour and complementarity) or a strategic autonomy meaning isolation

from the US? This is definitely an issue, which will shape NATO-EU relations in the upcoming years. One thing becomes quite visible when dwelling on the strategic autonomy and that is “the recognition that the real partner of the EU is not so much NATO per se as the US – and that it is with this actor, above all, that EU needs to establish a deep and complementary partnership” (Howorth, 2018, p8). So – it is not only EU’s attitudes that should be analyzed, but US engagement or disengagement with Europe as well.

Role of Leaders

The last remark that would be made in connection with the driving factors influencing EU-NATO cooperation is the one about leadership. Personal qualities, background, reactions, temperament of leaders have always had if not decisive at least substantial effect and significance in politics, which is why the direction of development of EU-NATO or EU-US interaction will also depend on the subjective characteristics and assessments of their leaders.

Several conditions have been outlined by Valerie M. Hudson in her book *Foreign Policy Analysis. Classic and Contemporary Theory* on the personality of the leader and its importance in decision-making. First of all leader characteristics do matter in the regime type although they offer different levels of constraint on leader control of policy. Secondly, it is important to know whether the leader is interested in foreign policy, because if this is not the case - a large measure of authority could be delegated

to subordinates. Thirdly, severe crises are usually handled at the highest levels of government power, and almost by definition top leaders will be involved regardless of their general level of interest in foreign affairs. The fourth contextual variable is the role of leaders in ambiguous or uncertain situations, when their judgement maybe called upon. The level of diplomatic training of the leader should also be explored as a fifth condition. Sixth characteristic is the personal imprint that a leader might have left in policy-making. On the seventh place Valerie Hudson underscores the style of leadership and whether a leader is willing to delegate information processing and decision tasks or prefers to sort them out by him or herself. Last, but not least comes the eighth contextual variable - the behaviour of the leader in group interactions, either small or large (Hudson, 2014, pp 40-41).

It is in this respect advisable to include political anthropologists and psychologists in the foresight analysis project teams.

Various Scenarios on the Future of EU-NATO Relations

As it was already commented, a trustworthy foresight analysis is rarely in the capacity of a single researcher. For this reason, the last part of the current article will present the results of several analyses performed by different authors and teams and the scenarios that they have suggested for the future of the transatlantic link and EU-NATO relations.

The aforementioned Dahrendorf Forum's project performed in 2016 identified the mainstream scenario, the downside risk scenario, the opportunity scenario and the emerging trend scenario. Indicators to help gauge the unfolding of each scenario as well as its implications were described together with its drivers, characteristics and chronology (Sus and Pfeifer, 2016, pp 3-4). The first two scenarios present an interdependency showing that if EU is strong in the defence field, NATO weakens and vice versa. They step on the understanding that the protection of Europe would be taken by either of the two actors, which would cooperate, but still one of them will perform the leading part. The other two scenarios are more worrying as they depict rivalry and isolation. According to Dahrendorf's Forum analysis there is no option in which NATO and EU maintain balanced dialogue and cooperation.

A year after the Dahrendorf foresight analysis was presented, the European Commission came up with its *White Paper on the Future of Europe* including five scenarios for Europe by 2025 (European Commission, 2017a)q each of them analyzing options for European defence. They were further analysed in the *Reflection Paper on the Future of European Defence* presented by the European Commission three months after the White Paper (European Commission, 2017b).

In contrast to the Dahrendorf Forum's predictions, which are more or less diverse and constitute different alternatives on the basis of different predominating trends, the scenarios of the

European Commission present stages of one and the same upward trend. The first option is the status quo and according to the second and third scenario from the Reflection Paper it could only improve. The White Paper though, suggests that a certain regress is possible if the only aim of the European Union is to keep and deepen the single market while abandoning integration processes in other policies. This alternative could be defined as a “status quo minus” option.

All in all the European Commission presents a positive future about EU’s development since most of the scenarios either describe the current state of affairs or rely on deepening of the integration process. In the second case it is only the tempo and timeframe of the expected change that is unknown, because if the EU wishes to proceed with integration, a moment would come when it would also encompass foreign and security policy. As for the relations with NATO, it is evident that the Union is hesitant to formulate an option for being a leader and dictating the shape of this partnership. Although cooperation is supposed to get more intense, there is no scenario that NATO would gradually become obsolete and EU would take full care and responsibility of European security and defence. At least not in the perspectives outlined by the European Commission up to 2025. The higher the ambition to develop and integrate European defence capabilitites, the more balanced the relationship with NATO according to the Reflection Paper.

In order to be able to compare different foresight analyses, two more of them will be presented here. They were performed in 2018 by researchers Jolyon Howorth and Hans Binnendijk. The two of them working independently have each drawn three scenarios of EU-NATO partnership.

Their first option could be defined as a US or NATO-led dominance based on the current status or a trend of declining cohesion in CSDP.(Howorth, 2016, p 14) A second scenario described by Howorth is one, in which significant, yet limited progress is made via the implementation of the new defence initiatives in the EU. In this case a serious step would be made beyond the status quo, but would still leave the EU as a subordinate security entity to NATO (Howorth, 2018, p 14). A more balanced relationship between NATO and EU according to Binnendijk's second scenario could happen under the condition that EU maintains its political cohesion and becomes more self-sufficient in defence (Binnendijk, 2018, p 4).

The third scenario of the two researchers draws quite a different picture based on one and the same presumption – a withdrawal of the US from European security. Howorth's scenario is for a Europeanized-NATO (Howorth, 2018, p 15). The analysis of Binnendijk considers a US withdrawal from NATO in combination with a loss of cohesion in the EU as an erosion of the transatlantic consensus and institutions that would mostly serve Russian President Putin's efforts to divide the transatlantic partners and

promote authoritarian populism in Europe (Binnendijk, 2018, p 4).

Conclusion

The reasonable question at the end of this research paper is which the most likely, the most favourable and the most dangerous options are. Based on the comparison of all four foresight analyses, the following conclusions on the future of EU-NATO partnership could be drawn.

The first one is that a very slight step back of the US from European defence might be a motive for consolidation of EU efforts in CSDP, which could result in a more balanced and just EU-US relationship and a stronger transatlantic bond. This would require maintaining the trust between the transatlantic allies, increase in defence spending by European Union members, continued US support to deter Russia and stronger CSDP with fair third party involvement in the new defence initiatives of the European Union. Such a development would probably constitute the best scenario for NATO and EU.

If on the contrary both the US and the EU continue to ride the wave of populist, nationalist and even isolationist ideologies, this would ruin both the EU as an integration community and NATO as a transatlantic Alliance. Before their final deconstruction there might be a stage of rivalry instead of cooperation, which would additionally increase the gap between them. This could be determined as the worst-case alternative.

There are two more distinctive options in-between the worst and the best cases. The first one is a definite loss of interest of US in NATO affairs and European defence and gradual emergence of a very strong and solid European Union at the same time, which could turn the Alliance into a rudimentary structure especially if the US and the EU begin to dramatically talk at cross-purposes when it comes to policies, goals and values.

The second one is a solid engagement of the US with NATO and a European Union, which is more focused on other than security and defence policies. This option resembles very much the state of affairs before the presentation of the new Global Strategy of the European Union and is probably closest to current situation with a new Defence Package of the European Union, which has been already introduced, but has not yet produced tangible results in terms of defence investment and cooperation.

Still, if the promises on defence spending are to be kept and the new defence initiatives of EU become workable and effective as the political will clearly demonstrates, the European pillar of NATO would be strengthened in the years to come and the relations between the EU and NATO would be categorized as more intensive and more fair. The most likely scenario in this respect is that in the short to medium term the attempts to near the distance between EU and NATO will continue, because the ambition of the EU to be strategically autonomous would not yet correspond to its real capacities to defend itself alone, if needed. In parallel to this, the US cannot afford to lose allies in

a world of high competition with rising powers such as China and aggressive rivals such as Russia. As a result, despite of the differences and the harsh rhetoric, both sides of the Atlantic would be much more interested to keep the bond rather than destroy it.

Bibliography

Barker, A. (2018) Brussels Plans to Block US and UK Groups from Defence Programme, Financial Times, June 13th 2018. Available at: https://www.ft.com/content/ec7728a4-6e85-11e8-852d-d8b934ff5ffa [Accessed: May 17th 2019]

Binnendijk, H. (2018) Between Continuity and Erosion: Three Scenarios for the Future of Transatlantic relations, College of Europe Policy Brief #7.18. Brussels: College of Europe

Brattberg, A.; Fly, J. (2018) Two Cheers for European Defence Cooperation, Foreign Policy, March 9th 2018. Available at: https://foreignpolicy.com/2018/03/09/two-cheers-for-european-defense-cooperation/ [Accessed: May 16th 2019]

Council of EU (2018) Council decision establishing a common set of governance rules for PESCO projects, Luxembourg: Foreign Affairs Council Meeting, June 25th 2018. Available at: https://www.consilium.europa.eu/media/35786/council-decision-pesco-projects.pdf [Accessed: May 17th 2019]

European Commission (2016) Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. European Defence Action Plan, Brussels: European Commission. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0950&from=EN [Accessed: June 3rd 2019]

European Commission (2017a) White Paper on the Future of Europe. Reflections and Scenario for the EU27 by 2025, Brussels: European Commission. Available from: https://ec.europa.eu/commission/future-europe/white-paper-future-europe_en [Accessed: May15th 2019]

European Commission (2017b) Reflection Paper on the Future of European Defence, Brussels: European Commission. Available from: https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_en.pdf [Accessed: May 27th 2019]

European Commission (2018) Communication from the Commission to the European Parliament, the Council, the European Council. The Economic and Social Committee and the Committee of the Regions. A credible enlargement perspective for an enhanced EU engagement with the Western Balkans, Strasbourg: European Commission. Available from: https://ec.europa.eu/commission/sites/beta-

political/files/communication-credible-enlargement-perspective-western-balkans_en.pdf [Accessed: May 16th 2019]

European External Action Service (2016) Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy, Brussels: EEAS

European Parliament (2018) Regulation (EU) 2018/1092 of the European Parliament and of the Council of 18 July 2018 establishing the European Defence Industrial Development Programme aiming at supporting the competitiveness and innovation capacity of the Union's defence industry, OJ L 200 of 7.8.2018, Brussels: European Parliament and Council. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1092 [Accessed: June 3rd 2019]

Fitch Solutions (2018) The Future of NATO: Four Scenarios for the Coming Decade. Available at: https://www.fitchsolutions.com/country-risk-sovereigns/future-nato-four-scenarios-coming-decade-02-08-2018 [Accessed: May 16th 2019]

Georghiu, L.; Cassingena Harper, J.; Keenan, M.; Miles, I.; Popper, R. (eds) (2008) The Handbook of Technology Foresight: Concepts and Practice, Cheltenham, UK; Massachusettes, USA: Edward Elgar Publishing

Howorth, J. (2018) EU-NATO Cooperation and Strategic Autonomy: Logical Contradiction or Ariadne's Thread? Kolleg-Forshergruppe. The Transformative Power of Europe Series, № 90, Berlin: Freie Universität Berlin

Hudson, V. (2014) Foreign Policy Analysis. Classic and Contemporary Theory, Lanham, Boulder, New York, Toronto, Plymouth, UK: Rowman & Littlefield

Joint Declaration (1998) Joint Declaration on European Defence, issued at the British-French Summit (Saint-Malo, 4 December 1998) Available at: https://www.cvce.eu/content/publication/2008/3/31/f3cd16fb-fc37-4d52-936f-c8e9bc80f24f/publishable_en.pdf [Accessed: May 17th 2019]

Joint Declaration (2016) Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization (Warsaw, July 8th 2016). Available at: https://www.nato.int/cps/en/natohq/official_texts_133163.htm [Accessed: June 3rd 2019]

Joint Declaration (2018) Joint Declaration on EU-NATO Cooperation by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization (Brussels, July 10th 2018). Available at: https://www.nato.int/cps/en/natohq/official_texts_156626.htm [Accessed: June 3rd 2019]

NATO Allied Command Transformation (2017) Strategic Foresight Analysis 2017 Report, Norfolk: Allied Command Transformation. Available from https://www.act.nato.int/images/stories/media/doclibrary/171004_sfa_2017_report_hr.pdf [Accessed: May 15th 2019]

NATO (2014) Wales Summit Declaration. Brussels: NATO. Available from: https://www.nato.int/cps/en/natohq/official_texts_112964.htm [Accessed: May 16th 2019]

Pilkington, E.; Chrisafis, A. (2018)Trump Ramps up Macron Spat by Mocking France in World Wars, The Guardian, Nov 13th 2018. Available at https://www.theguardian.com/us-news/2018/nov/13/trump-macron-eu-army-german-second-world-war [Accessed: May 17th 2019]

Rankin, J. (2018) Merkel Joins Macron in Calling for a 'Real, true European Army', The Guardian, Nov 13th 2018. Available at: https://www.theguardian.com/world/2018/nov/13/merkel-joins-macron-in-calling-for-a-real-true-european-army [Accessed: May 17th 2019]

Smith, S.J.; Gebhard, C. (2017) EU-NATO Relations: Running on the Fumes of Informed Deconfliction, European Security, Vol.26, (№ 3), p 303-314

Sprenger, S. (2019) European Union Rejects US Claims to Internal Defense Coffers, Defence News, May 17th 2019. Available at: https://www.defensenews.com/global/europe/2019/05/16/european-union-rejects-us-claims-to-internal-defense-coffers/?fbclid=IwAR3gQZEKPyLGxjixBeTEL7lJZOO4TCYO_hzgqDYP6HT3wXq4tToicjnuCH4#.XN7r7fXIlgE.facebook [Accessed: May 22 2019]

Stone, J. (2018) Emmanuel Macron Calls for Creation of a "True European Army", Independent, Nov 6th, 2018. Available at: https://www.independent.co.uk/news/world/europe/emmanuel-macron-european-army-france-russia-us-military-defence-eu-a8619721.html [Accessed: May 17th 2019]

Sus, M. (2017) Towards the European Union's Foreign Policy 2025 – Taking Stock of the Dahrendorf Foresight Project, Global Policy, Vol. 8, (Supplement 4), p 115-125

Sus, M.; Pfeifer, F. (eds) (2016) European Union in the World 2025. Scenarios for EU relations with its neighbours and strategic partners, Hertie School of Governance and LSE Ideas: Dahrendorf Analysis

Zandee, D. (2018) The Future of NATO. Fog over the Atlantic? Hague: Clingendael. Available at: https://www.clingendael.org/pub/2018/strategic-monitor-2018-2019the-future-of-nato [Accessed: May 16th 2019]

NATO-EU COOPERATION IN CRISIS MANAGEMENT: CURRENT STATE OF AFFAIRS

Aglika ATANASOVA[1]*,*
CMDR COE

Abstract: This paper is aimed at providing a well-informed overview of the current state of affairs of NATO-EU cooperation in crisis management based on in-depth analysis of the most recent developments in the field. Firstly, the paper tracks the evolution of the partnership and identifies the key factors which led to the existing cooperation framework. After that it focuses on the most recent dynamics resulting from the two NATO-EU Joint Declarations signed in Warsaw (2016) and Brussels (2018) by the President of the European Council and the President of the European Commission, together with the Secretary General of the North Atlantic Treaty Organization as well as the common set of 74 proposals endorsed by the two partners and the four progress reports on the implementation of the common proposals. The main research interest of the paper is to examine and explain how the intended new level of ambition of the Euro-Atlantic strategic partnership declared in 2016 in Warsaw and reaffirmed in 2018 in Brussels is being translated in practical terms. The methodology used in this paper combines analysis of the above-mentioned set of written sources and a round of interviews conducted with both CSDP and NATO practitioners. Furthermore, in-depth research of the existing academic literature adds a more critical dimension to the analysis. Last, but by no means least, the paper identifies concrete constraints and uncertainties within the cooperation framework which remain unsolved and hence hinder further optimization of the relations.

[1] Ms. Atanasova has a background in Political Science from Sofia University "St. Kliment Ohridski" and International relations and European Studies from the Central European University in Budapest, Hungary. She was a part of the Bulgarian Presidency of the Council of the EU coordination team at the Bulgarian Ministry of Defense.

Key words: EU-NATO cooperation, EU-NATO strategic partnership, crisis management, security, defense

Introduction

Cooperation between the EU and NATO takes place on a daily basis within the framework of a long-sustained strategic partnership based on common values. The two partners share common interests and face strongly interconnected global risks in the context of a complex and unpredictable security environment. The double membership of 22 EU Member States who are also NATO Allies adds significantly to the level of interconnectedness between the EU and NATO. In addition to the high level of interconnectedness, the common will for deepening cooperation expressed in Warsaw (2016) and reaffirmed in Brussels (2018), make the cooperation framework a matter of utmost importance. However, the lack of a common agreement on a specific division of labor which takes into consideration the different nature of the two partners as international entities continues to hinder further progress toward a new level of ambition:

"(…) we have to step-up our efforts: we need new ways of working together and a new level of ambition;"

The common set of proposals endorsed by the EU and NATO is designed for the purpose of intensifying joint efforts in order to deliver on the common will to deepen cooperation and reach a new level of ambition expressed through the two joint

declarations. Altogether 74 concrete actions covering seven policy areas are under implementation. This paper was written in parallel with the release of the fourth progress report on the implementation of the common set of proposals. The paper examines in detail the impact of the implementation of the common set of proposals on the existing coordination mechanisms in the field of crisis management. Furthermore, it maintains the argument that addressing the shortfalls of the current cooperation framework will bring crucial added value to the joint efforts to increase interoperability and achieve synergies through intensified coordination at all levels engaged in the crisis management process.

In order to provide a good understanding of the interaction channels through which the EU and NATO representatives cooperate with each other on a daily basis, interviews with practitioners from both organizations were carried out. The interviews add a more practical perspective on the cooperation framework in addition to the analysis of the above-mentioned written sources such as the joint declarations and progress reports. And last, but certainly not least, the used methodology results in outlining the specific constraints of the cooperation framework which remain unresolved despite the intent of the two declarations to step-up joint efforts. Again, the paper argues that leaving these constraints unresolved hinders the attempts to make a decisive step toward greater efficiency in addressing common threats together because as the first of the four progress

reports on the implementation of the common set of proposals clearly states:

“Cooperation between the two organizations is essential. In the current strategic environment, EU and NATO are faced with unprecedented challenges: neither organization has the full range of tools to address these security challenges on its own”.

The key element of the above-mentioned statement from the first progress report related to the full range of capabilities for addressing common threats draws the attention to the pressing need for a common understanding of the capabilities limitations that both of the partners are facing. These limitations are directly linked to the different nature of the two partners which imposes the need for a common agreement on specific division of tasks in the field of crisis management. Such a common understanding is a crucial point of departure in intensifying cooperation and optimizing the efficiency of coordination mechanisms. However, before expanding on these interesting aspects of the Trans-Atlantic strategic partnership in greater detail, I would like to briefly discuss the main developments which paved the way towards the current state of affairs of NATO-EU cooperation in crisis management.

Partnership development

This part of the paper suggests a concise overview of the key developments in the field of crisis management cooperation between the EU and NATO, which led to the current state of

affairs. To begin with, before the Common Security and Defense Policy of the EU (CSDP) came to being, the Petersberg tasks defined the spectrum of actions that the EU can undertake in Crisis management operations. The Petersberg tasks were initially agreed on within the framework of the Western European Union. The initial list of tasks enshrined in the 1997 Treaty of Amsterdam was expanded with the Lisbon treaty. This list includes: humanitarian and rescue tasks; conflict prevention and peace-keeping tasks; tasks of combat forces in crisis-management, including peacemaking; joint disarmament operations; military advice and assistance tasks; post-conflict stabilization tasks;.

However, a plethora of factors mainly related to the inability of the EU to take autonomous action in response to the severe crisis in former Yugoslavia led to a common declaration signed by the political leaders of France and the UK in 1998 in Saint-Malo. The Franco-British declaration signed on 4 December 1998 committed the two member states to developing EU defense capabilities for enabling the Union to undertake autonomous action in response to crises. The Franco-British Joint Declaration gave impetus to the creation of a European Security and Defence Policy within the wider framework of the Common Foreign and Security Policy of the EU. The Common Security and Defense Policy (CSDP) of the EU became the political framework for developing EU defence capabilities for crisis management operations.

The agreement between France and the UK which led to the creation of CSDP laid the foundations for developing the current cooperation framework. According to a report of the International Centre for Defense and Security, CSDP was conceived as "recognition that many of the security challenges facing Europe were in the area of "crisis management": how to prevent conflict, how to build economically sound states with good governance and democracy, and how to maintain peace post-conflict."[2] In parallel with the creation of CSDP, the EU invested additional efforts in supporting the political framework with an institutional one by creating the post of "High Representative for Common Foreign and Security Policy" which raised significantly the profile of its Common Foreign and Security Policy (CFSP). The Political and Security Committee (PSC), the EU Military Committee (EUMC) and the EU Military Staff (EUMS) were also created in support of the political framework.

Nevertheless, the lack of crucial capabilities at EU level remained a key impediment for undertaking autonomous action in crisis management operations. The EU tried to address this unresolved issue through the 2003 Berlin Plus Agreement - a comprehensive package of agreements made between the EU and NATO, which allows the EU to draw on NATO assets and capabilities for carrying out EU-led crisis management

[2] Raik, Kristi and Järvenpää, Pauli, 2017. 'How to Make the Best of a Marriage of Necessity?'. ICDS Reports. Available at: https://icds.ee/wp-content/uploads/2018/ICDS_Report_A_New_Era_of_EU-NATO.pdf

operations. The Agreement provided the initial framework for NATO-EU cooperation after the creation of CSDP. Also, the Berlin Plus agreement enabled the Alliance to support EU-led operations when the NATO as a whole did not want to intervene itself.

In principle, under Berlin Plus if NATO decides not to intervene, the EU can undertake action and be guaranteed access to NATO headquarters. In that case the NATO Deputy Supreme Allied Commander (DSACEUR) takes over the role of operational commander of such an EU-led operation. However, there is one specific constraint related to EU-led operations under Berlin Plus, which I identified as particularly problematic from the perspective of crisis management operations. I am referring to the fact that the Berlin-Plus arrangements do not provide for the cooperation between the two partners on the ground when they are both present in the same theatre of operations. The potential occurrence of such a scenario imposes the need for establishing such cooperation on the ground through informal channels for staff-to-staff interaction following a predominant logic on non-duplication rather than complementarity. The lack of specific cooperation guidelines results in informal interactions established out of necessity rather than striving for complementarity through coordinated joint efforts.

In parallel with the Berlin-Plus agreement there are a few other important elements which need to be considered when analyzing the development of the partnership such as the establishment of

the NATO-EU capability group (launched in 2003), the reciprocal institutionalization of the presence of the EU in the headquarters of the Alliance by establishing the European Union Cell at SHAPE (EUCS) and respectively the NATO Permanent Liaison Team (NPLT) at the European Military Staff (EUMS).

Current state of affairs

Before embarking on the analysis of the current state of cooperation in greater detail, it is important to highlight the significant progress achieved through the implementation of the common set of proposals. The implementation reports account for the progress in seven policy areas: countering hybrid threats; operational cooperation including at sea and on migration; cyber security and defence; defence capabilities; defence industry and research; exercises; supporting Eastern and Southern partners' capacity-building efforts. It is clearly stated in the very first progress report that:

"*The key impact of the common set of proposals and their implementation is that cooperation between the two organizations is now becoming the established norm, a daily practice, fully corresponding to the new level of ambition referred to in the Joint Declaration*".

This statement leaves no doubt that the two partners have made a decisive step beyond a predominant logic of cooperation based on non-duplication. Moreover, the report states that:

"*Activities of the two organizations are complementary to each other*".

