BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

No. 1/2024

ISSN 2284-936X
eISSN 2284-9378

Publication founded in 1937

SCIENTIFIC PUBLICATION HIGHLY ACKNOWLEDGED IN THE FIELD OF "MILITARY SCIENCES, INFORMATION AND PUBLIC ORDER" OF THE NATIONAL COUNCIL FOR ATTESTATION OF ACADEMIC DEGREES, DIPLOMAS AND CERTIFICATES, INDEXED IN INTERNATIONAL DATABASES EBSCO, CEEOL, GOOGLE SCHOLAR, INDEX COPERNICUS, PROQUEST, DOAJ, ERIH PLUS, CROSSREF

"CAROL I" NATIONAL DEFENCE UNIVERSITY PUBLISHING HOUSE
BUCHAREST, 2024

The articles published in the Bulletin of "Carol I" National Defence University, ISSN 2284-936X, L 2284-936X, are also found – title, author, abstract, content and bibliography – in the Romanian version of the journal, ISSN 1584-1928.

Content

No. 1/2024

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Military culture: Understanding deeper dynamics through the warrior archetype

Eric Ouellet, Ph.D.*

*Full Professor at the Department of Defence Studies with the Royal Military College of Canada and the Canada Forces College in Toronto, Canada
e-mail: eric.ouellet@rmc.ca

Abstract

This paper proposes a new psycho-sociological approach to understanding military culture change, built on the notion of warrior archetype, in line with psychiatrist Carl Jung's concept of archetype. It contends that military culture and its related institutional forms fundamentally seek to mobilize on an ongoing basis human energy produced through the activation of the warrior archetype. The archetype is built on enhancing feelings of strength in numbers, and empowerment through socially sanctioned actions and potential use of violence. It uses the example of the Canadian Armed Forces culture change effort to illustrate that any such planned organizational culture change will fail if it does not remain consistent with activating the warrior archetype, as its central dynamic and purpose.

Keywords:

Archetype; Canadian Armed Forces; Carl Jung; military culture; organizational behavior; psychology; the unconscious.

Article info
Received: 7 February 2024; Revised: 29 February 2024; Accepted: 18 March 2024; Available online: 5 April 2024

Citation: Ouellet, E. 2024. "Military culture: Understanding deeper dynamics through the warrior archetype". *Bulletin of "Carol I" National Defence University*, 13(1): 07-30. https://doi.org/10.53477/2284-9378-24-01

Military culture has become a prominent research topic over the last twenty years, as numerous books and articles have been written about it within and beyond NATO countries. Most of these researches seek to legitimize specific normative outcomes through changing military culture, so as to be more aligned with new political and ideological beliefs. A key present-day example of such normative change approach can be seen through the Canadian Armed Forces (CAF) culture change project, as illustrated in a recent special issue of the *Canadian Military Journal* (Government of Canada 2023a). By many accounts, it has generated significant controversies in military circles in Canada.

One of the fundamental difficulties behind any debate about military culture is that such a notion is not well defined, and core social dynamics are rarely analyzed in rigorous ways. For instance, in the Canadian case, cultural contexts enabling sexual misconducts have been described as caused by hyper-masculinity, but without explaining why hyper-masculine norms exist in the first place. As of November 2023, although the Canadian military recommended and enacted a series of administrative changes, and has engaged widely the personnel with culture change, limited progress has been observed in defining what kind of culture the CAF is looking to implement and how (Government of Canada 2023b). This situation should not surprise anyone, as the very notion of corporate culture change is very much a contested one, let alone when applied to the military. Research in organization studies shows that the majority of planned organization cultural changes fail (O'Donovan 2018), in the order of 70% (Jones et al. 2019), however, one defines failure. Some even contend that notions of culture change and culture management are highly questionable in themselves (Grey 2017). Unsurprisingly, most of the recent literature on planned culture change and change management is about ways of avoiding failure (Marion and Lewis 2020; Hughes 2022).

Central in all this research literature on cultural organizational change is the finding that failure to enact change is fundamentally caused by ineffective attempts to gain buy-in from personnel (Maurer 1996; Waddell and Sohal 1998; Geisler 2001; Pardo-del-Val and Martínez-Fuentes 2003; Oreg 2006; Erwin and Garman 2010; Rafferty, Jimmieson and Armenakis 2013; Gover, Halinski and Duxbury 2016). Failure to get buy-in can be linked in turn to numerous particular malpractices such as poor leadership, poor messaging, and communication, poor consultation, mismatch between mandatory tasks and proposed new ways, insufficient resources to manage transition, poor understanding of power relations, etc. In sum, appreciating candidly human dynamics and perspectives animating any organization from the point of view of its members is oftentimes a missed fundamental first step.

This article states that any attempt at military culture change must start with an understanding of the fundamental and deeper dynamics behind military culture so that genuine buy-in can be achieved. It is in this context that the notion of archetype developed by the famous psychiatrist Carl Jung is proposed to describe and explain

fundamental social and psychical forces behind any military cultural manifestations. A short overview of unconscious forces in organizations is presented, followed by an explanation of the Jungian archetype in order to propose an operationalized notion of the warrior archetype. Then, a general framework is developed to show how the warrior archetype is the central driver of military institutions, including the case of its dysfunctional version of the shadow archetype. In conclusion, some high-level recommendations about military culture change are suggested, using the Canadian military culture change as an illustration.