However, this paper is intended to go beyond the strict wording of the reports and translate these statements in practical terms by juxtaposing them to the observations made by EU and NATO practitioners throughout the interviews. I also carried out in-depth research based on the existing academic literature on this topic which added a more critical perspective to the analysis. The main conclusion based on the interviews is that interactions between the EU and NATO are still taking place on informal staff-to-staff level. This conclusion is based not only on the interviews which I carried myself; it is also supported by specific papers of representatives of the academia who had the rare opportunity to conduct rounds of interviews with a sample of high level practitioners on both ends of the partnership.[3] Furthermore, in addition to this conclusion based on the interviews particular practical constraints related to cooperation at strategic level were attributed to the tensions between Turkey and Cyprus which resulted in concrete inter-institutional blockages.

For instance, since Cyprus joined the EU, the country invested continuous efforts in actively blocking any attempt of Turkey to play a more active role in CSDP-related activities. The problematic relationship also had a negative effect on EU-Turkey accession negotiations, and resulted in the practical impossibility

[3] Ibid

for Turkey to take part in EU-led missions as well as in blocking Turkey's membership in the European Defence Agency (EDA). In return, Turkey blocked participation of Cyprus at formal EU-NATO meetings between the North Atlantic Council and the PSC which impeded practical coordination progress at this level of cooperation.[4] However, the most significant negative impact of the Turkey-Cyprus issue on the practical cooperation between the EU and NATO relates to the fact that the conflict de facto undermines the efficiency of the Berlin Plus framework making it irrelevant to the practical challenges to cooperation. In the following paragraph, allow me to support this argument with concrete examples.

To begin with, in principle, based on the provisions of the Berlin Plus arrangements if the EU wants to launch an operation under Berlin Plus, the Union should be guaranteed access unless NATO decides to intervene itself. However, under Berlin Plus the EU runs the risk of being denied access due to the possibility for a non-EU NATO Ally to veto the decision of guaranteeing access to NATO headquarters. The mission in Libya is a concrete example which decisively undermines any doubts about the probability of such a scenario. Amid all the uncertainties accompanying the initiation of this mission there was one particular EU member state that repeatedly insisted on conducting the mission under the flag of the EU. However, despite of this bold attempt to initiate an EU-led mission in Libya,

[4] Ibid

a decision to launch a NATO-led operation in the North-African country was finally taken instead.

However, the idea of launching a NATO-led military intervention in Libya was not unanimously endorsed by all the actors who had a say in the decision making process which is again a direct consequence from the complexities related to the non-EU NATO Ally status of Turkey. In other words, carrying out a military intervention under the flag of NATO was constrained by the reluctance of Turkey to support an operation in the North-African country which only added to the already complicated situation. In summary, this is a concrete illustrative example of a scenario in which the reluctance of a non-EU NATO Ally to support a military intervention initiated by the EU prevents the EU from the possibility to undertake autonomous action under Berlin Plus. Such a scenario explains very well in practice the rationale behind EU's motivation to invest efforts in developing its own capabilities for autonomous action.

After examining the scenario of a non-EU NATO Ally being reluctant to a military intervention initiated by the EU, allow me to draw the attention to another major constraint related to the fact that the Berlin-Plus agreements do not provide for the cooperation between the two partners on the ground when they are both present in the same theatre of operations. Here, again allow me to introduce a concrete example which illustrates the probability of such a scenario to occur in reality. The situation in Afghanistan where both the EU and NATO had police training

missions in the country shows very well the implications of the lack of mutually agreed guidelines for cooperation on the ground. This gap imposes the necessity of establishing such cooperation on the ground through informal channels on an ad hoc basis.

In summary, these concrete examples illustrate very well the irrelevance and the obsolete character of the Berlin Plus agreement as the principal framework defining the scope of EU-NATO cooperation in crisis management. In addition to these practical examples, it is also important to highlight the fact that only two operations have been carried out under Berlin Plus since the agreement was concluded: Operation Concordia conducted in Republic of North Macedonia, launched in March 2003 and terminated in September 2003 as well as the only ongoing operation under Berlin Plus which is Operation Althea in Bosnia and Herzegovina (launched since 2004).

But how are these concrete shortfalls of the Berlin Plus Agreement related to the current state of affairs? To begin with, the recent developments in the field of NATO-EU cooperation do not solve the issue of the possibility for non-dual members to influence the decision making process for initiating an EU-led operation under Berlin Plus. Then, it is just as important to note that the joint declarations from Warsaw and Brussels also do not address the possibility for the two partners to be present simultaneously in the same theater of operations and the respective need to establish cooperation on the field at the

operational and tactical level through informal channels on an ad hoc basis due to the lack of existing pre-defined guidelines.

Furthermore, I argue that the joint efforts to raise the degree of coherence and interoperability between NATO and the EU can only be based on a joint threat analysis backed by common exercises and joint-planning activities. However, although it is true that great progress has been made in this direction through the 74 proposals, there is still one last major constraint I would like to highlight. This constraint is related to the different nature of the two partners. And here, I would like to refer to an excellent article written by Sven Biscop[5] in which the author elaborates on the relationship between the different nature of NATO and the EU and the optimization of NATO-EU relations. Biscop regards NATO as an instrument and the EU as an actor[6]. The different character and logic of the two pre-supposes a specific division of labor on which the two partners can agree. However, if we look beyond the different nature of the two organizations, the lack of a common understanding of the need of a specific division of labor and the political constraints related to non-dual members, the lack of crucial strategic enablers in the field of crisis management on behalf of the EU remains a matter of utmost importance. This matter is directly linked to the debate on EU strategic autonomy embedded in the European Union Global

[5] Biscop, S., 2018. 'EU-NATO relations: A long-term perspective.' IDN, NAÇÃO E DEFESA, Special issue n.150.
[6] Ibid

Strategy (EUGS). It is also related to the ongoing debate about trans-Atlantic burden sharing.

Therefore, a good understanding of capability limitations that both of the partners are facing is also crucial especially in the context of the discussion about optimizing EU-NATO cooperation particularly in the field of crisis management. As it was previously discussed, the constraints to optimizing the cooperation framework can be divided in two main categories – constraints related to non-dual members and constraints related to dual members. Since the constraints related to non-dual members were already examined in detail, allow me to elaborate on the constraints related to dual members from a capabilities perspective. Here I would like to point out that despite of the significant progress made by the European Defense Agency (EDA) in coordinating national defense planning efforts, a significant gap between different national defense spending plans is still in place. This gap results in individual dual members investing in small scale capabilities of limited deployability on a national level which undermines cost-effectiveness.

In summary, the lack of crucial strategic enablers at the level of the EU attributed to significant capability gaps is aggravated by concerns over the current relevance of the Berlin Plus Agreement raised by the fact that at the moment there is only one ongoing EU-led operation under Berlin Plus - the operation Althea in Bosnia and Herzegovina. To conclude, undoubtedly significant progress is made with the most recent developments related to

crisis management cooperation. However, a plethora of gaps related to capabilities, interaction channels and coordination mechanisms on all levels of the cooperation framework remain to be addressed.

Conclusion

To conclude on a positive note, allow me to reiterate again my observations regarding the considerable progress made toward optimizing the EU-NATO cooperation framework through the most recent developments undertaken at the highest political and military level through the joint declarations and the common set of proposals. Nevertheless, concrete constraints still remain to be addressed. Especially in the context of a highly dynamic and complex strategic environment – an environment in which neither of the two partners has the full range of civil-military capabilities to address the unprecedented challenges individually. Furthermore, according to interviews with both EU and NATO practitioners, ad hoc interactions carried out through informal channels on a staff-to-staff level raise concerns over the lack of a common understanding on a specific division of labor based on the different nature of the EU and NATO as organizations. The lack of a common agreement imposes the need to establish such a division informally and out of necessity directly on the ground instead of following concrete pre-defined guidelines. Such an informal approach severely can be attributed to a predominant logic of non-duplication rather than complementarity. Furthermore, the lack of a common agreement on how and when

a division could be applied in practice also adds to the general frustration expressed by practitioners.

This general frustration relates to a large extent to the acute need for conceptual rapprochement which can mainly be achieved through intensified education and training and joint planning activities. A high-level EU representative recently touched on that topic referring to one of the 74 concrete proposals which is related namely to the closer interaction between NATO and EU Centres of Excellence. Such closer interaction can bring important added value in achieving conceptual rapprochement and reaching a practical agreement on a clear division of labor between NATO and the EU in crisis management. In this regard, the Crisis Management and Disaster Response NATO Centre of Excellence is placed in an excellent position for bridging the conceptual gaps between the EU and NATO in the field of crisis management through education and training activities and by providing a common platform for discussion between practitioners on both ends of the partnership and academia.

To conclude, based on my analysis, I argue that a common agreement on a specific division of labor in crisis management will result in optimizing the cooperation framework and maximizing the joint impact through synergies when the two partners act together on their common strategic interests (when these interests coincide) in addressing common security threats identified through joint-threat analysis. In any case, a concrete approach toward increasing coherence and interoperability

between the EU and NATO based on a common agreement on the division of labor in crisis management can only be developed through rational, in-depth policy analysis leading to concrete policy recommendations aimed at reaching concrete solutions. Such a common agreement requires a well-informed debate across all strata involved in EU-NATO crisis management. Practitioners on both ends of the partnership can play major role and contribute significantly by engaging actively in various discussion platforms aimed at finding practical solutions for optimizing the current cooperation framework.

Last, but by no means least, a good analysis of the existing cooperation framework cannot be complete without a well-informed strategic foresight based on the examination of different scenarios and their potential implications on EU-NATO cooperation. Optimizing the cooperation framework can only be relevant from the perspective of a shared vision of the common strategic interest the two partners want to act upon in the future. Therefore, exploring foresight scenarios for the future of EU-NATO relations is another matter of utmost importance that Ms. Karaivanova-Koburova, PhD, examines in great detail in the following article.

Bibliography

Aghniashvili, T., 2016. Towards More Effective Cooperation? The Role of States in Shaping NATO-EU Interaction and Cooperation. Connections 15, no. 4 Available at: http://www.jstor.org/stable/26326460 .

Howorth, J., 2017. Strategic Autonomy and EU-NATO Cooperation: Squaring the Circle. Security Policy Brief nº85. Brussels: Egmont. http://www.egmontinstitute.be/content/uploads/2017/05/SPB85.pdf?type=pdf .

Howorth, J., 2018. EU-NATO Cooperation and Strategic Autonomy: Logical Contradiction or Ariadne's Thread? KFG Working Paper No. 90 | August 2018.

Raik, Kristi and Järvenpää, Pauli, 2017. 'How to Make the Best of a Marriage of Necessity?'. ICDS Reports. Available at: https://icds.ee/wp-content/uploads/2018/ICDS_Report_A_New_Era_of_EU-NATO.pdf

Biscop, S., 2018. 'EU-NATO relations: A long-term perspective.' IDN, NAÇÃO E DEFESA, Special issue n.150.

Stavridis, JAMES G., 2011. 'The Comprehensive Approach in Afghanistan.' PRISM 2, no. 2 Available at: https://www.jstor.org/stable/26469113 .

Lachmann, N., 2010. NATO-CSDP-EU relations: Sketching the map of a community of practice. CEPSI, University of Montreal, FALL.

'European Union Concept for Military Planning at the Political and Strategic Level', Council doc. 10687/08.8. Available at: http://data.consilium.europa.eu/doc/document/ST-5008-2015-INIT/en/pdf .

Kriendler, J., 2004. NATO crisis management: Cooperation with PfP partners and other International Organizations. Connections, 3(4), pp.59-68.

Smith, S., 2014. The European Union and NATO Beyond Berlin Plus: the institutionalisation of informal cooperation (Doctoral dissertation, Loughborough University).

COLLABORATIVE INTERACTION – IMPLICATIONS ON SECURITY

Tarik NDIFI,
OSCE

Abstract: In the OSCE's understanding, security in Europe can only be achieved, maintained or restored if the interests of all concerned states are taken into account. The Organisation has been closely cooperating with other international actors from its onset in the 1990s, which includes cooperation between the OSCE's field operations and other international actors in the respective country. Such cooperation is seen on the policy and on the working level, such as with the European Union, the Council of Europe, UN agencies, or NATO. The OSCE's comprehensive approach to security adds to this since security is understood to touch not only on political-military aspects, but also on security in the economic, the environmental, and the human dimension. This broad approach, in addition to the need to seek synergies and to closely co-operate with other international actors, helps to work in a complementary way that allows all sides to make the best use of each organisation's capabilities and capacities. Co-operation is hence seen as a necessity to achieve an efficient implementation of mandated activities in the OSCE's work. One of the areas where this request for cooperation and synergies can be found in OSCE documents is the area of peacekeeping mission, which the OSCE might potentially deploy or contribute to.

Key words: collaboration, interaction, OSCE, European Union, Council of Europe, United Nations, NATO

The OSCE as platform for international dialogue

The Organisation for Security and Co-operation in Europe (OSCE) puts emphasis on establishing and providing a "Platform for Co-operative Security", as it was called in 1999.[1] To understand the organisation's reasoning about security, one

[1] OSCE (1999)

needs to go back in time a little bit and see the later developments in light of a changing security architecture in Europe which evolved since. Otherwise, the working structures and the opportunity this unique organisation provides would not be fully caught and the potential for cooperation with other international actors might be lost.

In the organisation's understanding, security can only be achieved and maintained if all states that participate in the former "Conference for security and Co-operation in Europe" – hence their name "participating States" (pS) – have insurances that their security concerns are taken note of by the other states and, where deemed necessary, that each state has the opportunity to explain and discuss these issues in a forum where voices are heard equally and without prejudice to the economic or political power the state enjoys otherwise.

The so-called "comprehensive approach to security", as adopted by the OSCE in 1996[2], stipulates that security is not limited to political or military confrontation and consultations, but that it includes other thematic baskets, which the states agreed to form the basis for the OSCE's security understanding. Those are the economic and environmental, and the human dimension of security, which are in an OSCE context called the second and third dimension of security.

[2] OSCE (1996)

Additionally, states agreed in their understanding that the security of one of them might be affected by developments in another one of the region without necessarily directly impacting on its soil or even touching on its borders. Therefore, the OSCE agreed to pursue an approach to security that is a) indivisible, b) comprehensive, and c) co-operative, as outlined in the 1990 "Charter of Paris for a New Europe", where participating States declared that "security is indivisible and the security of every participating State is inseparably linked to that of all the others."[3] Thereby, the OSCE ensured that not only the different perspectives of each pS are taken into account but that areas which would in other international fora not necessarily fall under the concept of security, can brought to the table as well.

This combination of an inclusive, comprehensive and co-operative approach to security helps, in theory, bridging differences and to build trust between states by co-operating on all areas of conflict prevention, crisis management and post-conflict rehabilitation, based on the common agreement among states that "each participating State has an equal right to security", as was repeatedly stated since, such as prominently in the Istanbul Declaration of 1999[4], which itself was a more elaborated follow-up decision to the Charter of Paris from 1990. Eventually, in 2003, the states decided to "furthering the role of the OSCE as a forum of political dialogue in the Euro-Atlantic

[3] OSCE (1990)
[4] OSCE (1999)

space", meaning that, besides providing a platform for security, the aspect of dialogue was added.[5]

Using the platform for security/dialogue principle allows also addressing issues which might, on first sight, not be relevant for other states or could be considered to be rather an internal affair – such as freedom of the media or the conduct of free and fair elections. But in the OSCE's view, these topics have an equally important place on the agenda, as seen by the creation of the Office for Democratic Institutions and Human Rights (ODIHR; initially established in 1990 as "Office for Free Elections"[6]) and the Representative on Freedom of the Media (RFoM; established 1997[7]), to stay with these two thematic examples.

In the same regard, cooperation with other international and regional organisations increased over time because the participating States of the OSCE realised that security cooperation was not only important but, in view of scarce resources and a deteriorating security setting between what used

[5] In current times, participating States use the terms "platform for dialogue" and "forum for security cooperation" interchangeably, often depending on whether their focus is on the wish to talk publically about an issue they are concerned with and might feel needing to have a broader audience listening and potentially helping them to address the issue, or if they would like to address a security issue that they are concerned with and would like to hear the views of others before taking further steps. At the same time, the fact that the OSCE is not taking legally binding decision but only politically and morally binding ones reduces the credibility of these efforts to a certain extent.

[6] OSCE (1990)

[7] OSCE (1997)

to be Western and Eastern Europe, needed to be improved and expanded.

Co-operation with other international organizations

In order to use synergies and draw on the comparative advantages of each organization, not least as an arrangement under Chapter VIII of the United Nations Charter that foresees regional arrangements to deal with “matters relating to the maintenance of international peace and security”, the OSCE supports these UN efforts at the regional level. The then CSCE developed its relationship with the UN in the framework for co-operation that it had signed with the UN in 1993[8]. It is therefore that, already the year after, high-level meetings between the UN and CSCE representatives have taken place regularly. Also already back in 1996, the pS reaffirmed “that European security requires the widest co-operation and co-ordination among participating States and European and transatlantic organizations.”[9]

Since 2003, the UN Security Council has met annually with other regional organizations on thematic issues related to peace and security, in which context the OSCE played the major role for security in Europe, which geographically includes in the OSCE’s

[8] CSCE (1993)
[9] OSCE (1996)

understanding the northern hemisphere "from Vancouver to Vladivostok"[10].

In consequence, the OSCE established and maintains cooperation with a number of considerable international organizations, e.g. with the United Nations (UN)[11], the European Union (EU), the Council of Europe (CoE), the International Organisation for Migration (IOM), and NATO[12].

After 2001, in an atmosphere of general considerations how security cooperation could be strengthened worldwide, relations between the OSCE and other international organizations within and beyond the OSCE region have gained momentum. Due to

[10] CSCE (1994)

[11] UN (1992). In 1992, the cooperation agreement with the UN was in fact the first such document the CSCE signed with another international organisation. It was followed, soon after, by the "Framework for cooperation and coordination between the United Nations Secretariat and the CSCE" (A/48/185; 1 June 1993, endorsed in November 1993).

[12] The list of partners with whom the OSCE, respectively OSCE Field Operations, signed Memoranda of Understanding or had an exchange of letters or similar agreements of different commitment, is quite extensive and includes, besides international political organisations, also institutions that deal with topics the OSCE is working on as well or has an interest to cooperate with to increase their knowledge and get access to expertise which would otherwise not be available within the OSCE's structures.
Among others, these institutions include agreements with the European Commission, the European External Action Service (EC/EEAS), INTERPOL, the Geneva International Centre for Humanitarian Demining (GICHD), the Geneva Centre for the Democratic Control of Armed Forces (DCAF), the Office of the High Representative (OHR) in Bosnia and Herzegovina, the European Bank for Reconstruction and Development (EBRD), UN Women, the International Committee of the Red Cross (ICRC), or the United Nations Economic Commission for Europe (UNECE), to name but some. But already this rather limited list shows that the OSCE not only speaks about international cooperation but invests time and efforts to formulate how they wish to fill these different agreements with life as is visible in each MoU/agreement.

its norms and values, including the promotion of respect for human rights, there has been considerable interest from other organizations to learn more about the OSCE, its principles, and its consultative mechanisms and procedures which could potentially also be applied between states to counter terrorism.

As outlined in the OSCE's 2001 "Bucharest Plan of Action for Combating Terrorism"[13], participating States agreed on the need to address transnational threats (TNT) and to work in concert with, for example, the United Nations Office on Drugs and Crime (UNODC). The Plan set the basis for an enhanced focus on issues that the OSCE had already been dealing with before. But now these issues were put higher on the agenda and summarised under the umbrella of TNT, where the topics of anti-terrorism efforts[14,15] and cybercrime, border security, and police issues are centrally coordinated from the OSCE Secretariat.[16] In this sense, the changing security environment had shown its effects on the work of the OSCE which was, until then, rather seen as an institution where discussions would be around more

[13] OSCE (2001)

[14] The OSCE's "Charter On Preventing And Combating Terrorism", adopted in 2002, further details the work in this area.

[15] The Anti-Terrorism Unit's creation was suggested in the same Plan.

[16] N.B.: The Decision goes as far as requesting participating States to "take the necessary steps to prevent in their territory illegal activities of persons, groups or organizations that instigate, finance, organize, facilitate or engage in perpetration of acts of terrorism or other illegal activities directed at the violent overthrow of the political regime of another participating State", i.e. states would support each other in preventing the overthrow of a government – a decision that is worthwhile being seen in the light of the policy of "regime change" that several states pursued in the years to follow this very decision *not* to support illegal activities to violently overthrow a political regime.

political, bilateral or other topics that concern governance, elections, media or similar, and not that much hard security as provisions on countering terrorism require. However, the link between maintaining the OSCE principles and applying measures to prevent and counter terrorism, are an added value that the OSCE could provide due to its flexible approach to their work which is not limited by agreed documents, but rather limited by the will – or lack of will – of the participating States who committed to specific issues.

The same decision taken by participating States in Bucharest suggested "broadening dialogue with regional organizations", such as the Shanghai Co-operation Organization (SCO), the Conference on Interaction and Confidence-Building Measures in Asia, the Organization of the Islamic Conference (OIC), the Arab League (AL) and the African Union (AU). Already at this early time after the transformation from a conference to an organisation, the naming of such a variety of international organisations as potential partners in working on security shows how broad and inclusive the OSCE's participating States understood their work, aiming at good cooperation and synergies between the various actors in the field of security, or in this case more precisely: on countering terrorism.[17]

[17] In a later decision, taken in 2005, the participating States explicitly named „UNODC, the Council of Europe and other pertinent international organizations" as the partners with whom they would see the OSCE working on "improving and promoting the functioning of criminal justice systems" with a view to Combating Transnational Organized Crime (OSCE: 2005).

By adhering to the principles and human values the OSCE participating States set for themselves, the organisation ensures that their understanding of comprehensive security was also understood by other actors. Keeping an eye on the different aspects of security, e.g. strengthening the rule of law and state authorities, promotion of human rights, the promotion of media attention to tolerance of ethnic, religious, linguistic and cultural diversity, or addressing the issue of protracted displacement, helps maintaining these standards in a variety of fields where the risk of undermining the said standards is likely if national security concerns are given higher priority.

But to concretely address the issues that were and are of concern for the different states and organisations, these cooperative mechanisms were supposed to be activated on the working level as well. Obviously, contacts at the decision-taking level were needed. But the proper exchange of information, knowledge sharing and discussions about how to apply the different standards and measures required engagement on all levels. Increased participation in conferences was seen as one path to achieve this. The OSCE regularly invites speakers from the mentioned regional organizations to their events, such as to the highest periodic meeting, the Ministerial Council which takes place once a year to conclude the annually changing OSCE Chairmanship, as well as to other conferences and workshops throughout the year. Vice-versa, organisations invite OSCE representatives to participate in their events and workshops.

To address the potential spill over of security threats between the OSCE area and neighbouring regions, such as the Southern Mediterranean area, the Organisation also works with regional organizations from outside the OSCE area. Among others, the goal is to share good practices in all phases of what the OSCE calls the "conflict cycle"[18], which includes the four phases of early warning, conflict prevention, crisis management, and post-conflict rehabilitation, as well as the promotion of human rights and democratic elections.

In this regard, the OSCE Ministerial Council Decision which detailed the conflict cycle tasked the organisation's executive structures to "enhance their co-operation and co-ordination with other international and regional organizations, especially with their respective structures in the field, and with civil society organizations, to increase financial, technical and political efficiency and burden-sharing, reduce unnecessary duplication and promote the best use of available resources." Further, they should "develop lessons identified and best practices as regards co-operation and co-ordination with other international actors in the field". While the tasking is quite clear, there is no agreement on the scale, the direction or the limits of such cooperation and coordination, i.e. on whether the OSCE should increase their cooperation with specific agencies or organisations, such as NATO or the EU or the Common Security Treaty Organisation to work, for example, on conflict prevention or crisis management.

[18] OSCE (2011)

Also, the decision and later decisions that build on the elements spelled out in makes no reference to peacekeeping operations which had been explicitly mentioned as one tool the OSCE might deploy to support the conflict resolution efforts of the UN, as will be discussed in more details in the last chapter.

The OSCE and NATO

The fact that the OSCE region covers North America, all of Europe, the Russian Federation and large parts of Central Asia, as well as Mongolia, meaning all EU member states and all NATO member states, ensures that the perspectives of a variety of often opposed political stakeholders are represented in the OSCE's discussions, including on topics which would, otherwise, only be addressed by one side. A prominent example of such dispute is the – so far largely only verbally – belligerent confrontation between NATO and the Russian Federation since 2014 over the partly alleged, partly confirmed Russian military activities in the Black Sea, in the Baltic Sea, and, most important, in Ukraine.

However, before the current "crisis in and around Ukraine"[19] as the OSCE calls the conflict in Ukraine, NATO's important role in promoting security in Europe has been emphasized in several OSCE documents for many years, i.e. from before the current crisis in Ukraine started in 2013/14. Such example is the 2003 "OSCE Strategy to Address Threats to Security and Stability in

[19] OSCE (no date)

the Twenty-First Century"[20] where NATO is named in one row together with the UN, the EU, and the Council of Europe as a valid partner in contributing to peace and stability in the European region. Obviously, at the time, none of the OSCE participating States had an issue to name NATO as a partner, but this changed for obvious reasons since.

In return, the view that NATO took on the OSCE is of similar importance as the Organisation was praised as "the most inclusive security organisation in Europe" that "plays an essential role in promoting peace and stability, enhancing cooperative security, and advancing democracy and human rights in Europe"[21].

The 2003 Strategy – which is one of the few documents that even mentions the term "strategy", emphasizing how crucial the document was considered to be at the time of agreement – states that the OSCE "seeks to expand its relations with all organizations and institutions that are concerned with the promotion of comprehensive security within the OSCE area", and that the organisation needs to remain flexible in order to be able "to co-operate with different organizations as their capabilities and focus may change over time, with developments in perceptions of threat and organizational capacities."

[20] OSCE (2003)
[21] NATO (1999)

The same Strategy describes the OSCE's response as being multidimensional and that the Organization would "provide an effective framework for co-operation with other international actors in order to address threats in a co-ordinated and complementary way". This commitment was built on the already mentioned "Charter for European Security and its Platform for Co-operative Security" from 1999.

It was in 2004, at NATO's Istanbul Summit, when the concluding communique stated that NATO and the OSCE had "largely complementary responsibilities and common interests, both functionally and geographically."[22] And that NATO would "continue to further develop co-operation with the OSCE in areas such as conflict prevention, crisis management and post-conflict rehabilitation." These are the same areas where also the OSCE underlined five years earlier their will to increase cooperation with NATO, among other international actors.

The most prominent cases of close cooperation between NATO and the OSCE can be found in the Balkans, where both organisations have field operations deployed, i.e. in Kosovo the OSCE Mission and the NATO-led Kosovo Force (KFOR), as well as in Bosnia Herzegovina the NATO-led Stabilization Force (SFOR) and the OSCE Mission which worked closely together to implement the Dayton Peace Agreement. But also in Afghanistan, the cooperation between the two organisations

[22] NATO (2004)

turned out to be effective and pragmatic: In 2004, 2005 and 2014, the NATO-led International Security Assistance Force in Afghanistan provided security assistance to the OSCE's Election Support Teams which were deployed to support the Presidential and Parliamentary elections.

All three cases show that a division of labour along the lines of each organisation's core mandate is well possible and can function if their respective role are clearly defined and – even more importantly – if the political will is there on both sides.

But one needs to step back a little bit in time to get the full picture of the relationship. The relations that the OSCE maintains with NATO fall into a similar understanding of mutual security interests as they do with other regional organisations. In the OSCE's view, NATO has significantly contributed to the discussions about Europe's security architecture from the very beginning of the Helsinki discussions in in the 1970s.

However, obviously in today's political setting with opponents that do not shy away from threatening the respective adversary from using maximal military power to achieve their goals, NATO's defence agenda is less inclusive as regards some of OSCE's participating States which are not member to the Alliance, namely the Russian Federation. Even though NATO tried, for more than 20 years, to build a partnership with the Russian Federation, this cooperation has been suspended since 2014 in response to the Russian military intervention in Ukraine.

Due to the fact that, additionally, the European Union progressively imposed restrictive measures, including sanctions, against the Russian Federation since the “illegal annexation of Crimea and Sevastopol”[23] and the “deliberate destabilisation”[24] of Ukraine, in total, more than half of the OSCE’s 57 participating States have chosen to suspend direct political collaboration with the Russian Federation.

The North Atlantic Council’s decision, dating 1 February 2019, to issue a statement that supported the United States’ decision to suspend its obligations under the Intermediate-Range Nuclear Forces Treaty[25], together with the extension of the EU sanctions until September 2019, makes the OSCE the last remaining platform for political dialogue where all stakeholders, from the EU, NATO and the Russian Federation, as well as Ukraine and other states of the broader European region, sit around the same table and have a chance to freely express their view on things.

At the same time, the OSCE became an important partner for NATO as it attaches great importance to the role of the OSCE in fostering dialogue, building trust, and upholding the rules-based international order through inclusive dialogue. The two organisations do have complementary roles in building security and maintaining stability in the region as they both acknowledge

[23] EU (2014a)
[24] EU (2014b)
[25] NATO (2019)

the need for a coherent and comprehensive approach to conflict prevention and crisis management.

Both organisations cooperate at the political and operational level on conflict prevention and resolution, on post-conflict rehabilitation which includes border security, on countering the proliferation of small arms and light weapons as well as arms control, and on counter-terrorism, to name a few. Through staff talks, regular exchange of views on thematic and regional security issues of common interest take place as well.

It must be remembered that, when the OSCE was founded in 1975, i.e. in the middle of the Cold War, confrontations between NATO and the signatory states to the "Treaty of Friendship, Cooperation and Mutual Assistance" (aka "Warsaw Pact") was at its height. In this regard, the OSCE could, once again, become the platform where concerns of utmost security are discussed and opposed views are expressed by concerned states.

Not least do the OSCE's efforts in (military and non-military) confidence- and security-building measures, such as through the application of the Vienna Document, contribute to the intensive cooperation between the two organisations.

Peacekeeping and the OSCE

Despite the fact that the OSCE has never established or contributed to military field operations, the political commitments to do so have been agreed already back in 1992 with the signing of the Helsinki Document. The MoU between the CSCE and the

United Nations, signed in August 1994, which detailed the cooperation modalities with regard to the CSCE's engagement and cooperation with the UNPROFOR Mission in Bosnia and Herzegovina, was a milestone that underlined the role that the CSCE could and – in the understanding of the time – would take with regard to engaging in future peacekeeping operations.

More recently, after the beginning of the crisis in and around Ukraine, calls for the deployment of an OSCE peacekeeping mission, or the OSCE's contribution to the same under a UN mandate, have been heard again: the Ukrainian representative spoke in favour of such deployment, saying that Ukraine had been "advocating since 2015 for deployment of a full-fledged multinational peacekeeping force throughout conflict-affected part of Donbas to enable the necessary security environment, facilitate full implementation of the Minsk agreements, end the conflict and restore the sovereignty of Ukraine in the region."[26] However, the controversial question remains about the mandate and area of operation such mission would be entitled with.

As mentioned before, the Ministerial Council Decision on Elements of the Conflict Cycle from 2011 includes, among others, the pledge to increase efforts at resolving existing conflicts in the OSCE area in a peaceful and negotiated manner. To that end, the Decision calls on the OSCE Chairmanship and participating States to pursue steps to strengthen OSCE

[26] OSCE (2019)

capabilities in further addressing the conflict cycle. Taking this into account in combination with the 1992 Decision to consider the possibility of OSCE's engagement in peacekeeping in cases of conflict within or among pS which could be mandated in support of efforts at achieving a political solution, such operations are still – and again – well thinkable

The Helsinki Document from 1992 went as far as detailing which requirements and constellations might be faced where the OSCE could deploy a peacekeeping mission, e.g. that they could involve both, civilian and military personnel, that they could range from small-scale to large-scale missions, and that they could assume a variety of forms, including observer or monitoring missions and be tasked to observe ceasefire adherence, monitoring troop withdrawals, assisting refugees, supporting law and order and/or providing humanitarian and medical aid. When reading the Document without prior knowledge to its date of issuance, one could easily assume that the authors gathered only recently and brainstormed on the current challenges in Europe. The more surprising it might be to find that, at the moment, there is little to no appetite among participating States to seriously consider establishing such peacekeeping field operation. And this despite the Document, i.e. the participating States' decision to be ready to deploy peacekeeping forces, being quite clear that none of the operations would include peace enforcement elements.

Based on the increasing understanding also within the UN that there is no more sharp distinction between predominantly military peacekeeping missions and purely civilian operations, the complementary use of tools and assets would be the most promising option to cope with the challenges current crisis situations require. The limits that the Helsinki Document sets are also easy to observe, as they state that they would “require the consent of the parties directly concerned”, which precludes a UN Chapter VII mission, and further that the mission would “be conducted impartially.”

As a regional organization with a comprehensive concept of security and nearly 30 years of experience in deploying field operations with multi-dimensional mandates, the OSCE would be well placed to address such modern challenges.

The last serious efforts by participating States to discuss and assess the possibility to engage in peacekeeping missions dates back to 2002, when the Ministerial Council tasked the Permanent Council, i.e. the weekly convened meeting of representatives of the participating States, “to conduct a review of peacekeeping, with a view towards assessing OSCE capacity to conduct peacekeeping operations and identifying options for potential OSCE involvement in peacekeeping in the OSCE region”. The result of this thorough process was, however, a lack of consensus on the way ahead after the established working group had presented their results in the course of 2003. Examples of this experience are, among others, the Kosovo Verification

Mission, the Special Monitoring Mission to Ukraine, the Mission to Moldova, or the Mission to Georgia, which had all been tasked to monitor a ceasefire agreement, respectively the verification of the same; or the tasks given to the Mission to Georgia and the SMM to monitor territories between conflict parties and report on issues related to security and stability on the ground; or protecting the distribution of humanitarian aid as well as protecting refugees, as the Mission to Croatia and the Mission in Kosovo were mandated to do; and lastly the broadest mandate that several OSCE Missions have seen, which is supporting the political conflict resolution processes through mediation and dialogue facilitation, including implementing confidence building measures, as seen in the Mission to Skopje, the Mission to Moldova, the Mission to Georgia, and the Assistance Group to Chechnya.

In view of the vast experience that the OSCE gained through the deployment of field operations which obviously included elements which can be considered to appear typically in peacekeeping operations, the discussions about their deployment might re-emerge at a certain point.

Bibliography

CSCE: Framework for Co-operation and Co-ordination between the United Nations Secretariat and the Conference on Security and Co-operation in Europe, in: Journal of the 14th CSO Vienna Group Meeting, 1993; https://www.osce.org/node/424574

CSCE: Towards a genuine partnership in a new era, 1994; https://www.osce.org/mc/39554

EU: Council Regulation (EU) No 692/2014 concerning restrictive measures in response to the illegal annexation of Crimea and Sevastopol, 2014a; https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02014R0692-20141220&qid=1444987014323&from=EN

EU: Statement by the President of the European Council Herman Van Rompuy and the President of the European Commission in the name of the European Union on the agreed additional restrictive measures against Russia, 2014b; https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/144158.pdf

NATO: The Alliance's Strategic Concept, 24. April 1999; https://www.nato.int/cps/en/natolive/official_texts_27433.htm

NATO: Istanbul Summit Communiqué, 2004; https://www.nato.int/docu/pr/2004/p04-096e.htm

NATO: Statement on Russia's failure to comply with the Intermediate-Range Nuclear Forces (INF) Treaty, 2019; https://www.nato.int/cps/en/natohq/news_162996.htm

OSCE: Charter of Paris for a New Europe, 1990; https://www.osce.org/mc/39516

OSCE: Budapest Document 1994 – Towards A Genuine Partnership In A New Era, 1994; https://www.osce.org/mc/39554

OSCE: Lisbon Declaration On A Common And Comprehensive Security Model For Europe For The Twenty-First Century, 1996; https://www.osce.org/mc/39539

OSCE: Mandate Of The OSCE Representative On Freedom Of The Media, 1997; https://www.osce.org/pc/40131

OSCE: Operational Document - the Platform for Co-operative Security, 1999; https://www.osce.org/mc/17562

OSCE: The Bucharest Plan of Action for combating terrorism, 2001; https://www.osce.org/atu/42524

OSCE: Charter On Preventing And Combating Terrorism, 2002; https://www.osce.org/mc/42536

OSCE: Strategy to Address Threats to Security and Stability in the Twenty-First Century, 2003; https://www.osce.org/mc/17504

OSCE: Decision no. 4 – Reviewing the OSCE role in the field of peacekeeping operations, in: Final Document of the Tenth Meeting of the OSCE Ministerial Council, Porto, 6-7 December 2002; https://www.osce.org/mc/40521

OSCE: MC.DEC/3/05 – Combating Transnational Organized Crime, 2005; https://www.osce.org/mc/17419

OSCE: The OSCE Concept of Comprehensive and Co-operative Security – An Overview of Major Milestones, 2009; https://www.osce.org/secretariat/37592

OSCE: Decision No. 3/11 on elements of the conflict cycle, related to enhancing the OSCE's capabilities in early warning, early action, dialogue facilitation and mediation support, and post-conflict rehabilitation, 2011; https://www.osce.org/mc/86621

OSCE: The crisis in and around Ukraine, no date; https://www.osce.org/ukrainecrisis

Permanent Mission of Ukraine to the International Organizations in Vienna: Statement by the Delegation of Ukraine at the 72nd Joint FSC-PC Meeting on Lessons Learned from Conflict Resolution, 2019; https://www.osce.org/forum-for-security-cooperation/412502

UN: Cooperation between the United Nations and the Conference on Security and Cooperation in Europe, 1992;https://www.un.org/documents/ga/res/47/a47r010.htm

UN: General Assembly Resolution on Cooperation between the United Nations and the Conference on Security and Cooperation in Europe, 1993; http://www.worldlii.org/int/other/UNGA/1993/39.pdf

UN: General Assembly Resolution Cooperation between the United Nations and the Conference on Security and Cooperation in Europe, 1994; https://undocs.org/pdf?symbol=en/A/RES/49/13

THE RISE OF THE ROBOTIC WEAPON SYSTEMS IN ARMED CONFLICTS

Walter David, (Ronin Institute, Montclair NJ)[1],

Col. Paolo Pappalepore, (Italian Defence General Staff)[2],

Judge Brindusa Andreea Sarbu, (1st District Court Bucharest)[3],

Abstract: Disruptive technologies like robotics and artificial intelligence (AI) are changing workplaces, business and can support disaster management; however they are also going to transform the operational environment and warfare. Future technologies can be assessed with the Disruptive Technology Assessment Game and wargaming tools that let military and technologists analyze and assess their impact on military operations and defence planning in the domains of Doctrine, Organization, Training, Materiel, Leadership, Facilities, Personnel and Interoperability. Robotic, cyber, space, and autonomous weapons enable precise strikes. In particular, the paper addresses the AI powered Lethal Autonomous Weapons Systems (LAWS) promising valuable military advantages. LAWS efficiency, effectiveness and speed of decision compared with the human brain decision-making, can lead to the reduction of deployed human soldiers, and minimize loss of civilians and destruction of infrastructures. However, the deployment in armed conflicts of weapons that will be more and more autonomous from the human control poses ethical issues, highlights gaps in the international humanitarian law (IHL) and present major risks to security related to potential uncontrolled proliferation. While it looks very unlikely that nations could agree on a ban to research and development of LAWS, the international community must agree on the acceptable level of autonomy in weapons, address the danger of their acquisition and use by organized criminal gangs, terrorist groups and

---

[1] Senior engineer, geospatial analyst and modelling and simulation expert, researcher of the Ronin Institute Montclair NJ United States. Currently posted as Chief of Analysis & Lesson Learned Section at NATO M&S Centre of Excellence.

[2] Deputy Chief of the Juridical Affairs General Office of the Italian Defence General Staff, Rome.

[3] Judge at the first court of 1st District of Bucharest.

malicious non-state actors, and put in place an export control mechanism.

Key words: robots, autonomy, decision-making, lethal autonomous weapon systems, international humanitarian law, security, proliferation.

Introduction

The **Fourth Industrial Revolution** is changing our life. Emerging technologies like artificial intelligence (AI), robotics, big data, quantum computing, nanotechnology, biotechnology, the Internet of Things (IoT), the Industrial Internet of Things (IIoT), the 5th generation (5G) wireless, 3D printers and autonomous systems (Vincent, 2017) are fusing the physical, digital and biological worlds, combining hardware, software, and biology into ***cyber-physical systems*** (Schwab, 2015). Robots are automating health-care, office work, search and rescue operations, services, with a growing ethical, physical and emotional impact on our lives; human-machine interactions will develop further (Sullins, 2011). In 1997, IBM's Deep Blue won against the Soviet world chess champion Garry Kasparov. Recently, DeepMind's AlphaZero, trained in just 4 hours from scratch by a reinforcement learning technique playing about 60 million games with itself (instead of analyzing human game) crushed the top chess computer Stockfish using moves never seen before.

Figure 1 Human playing chess with computer (Image © Shutterstock / ARKHIPOV ALEKSEY

The human-machine interaction (and integration) is going to expand. Due to the challenges from the growth of (big) data and the complexity of the *confused, congested, conencted,contested, constrained* future operating environement, Artificial Intelligence (AI) will provide time– critical decision making and operational planning support. Future wars will be fought by AI powered machines but will humans still be in charge?

Robots. Asimov's Three Laws of Robotics

What is a Robot? The Oxford dictionary defines a robot, from the Czech language *robota* 'forced labour', a machine capable of carrying out a complex series of actions automatically, especially one programmable by a computer. Isaac Asimov introduced **the Three Laws of Robotics** in his 1942 short story "Runaround".

First Law – A robot may not injure a human being or, through inaction, allow a human being to come to harm.

Second Law – A robot must obey the orders given it by human beings except where such orders would conflict with the First Law.

Third Law – A robot must protect its own existence as long as such protection does not conflict with the First or Second Laws.

Later, Asimov in a new fiction where robots had taken the power in whole planets and human civilizations, added a zeroth law, to precede the others.

Law Zero – A robot **may not harm humanity,** or, by inaction, allow humanity to come to harm.

Asimov's laws are referred to in books, films and have impacted thought on ethics of artificial intelligence. In the TV show *Person of Interest*, a sentient machine tries to prevent violent crime. In the movie *Avengers: Age of Ultron*, an AI robot sets out on a mission to kill all humans. Should we worry about science fiction becoming reality (Kaspersen, 2016). However, after 75 years Asimov's laws could be misinterpreted, in fact, they do not provide a definition of what is a robot. Nowadays robots include vacuum cleaners, industrial machines and even surgery could use robots made from DNA and proteins. For military robots, the First Law – **not harming humans** and the meaning of "harming a human being" might need to be considered from different perspectives (Anderson, 2017).

Robots in Conflict – Lethal Autonomous Weapon Systems (LAWS)

Robotic weapons include systems, from fully autonomous weapons that can launch attacks without any human involvement to semi-autonomous weapons that require an affirmative human action to execute an order. Robots search and explode improvised explosive devices. UAVs perform reconnaissance and strike missions around the world (Rabkin & Yoo, 2017). Semi-autonomous Predator and Reaper drones hover over a target for days but still a military is in charge of the decision about firing its Hellfire missiles (Walsh, 2018). But, soon, one human could control hundreds/thousands of systems able to identify and attack targets automatically through pattern-and facial recognition algorithms (Macaulay & Magee, 2018) and in the future, machines could be killing on their own initiative.

In 2017 the US Department of Defense demonstrated a micro-drone swarm of 103 drones able to collaborate in decision-making and fly in adaptive formation (Macaulay & Magee, 2018). In fact, swarming offer great advantages and countering small autonomous weapon systems is pretty difficult because the available anti-air defences are not designed to track things of small size and those proposed by industry are not always working as advertised.

The United Nations Office for Disarmament Affairs-UNODA, in the Perspectives on Lethal Autonomous Weapon Systems, 2017 defined a Lethal Autonomous Weapon System (LAWS) as any

weapon system with autonomy in its critical functions, that is, a weapon system that can:

- **select** (*search for, detect, identify, track or select*) **and**
- **attack** *(use force against, neutralize, damage or destroy)* **targets without human** intervention.

Decision Making and Autonomy

Created by US pilot John Boyd as a way to be superior in dogfights with enemy pilots during the war in Korea, the Observe Orient Decide Act (OODA) recurring loops of observation, orientation, decision and action (Figure 2) happen in the human mind in response to a situation. This human decision-making model is very useful in situations that require rapid decisions like in combat or in business.

In order to define systems' autonomy and the levels of autonomy (LOA), different multi-dimensional scales are used with descriptive indicators. But, how autonomous should an unmanned aircraft vehicle (UAV) be? NASA demonstrated the feasibility of a fully autonomous spacecraft from the launch of Deep Space 1 in 1998 (Frost, 2010). Proud from NASA Johnson Space Center established a scale of autonomy based on eight levels for each OODA category (Figure 3). The LOA fit the tasks encompassed by the functions of the Observe, Orient, Decide, Act (OODA) categories. Such approach allows to weight the function types across a particular level and to determine how autonomous to design each one.

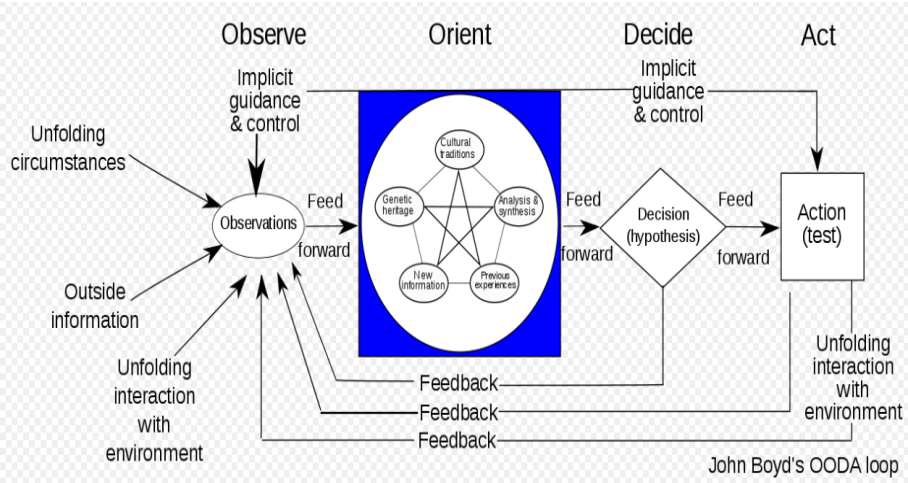


Figure 2. Human Decision Making model: the OODA Loop

The Observe column deals with data collection and filtering, the Orient column refers to options coming from analysis, prediction and integration, the Decide column refers to decision-making in accordance with the available options and the Act column refers to how autonomously the Unmanned Aerial System (UAS) can act. In levels 1-2, the human is primary, in levels 3-5 the system operates with human interaction but in levels 6-8, it operates independently of the human who can get limited information (Proud et al, 2003).

Level	Observe	Orient	Decide	Act
8	The computer gathers, filters, and prioritizes data without displaying any information to the human.	The computer predicts, interprets, and integrates data into a result which is not displayed to the human.	The computer performs ranking tasks. The computer performs final ranking, but does not display results to the human.	Computer executes automatically and does not allow any human interaction.
7	The computer gathers, filters, and prioritizes data without displaying any information to the human. Though, a "program functioning" flag is displayed.	The computer anlayzes, predicts, interprets, and integrates data into a result which is only displayed to the human if result fits programmed context (context dependant summaries).	The computer performs ranking tasks. The computer performs final ranking and displays a reduced set of ranked options without displaying "why" decisions were made to the human.	Computer executes automatically and only informs the human if required by context. It allows for override ability after execution. Human is shadow for contingencies.
6	The computer gathers, filters, and prioritizes information displayed to the human.	The computer overlays predictions with analysis and interprets the data. The human is shown all results.	The computer performs ranking tasks and displays a reduced set of ranked options while displaying "why" decisions were made to the human.	Computer executes automatically, informs the human, and allows for override ability after execution. Human is shadow for contingencies.
5	The computer is responsible for gathering the information for the human, but it only displays non-prioritized, filtered information.	The computer overlays predictions with analysis and interprets the data. The human shadows the interpretation for contingencies.	The computer performs ranking tasks. All results, including "why" decisions were made, are displayed to the human.	Computer allows the human a context-dependant restricted time to veto before execution. Human shadows for contingencies.
4	The computer is responsible for gathering the information for the human and for displaying all information, but it highlights the non-prioritized, relevant information for the user.	The computer analyzes the data and makes predictions, though the human is responsible for interpretation of the data.	Both human and computer perform ranking tasks, the results from the computer are considered prime.	Computer allows the human a pre-programmed restricted time to veto before execution. Human shadows for contingencies.
3	The computer is responsible for gathering and displaying unfiltered, unprioritized information for the human. The human still is the prime monitor for all information.	Computer is the prime source of analysis and predictions, with human shadow for contingencies. The human is responsible for interpretation of the data.	Both human and computer perform ranking tasks, the results from the human are considered prime.	Computer executes decision after human approval. Human shadows for contingencies.
2	Human is the prime source for gathering and monitoring all data, with computer shadow for emergencies.	Human is the prime source of analysis and predictions, with computer shadow for contingencies. The human is responsible for interpretation of the data.	The human performs all ranking tasks, but the computer can be used as a tool for assistance.	Human is the prime source of execution, with computer shadow for contingencies.
1	Human is the only source for gathering and monitoring (defined as filtering, prioritizing and understanding) all data.	Human is responsible for analyzing all data, making predictions, and interpretation of the data.	The computer does not assist in or perform ranking tasks. Human must do it all.	Human alone can execute decision.

Figure 3. Autonomy levels and OODA (Proud et al., NASA, 2003)

Wargaming of disruptive technologies

NATO defines a **disruptive technology** as *"a technological development which **changes the conduct of operations** (including the rules of engagement- ROE) significantly **within short time** and thus **alters** the long-term goals for concepts, strategy and planning".* The methods useful to assess the potential disruptiveness of a technology, its potential benefits for military activities and the impact on defence include text-mining, morphological analysis, scenario building, Delphi, structured brainstorming, multi-criteria analysis and crowdsourcing, the Disruptive Technology Assessment Game (DTAG) and war gaming (Kindvall et al., 2017).

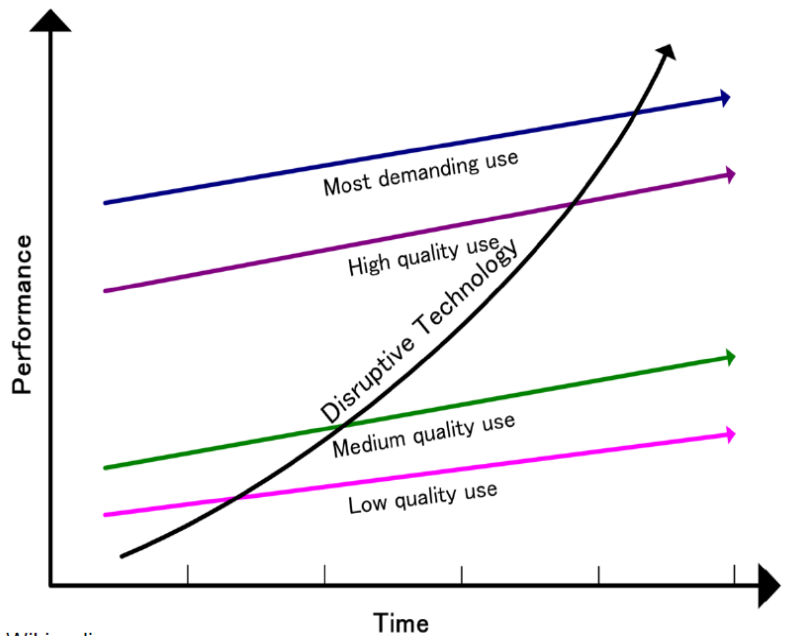


Figure 4 Disruptive Technologies (https://en.wikipedia.org/wiki/Disruptive_innovation)

In particular, the DTAG was developed during NATO studies SAS-062 and SAS-082.88 as a low-cost, effective, analytical, table–top seminar game to reduce the risk of failure of a technology or capability-focused project by simulating its use in a theoretical, low-risk environment. The DTAG process includes (Kindvall et al., 2017):

- **The identification of future technology development,** using as a standardized description, Ideas of Systems (IoS) cards;
- **The war gaming** where the Blue and a Red teams' military and technology experts develop their plans and put them against each other in front of the whole group. For each vignette of the scenario there are two confrontations, the first without, the second with the new technology. IoS cards enable to evaluate the strengths and weakness of new technologies within military concepts of operations. War game facilitate group discussions;
- **The analysis** to assess what systems/ technologies have a truly disruptive effect if used in the vignettes. The focus is on systematic capture of data, through a computerized tool, analysts' notes and questionnaires.

Examples of investigated technologies include *Support / Logistics Unmanned Ground Vehicle, High-Energy Laser on Ships, Unmanned Combat Aerial Vehicle, Multi-Purpose UAV Swarm, Situational Awareness Sensor System, Global Information Satellite Constellation, Multi-Purpose RF System for*

Tactical UAV/UGV/USV, Unmanned Surface Vehicle, Bionic Autonomous Underwater Vehicle, Subsea Network-Centric Warfare, Stratospheric Surveillance Platform

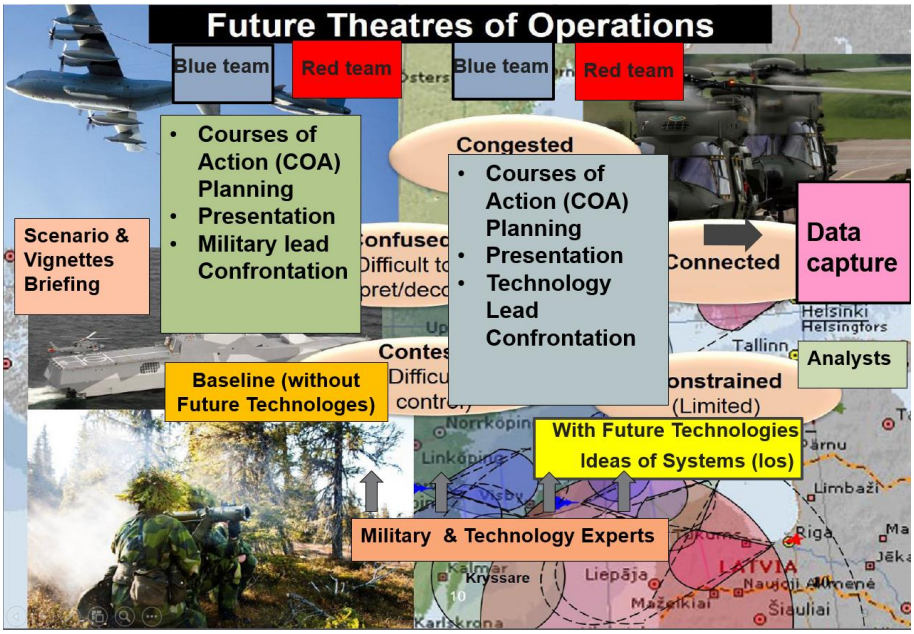


Figure 5: DTAG game process in a future operating environment scenario

As an example, swarms of Unmanned Aerial Vehicles (UAV) have been assessed with regard to what impact they could have on defence capability planning. A *Doctrine Organization Training Materiel Leadership Facilities Personnel Interoperability (DOTMLFPI)* perspective has been included in order to indicate the impact on military operations and organisations (FFI, 2016).

DOCTRINE	Combining assets, sensors and effectors. **Reduction of risk for human soldiers and equipment.** Special attention to Airspace management. Change doctrine.
ORGANISATION	Swarms assets will replace traditional weapon systems
TRAINING	Optimize, learn use of systems in logistics, mechanics and operations, management of multiple systems in confined space
MATERIEL	Procurement of new materiel, in particular "swarming assets"
PERSONNEL	Skilled operators and technical staff for maintenance, upgrading etc.. Personnel could be in smaller numbers
LEADERSHIP	Out of the box thinking. Better situational awareness facilitating decision-making. High level discussion on **Ethical/ legal issues**
FACILITIES	Systems' scale/type influencing choice of required facilities
INTEROPERABILITY	Focus on interoperability issues in connection with cooperative ventures

Figure 6: Impact of Unmanned Aerial Vehicles (UAV) Swarms on Defence planning

AI-powered Lethal Autonomous Weapon Systems (LAWS) in Warfare Transformation

Technology produces advances in warfare, combat is moving toward the robotic. Unmanned aerial systems (UAS) are leading great technological innovations in warfare (Rabkin & Yoo, 2017). The first warfare revolution was the invention of gun powder, the second was the invention of nuclear weapons, autonomous systems lead the Third Warfare Revolution (Walsh, 2018).

Lethal Autonomous Weapons Systems (LAWS) promise significant military advantages (Chertoff, 2018). Future advances will bring armed sentry robots, autonomous armored vehicles, missiles and artillery, unmanned surface and underwater vessels. Precision targeting will allow to strike any target in the

world. Armed conflicts could be at lower cost and shorter. Nations will be able to coerce each other with fewer casualties and less destruction as technology can disrupt the opponent's networks (finance, transportation, etc.). Autonomous systems have the ability to integrate more information from more sources for better intelligence and situational awareness. Armed conflict often results from miscalculation when aggressors doubt the resolve of the other side to resist. Reducing uncertainty will help nations to negotiate and reach settlements with less need for armed fighting by giving options to resolve disputes, or even more information to prevent conflicts (Rabkin & Yoo, 2017).

In a crisis situation, autonomous systems are more predictable than humans, human judgment in crises often lack the flexibility to adapt and control the escalation; the robot could be a perfect soldier, never violating its orders.

Robots allow expanding the battle space over larger areas and extend the warfighter's reach deeper by seeing and selectively striking targets like terrorists.

Force multiplication. With robotics, cyber and space weapons soldiers can be removed from many dangerous missions thus reducing the size of ground forces. Surgical strikes and cyber-attacks can concentrate the lethal force on selected targets with more precision, reducing civilians and even combatants casualties (Rabkin & Yoo, 2017) and the destruction of critical infrastructures, buildings and properties. As often military tools evolve into non-military devices, robotics can support innovation

in humanitarian action, in natural disasters or complex emergencies.

Ethical and legal issues, risks for security

Soon, autonomous weapons systems **might be able to act** free of direct human control (Rabkin & Yoo, 2017) but **trust in autonomy** is a big issue. It is possible to develop systems with high levels of autonomy (LOA) but we lack suitable verification and validation (V&V) of the almost infinite outcomes from high levels of adaptability and autonomy. Current V&V methods are not suitable for certification of the higher LOA for operational use, requiring new methods to be developed.

However, there is a risk that adversaries might deploy systems with far higher LOA without any certifiable V&V thus gaining significant capability advantages.

Many states have ethical and legal concerns about the potential for systems to destabilize conflicts and inflict collateral damage (Chertoff, 2018). The International Human Laws (IHL) on the conduct of hostilities— in particular, the principles of **distinction, proportionality and precautions in attack**—are addressed to those who plan, decide upon and carry out an attack and **create obligations for combatants** in the use of weapons to carry out attacks. Combatants are responsible for respecting IHL rules and will be held accountable.

Who is a Combatant? According to the doctrine of the **moral equality of combatants** (MEC), the combatant, regardless the

side or if fighting a just war, is a **moral agent** who continuously exercises his choice and responsibility (Bazargan, 2013). Autonomous weapon systems are not specifically regulated by treaties on IHL (Davison, 2016) and they present issues regarding the compliance with the IHL principles:

- **Distinction** *The parties to the conflict must at all times distinguish between civilians and combatants. Attacks may only be directed against combatants. Attacks must not be directed against civilians* (Davison, 2016). Armed robotic systems cannot discriminate between military objectives and civilian objects, combatants and civilians, active combatants and those *hors de combat* and humanitarian actors. LAWS lack components to ensure compliance with the principle of distinction, they have sensors (cameras, infrared sensors, sonars, lasers, temperature sensors, ladars, etc.) but **their sensory or vision processing is not adequate** for separating combatants from civilians or for recognizing combatants *hors de combat*. IHL do not provide **a definition of a civilian** that might be easily translated into software code and provided to robots. Robots do not have battlefield awareness or **common sense reasoning** as required by the 1949 Geneva Convention.
- **Proportionality in attack**. *Launching an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a*

combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated, is prohibited.

They could not cancel or suspend an attack if the target is not a military objective or is subject to special protection, or the attack might violate the rule of proportionality, assessments of whether harm and loss to civilians is excessive in relation to anticipated military advantage. (W*hat is the balance between loss of civilian lives and expected military advantage?)* Again, robots **do not have the situational awareness or agency** to make proportionality decisions about the use of lethal force (Sharkey, 2012).

- **Precautions in attack.** *In the conduct of military operations, constant care must be taken to spare the civilian population, civilians and civilian objects. All feasible precautions must be taken to avoid, and in any event to minimize, incidental loss of civilian life, injury to civilians and damage to civilian objects.*

New systems will be produced with ever-increasing autonomy at each iteration (Chertoff, 2018). Some weapon systems already operate with a high degree of autonomy. South Korea has two weapons in use. The Super aEgis II sentry turret was originally designed with fully autonomous capacity. It was later updated with safeguards requiring human target approval, due to customer requests (Parkin, 2015), and the Samsung SGR-A1

semi-autonomous sentry gun for automated targeting (Velez-Green, 2015). Israel semi-autonomous drone systems, Harpy and Harop operate as “loitering munitions” around an area, searching and engaging targets.

Figure 7. SAMSUNG SGR-A1semi-autonomous sentry gun offers (Velez-Green, 2015)

Accountability. Imputation (imputatio) in the moral sense is the judgment by which someone is regarded as the author (causa libera, free cause) of an action, which is then called a deed (factum) and stands under laws (Kant, 1886). A robot does not have agency, moral or otherwise cannot be held accountable for its actions.

When things go wrong, who can be held accountable? The commander who gave the ordered the robot on a mission, the mission planner, the manufacturer of the robot, or the senior staff or the policymakers who decided to deploy it. Under the law of

State responsibility, a State could be held liable for violations of IHL resulting from the use of an autonomous weapon system (Davison, 2017).

Can we develop machines that can think and act rationally and like a human? A system able to make decisions based on the laws and ROE would need a considerable advancement in AI and computational power (Anderson, 2017).

What limits are needed on autonomy in weapon systems to ensure compliance with IHL? “Effective human control”, or “appropriate levels of human judgement” must be retained over weapon systems and the use of force.

Core components of human control include system’s predictability and reliability in its intended or expected circumstances of use (UN, 2016). The human control happens at different stages, from the development and testing (“development stage”); the commander’s (or operator) decision to activate the weapon system (“activation stage”); and when it independently selects and attacks targets (“operation stage”) (UNODA, 2017).

Autonomous weapons and Security

Autonomous weapons might affect stability (UNODA, 2017). Communications links among autonomous systems and command and control (C2) systems are vulnerable, a drone or robot could be hijacked and start firing, a virus could spread throughout the network and infect all units. Controlling escalation

and war termination could be difficult if an autonomous weapon that malfunctioned or was hacked continue attacking wrong targets or fire on civilians and the pace of battle could be accelerated the pace of battle beyond human reaction times.

Countering small autonomous weapon systems is a complex issue. Available anti-air defences and missiles are not designed to track small size systems. Non-state actors pursuit of autonomous weapons is not a question of if, but when Malicious armed non-state actors (ANSAs) have the potential to leverage LAWS for significant military advantage against states and acts of terror. They are not constrained by moral or legal rules and will soon adopt new technologies, indiscriminate violence may be the goal, violence would increase fear and intimidation (Chertoff, 2018). For non-state actors, LAWS could be a force multiplier in asymmetric conflict, increasing their reputation and symbolic legitimacy, by conferring them a status at the level of few nations (Chertoff, 2018). Innovation requires explicit knowledge and working experience, luckily the performance of the drones acquired from the market and modified by Mexican cartels, Hamas, Hezbollah and ISIS are still unsophisticated.

In April 2018, signatories to the UN Convention on Certain Weapons (CCWUN) met in the 2nd Group of Government Experts (GGE) discussion of LAWS to explore the technologies of LAWS within the context of the Convention (i.e. identify those relevant principles or restrictions applicable to LAWS) (Chertoff, 2018). So far, efforts largely focused on states' responsible

development and use of systems, respect for IHL and requirements for human control. The risk of diversion of LAWS and of their proliferation to malicious, non-state actors has not been adequately addressed (Chertoff, 2018) despite the risk of terror use of LAWS by such groups is far greater than that from use by militaries, where the introduction of any new weapons systems has to go from integration into active engagement requiring assurances of predictability and reliability.

The EU Parliament resolution of 02.27.2014 prohibits the development, production and use of autonomous weapons that allow attacks to be launched without human intervention, while the EU Council resolution of 11.15.2016 states that autonomous weapons must be governed by international humanitarian law and other relevant rules of international law (Pappalepore, 2018).

Conclusions & Recommendations

Lethal autonomous machines will enter future battlefields, incrementally. Tens of nations are developing or planning to develop autonomous weapons; they are unlikely to agree to treaties to limit technologies until they are more certain of their impact on war and the balance of power (Rabkin & Yoo, 2017). Malicious actors, not constrained by moral or legal considerations, will quickly adopt new technologies (Chertoff, 2018).

Should we prohibit LAWS? The LAWS characteristics demonstrate the inadequacy of the normative corpus of IHL, their

use poses complex ethical questions. The international community has long been debating necessary **restrictions** on the implementation of autonomy, even considering a ban on fully-autonomous systems (Chertoff, 2018). In 2015, more than 3,000 scientists including Elon Musk wrote an open letter calling for a ban on autonomous weapons (Open Letter, 2015). While treaties do not have 100% compliance, restraint is more driven by fear of reciprocity. Success in ban is often determined by the balance of how horrible a weapon is perceived versus its perceived military advantages. A ban would stop the development of systems more precise and less harmful for civilians. Autonomous weapons could limit the deployment of soldiers and minimize casualties. Combat operations often take place in difficult decision-making environments (the “fog of war.”) where facts may be difficult to discern.

Some argue that AI could make more coolly rational decisions than humans in the heat of battle (Kaspersen, 2016). Human capacities are becoming increasingly mismatched to the big data available, processing capabilities and speed of decision. I**n time-critical settings**, humans will be supported by machines providing better intelligence from multiple sources and actionable decision making information (Air Force Research Institute, 2011). Man-machine teams exploiting improved human-machine interfaces and/or direct augmentation of human performance will blend human and artificial intelligence for superior abilities. According to the world chess champion Kasparov *“If you can’t*

beat them, join them. Don't try and beat AI, merge with it. AI will help us to release human creativity. Humans won't be redundant or replaced, they'll promoted. From now we have no choice but to work with machines" (Quach, 2018).

Possible Immediate Solutions (on factual level)

What limits are needed on autonomy in weapon systems to ensure compliance with IHL? Limits on autonomy to ensure compliance with effective **human control.** The **"principles of humanity"** and the **"dictates of the public conscience"** are mentioned in article 1(2) of Additional Protocol I and in the preamble of Additional Protocol II to the Geneva Conventions, the ***Martens Clause***. "***Meaningful* human control** or **"appropriate levels of human judgement"** must be retained over weapon systems and the use of force with the human able to intervene in *real-time* (United Nations, 2016).

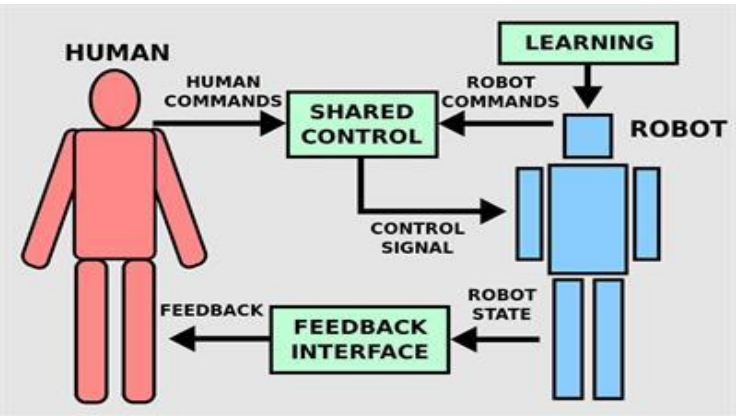


Figure 8. Example of shared human-robot control (Source: https://www.frontiersin.org)

Possible Immediate Solutions (in law)

Given the position taken on the issue by the EU, are finally outlined the possible legal solutions in the immediate, wishing, however, the prompt adoption of a specific regulation in the international arena. The issue is of vital interest for the entire defense sector. In a situation of considerable turbulence of the international chessboard, it is hoped the signing of an agreement that, **without prohibiting research & development**, **regulate the use of such systems** (Pappalepore, 2018).

Article 1 General principles and scope of application. In Additional Protocol I and in preamble of Additional Protocol II to the Geneva Conventions - the *Martens Clause*.

In cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience.

Article 36 New weapons. In Methods and means of warfare. Protocols Additional to the Geneva Conventions 12 August 1949

In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.

The art of the possible

Keeping humans in control of autonomous weapons and AI is an important element of UN Secretary-General António Guterres' action plan to implement the Agenda for Disarmament, *Securing Our Common Future*, presented in May 2018.

Humans will eventually try and build ethical robots gradually evolving their codes of conduct based on legal and ethical principles (Walsh, 2018). A system that could reason and make decisions based on IHL and Rules of Engagement (ROE) will need significant computer power (Anderson, 2017) and protection from being hacked to behave in unethical ways. Humans have to stay in the decision-making loop as a fail-safe. Protection from being hacked to behave in unethical ways.

States established numerous **arms and export controls** to restrict and regulate the transfer of weapons of mass destruction, sensitive goods, technology or services to hostile states and non-state actors. The international community **should implement export controls** also on LAWS, A transparent export controls regime for LAWS and their critical components could be established through the **Wassenaar Arrangement** (WA) platform (Chertoff, 2018). The WA maintains a list of dual-use goods and technologies that all signatories agree to incorporate into their respective national export control lists. Commercial enterprises seeking to transfer listed items must obtain an export license and all transactions are closely monitored by national export authorities. “States agree to report on the transfers and

denials of controlled items to parties outside the WA" and "exchange information on sensitive dual-use goods and technologies". (Chertoff, 2018). Such mechanism would mitigate the risk of transfer for military-grade LAWS and their critical components, to malicious actors.

Bibliography

Air Force Research Institute (2011) Technology Horizons. A Vision for Air Force Science and Technology 2010-30 Air Force Research Institute,155 North Twining Street, Maxwell AFB,AL,36112-6026

Anderson, M. R. (2017) After 75 years, Isaac Asimov's Three Laws of Robotics need Updating available at http://theconversation.com/after-75-years-isaac-asimovs-three-laws-of-robotics-need-updating-74501 March 17, 2017 12.03pm GMT [accessed on 28.05.2019]

Bazargan, S. (2013) Moral Equality of Combatants First published: 01 February 2013https://doi.org/10.1002/9781444367072.wbiee343

Davison, N. A legal perspective: Autonomous Weapons UNODA Occasional Papers, No. 30 on Systems under International Humanitarian Law [accessed on 28.05.2019]

Boyd, J. R. "The Essence of Winning and Losing," Excerpts in presentation format found on the web at http://www.defense-andsociety.org/fcs/ppt/boyds_ooda_loop.ppt, 1996. [accessed on 28.05.2019]

Chertoff, P. (2018) Perils of Lethal Autonomous Weapons Systems Proliferation: Preventing Non-State Acquisition http://www.css.ethz.ch/en/services/digital-library/articles/article.html/a4f0de69-1e0b-401e-871d-1956fa9063d3 [accessed on 28.05.2019]

FFI-NOTAT Eksternnotat 16/00336 Emerging Technology Concepts and Defence Planning in the Nordic Countries, February 1, 2016

Frost, C. (2010) “Challenges and Opportunities for Autonomous Systems in Space.” Speech at the National Academy of Engineering’s U.S. Frontiers of Engineering Symposium, Armonk, New York, September 23–24, 2010.

ICRC (2015) Autonomous Weapon Systems: Implications of Increasing Autonomy in the Critical Functions of Weapons, available at https://www.icrc.org/en/publication/4283-autonomous-weapons-systems [accessed on 26.05.2019]

ICRC (2015) International Humanitarian Law and the challenges of contemporary armed conflicts. 32nd International Conference of the Red Cross and Red Crescent, October 2015, 32IC/15/11, p. 44-47, available at https://www.icrc.org/en/download/file/15061/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf [accessed on 26.05.2019]

ICRC (2016)Views of the ICRC on autonomous weapon systems, paper submitted to the Convention on Certain Conventional Weapons Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS), 11 April 2016, available at https://www.icrc.org/en/document/views-icrc-autonomous-weapon-system [accessed on 28.05.2019]

Kant,,I. (1886) The Metaphysics of Ethics by Immanuel Kant, trans. J.W. Semple, ed. with Iintroduction by Rev. Henry Calderwood (Edinburgh: T. & T. Clark, 1886) (3rd edition) available at https://oll.libertyfund.org/titles/1443 [accessed on 03.05.2019]

Kaspersen, A., (2016) 3 technologies that will transform warfare, World Economic Forum available at

https://www.weforum.org/agenda/2016/02/3-technologies-that-will-transform-warfare/ [accessed on 28.05.2019]

Kindvall, G., Lindberg, A., Trané, C., Westman, J. (2017) Exploring Future Technology Development, FOI-R--4196—SE ISSN 1650-1942 June 2017

Macaulay, T. & Magee, T. (2018) The future of technology in warfare: From drone swarms to VR torture, Apr 18, 2018 available at https://www.techworld.com/security/future-of-technology-in-warfare-3652885 [accessed on 28.05.2019]

NATO (2010) Assessment of Possible Disruptive Technologies for Defence and Security, AC/323(SAS-062) TP/258, NATO RTO, February 2010.

NATO (2012) Disruptive Technology Assessment Game – Evolution and Validation, AC/323(SAS-082) TP/427, NATO RTO, April 2012.

Open Letter (2015) to the United Nations Convention on Certain Conventional Weapons." Future of Life Institute. Available at https://futureoflife.org/autonomous-weapons-open-letter-2017/) [accessed on 28.05.2019]

Quach, K. (2018) Don't try and beat AI, merge with it says chess champ Garry Kasparov 10 May 2018 available at https://www.theregister.co.uk/2018/05/10/heres_what_garry_kasparov_an_old_world_chess_champion_thinks_of_ai/ [accessed on 03.06.2019]

The Oxford Dictionary https://en.oxforddictionaries.com/definition/robot [accessed on 05.05.2019]

Pappalepore, P. (2018). Presentation: Implicazioni legali dell'utilizzo di mezzi autonomi dotati di intelligenza artificiale come sistemi d'arma, Workshop "La Trasformazione in ambito Difesa", Rome, 21-22.11.2018

Parkin, S. (2018) Killer Robots: the soldiers that never sleep. Accessed June 15, 2018 available at http://www.bbc.com/future/story/20150715-killer-robots-the-soldiers-that-never-sleep. [accessed on 24.05.2019]

Proud, R. W., Hart, J.J.,Mrozinski, R.B. (2003). Methods for determining the level of autonomy to design into a human spaceflight vehicle: A function specific approach, NASA Johnson Space Center: Houston, TX.

Rabkin, J. & Yoo, J. (2017) Disruptive Technologies to Upend Rules of War available at www.nationaldefensemagazine.org/articles/2017/10/31/disruptive-technologies-to-upend-rules-of-war [accessed on 23.05.2019]

Schwab, K, (2015) The executive chairman of the World Economic Forum, in a 2015 article in Foreign Affairs,

Sharkey, E, N. (2012) The evitability of autonomous robot warfare https://www.icrc.org/en/international-review/article/evitability-autonomous-robot-warfare International Review of the Red Cross Volume 94 Number 886 Summer 2012

Sullivans, J. P. (2011) When is a robot a moral agent? January 2011 DOI: 10.1017/CBO9780511978036.010

United Nations, Recommendations to the 2016 Review Conference submitted by the C

UNODA (2017) Occasional Papers – No. 30, November 2017 Perspectives on Lethal Autonomous Weapon Systems hairperson of the Informal Meeting of Experts, para. 2 (b); https://en.wikipedia.org/wiki/Three_Laws_of_Robotics [accessed on 28.05.2019]

Velez-Green, A. (2015) The Foreign Policy Essay: The South Korean Sentry—A 'Killer Robot' to Prevent War. Lawfare, March 1, 2015 available at https://www.lawfareblog.com/foreign-policy-essay-south-korean-sentry%E2%80%94-killer-robot-prevent-war. [accessed on 15.05.2019]

Walsh, T. (2018) Regulating the Third Revolution in Warfare, Australian Institute of International Affairs available at https://www.internationalaffairs.org.au/australianoutlook/2062-the-world-that-ai-made/

Wassenaar Arrangement (2018) "About us. avaialable at June 15, 2018. https://www.wassenaar.org/about-us/ [accessed on 28.05.2019]

DRONES & AI: INCREASING ACCESSIBILITY OF EMERGING TECHNOLOGIES AND SECURITY

Alexandra STEFANOVA, Anton PULIYSKI,
United Drone Community Association[1]

Abstract: As technologies evolve, we can no longer look at them separately. By combining them we are enabling and accelerating the innovation and development of the sector. Drones and AI are two emerging technologies, that even in the beginning of their development, undoubtedly show the enormous opportunities that they hide. Their nature and increasing accessibility enables them to be combined in different ways and to discover new dimensions of their vast potential. Taking the capacity of drones to gather large amounts of data and the capability of AI to analyze it, we are optimizing the beneficial results that we gather from both technologies. While looking for the optimal outcome, we should take into account that when they are misused, it could have serious implications for the security domain. This paper describes some of the opportunities and challenges this combination holds. We will present the results of our research we conducted in a period of 6 months about the possible combinations between the two technologies and the risks that they pose.

Key words: drones, AI, emerging technologies, increasing accessibility, security.

[1] A Bulgarian non-profit organization that aims to achieve safe integration and efficient operation of unmanned aircraft systems (drones) in the airspace. It emphasizes on security, safety, environment, privacy and data protection. In order to achieve our goals, we think it is important to create conditions for a broad dialogue between the administration, academic, expert, legal and business circles. The core values and driving force are sharing experience and willingness for mutual assistance. UDCA organizes and create educational articles, workshops, lectures and demonstrations. By analysing the legal, technical, aviation and ethical aspects, the association develops strategies to promote the use of drones and educate society.

Introduction

In recent years, we have witnessed a tremendous development in the field of Drones and Artificial Intelligence (AI). These two emerging technologies quickly demonstrated their potential applications not only in business but also in everyday life. At this point we cannot deny just how useful these technologies have been in our lives. This spike in their application is due to various factors such as technological development, leading to cheaper hardware, and availability of information for their use on the Internet. This expansion and accessibility of course hide potential risks, because technology evolves at a much higher speed than legislation. Even if rules are adopted for the use of these two technologies, the ability to apply and control them is also limited because of their expansionary nature. Everybody can get or make a drone, and train it as long as there is time, willingness and Internet access.

Drones

Drones as technology have been known since the 1940s, but their application has become available to the general public in recent years. With the proliferation of drones for non-military use, the problems began. Two of the most recent cases, that had a big impact, were just six months ago, when a drone near Gatwick and another near Heathrow Airport, forced authorities to close them. The number of cases of violation of privacy law increases daily.

There are a couple of reasons for that. First of all there are no common rules governing their use not only at national level but at global level as well. Global organization such as the EU and ICAO are making progress for the unification, but there is still a long way to go. There are many things over which the stakeholders have not yet reached an agreement. For example there are different terms that are used for the description of unmanned aircraft. The most popular ones are remotely piloted aircraft systems (RPAS), unmanned aerial vehicles (UAV), unmanned aircraft system (UAS) and drone, but they do not have an unified definition. Towards uniformity of definitions and to provide the fundamental international regulatory framework for UAS in 2011 ICAO published Circular 328. This Circular is a milestone towards the integration of drones throughout the world, in a safe, harmonised and seamless manner[2], although Circulars in the ICAO cannot introduce standard definitions applicable by all ICAO Contracting States. In Circular 328 there is a glossary where several terms are explained:[3] "Unmanned aircraft system - An aircraft and its associated elements which are operated with no pilot on board".

This year in the European Union (EU) two Regulations concerning the use of drones were adopted – Commission

[2] Masutti,A., Tomasello F., International Regulation of Non-Military Drones. Edward Elgar Publishing, pp.68,

[3] https://www.icao.int/Meetings/UAS/Documents/Circular%20328_en.pdf

Regulation (EU) 2019/947 of 24 May 2019[4] on the rules and procedures for the operation of unmanned aircraft, Commission Regulation (EU) 2019/945 of 12 March 2019[5] on unmanned aircraft systems and on third-country operators of unmanned aircraft systems. In Regulation (EU) 2019/947, a similar definition for UAS is given – "*an unmanned aircraft and the equipment to control it remotely*"[6].

From the differences in the meaning of the definitions and the way in which these terms are used by both lawyers and business, we can conclude that at this stage the scope of the existing regulations is still not fully clear and that in the coming years it will continue to improve the rules. The common thing that is in all of these definitions is that these are flying devices with no pilot on board.

Secondly for the successful integration of drones it is particularly important the way these rules are introduced to the society.

In the process of pursuing the goals of the organization, we realized that the integration of drones could only be successful if all related aspects are taken into consideration. For this we have used the **holistic methodology**. We must think of drones as being a piece of the big picture, not as something new and

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1561974410357&uri=CELEX:32019R0947
[5] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1561975633929&uri=CELEX:32019R0945
[6] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1561974410357&uri=CELEX:32019R0947

completely separate. When talking about the integration of drones in the airspace, several related aspects are distinguished as fundamental. In Regulation (EU) 2019/947[7] the European Commission has highlighted those that are vital for the integration of drones. According to the European act, these are - safety, security, privacy, data protection and environment protection. This list of priority directions is a good start, but it is not exhaustive. In the process of in-depth analysis, we can also pay attention to - healthcare, shared responsibility, insurance, etc. (see Figure 1). In order to have a smooth and sustainable model of integration, it is appropriate to treat each of them proactively by examining possible issues and creating the conditions for their preventive solution. The aim of our work in this paper is to draw attention to one of these related aspects, namely security and the challenges that we face regarding the rapid proliferation of drones. Every day, new applications and new connections are emerging in diverse areas of science and business. This in turn leads to the need to adapt security procedures and policies. The main reason for this expansion is the ever-increasing availability of the drones due to the reduction of the prices for their component elements. Their price is also initially lower than that of other aircraft, because the absence of a pilot reduces the flight weight, the cost of the construction and the risk of falling of these devices.

[7] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1561974410357&uri=CELEX:32019R0947

Figure 1

In recent years, technology development has allowed manufacturers to increase the scope of consumers - not only for professional but also for private use. This new wave gained popularity among people who did not have the financial opportunity or the need to buy a drone. The increased accessibility has two directions - technological and financial.

For the last 7-8 years, the cost of drones has decreased significantly. Now you can get a drone for less than 80 euros and

it is just as effective in taking video and pictures as is the drone that costs 400 euros. Yes, there will be a difference in the quality of the material, but it will not be so significant. The main function will be achieved – capturing an object. When the price is decreasing, accessibility increases. Today in the EU it is easier than ever to get a drone. They are available both online and in different types of shops – toy shops, mobile operators, electronic stores, etc. This naturally leads to an increase in their number.

Everything indicates that in the coming years we will witness a precedent throughout aviation history. For the first time so many participants will enter the airspace at once. That means the risk they hide is increasing too. We must also consider that the accessibility has led to the development of these technology itself. The number of people who develop projects with application in different areas has increased tremendously, and this also has led to a significant increase in security threats.

When we speak about the risk that drones pose to safety and security we have to know that risk assessment process is based on an impact (the impact that an event may cause) and the probability of its occurring. Until recently, there was no dispute about the impact of such an event, but the probability of actually happening was small. This trend is rapidly changing, as the number of drones is increasing.

Drones themselves are recognized as a potential threat to safety and security in the aviation sector, but the increased accessibility and the opportunity for combining them with another technology

reveals new aspects. We are already talking about possible security issues with areas far beyond the physical dimension. Initially, the drones were considered as a means by which something physically restricted can be accessed - the transfer of prohibited objects to the prison, the capture of secret objects etc. But now the forms in which drones can threaten security in certain areas such as personal security, group security, corporate or national security, is increasing due to their proliferation. It is only a matter of time before we discover new and innovative methods for the use of drones.

Artificial Intelligence

In the media and scientific field, AI is equated with other terms such as Machine learning and Deep machine learning. Other terms that are used together with AI are Data set and Open source database. The definition that we use in this article for AI is from Artificial Intelligence for Business, there AI "refers to manifold tools and technologies that can be combined in diverse ways to sense, recognize and perform with the ability to learn from experience and adapt over time"[8]. To be precise, at this stage AI in its full potential still does not exist. Machine learning and deep machine learning are used to train systems to perform certain actions such as object recognition, process automation, etc. The difference between AI and machine learning is best described as "Machine learning is a core concept which is

[8] Akerkar, R., Artificial Intelligence for Business. Springer International Publishing, pp. 3

integral to AI. In machine learning, the conceptual models are trained based on data and the models can predict outcomes for the new Data sets. AI systems try to emulate human cognitive abilities and are context sensitive. Depending on the context, AI systems can change their behaviors and outcomes to best suit the decisions and actions the human brain would take.[9]

On their own drones and AI have demonstrated their value[10], though none have been mainstreamed enough that anyone can yet estimate their true maximum potential, or if an upper limit even exists. We can accelerate the development of these emerging technologies by combining them.

They are becoming more and more accessible, because of two main elements. First we have hardware and its affordable price. For example on the market there are several products that are designed to facilitate the development and deployment of deep neural networks. They have the ability to perform these complex mathematical operations required for modern deep neural networks at high speed and low power. Their price is around 100 dollars. Secondly, anyone with access to the Internet can take advantage of various sources such as Arxiv, Github, Paddle Paddle, Keras, MXnet ect. containing Data sets. There are also teams that publish their own projects and you do not even need

---

[9] Deshpande, A., Kumar, M.,Artificial Intelligence for Big Data. Packt Publishing, pp 21

[10] https://www.fastcompany.com/3032977/when-technologies-combine-amazing-innovation-happens

to know how to code to actually train a neural network. Like any other technology, accessibility is a two-edged sword. It is the basis of this rapid development and only because of it these new dimensions are being discovered every day. At the same time, however, such rapid development does not allow for adequate measures to be taken to ensure that this knowledge doesn't fall in the wrong hands. Everyone can have access to this information and it can be used with the same ease to detect cancer at an early stage, as well as to assassinate people.

To make it clearer how the same process can be used for two very different reasons, on Figure 2 we have given an example – Speech recognition. Each of us who owns a smart device has encountered in one way or another speech recognition. For example a person is driving a car and want to call the dentist and make an appointment, or want to ask the device assistant for suggestion where to have dinner, or need to be reminded that has an appointment tomorrow at nine. In all these cases the device is following this procedure – trigger word, speech recognition, intent recognition, command execution.

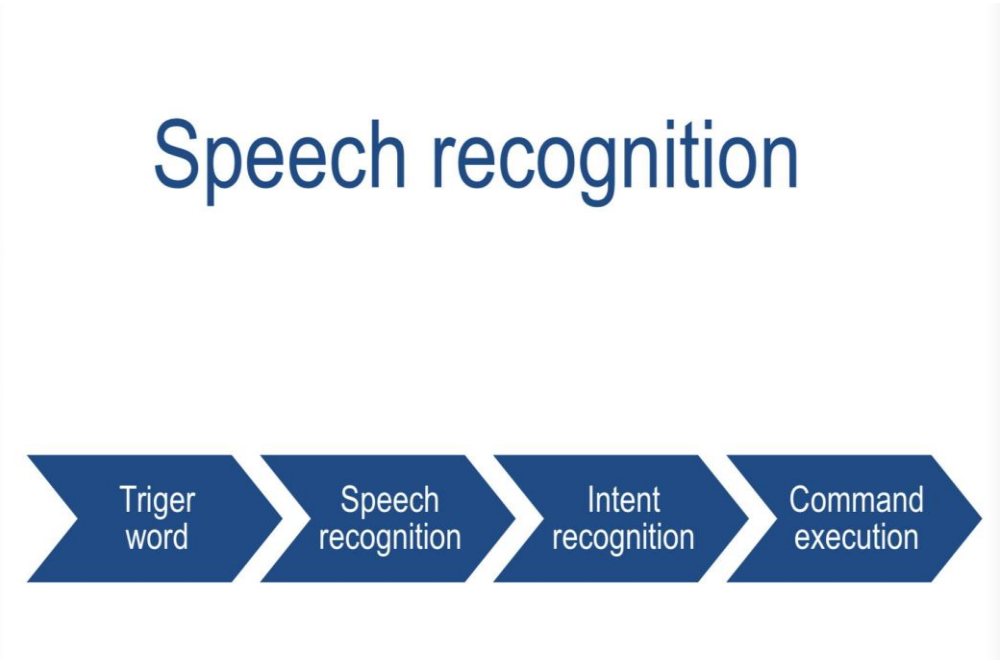


Figure 2

In the beginning, there are always mistakes – instead of Mike it understands May, or instead of chicken, it understands chilli. But every mistake trains the system and it gets better. Every step that you see here is a very complex equation. And the advantage of the open source policy is that a person doesn't need to write them, he can take them and change them to fit his purpose. Let us now imagine that this person wants to train his device to recognise a trigger word and a certain voice and add a drone in the picture. In this case the drone can be left in a building in sleep mode and when the specific person is in the room it can activate, record a meeting or execute a different type of command.

In the past six months our team has developed different projects that have combined drones and AI. Two of them were focused

on examining the potential threats that two technologies pose to security domain. The names of the projects are “Mini SeeK3R” and “Stinger Drone”. The first is a 25 gram drone toy, but when it is equipped with a camera with a transmitter and combined with trained neural network to recognize different objects, the toy aspect fades away. We have proven that if we have a machine with a trained neural network it can recognise more than 80 objects, including people (Figure 3), with a low quality camera (640x480px). It is important to note that this drone is not in the scope of the above mentioned regulation – 250 grams is the minimum weight there. The price of this drone is around 32 euros. Its physical specifications make it possible for it to execute certain operations undetected. Depending on the intent of the person, who use them, they can pose a security breach and can compromise privacy.

Figure 3

The second drone is the Stinger drone. It is a proof that the world of cybersecurity does not remain unaffected by the increasing availability of Drones and AIs. The goal was to create a cheap drone that is equipped with tools for pen testing of computer networks. Its price is around 400 US dollars, and it is equipped with hardware that runs Linux Kali[11] operating system and radio frequency interception equipment that operates in different ranges. Thanks to its built-in programs for automated execution of certain processes, it shows that such a device can act relatively autonomously in a particular environment. This is the point where Drone, AI and Cybersecurity intersect.

Conclusion

The distribution of drones and AI, the availability of different resources has a potential that can be used in different ways. Whether they are used properly depends only on the person who uses them and his intentions.

One of the aims of this article was with limited resources and free access to the internet to assemble a device, that is practical and useful - “Mini SeeK3R” can detect up to 80 objects and does not fall within the existing regulation.

The other aim of this article was to emphasise on the importance of understanding the impact of emerging technologies on security. Different new aspects are appearing in personal, group,

[11] Kali Linux is a Debian-derived Linux distribution designed for digital forensics and penetration testing. It is maintained and funded by Offensive Security Ltd.

corporate and national security. It is necessary to make new procedures and policies and also update old ones, so that we can adequately and in time respond to the new challenges that these technologies hide.

ADDITIVE TECHNOLOGIES AND THEIR INTEGRATION INTO MOBILE 3D PRINTING ENGINEERING LABORATORY

Dr Iliyan Hutov (Bulgarian Institute of Defence)[1],

Viktor Stoyanov (BulMould)[2],

Violetka Dencheva (GosVik Ltd)[3],

Atanas Zhelev (Digital Architects Ltd)[4]

Abstract: New technologies, such as additive manufacturing of parts and components using 3D printers, are widely implemented in a variety of fields, such as aviation, automotive, medicine and defense. Through the accumulated knowledge from these industries and through careful consideration of the specific challenges for resolving logistical problems in crises situations and natural disasters, a new technological solution can be developed to further increase the capabilities of individual organizations to address these issues. Within the framework of this project, specific technical solutions are proposed, namely the choice of technologies and the way and organization of the communication with other structures. Innovation is the solution offered by the team. The Mobile 3D Printing Engineering Laboratory is a standard 20-foot volume container for air, land and water transport, equipped with various additive manufacturing tools, and capable to

[1] Associate Professor in Bulgarian Institute of Defence-BDI, National coordinator for the NATO STO program

[2] Co-Founder of AccForge 3D Print, private consultant in realization of complex 3D Printing Parts, FEA and CFD engineering project, degree in the field of Aerospace Technology, Major: Aircraft Construction and Thermodynamics, Stuttgart University Germany.

[3] Project coordinator and nanotechnology expert of plastic composites, TANOCOMP EU Project, Zaragoza, Spain.

[4] Master Degree in Architecture form the University of Applied Arts Vienna. Degree in Engineering from Tokyo University of Science, Institute of structural and civil engineering architecture, Prof. Kawamukai Masato.

increase it is working area by 200%. Through the careful research by team of professionals, highly experienced on development of Antarctic Basics and through discussions with CMDR COE, the aim of this project is to propose a mobile engineering laboratory equipped with additive technologies as part of a strategy for dealing with crises situations and natural disasters. The proposed solution solves basic logistics problems and allows the lab to be used in various civilian projects and locations around the globe.

Key words: mobile engineering laboratory, 3d printing, additive technologies, innovative construction.

Problem definition and state of the art in the field of research related to the project

Additive manufacturing plays a key role in the developed Mobile 3D Printing Engineering Laboratory (M3DPEL). Analysis are made over the primary means of 3D printing of parts, the necessary technical means for finishing manipulations of the 3D printed parts, and over the necessary working premises for such activities and the communication structure with the different subdivisions.

3D printing or additive manufacturing is a new technology for production, mostly for single complex metal, polymer or other parts using different row materials for scientific, military and industrial purposes. In recent years, a number of industrial pilot projects have been carried out, such as the DAIMLER AG (1), with the aim of finding a new strategy for the production of vehicle spare parts, namely a production through 3D printing. In this way, there is no need to over-produce parts and to provide rooms with special storage conditions. A key element in this new strategy is

the need to use 3D printers and perform the necessary additional work on the individual parts. The popularity of the additive technologies is due to the fact that they use an innovative approach in the process of creating three-dimensional hard objects from a single digital file. Creating 3D parts through this process is based mostly on the material additive process. This is achieved by layering successive layers of the material, each of which can be considered as a thin horizontal cut in the cross-section of the final object. Three-dimensional printing allows to produce sophisticated (functional) objects using less material than traditional manufacturing methods. In the interview with Mr. Shane Wahl (2), HP's Chief Technical Officer, in Bulgaria in 2016 by Mrs. Kozubarovasa, he describes 3D printing as the technology that will completely change the way we live. These words are supported by the fact that only for the period of 2016 to 2019, a 3D printer from the Industrial Revolution 4.0 is already on the market. Other leading manufacturers also offer completely new solutions for the production of parts, with the most prevalent one – the Selective Laser Melting Technology (SLM), the bases of 3D Metal Printing. In recent years, there has been a remarkable development in this area and the emergence of new companies producing 3D metal printers, mainly from the USA, England, Germany and Australia. From 2015, this industrial development is also a priority in Russia. However, by year 2018 there has been no formal announcement to plan the production of 3D metal printers in any Eastern European state. Only in the middle of 2019 AccForge, in partnership with BulMoold Ltd. and

GosVik Ltd., from Bulgaria, after carrying out technical expertise with various scientific organizations, jointly started the development of its own prototype model for 3D metal printing, whose dimensions and weight are used in this project as reference values. The project AccForge 3D Metal Printing Bulgaria also serves to analyze and identify technical solutions to solve problems with the use of additive technology in areas with extreme temperature conditions such as the Bulgarian Antarctic Base and the Bulgarian Antarctic Institute as a national operator of Bulgarian Antarctic activities and member of the Council of Managers of the National Antarctic Program (COMNAP) with which an agreement on technical and scientific cooperation has been signed. In this subject, there have been technical discussions with members of the leadership of the Crisis Management and Disaster Response Center of Excellence (CMDR COE), located in Sofia, the Republic of Bulgaria and the Bulgarian Defense Institute “Prof. Cvetan Lazarov”.

The advantages of the additive technology are the combination of technical processes, such as casting and sputtering of metal, without the need for metal billets and the provision of injection molding machines (3) (4). In 3D metal printing, after the part has been prepared using digital tools, it is directly manufactured. With the use of specialized software, such as OptiStruct by Altair Engineering (5), another advantage of this method can be observed, namely the ability to perform topological optimization of the parts themselves. After consultations with experts in

topological optimization from GosVick Ltd., a representative of Altair Engineering for Bulgaria, it was confirmed that the parts produced by this method can be 40% lighter than the parts produced by conventional metal injection molding (5). With the use of fluid simulation software, it is possible to develop and then manufacture with 3D printers complex geometry details that can significantly improve heat exchange or reduce pressure loss while retaining its own weight. (6). At present, the great challenge for all scientific and industrial organizations is finding an innovative strategy to integrate this production process into multidisciplinary projects in order to maximize the efficiency and expedience of the resources and address the problems of modern times. There are active companies from different sectors working in this direction, such as automotive, medical, aerospace, software, and there will be even more opportunities for the use of additive manufacturing in other industries in the near future. The main advantage of this method is the significant reduction in the time for production of complex parts and the capability to join the knowledge of experts from every point of the globe as well as the possibility to produce complex parts, designed by specialists with experience in other fields different from the respective field of application of the subject part, bringing very valuable interdisciplinary knowledge to the production process.

Following initial study by the team of project M3DPEL, it has been found, so far, only one similar development by the Rapid

Equipping Force (REF) of the U.S. Army in the scope of the project US Army Deploys 3D Printing Labs to Battlefield 2012 by the company (6). However, the difference with M3DPEL is that the proposed solution is for military purposes only and the technology used for 3D printing is limited to the use of polymers. The common similarity of the two projects is the use of transport module type 20-foot containers, however, in the proposed US project, there are no major modifications to the container. In project M3DPEL, by means of additional technical solutions, the volume of the enclosed work space is increased from 20-foot, when it is transported, to 60-foot when is ready to use, without any negative impact or constraints on its mode of transport. In both developments, standard land transport can be used to move the 20-foot container base as well as alternative sea and air transport. In both projects, it is necessary to provide a core team of experts to the mobile 3D printing engineering laboratory. The team is composed of two to three people, one of which has a leading function and a high level of expertise in solving problems using additive technologies.

Design and Technical Solutions for Mobile 3D Printing Engineering Laboratory (M3DPEL)

Preliminary analysis of current problems and the state of the art in the research topic of the project concerns the following main points, to which is offered a constructive and organizational solution with the purpose of optimal integration of a mobile 3D printing engineering laboratory in the scope of The Crisis

Management and Disaster Response Center of Excellence to solve logistical challenges in building a sustainable strategy for crisis and disaster response.

- Leading criteria for choosing base technology.
- Selection of machines and the need to modify them to meet the specific conditions for their use in crises and disasters.
- Transport and logistics of M3DPEL to a place of use. Autonomous power supply.
- Construction of M3DPEL.
- Ability to upgrade and fit with other additional technical modules.
- Possibility for modifications depending on climatic conditions.
- A team of specialists working in a mobile 3D printing engineering laboratory.
- Communication and compatibility with NATO teams and subdivisions in order to organize the production process.

Selection of leading and supportive technologies for the assembly of mobile 3D printer engineering laboratory in order to maximize efficiency and multidisciplinary approach of the manufacturing process

Leading criteria for choosing base technology as the primary technical solution in the M3DPEL assembly, adaptable to diverse logistical challenges in crisis areas for which is necessary to find an adequate universal solution, are as follow:

- Technology that requires a minimum of technical equipment and offers complex production capability.
- Possibility of using them in various scientific fields, including: Engineering Sciences, Medicine, Oceanography, Geodesy and Earth Sciences, and all other new opportunities for the integration of such solutions.
- Decentralized ability to find a technical solution by teams located at different points of globe.
- Merging different technological production processes to reduce dependence on the need for different types of machines needed to produce details.
- The use of a variety of materials from different manufacturers to solve technical issues in a wider range.
- Minimizing the waste in the production of metal parts and completely eliminating waste in similar polymer production processes.
- Possibility for parallel work of experts from different teams.

The chosen leading technology, as the optimal technical solution, which largely fulfills the above-mentioned criteria for choosing the leading technology for M3DPEL, is namely the Additive Manufacturing of metal and polymer parts. The advantages of this production method are most often seen in the development of single complex parts and in small series production for scientific, military and industrial purposes. A great application of

this technology is currently being observed in the areas of aviation, aerospace, automotive and medicine.

Machinery selection and modifications needed to meet the specific conditions for their use in crises and disasters areas

The production of parts using 3D metal printers is based on the material additive process and this is most often achieved by layering successive layers of melted metallic powder, each of which can be considered as a thin horizontal cut in the cross-section of the end product. Three-dimensional printing allows to produce sophisticated (functional) shapes using less material than traditional manufacturing methods. Leading manufacturers of 3D metal printers are located in America, England, Japan and Germany. Over the years, Russian companies offer 3d metal printers on the market, however there is still lack of specific information in Europe about their solution. Interesting fact is that Eastern European countries have so far not stated ambitions to produce prototypes of 3D metal printers or to modify existing products. BulMoold Ltd. and GosVick Ltd. from Bulgaria together with AccForge, as part of the team in this development, have begun a process of technology transfer and production of prototype for new model of 3D printers under the trade name AccForge 3D PRINT. Important in this project is the fact that in the same time as the production of the first prototype, research and technical proposals for its modifications are made for its use in: extreme meteorological conditions, transport as part of M3DPEL, the possibility of production of parts from metal powder with a wide range of tolerances. These studies will allow the

development of methodologies for the modification of industrial 3D metal printers to be used for the purpose of such projects, namely in adverse weather conditions, high ambient air humidity, dustiness and different vibrational effects during transport.

In addition to the use of two 3D metal printers, the possibility of a combination of one 3D printer for polymers and one for metal as part of the laboratory equipment is optional for the M3DPEL. In this way, the M3DPEL's production capabilities are completed not only for metal, but also for polymer parts and will allow to solve a wider range of tasks.

Transport and logistics of M3DPEL to a place of use. Autonomous power supply.

An optimal mobility analysis of M3DPEL has been carried out. Considering transport without the need for special vehicles and by comparison with other similar models proposed by the Rapid Equipping Force (REF) of the U.S. Army the team made a choice to deploy all technical equipment in a standard 20-foot container. Such container offers the opportunity to transport it to different parts of the world from civilian and military subdivisions, both by land, by air and by water.

Construction of M3DPEL

With careful consideration of the technical solution for the Expeditionary Lab Mobile (ELM) as part of the REF, we can observe that one of the main problems defined in the initial study is the placement of the necessary work equipment and machines in a limited volume of a 20-foot container. The need to provide a

closed manufacturing process requires, in addition to the installation of 2x 3D metal and polymer printers, a number of additional machines such as 1x laser scanner, 1x plasma cutter, 1x metal CNC mill, 4x desktop computers, 1x satellite dish, 14x solar panels with sizes 1.0x0.75m, air conditioner, insulating panels, batteries or diesel generator. Additionally, there are working desks where field experts can connect with other experts from different parts of the world through satellite communications. The power supply of the equipment can be autonomous with solar panels and batteries or externally with a diesel generator, however, in both cases it is necessary to provide a working environment with a certain temperature based on the current requirements of the manufacturers of 3D metal printers. In order to ensure that M3DPEL can be used in a wider range of extreme ambient temperatures and under additional negative impacts associated with transportation and polluted environments, developments are being made to produce new generation of 3D printers from AccForge 3D Print that allow to exploit 3D metal printing under extreme conditions. All this analysis led to the conclusion that the transport of a 20-foot container will allow maximum freedom in choosing a way of delivery (land, sea or air) to M3DPEL to the disaster site, but the workspace volume is totally inadequate to accommodate the entire range of machines and additional equipment for M3DPEL operation.

This is the reason why a Digital Architects Ltd., an architectural and engineering firm with large experience in the design of complex architectural constructions, based in Vienna Austria has been summoned to the team of GosVik Ltd. and BulMoold Ltd. to develop new strategy for the construction of the mobile 3D printing engineering laboratory, which allows the entire M3DPEL and the corresponding equipment to be transported in a compact form into a 20 foot container (see Figure 1)

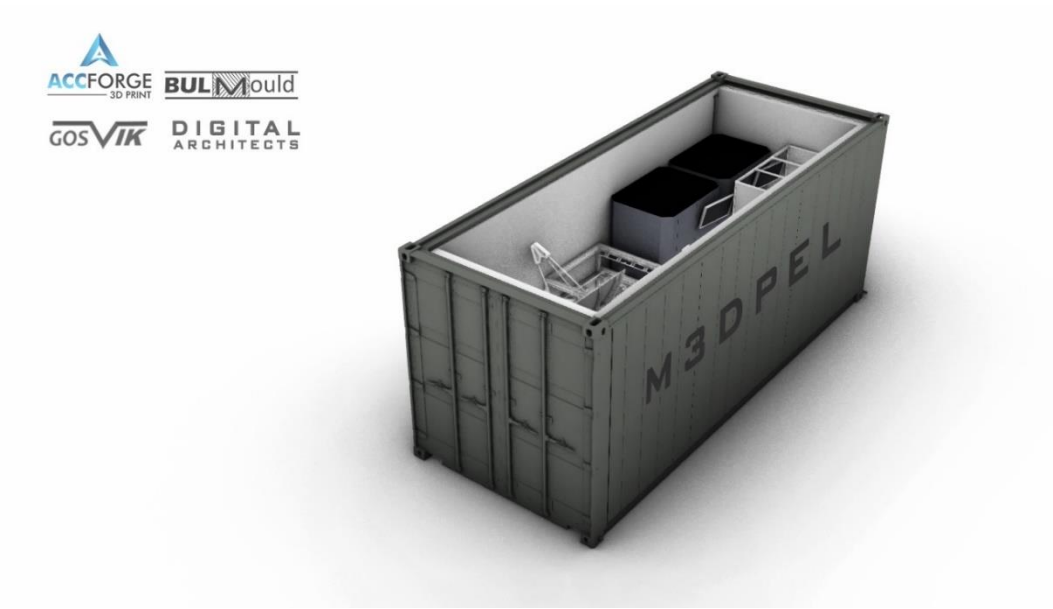


Figure1. M3DPEL in transport mode

and upon reaching the work area, the laboratory can be deployed in several steps, including collapsible container side walls (see Fig. 2),

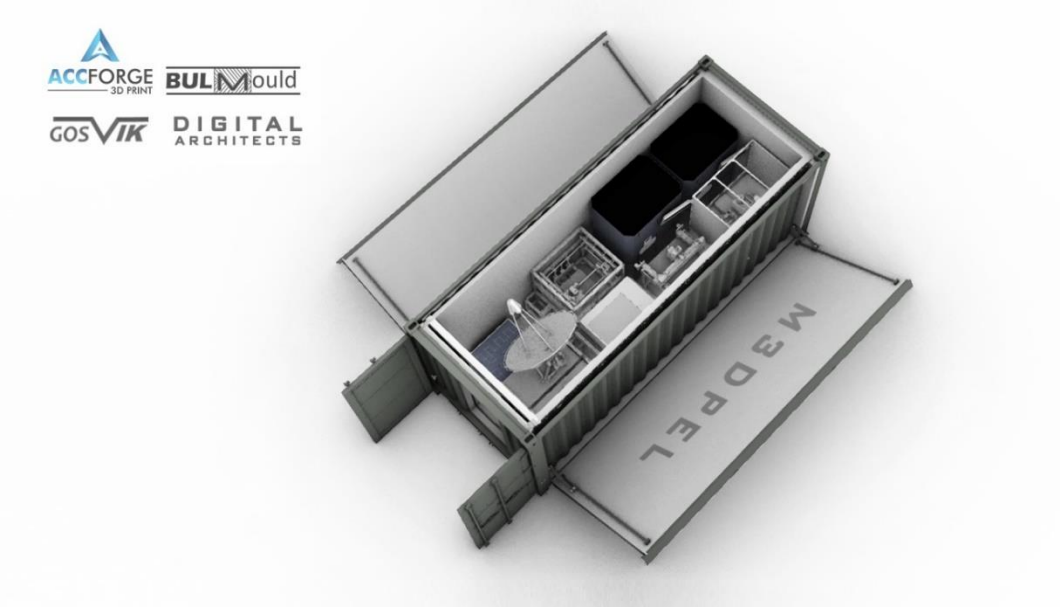


Figure 2. First steps to deploy additional work spaces

providing a stable supporting structure and floor area for additional work space. (see Figure 3).

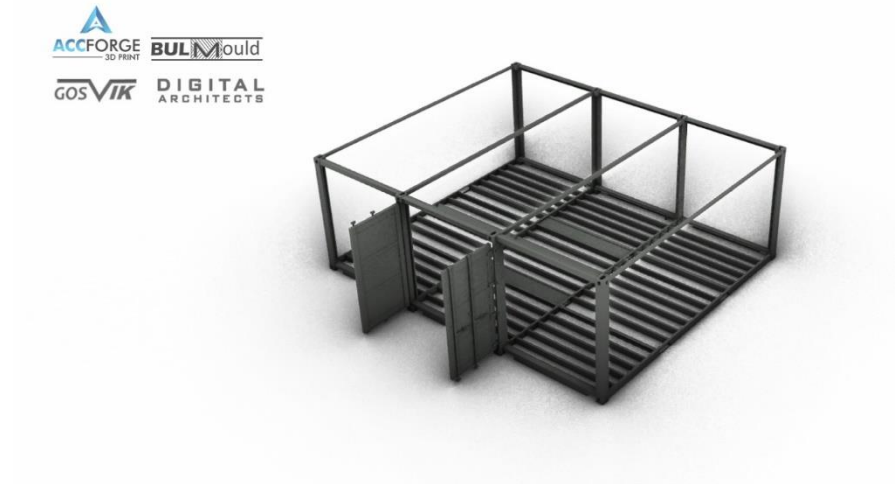


Figure 3. M3DPEL caring structure

The transported container includes all the structural elements for its construction, including panels of varying degrees of insulation and beams for the mounting of the roof structure and side walls, as well as solar panels, batteries or alternative sources for powering the M3DPEL. After being fully build up the M3DPEL increase in size from an initial volume of 20 feet, to a final working area of 60 feet (see Figure 4), allowing all the technical capabilities involved in the manufacture of 3D printed parts to be installed.

Figure 4. Above, M3DPEL fully deployed. Down, ISO view to the right front view

Constructional sketch of the different steps in the M3DPEL deployment, including two industrial 3D printers and all additional equipment located inside is shown in Figure 5.

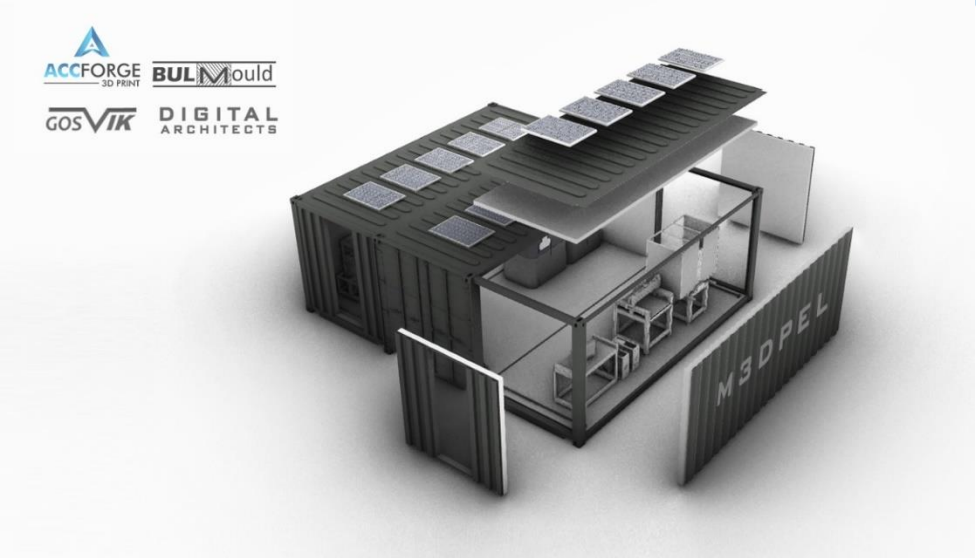


Figure 5. Construction drawing of M3DPEL with a maximum working area of 60 feet

The achieved effect of multiplying the work area has a positive impact not only on improving the operating conditions of the equipment operators and other workers, but also allows the use of free areas for additional purposes occasionally occurring during the operation of M3DPEL in the areas of disasters, and the installation of new machines to complement the M3DPEL's functionality. The proposed basic version of the M3DPEL and the location of the main technical devices, such as 2x 3D printers, 1x laser scanner, 1x plasma cutter, 1x metal CNC mill, and others is visualized in Fig. 6.

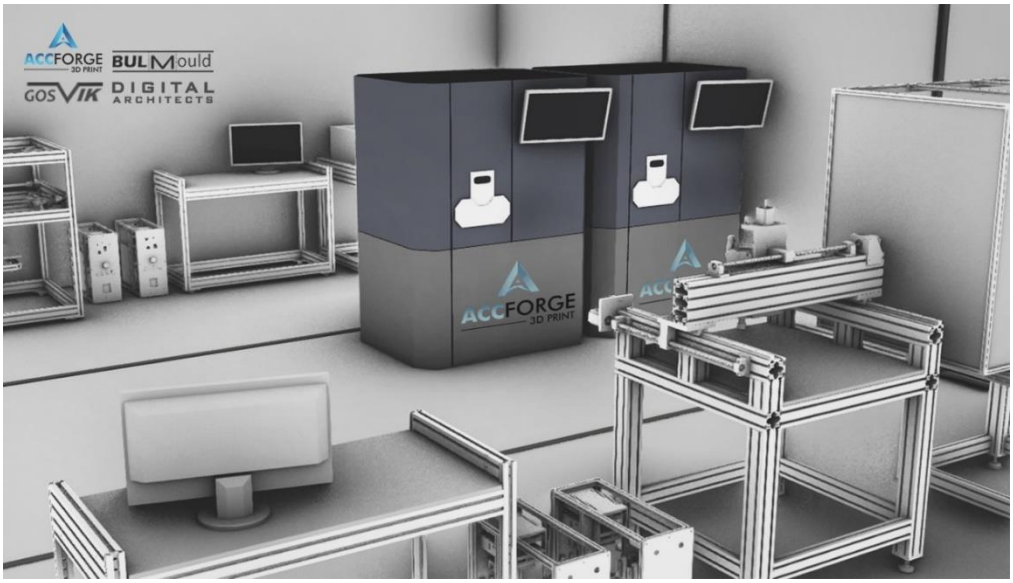


Figure 6. Layout of work area in M3DPEL

Ability to upgrade and fit with other additional technical modules.

M3DPEL allows to solve the major challenges in the production of parts, both metal and polymer, in the disaster areas, which significantly increases the possibilities of coping with problems caused by unexpected logistical delays. The solution proposed in this work can be further developed and adapted to the specific situation. An option is provided whereby M3DPEL plays a central role in a set of other technical solutions. On-line connection between individual M3DPELs located in different disaster areas, and wider communication centers can be realized as part of the disaster and accident management strategy. Due to the 60-foot capacity, enclosed and air-conditioned additional machines tailored to the requirements of the specific situation can be pleased inside the individual M3DPELs. The additional access

doors provided in the two M3DPEL extensions are intended to attach additional 20 or 40 ft containers if necessary. The M3DPEL is a central technical unit in a whole set of work rooms and serves as a link to all peripheral technical modules.

Possibility of modifications in response to climatic conditions

Preliminary analysis of possible M3DPEL operating temperature ranges indicate that a similar solution can be used at both -40 ° C in Antarctica and 50 ° C in desert areas. The large temperature range necessitates the possibility of installing additional insulating panels in the M3DPEL walls, which in turn will save the energy needed to heat or cool the work space.

A team of specialists working in the M3DPEL.

A team of specialists who will serve M3DPEL is foreseen to consist of two, up to a three people. Minimum one expert, is required to have in-depth knowledge in the field of additive technology and the production of metal and polymer parts using 3D printers. Due to the fact that satellite communications are used for connection with other M3DPELs, as well as with experts and coordination centers it is not required to locate large teams of specialists in the disaster area in order to operate the M3DPEL. The members will have the main task of localizing the problem, passing the information to the coordination centers or expert teams, and by receiving a ready-made technical solution to the problem, to produce the specific parts. This workflow is an innovative strategy to solve logistical problems while involving

experts from different technical fields with the common goal of finding a multidisciplinary solution to the challenges posed in crisis and disaster. At the same time, the optimal utilization of the available human and material resources is achieved in the time frame needed for the production of key elements necessary for the successful technical implementation and effective crisis and disaster relief.

Communication and compatibility with NATO teams and subdivisions, in order to organize the production process

As in point 2.7, it was mentioned that M3DPEL can function in close contact with expert teams and communication centers at any point on the ground trough an internet connectivity. Satellite link is provided to coordinate the M3DPEL team's operations with other logistics support units. In order to achieve maximum compatibility with other 3D printing teams, it must be considered the fact that there are currently a variety of software products and 3D printers that do not work with competing ones. For this reason, the AccForge 3D Metal Printing, BulMoold and GosVik team are summoned in the development of a prototype printer with the ultimate ability to use open source data in extreme conditions. In addition, the possibility of using other products for 3D printing from different manufacturers are explored. The aim is to achieve maximum compatibility, not only at the level of communication and integration into the network of coordination centers for disaster relief, but also at the technical level, namely the use of the largest possible range of raw material suppliers for the production of parts.

Conclusions

With the introduction of 3D printing, as an indispensable part of today's digitalization, and as an innovative technology in the development of single and serial production of complex parts, with different functionality and from diverse materials, they are new opportunities for implementing such solutions available to numerous scientific fields including: Aviation, Defense, Medical and Automotive, all of which contribute to improving the quality of scientific excellence on a local and global scale and have multidisciplinary nature.

The aim of this work is to use the collected scientific and practical knowledge in 3D printing as well as on the basis of the international experience in scientific fields (engineering and medicine) of the members of the international team and experts from AccForge 3D Print, BulMould, GosVik, The Bulgarian Antarctic Institute as, national operator of Bulgarian Antarctic activities and member of the Council of Managers of the National Antarctic Program (COMNAP), Bulgarian Defense Institute "Prof. Cvetan Lazarov "and the Architectural Bureau Digital Architects from Austria with large experience in the urbanization of marine regions and redevelopment of post war cities, to develop a strategy for the equipment and functionality of the M3DPEL – Mobile 3D Printing Engineering Laboratory as part of a multidisciplinary project to achieve a new technical solution for logistical challenges in crises and disasters situations. The main advantage of this type of innovative manufacturing laboratory is

the multidisciplinary approach to solving challenges from different scientific areas, overcoming logistical problems and providing individual technical solutions tailored to the specifics of each assigned task. Another important advantage of the solution proposed by the team in this project is the fact that this approach allows to minimize the waste product in the production of metal parts and to completely eliminate the presence of waste with similar polymer production techniques, which will lead to preservation of the biological and ecological balance of protected natural areas. With regard to the multidisciplinary application of a mobile 3D printing engineering laboratory, it is necessary to note the fact that with the help of this technology it is possible to manufacture both engineered parts and full medical devices. This is possible due to the fact that experts from different scientific fields can develop at the same time a specific solution for a problem from anywhere in the world and which solution can be transmitted digitally to the team located in the M3DPEL in the disaster zone and produced on site without need of specific knowledge and regardless of the weather conditions. M3DPEL brings together the knowledge of people from international teams that are summoned to The Crisis Management and Disaster Response Center of Excellence for the production of specific and, if necessary, unique parts. This strategy of uniting scientific excellence, digitization and innovative manufacturing techniques provides the fastest and most effective way to produce and implement parts and devices in a very short period of time.

Bibliography

V.Stoyanov at all „Numerical study of heat transfer between impinging gas jets and solid surfaces “, 8th International Scientific Conference “Engineering, Technologies and Systems” TechSys 2019 Plovdiv, Bulgaria

V.Stoyamov, K. Matauschek, M. Waga, F. Lechler, P. Nikoleizig HELLA GmbH & Co. KGaA. , Patent application: E06431 from 13.11.2017 „Hybrid headlight housing“

V.Stoyamov Impetor GmbH and S.Recker /Elektror airsystems GmbH „Reducing development costs for industrial fans using imulation “ Dynamics ISSUE38 Cd-Adapco Juni 2015, USA

M.Grundler, V.Stoyanov at all „Hochwärmeleitfähiges Polymer-Compound für LED-Scheinwerfer“, 6. Workshop „Brennstoffzelen-Allianz“ im Zentrum für Brennstoffzellen Technik, April 2013, Duisburg

M.Korolova, A.Zhelev, Digital Architects Ltd., Altair Engineering Inc. „Wood Carbon Composites for Archietcture“ – developing innovative production and construction methods for complex architectural projects, Composites World Magazine, April 2018, USA

M.Korolova, A.Zhelev, I.Suchak, Digital Architects Ltd., Altair Engineering Inc. „Adaptive Intelligent Architecture“ – developing innovative wood carbon composite product for complex 3D curved large span roofs, Composite Solutions Magazine, September 2018, Italy

CONTEMPORARY CRISIS RESPONSE: THE CASE FOR INFORMATION 'WARFARE'

Dziugas Kuprevicius,
CMDR COE Intern 2019

Abstract: Asymmetric warfare encompasses hybrid warfare, which, in turn, encompasses information warfare. Information warfare consists of propaganda, fake news and establishment and furthering of "narratives". Recent security developments, especially in Europe since 2014, have led to paradigm shift and hybrid and informational threats being included as priorities by governments and security organisations. Information attack can involve state-sponsored practices in combination with other hybrid techniques, such as cyber activity, guerrilla warfare and terrorism. As with conventional warfare, crises can occur in hybrid and, more specifically, information environment. These crises can be artificially-provoked, escalated or related to conventional crises. In order to protect the integrity of the state, swift resilience mechanisms must be established, and those existing must be updated to include hybrid threats. The resilience to possible hybrid crises should include intelligence, legislative improvements, involvement of the civil society and NGO's and, most importantly, education. For the resilience to be truly effective, there must be a universal agreement of what constitutes hybrid threat, hybrid attack and hybrid crisis.

Keywords: asymmetric warfare; hybrid; information; crisis response; non-conventional threats; narrative.

Introduction

Until recently, "warfare" was traditionally associated with a conventional military combat on behalf of the particular entity[1]

[1] Entity in this context can refer to a country, a society, a specific ethnic group, a community, etc.

(usually a state), with high capacity weaponry used and a large number of casualties inflicted amongst the troops and civilians (National Defence University, 2011). Within the "warfare" term there is a significant notion of asymmetry –marking the unequal possession of power (National Defence University, 2011). Although there have been a number of cases of asymmetric conflicts throughout the history, such as Soviet War in Afghanistan or Anglo-Irish War, nowadays, the term "asymmetric warfare" is increasingly being used to label some different actions, which include other-than-military tools, such as terrorism, guerrilla warfare, cyber-attacks, information and propaganda, techniques considered *hybrid*. The increase in usage of hybrid techniques, which can often summoned from the asymmetry in conflict, in recent years has led to more awareness about the issue being raised in many countries and the need to establish a swift crisis response to such threats. The information part of the afore-mentioned hybrid warfare had specifically increased fears of the security of some countries, since, under the disguise of the freedom of speech, potentially false information can be used to radicalize and impose a specific "narrative", which could be then, in some instances, used against the interests of, or even as a threat to, a particular country. However, this should not imply that the "narrative" creation always serves as a technique for "destabilization", but there have been recent instances, where the "narrative" is established for the purpose of causing instability, as will be later shown in this

work. Since the beginning of the conflict of Ukraine[2] in 2014 and the spread of so-called Islamic State of Levant and Syria, more and more the hybrid threats are being discussed in the societies and amongst the decision-makers. There has been a realization that there is an urgent need to understand what constitutes a hybrid threat, attack and crisis by many politicians and military professionals. That is why, in this contemporary hybrid warfare environment it is essential to define hybrid and informational warfare, its asymmetry, the notion of "narrative", to present the examples of hybrid warfare and hybrid crises. The resilience against such hybrid and informational threats must be discussed for a comprehension on which of the tools are the best to counter hybrid aggression and informational attacks. In this paper, the definitions hybrid warfare will be analysed and contrasted to examples and contemporary security threats. Hybrid threats to security will be presented and also analysed in the comprehensive approach. The possible information-related hybrid crisis scenarios will be presented and crisis management tools within the hybrid environment will be discussed.

[2] In this work, the events in Ukraine since 2014 will be referred to as "conflict". While Ukraine, NATO and EU argues that there is a war between Russia's regular troops and troops officially supported by the government of the Russian Federation against the troops of Ukrainian Armed Forces, Russia and Russian state-media argues that the situation in the country's east should be considered a "civil war". There has been no official declaration of war by either side. Since there is a significant amount of reported combat activity, involving Ukrainian troops and so-called "separatists", the situation in Ukraine can be referred to as "conflict", per the definition of conflict by the International Humanitarian Law (Chelimo, 2011).

Defining warfare

Since the beginning of the conflict in Ukraine in 2014, there has been an increase in the debate about what exactly constitutes hybrid warfare. As there is no universal agreed definition of the hybrid warfare, it will be looked at from several definitions, offered by different scholars, which could be used for describing the contemporary global security situation. International security experts are now often referring to destabilizing actions of Russia, ISIL, as well of some other states and entities, as a "hybrid warfare". Henrik Praks defines hybrid warfare as "the employment of, in a co-ordinated way, a mixture of military and non-military components to achieve political ends" (Praks, 2015). Petri Houvinen describes "hybrid warfare" as "a cocktail of conventional military capabilities, insurgencies, terrorism, guerrilla warfare, organized crime, cyber warfare and advanced military technology" (National Defence University, 2011). Essentially, hybrid features under a notion of "asymmetry", which is defined by the NDU as "alternative way to fight a war, a way for a weaker party to counter a stronger opponent" (National Defence University, 2011). Hybrid warfare can then clearly be distinguished as a fit under the "umbrella" of what asymmetric warfare contains. What could be described as lacking from the NDU definition of hybrid warfare is the usage of information tools to relay a particular "narrative", although its asymmetry explanation seems to suggest that the "weaker party" employs other than traditional military means to withstand a stronger

opponent, one of them likely the information assets. The definition of “hybrid” that will be used in this work, however, will be that of NATO – “a type of threat that combines conventional, irregular and asymmetric activities in time and space” (NATO Standartization Office, 2018). It is the definition that offers a lot of room for various possible aspects of hybrid, thus increasing the flexibility of the term. As it can be seen, the asymmetric and information techniques can be included within the hybrid term and hence, will be considered as constitutive parts of hybrid warfare.

Another essential term in the informational environment is “narrative”, defined as “a structure of events and stories to reduce complexity, increase understanding of identified strategic goals and offer a path towards a desired conclusion.”[3] The terms “asymmetric warfare” and “informational warfare” are also significant in explaining the current security situation and their importance comes by distinguishing them from hybrid warfare. The asymmetric warfare encompasses hybrid warfare, because, as mentioned above, hybrid falls into the features of asymmetric warfare. Hybrid itself, in turn, encompasses information, as one of the main features of the hybrid warfare, in addition to cyber activity, terrorism and guerrilla warfare.

There is also a need to analyse the usage of the word “warfare”. If in these “hybrid” or “informational” cases no conventional

[3] The definition was presented at the November, 2018 Strategic Decision Making for Crisis Response Operations Course at the CMDR CoE in Sofia, Bulgaria.

warfare techniques are involved, is the “warfare” definition really relevant? Andrew Monaghan presents an important argument by analysing Russia’s hybrid warfare strategy, that while the “rules of war” have changed to no longer involve any of the conventional warfare tools, the consequences of these “hybrid” actions remain somewhat similar (Monaghan, 2015-2016). James K. Wither argues that before Russia’s 2014 actions in Ukraine and its occupation of the Crimean Peninsula, “hybrid warfare” was mostly analysed within the military circles of the national defence strategists, but after these events the topic has entered the scope of the wider public (Wither, 2016) with a growing focus on information tools. What could be derived in analysing the Wither’s theory, is that as the “hybrid” itself and the informational tools employed in it, the whole process is difficult to attribute mostly due to its wide-ranging techniques, hence it is up to a debate whether an employment of various non-conventional tools by one entity against another should be considered an “attack” or, even more, a “warfare”. It also shows that the events of 2014 in Ukraine triggered the paradigm shift with regards to hybrid warfare and its importance and made many security strategists realize the need for a larger amount of resilience against these hybrid threats, especially in the information domain (Davis Jr., 2015).

Taking into consideration that various scholars offer different definitions of hybrid, we can distinguish that all of them suggest the usage of unconventional tools in the warfare environment, of

which the information, although may not be directly linked, is a very important component. Other components importantly include cyber, guerrilla warfare -significant aspects of asymmetric warfare, which can also be used to achieve the goals of the contemporary hybrid attacks and considered as threat to security in attacked entities.

Contemporary security environment/threats to security

With escalating conflicts in Syria, Ukraine, Afghanistan and elsewhere, the contemporary global security situation is further threatened by the non-conventional threats, such as influence and propaganda campaigns, cyber-attacks, conducted with an aim of causing destabilization of a particular entity.[4] In recent years, the perception of contemporary security situation, especially in Europe, has significantly shifted to encompass these threats. This had led to the improvement of terms, strategies and crisis response mechanisms, encompassing a larger range, being established. The emergence of so-called "non-conventional warfare", to a certain extent, has shown that the focus, dominated on conventional military threats by national security institutions, is not sufficient and cannot protect from such digital and information-based attacks.

The security situation has been perceived as significantly worsening in Europe, since 2014, when Russia interfered in a

[4] Entity in this context can refer to a country, a society, a specific ethnic group, a community, etc.

conflict in Eastern Ukraine and it had also attempted to interfere in the sovereignty of the Baltic States, Montenegro and North Macedonia – countries, mostly within, or willing to integrate in the Trans-Atlantic politico-military alliances, by various, including non-military means, which has left security officials and intelligence agencies scrambling to seek a proportionate response, not yet necessarily developed in the national security strategies. According to the United States intelligence agencies (National Intelligence Council, 2017), Russia used informational assets it possess and created various new ones to interfere with 2016 United States Presidential election, it also allegedly interfered with the 2016 referendum on membership of the United Kingdom in the European Union (Narayanan, Howard, Kollanyi, & Elswah, 2017) and the 2017 France's Presidential election (Vilmer & Conley, 2018). Furthermore, Russia reportedly sponsored mass protests in Macedonia and Greece, trying to enhance the opposition towards the Macedonia's name deal and subsequent possible integration of this country to the trans-Atlantic alliances, stoking ethnic and racial tensions in the Baltics and the United States (ETH Zurich Center for Security Studies, 2017). Allegedly, Russia used attempted murders of the regime critics or attempted coups, to influence the internal politics or otherwise meddle in other states. In early 2018, a former Russian spy Sergey Skripal was poisoned in the United Kingdom, with all evidence showing likely Russian state involvement. The Russian state and its media denied any involvement and emphasized the need for evidence, as did some Western commentators (Jenkins,

2018). Russia has also been accused of organising a failed coup d'état in Montenegro, with dozens of allegedly involved persons arrested in the coastal Western Balkan state (Bajrovic, Garcevic, & Kraemer, 2018).

The Western world has also seen an increase in the activity of jihadists, an emergence of so-called Islamic State of Iraq and Levant.[5] ISIL targets young, usually second- or third- generation descendants of immigrants from Muslim-majority states in the Middle East and North Africa by propaganda, appealing to grievances based on discriminatory practices or perceptions of such practices leading to feelings of disintegration and estrangement thus increasing the appeal, decreasing linkages with any societal support system, of the ISIL propaganda (Gates & Podder, 2015). ISIL had employed the capabilities of modern-day technologies and social media to recruit and radicalize, persuade into fighting, particularly in Syria, and into organising terror attacks, i.e. Western countries (Gates & Podder, 2015). This has led to a creation of "terrorist cells", the most notable in Brussels, which organized the November 2015 attack in Paris and 2016 attacks in the Belgian capital (Estrada & Koutronas, 2016). On the other hand, some individuals, affected by the radicalization techniques of ISIL, had individually organized

[5] There are various references existing, of which - Islamic State of Iraq and Levant in Syria and Iraq, or *Da'esh*. For the purpose of this paper, the author shall use, hereafter, the name "ISIL" because this has been the name the group officially adopted after its establishment, and this name is often used in a mainstream global media.

attacks with no or little logistical support from the command of ISIL, like ramming attacks in Nice, Berlin and Strasbourg. This is all part of what could be considered an ISIL attack against the European societies, which can also largely studied as a manifestation of hybrid warfare, with large informational assets targeting individuals most susceptible to propaganda in Western societies.

Changes in peace and conflict – paradigm shift

The increasing significance and usage of hybrid warfare in recent years has led to notable changes in the perception of peace and conflict in the contemporary security environment, representing an important paradigm shift. It widely understood now that there are a number of security threats which now form part and parcel of hybrid warfare. A growing number of scholars and practitioners alike consider hybrid attacks no less damaging than conventional military attacks (Monaghan, 2015-2016). The ill-willing state or non-state actors are determined to use their hybrid and information assets to target the vulnerabilities of a particular state or a society (Praks, 2015), and escalate, in a very short period of time, into crisis.

The example showing the hybrid escalation scenario and perfectly fitting the definition of hybrid, non-conventional attack, used in this paper is the 2007 Estonian Bronze Soldier riots and subsequent cyber-attacks on Estonian government IT systems and the country's media. This informational and hybrid attack caught Estonia off guard and quickly escalated into a crisis, with

much material damage done during riots and cyber-attacks. One Russian citizen was killed during rioting and the crisis received diplomatic tint, involving blockade of the Estonian embassy in Moscow by the Russian state-sponsored youth group “Nashi” (Praks, 2015). There was no involvement of any armed forces in this conflict, however the attack against the state was still carried out, but in a rather different, hybrid manner – by employing cyber and informational tools. The cyber-attacks had serious implications for the Estonian state – the government has dedicated a lot of effort to prepare to withstand similar cyber-attacks in the future, so that the main governmental functions are not disturbed in a similar scenario, illustrating the above-discussed paradigm shift and the subsequent understanding of the government to be prepared for this type of non-conventional crisis.

Hybrid threats to security and stability

The fast evolution of modern technologies and social media resulted in conducive environment for state and non-state entities to exploit the hybrid warfare tools for potentially informational warfare activities. This has led to an increase in the use of cyber activity, as alleged by the U.S. intelligence agencies (National Intelligence Council, 2017), to make and impact or at least support the “narrative” of the “attacking” state, the “robotrolling”, employment of the social media for the purpose, for instance, narrative establishment. The other technology, although not novelty, such as radio, television and print press is

increasingly being used for the same purpose. In this section, the hybrid and, more specifically, information techniques and the related potential, or already existent and related contemporary threats, will be discussed, from a crisis response perspective.

The spread of false information and boost by the third-parties to specific narratives in the social media is now more often mentioned in discussions on the influence campaigns in the West, mostly to achieve a desired outcome in elections and is mostly used by Russia (National Intelligence Council, 2017). There are 10 main technique used by Russia in the social media, to influence a targeted audience.[6] They are the "moral superiority" of Russia in comparison with the Western ideas, usage of experts, also described as "useful idiots", the use of authority, the placement of the report, its repetition and/or length, selective reporting, employment of testimonies by "witnesses", simplification, statistics, humour and trolling.

The above-mentioned techniques are employed in order to establish a "narrative", which can be both long-term, to solidify the audience in following the desired line, sometimes even in events with no direct link between each other, and short-term, mostly in various crisis scenarios. To illustrate the long-term "narrative" creation, the ISIL propaganda example can be explored. With the propaganda techniques it possesses ISIL recruits its followers, but the "narrative" is kept being sustained

[6] November 2018 Strategic Decision Making for Crisis Response Operations Course at the CMDR COE, Sofia, Bulgaria.

afterwards. ISIL continues to flood the recruits with propaganda before their arrival to ISIL-held territory or the attack they perpetrate in various cities, in order to keep the ISIL narrative in the beliefs of the people strong. If the recruits arrive to join ISIL in Syria or Iraq, the narrative can be sustained easily, through intimidation, threatening, the limitations on free movement and else (Gates & Podder, 2015), which is easier than to justify harsh living conditions and violence with propaganda.

Russia, on the other hand, although also attempting to establish a long-term narrative, is better equipped to establish short-term narratives, especially linked to crisis scenarios, or to highjack an already existing narrative, with no direct link to Russia, Russian politics or culture overall. The crisis "narrative" was employed and strongly promoted by Russia, for example during the conflict in Ukraine (European Union Institute for Security Studies, 2016) and the downing of Malaysia Airlines flight 17 and its aftermath. Russia's international media reported news and opinions about the events in a specific manner, promoting falsehoods[7] (Bachmann, 2014). The aim of such actions was to establish a short-term confusion and support for the Russian version of the events, which would, in broader context, further the narrative of Russia as not an aggressor, but a neutral party to the conflict.

[7] Reports on fighter jet near the doomed aircraft, promoting theories that it was downed by Ukrainian Armed Forces BUK long-range anti-aircraft missile, that it has targeted the plane of the Russian President Vladimir Putin.

The highjacking of an already existent narrative is also employed by Russian informational assets. This can be seen in the alleged Russian efforts to influence the 2016 United States Presidential election. Russian-run social media accounts had been strongly involved in the most sensitive debates of the American society, such as racial relations and police brutality. Russia had instigated social divisions within the U.S. society by promoting liberal and conservative ideas, events and tensions at the same time, to sow further discord and distrust between the Americans (Scott, 2018). To achieve that, Russia employed social media, mostly Facebook and Twitter and its international media tools, RT (former Russia Today) and Sputnik News being the most famous of them. This shows how the "narrative", which is not directly linked to Russian affairs, can be used in order to influence the societal relations and thus, politics of another state, exploiting existent tensions, which could, to some extent, also be attributed to be a societal divisions within the U.S.

Comprehensive approach

The comprehensive – people-centred, whole-on-government approach is essential when discussing hybrid warfare in the contemporary security environment. The most significant part of it is that the information techniques employed in hybrid conflict target the population, usually in order to create or, more often, bolster, as discussed above, a "narrative", to shift the views of the population or to enhance their emotions in order of achieving certain political or geo-political aims, the difference from any

regular information flow being the manipulative techniques, the most extreme being false information, but not limited to stereotyping or mockery. Thus, it is essential to discuss how various groups in a given society are targeted in information campaigns or how various societal groups or aspects are used in the presentation of the particular piece of information, in order to create a specific "narrative" about them, with positive or negative connotations, when the information is delivered to a wider population.

In the information warfare environment gender, racial and ethnic sentiments are often exploited in attempts to influence the mind-set of a certain group of people. The employment of these narratives can facilitate a division effect or to help the audience arrive at the conclusion of these roles being deliberately shifted in order to destabilize the hegemony of the society. Most importantly, delivering of this information is in a very negative connotation, creating the sense that the receiver should be opposing it.

Gender Perspective

Gender is often employed in informational warfare to exploit emotions, playing on an audience's social views, especially targeting the more conservative parts of societies. This is usually depicted by attributing traditional gender roles (Ozoliņa, Šķilters, & Struberga, 2018) based on stereotypical traits of masculinity[8]

[8] Masculinity - Qualities or attributes regarded as characteristic of men.

and femininity[9] imposed, respectively, on men and women. These traditional, understood as representing core cultural and ethical values, are contrasted to the "new", "unorthodox", "non-traditional", "Western values", usually presented in a very negative manner and related to women's masculinisation, and respectively – men's feminisation. A technique often used to enhance audience's emotions is either to contrast these with topics such as homosexuality or trans-gender or by contrasting with zoophilia or pedophilia, suggesting that they are accepted in the "liberal societies" together with gender equality or LGBT rights, or to portray them in a largely humorous way (Ozoliņa, Šķilters, & Struberga, 2018). This shows that people's emotions are being manipulated in order to change or strengthen the desired narrative on gender, which, in turn, applies to the more general narrative, which might be promoted by the government.

For example, Russia's state-owned media's coverage of the 2014 Eurovision Song Contest aftermath. The contest was won by the Austrian entry – Conchita Wurst, a drag queen[10], which mixes the looks of both what is traditionally considered female (long dress, long hair, high heels) and men (beard). The Russian state media has given the win of Conchita Wurst a large media attention. Some Russian politicians publically proposed creating an alternative, family-friendly, song contest (Westcott, 2014).

[9] Femininity - Qualities or attributes regarded as characteristic of women.
[10] Drag queen - a man, often a gay man, who dresses as a woman for entertainment (Cambridge Dictionary)

The character of Conchita Wurst has been mocked, usually emphasizing “traditional-values”. Several factors should be taken into account when discussing whether Russian state media has been using the analysis of Conchita Wurst Eurovision win as a political, influence campaign within Russia, or as a genuine worry for the “decaying moral values” in the West. Before 2014, when Ukrainian and Russian entertainment industries were largely interconnected, one of the most popular Russophone singer was Ukrainian Andrey Danilko, better known by his stage-persona, drag queen name “Verka Serduchka”. In 2007, his Eurovision entry finished second, with little or no recorded outrage in Russian media about “non-traditional” values. Serduchka has been, and to some extent, still is, one of the most favourite TV personas in Russia, appearing in televised concerts, TV shows and generally Russian media. Other Russian or Russian-speaking (and popular in Russia) entertainers have also enjoyed high praise from the Russian media, besides theirnon-traditional reading of societal values. Most popular 2000’s Russian duo “t.A.t.U.”, often featured homosexual themes in their clips and on-stage performances, many Russian male Estrada singers openly demonstrate their flamboyance, extravaganza and other traits, usually considered as countering the traditional masculine/feminine images, however Russian state often feature them in media shows and provide them with state awards (Khazan, 2013). Against this backdrop, it could be concluded that Russian state media employs the “traditional *versus* non-traditional” gender narratives, to their convenience, in order to

affect the emotions of the audience and portray particular entity as “morally decaying”.

Russia seeks to influence the emotions of the audience by using gender stereotypes and instigating the audience’s negative views towards certain societal processes. Since Russian state media draws a clear link between the “non-traditional values” and the West, such information campaign can be considered as anti-Western, since it serves a purpose of enhancing the audience’s negative emotions towards the “propagators” of these “non-traditional values”. In the event of a crisis, gender stereotypes could be further manipulated with the help of information assets in order to shift the public opinion or enhance the loyalty of the audience.

The ISIL has also employed gender in its controlled media to facilitate the larger control of the society, something which could also be described as a tool in informational warfare. The ISIL media outlets project an image of women strictly following the teachings of Sharia Law, obeying their husband and taking care of the children. However ISIL also uses the sexualized image of women in its propaganda so as to increase its appeal to men (Ali, 2015). The establishment of obedience upon the population can also be considered as part of informational warfare, since one of the primary goals of ISIL is to gain the obedience of the population, which can then be used to pursue other objectives.

The conflict areas, which are in Ukraine, Syria and Iraq particularly related and possibly vulnerable to the propaganda

by, respectively, Russia and ISIL, also have information-related gender issues, which must be addressed in this section. The handling of information, information-gathering, especially of that related to gender, is extremely sensitive within the conflict environment. The way the information is handled within the conflict can have significant implications on the society where the conflict is taking place, and also to the outcome of the conflict itself. Various societal aspects must always be kept in account in a conflict situation, for example gender relations, culture, stereotypes and perception biases.[11] Gender-insensitive handling, collating or disseminating of information can result in a disturbance of long-term societal norms, which in turn can result in people becoming victims to gender-related violence.

Setting the stage for crisis response

Hybrid warfare actions require a substantive response from the local, regional, national and international institutions. Crisis response to a hybrid threat requires both short- and long-term approaches. As explained in the previous paragraphs, hybrid environment hugely differs from the conventional one, thus it can differ widely in its nature and the perception of the hybrid attack on an entity can also differ. Hence, crisis response to a hybrid attack should be multi-layered and involve various tools, from the general raise of societal awareness and improving education, to

[11] The ideas and experiences about gender in conflict were shared by the instructors of the "Gender Focal Point" Course at the Crisis Management and Disaster Response Center on 5-7 February, 2019 in Sofia, Bulgaria.

a possible conventional military attack in some instances. The main issue in the contemporary security environment is that hybrid threats are complex and difficult to attribute. Many states and international organizations do not have, or not to a sufficient degree, established relevant crisis response mechanisms. As will be later discussed in this part, often the society and various NGOs engage in education activities and in raising societal awareness with regards to hybrid threats, especially in societies, which are more exposed to the hybrid threats. Since the hybrid crisis response can encompass so many various techniques and methods, the comprehensive approach must be also taken into account.

NATO Crisis Response System (NCRS), established to counter the crises in the states of the alliance, is, however, mostly prepared to handle clearly defined crises of the particular type, which is not well-suited for the abstract and multi-layered approach of the hybrid warfare, especially its informational wing. The most important challenge for NATO, other organizations and national governments is the fact that the hybrid warfare requires resilience and efficient crisis response not only from the military, but also from politicians, media and society. Hence, due to lack of coordination between these institutions, the particular entity could become especially vulnerable to the hybrid threats.

Defining crisis

Crisis may be defined as a time-bound state of (objective or subjective) uncertainty as non-routine events are deteriorating the overall entity (resilience and preparedness) of a system and its established procedures. The essential in such case of definition is that resilience is challenged, therefore, it is critical to strengthen the resilience of various entities. The CMDR COE apprehends crisis management as 'an iterative process of organised and coordinated actions, by and among all responsible stakeholders, at the local, national, regional and international levels, aimed at handling a crisis at all its phases'[12]. It is essential to note that crisis management begins not when a crisis is unfolding, but rather in the anticipation of the crisis, establishing resilience and preparedness. The NATO-wide approved description of resilience is "the ability to resist and recover easily and quickly from shocks and stresses, combining civilian, economic, commercial and military factors"[13]. The societal part of the resilience establishment is especially important when discussing resilience in the informational dimension – the one, arguably least intertwined with the military part of resilience.

Crisis scenarios

As discussed above, the definition of crisis within a hybrid environment is largely not set up by security-oriented

[12] Definition under consideration set by CMDR COE Annual Booklet, issued 2018.
[13] https://www.nato.int/cps/en/natohq/topics_132722.htm

organizations, such as NATO or OSCE, or by most of the national governments. However, as illustrated in the first part, some recent events can be, to a certain extent, considered as a hybrid crisis, for example the 2007 unrest in Tallinn, Estonia. This crisis contained the elements that the CMDR COE name as pre-requisites for a crisis to be caused. There was a factor – ethnic tensions, and a stressor – a move of a sculpture, which an ethnic minority considered very dear. The second factor was rather unstable relations between Estonia and Russia and the stressor has been the Russian cyber-attack on Estonian internet, the informational campaign it had started and the blockade of an Estonian embassy in Moscow. It does not by any means constitute a conventional crisis, rather the different areas in which it had occurred demonstrates its asymmetry. The Estonian government lacked the necessary degree of resilience (Praks, 2015) and the country was caught unprepared to withstand the asymmetric attacks in various fronts – cyber, propaganda and diplomatic.

Another prominent example of a hybrid crisis was the 2004 Beslan school siege in Russia. The terrorists, which had taken the school children hostage, wanted to send a message of fear to the population, and, in this action, to achieve their political goal – the independence of Chechnya. However, the action was in turn also used as a tool for information warfare by the Russian government – the events showed that there is a justification for the war in the Russia's south and instigated support for the

Kremlin and its actions (Tuathail, 2009). Thus, political events, terrorist attacks, insurgencies and the information surrounding them can serve as a tool of information warfare.

Escalation scenarios

Within a hybrid environment, a crisis can be artificially escalated by a state or other entity to a conventional scale. An event could be triggered by the same entity or it could be an unrelated event, about which the information could be manipulated in order to further specific established “narrative”, as previously discussed. A similar scenario is an information crisis, which could be described as “naturally inflicted”, when an event leads to an overflow of information, positive or negative, and possibly involving false information and manipulative facts, which could have a deep effect on the society in the aftermath of said event. For the sake of simplicity, these will be called the “escalation scenarios”. Although there has not been a clear, highly effective case of a crisis “escalation scenario”, some events in recent years show how information about deeply emotional event, which can be perceived as threatening the audience can be manipulated. In the immediate wake of the Paris terror attacks in 2015, the so-called ISIL terror group had spun its propaganda machine in order to portray the attack as one in the French capital is only the first of many that will soon follow (Bonikowski, 2016). The “narrative” of uncontrolled terrorist cells in Europe and the criticism of the results of massive migration from the Middle East has been adopted by right-wing politicians in order to gain more

public support, by promoting ideas of fear and resentment (Bonikowski, 2016). This shows how the already existent crisis, which can be more or less described as "conventional", can be escalated into more-encompassing informational crisis, whereas the events are used for the long-term establishment and/or promotion of the particular "narrative", causing widespread panic or manipulating the public opinion on the said event, even possibly provoking public unrest or distrust of the authority. These "escalation scenarios" can lead to a sudden shift in the public perception and hence, the consequential political, diplomatic or societal crises.

Artificially-provoked crises

Hybrid crisis can be purposely created and directed against a particular entity, usually a state or a community. The provoked crisis differs from what has been already discussed as a "narrative" creation, because it is mostly aimed at establishing a short-term disruptions amongst the population of the entity targeted. However, these artificially provoked crises would still frequently use fear, tensions or other predominant features of the society, in order to further exploit it. An example of an artificial crisis is the 2014 Chemical Plant Explosion hoax in Centerville, Louisiana, United States. It was organized by the allegedly Russian state-funded Saint Petersburg-based "troll farm"[14]. It

[14] Troll Farm – an indirectly state-sponsored organization, involved in creating content desired by the state, while in disguise of independent content creators (Chen, 2015).

had spread fake news about an explosion at the chemical plant and about ISIS claiming the responsibility for it (Chen, 2015). The panic spread through the social media, with Twitter bots spamming the platform about the alleged incident, causing panic amongst locals in the area (Chen, 2015). This is an example of how a crisis situation can be caused without any other event, besides the flow of information, actually taking place in reality. At present, these types of crises are rather rare, and they are mostly related to the concept of "fake news"[15] – whereas they are harmful, but usually do not inflict any major crisis situation. A similar artificially-provoked crisis has been the so-called "Russian Liza" story in Germany in 2015, of an alleged assault by a gang of Middle Eastern refugees in Berlin against an adolescent Russian resident of Berlin, nicknamed Liza. This story was broadcasted by the Russian-state television "Pervyj Kanal" and afterwards was quickly picked up by the German media, causing outrage in a country dealing with a very large numbers of migrants and refugees at that time (Meister, 2015). Although it was soon discovered as propaganda of the Russian government, the story ignited more anti-immigrant sentiments in Germany and led to protests against the refugee community for their alleged crimes. This shows that in some instances, within a hybrid environment, crises can be completely artificially provoked by an entity in its offensive (hybrid) strategy.

[15] Fake news – unverified or factually incorrect information, usually presented in a news-like manner (Oxford Research Encyclopedia of Communication, 2018).

Crisis Response tools

As wide and complex as hybrid war itself is, the response and the resilience establishment to manage hybrid would be of an even greater and more cumbersome nature, since various aspects of it can only be addressed with very different crisis management tools. Strong measures are needed because of the hybrid warfare's whole-on-society approach (Aapo & Pasi, 2015). There exists a NATO Crisis Response System, which is supposed to be a safeguard of the possible crises in the alliance, by establishing a resilience system[16]. The NCRS is supposed to deal with any type of crisis within the alliance, however the hybrid type of crisis has only been increasingly considered in recent years. In addition to that, the issue of a hybrid warfare attack is closely related to NATO's Article 5. What constitutes an attack, is hybrid or an information attack an attack worthy of allied defence? These questions should be dealt with by all the member states of NATO before Article 5 could be invoked and a substantive response delivered. However, as part of the hybrid warfare itself, divisions could be set up between the member states on agreeing whether Article 5 should be invoked, until it may be too late and the attack is already in the stage of *fait accompli*.

[16] NATO Crisis Response System was presented and analyzed in Crisis Management and Disaster Response Course on 18-22 March, 2019 at CMDR CoE in Sofia, Bulgaria.

Some researchers point out that the offensive hybrid warfare actions require swift hybrid defensive actions as a response. Amongst them, are the national defence, protecting crucial infrastructure, investing in science and education, media and civil society (Aapo & Pasi, 2015). The national defence structures can be involved in the establishment of resilience from hybrid threats by developing cyber-defence capabilities, counter-terrorism measures, strengthening its intelligence structures, creating frameworks for what constitutes a hybrid attack and what should a response to it be like. This is, to some extent, being implemented in many countries and organizations, such as NATO, as the hybrid threats have intensified in recent years.

However, the most difficult part to deal with for national defence structures is the information component of the hybrid warfare. Informational warfare threats can hardly be dealt with by the armed forces or other military entities. Hence, the element of societal awareness and civil society education here becomes essential. There exists a great deal of examples of entities, affected by information warfare, which had established techniques on how to deal with them, as will be illustrated in the following paragraph. In the European Union, there exist several established systems, which are tasked to deal with information threats. One of the most prominent examples is the platform “EU vs. Disinfo”, established by the European Union External Action Service to find and “debunk” false news stories (EU vs. Disinfo). The concept of “debunking” has been recently adopted by

various media organizations, such as The Washington Post or CNN, which serves as a way to check the validity of the news stories and, if that is the case, prove their falsehood. There are several similar platforms established by the state or the civil society – “stopfake.org” is an organization, established by the students and lecturers at Kiev’s Mohyla University (StopFake), while NATO member states and allies had established the Hybrid Warfare European Centre of Excellence, as well as NATO Strategic Communications Centre of Excellence, which are in part involved in the fight against false news and the informational warfare in general.

The importance of education of the population and free media must also be underlined. Democratic countries are most vulnerable to the information warfare because, while the autocracies can create and spread propaganda, democratic countries must guarantee freedom of speech, so the ban of the malicious information should not be considered as an appropriate response for such states in the long-term. Therefore, the notion of free media and education becomes especially relevant. Free media ensures that mostly verified and correct information is received by the population, increasing its trust, and hence, hindering the efforts to extort the vulnerabilities of a weak national media for propaganda purposes. There is also an importance of national legislation with regards to information and related vulnerabilities. In order to increase the resilience of the state with regards to information, laws regulating the accuracy of

information and detailing the process of penalizing false information and propaganda should be in place. However, the efficiency is increased in its combination with education. Education of the importance of freedom of speech, how to verify information and sources distinguishing "fake news" can also lead to increased resilience to information warfare and serve as a preventative tool from crises in a hybrid environment.

Conclusion

Hybrid warfare is a multi-dimensional, multi-faceted and ever changing matter, which requires anticipation and adaption. The very essence of the hybrid warfare is its fluidity, unpredictability, which is intended to be hard to counter. Crises in hybrid environment can vary in their type, scope and target so much that the resilience becomes the responsibility not only of the military structures, but of all the subjects of the state or other entity (legislature, society, NGOs). Therefore, hybrid crisis management should not be a sole responsibility of national militaries and international alliances. As illustrated in this paper, hybrid attacks and subsequent crises can be related to information, terrorism, cyber activity or attacks of a mixed nature. Information warfare, especially its technique of propaganda, must be countered by the society as much as the governments and international organizations. Furthermore, information-related crises can evolve to encompass furthering the "narrative" or establishing it in order to have an outcome on the targeted audience, such as civil unrest, political turmoil or instability.

Hence, threats of such scale require high degree of resilience, both at societal and government (state authority) levels. The most important components in information warfare resilience are the democratic principle of free media and education. This could be even considered as the sole long-term solution for establishing resilience to informational warfare threats as the democratic states, in accordance with the principles of the democratic country, should not embark on bans and restrictions on the freedom of speech. However, in the short-term various other tools may apply, such as debunking, strengthening national intelligence, and establishment of centres for strategic communications. In this paper, several different definitions on hybrid warfare were presented and contrasted. It is important to note, though, that in a contemporary security environment, there is a clear need to fully understand and adopt universal understanding of what constitutes information and other hybrid threats and warfare. This is essential to efficiently manage crises that hybrid could inflict on various entities, as it would lay down the pathway for an establishment of efficient resilience system against newly emergent and already existent hybrid threats. Therefore, besides various long- and short-term solutions that are constantly offered, universalization of the broad definition of hybrid must be implemented. However, it would still face the challenge of possible new components and techniques being added, hence there must be a room for any possible changes and additions.

Bibliography

Aapo, C., & Pasi, E. (2015). How Can Societes be Defended against Hybrid Threats? *Strategic Security Analysis*. Retrieved from https://s3.us-east-2.amazonaws.com/defenddemocracy/uploads/documents/GCSP_Strategic_Security_Analysis_-_How_can_Societies_be_Defended_against_Hybrid_Threats.pdf

Ali, M.-R. (2015). *ISIS and Propaganda: How ISIS Exploits Women.* University of Oxford. Oxford: Reuters Institute for the Study of Journalism. Retrieved from https://reutersinstitute.politics.ox.ac.uk/sites/default/files/research/files/Isis%2520and%2520Propaganda-%2520How%2520Isis%2520Exploits%2520Women.pdf

Bachmann, S.-D. (2014). Malaysia Airlines flight MH17: The day Russia became a state sponsor of terrorism. *Amicus Curiae*, 14-16. Retrieved from file:///C:/Users/CMDRCOE%20Training01/Downloads/2267-3412-1-SM.pdf

Bajrovic, R., Garcevic, V., & Kraemer, R. (2018). *Hanging by a Threat: Russia's Strategy of Destabilization in Montenegro.* Philadelphia: Foreign Policy Research Institute. Retrieved from https://www.fpri.org/wp-content/uploads/2018/07/kraemer-rfp5.pdf

BBC. (2018). What is Sharia and how is it applied? Retrieved from https://www.bbc.com/news/world-27307249

Bonikowski, B. (2016). Three Lessons of Contemporary Populism in Europe and the United States. *Brown Journal of World Affairs, 23*(1), 9-24. Retrieved from https://scholar.harvard.edu/files/bonikowski/files/bonikowski_-_three_lessons_of_contemporary_populism_in_the_united_states_and_europe.pdf

Cambridge Dictionary. (n.d.). *"drag queen".* Cambridge: Cambridge University. Retrieved from https://dictionary.cambridge.org/dictionary/english/drag-queen

Chelimo, G. C. (2011). Defining Armed Conflict in International Humanitarian Law. *Inquiries, 3*(4). Retrieved from http://www.inquiriesjournal.com/articles/1697/defining-armed-conflict-in-international-humanitarian-law

Chen, A. (2015). *The Agency.* New York: The New York Times. Retrieved from https://www.nytimes.com/2015/06/07/magazine/the-agency.html

CMDR CoE. (2018-2019). *Annual Booklet.* Sofia: CMDR CoE.

Davis Jr., J. R. (2015). Continued Evolution of Hybrid Threats. *The Three Swords Magazine*, 19-25. Retrieved from http://www.jwc.nato.int/images/stories/threeswords/CONTINUED_EVOLUTION_OF_HYBRID_THREATS.pdf

Estrada, M. A., & Koutronas, E. (2016). Terrorist Attack Assessment: Paris November 2015 and Brussels March 2016. *Journal of Policy Modelling*, 553-571. Retrieved from https://www.sciencedirect.com/science/article/pii/S0161893816300138?via%3Dihub

ETH Zurich Center for Security Studies. (2017). Hotspot Analysis: Cyber and Information Warfare in Elections in Europe. *CSS Cyber Defense Project*. Retrieved from http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-08.pdf

EU vs. Disinfo. (n.d.). *About.* Brussels. Retrieved from https://euvsdisinfo.eu/about/

European Union Institute for Security Studies. (2016). *Strategic Communications: East and South.* Paris: EU Institute for Security Studies. Retrieved from https://www.iss.europa.eu/sites/default/files/EUISSFiles/Report_30.pd

Gates, S., & Podder, S. (2015). Social Media, Recruitment, Allegiance and the Islamic State. *Perspectives on Terrorism, 9*(4), 107-116. Retrieved from http://www.terrorismanalysts.com/pt/index.php/pot/article/view/446

Jenkins, S. (2018). If the novichok was planted by Russia, where's the evidence? *The Guardian*. Retrieved from https://www.theguardian.com/commentisfree/2018/jul/05/novichok-wiltshire-poisoning-russia-putin-world-cup

Khazan, O. (2013). Why Homophobic Russia Loves Gender Bending Pop Stars. *The Atlantic*. Retrieved from https://www.theatlantic.com/international/archive/2013/08/why-homophobic-russia-loves-gender-bending-pop-stars/278833/

Meister, S. (2015). The "Lisa case": Germany as a target of Russian disinformation. *NATO Review Magazine*. Retrieved from https://www.nato.int/DOCU/review/2016/Also-in-2016/lisa-case-germany-target-russian-disinformation/EN/index.htm

Monaghan, A. (2015-2016). Putin's Way of War: The 'War' in Russia's 'Hybrid Warfare'. *Parameters, 45*(4), 65-74.

Narayanan, V., Howard, P. N., Kollanyi, B., & Elswah, M. (2017). *Russian Involvement and Junk News during Brexit.* Oxford: Oxford Internet Institute. Retrieved from https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2017/12/Russia-and-Brexit-v27.pdf

National Defence University. (2011). *HYBRID WARFARE – Just a Twist of Compound Warfare? Views on warfare from the United States Armed Forces perspective.* Washington, D.C.: National Defence University. Retrieved from https://core.ac.uk/download/pdf/39944364.pdf

National Intelligence Council. (2017). *Assessing Russian Activities and Intentions in Recent US Elections.* Washington, D.C.: Office of the Director of National Intelligence. Retrieved from https://www.dni.gov/files/documents/ICA_2017_01.pdf

NATO Standartization Office. (2018). NATO Glossary of Terms and Definitions. Retrieved from file:///C:/Users/CMDRCOE%20Training01/Downloads/AAP-06%202018%20EF.pdf

NATO Strategic Communications Center Of Excellence. (2018). Robotrolling. Retrieved from https://www.stratcomcoe.org/robotrolling-20183

Ozoliņa, Ž., Šķilters, J., & Struberga, S. (2018). Humour as a Communication Tool: The Case of the New Year's Eve Television in Russia. *Defense Strategic Communications, 4*, 105-132. Retrieved from file:///C:/Users/CMDRCOE%20Training01/Downloads/4.ozolina.pdf

Praks, H. (2015). Hybrid or Not: Deterring Russia's Ways of Warfare in the Baltics - The Case of Estonia. *NATO's Response to Hybrid Threats*, 219-242.

Scott, E. (2018). Russian trolls are still using the anthem controversy to sow division on social media. *The Washington Post*. Retrieved from https://www.washingtonpost.com/politics/2018/09/11/russian-trolls-are-still-using-anthem-controversy-sow-division-social-media/?utm_term=.a8405e2bd9f9

StopFake. (n.d.). *About Us.* Kiev: Stopfake.org. Retrieved from https://www.stopfake.org/en/about-us/

Tuathail, G. O. (2009). Placing blame: Making sense of Beslan. *Political Geography, 4*(15). Retrieved from https://ibs.colorado.edu/waroutcomes/docs/GT_Beslan_09.pdf

Vilmer, J.-B. J., & Conley, H. A. (2018). *Successfully Countering Russian Electoral Interference.* Washington, D.C.: Center for Strategic and International Studies. Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180621_Vilmer_Countering_russiam_electoral_influence.pdf?qFOz5qjpEuTzu5cvUa.UgOj0Dg3FklQP

Westcott, L. (2014). Russia Proposes a 'Straight' Eurovision After Conchita's Victory. *The Atlantic*. Retrieved from https://www.theatlantic.com/entertainment/archive/2014/05/russia-proposes-a-straight-eurovision-after-conchitas-victory/370960/

Wither, J. K. (2016). Making Sense of Hybrid Warfare. *Connections, 15*(2), 73-87. Retrieved from https://www.jstor.org/stable/pdf/26326441.pdf?refreqid=excelsior%3A1069fd27240fd7b4ae76f601e4ed0141

Wozniak, M. (2016). The Ukraine Crisis and Shift in US Foreign Policy. *International Studies, 18*(2), 87-102. Retrieved from https://www.degruyter.com/downloadpdf/j/ipcj.2016.18.issue-2/ipcj-2016-0011/ipcj-2016-0011.pdf

The CMDR COE 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 attended the annual conference and specialized workshops held during the last year.