1. Unconscious forces in organizations: the missing variable

Culture change, military or otherwise, cannot be successful without taking into consideration powerful and fundamental unconscious forces and dynamics that are too often ignored by researchers and practitioners. In fact, ignoring these unconscious forces has been described as the single most important factor in failing to get genuine buy-in for change. Already in the 1970s, organization studies literature has identified that analysis of cultural practices is too superficial if unconscious elements are not at the core of the analysis (Turner 1977). Recent literature in the field continues to highlight the lack of effort in trying to tackle unconscious dynamics within organizations (Diamond 2007; Carlsen 2016; Long 2019).

The study of collective unconscious forces can be a daunting task, as it does not lend itself easily to typical social science analysis. However, in the study of organizational culture, numerous researchers over the years have found Carl Jung's concept of unconscious archetype as being relevant and useful (Mitroff 1983; Bowles 1993; Aurelio 1995; Tallman 2003; Starr-Glass 2004; Kociatkiewicz and Kostera 2010; Brown et al. 2013; Moxnes 2013; Chen and Narasimhan 2015; Prince and Forr 2021). Unfortunately, organizational applications of Jungian archetypes to the military remain quite rare.

Most of the few research studies examining the warrior archetype have, unfortunately, limited themselves to superficial aspects, namely focusing on the traditional archetypal representations of the warrior in imagery and film instead of trying to assess its deep role in cultural dynamics. In particular, such researches tend to subsume the warrior archetype with a vague notion of "dysfunctional male identity," (see for instance Moore and Gillette 1990; Enns 1994; Pisch 2016; Bloeser and Ramirez 2019; Cloud 2019; Szitanyi 2020; Maloney and Doidge 2021). As discussed below, to subsume the warrior archetype to a particular identity only shows a poor understanding and normatively-based misconstruction and misappropriation of the concept of archetype developed by Jung.

1.1. The concept of archetype

The well-known Swiss psychiatrist Carl Jung has developed an entire clinical school of thought in psychology built around the concept of archetype. Jung's work is vast,

complex, and has evolved over time, and he does not provide a short and single definition of archetype (Roesler 2012, 224). However, it can be defined as universal unconscious thought-affect forms, pre-verbal and within the realm of the symbolic and the imaginary. These thought-affect forms are patterned in specific ways to channel libido (psychical/life-force energy), somewhat identifiable through collective myths and symbolism. It has as a fundamental function to be a compensating, or bridging, psychological mechanism trying to re-establish (imperfectly) in the face of emotional stress the primordial child-mother singularity of boundless safety (Young-Eisendrath and Dawson 1997). In other words, archetypes are deeply wired responses to resolve internal contradictions in the face of challenging external situations (Jung 1959, 174). The combination of all these universally based archetypes constitutes what Jung called the collective unconscious.

Yet, even more important is that Jungian archetypes are built on the idea that the human mind is actually designed for life in a group. The bridging/compensating function of archetypes, although operating inside individuals, is meaningful only in social contexts because archetypes are a by-product of life in a group. For instance, the mother archetype implies adults and children, the king archetype implies rulers and followers; the magician archetype implies those who have special knowledge and those who do not; etc. Recent research both in cognitive psychology and in neuropsychology are coming to very similar conclusions about the social nature of the human mind, although through significantly different paths. Furthermore, these disciplines have found fundamental brain dynamics that are very similar to what Jung described as archetypes over 100 years ago (Hunt 2012; Becker and Neuberg 2019a; 2019b).

There has been in the psychoanalytic literature a fair bit of controversy about whether archetypes are inherited from an ancient past (and therefore imply some sort of biological determinism) or whether they are acquired (Roesler 2012). This debate, however, can be solved by reducing the issue of biological determinism to its simplest expression, namely that humans, especially young ones, need to live in groups to survive, and therefore will necessarily encounter typical forms linked to life in a group (Gray 1996). The most obvious one is that to survive a child needs one or more caretakers, usually described under the "mother archetype." The mother archetype does not have to be linked to a woman, nor does it have to be a single person, but the situation of dependency of a child towards one or more adults caring for him/her (however imperfectly) is a universal experience, as otherwise the child, and ultimately humanity, would perish.

Jung discovered archetypes through a life-long and exhaustive search for basic themes recurring in myths and symbolism found in numerous cultures across geography and time. This led him to raise a number of methodological points regarding archetypes. A key point is the critical distinction between an archetype *as-such* (or *per-se*), and cultural expressions found in myths and symbolism where archetypal

forms can be perceived and are referred to as *archetypal representations*. For Jung, archetypes *as-such* are universal, but only in their most generic (or principled) forms, while archetypal representations found in myths, stories, particular events, imagery, etc., are socially, culturally, and historically situated, and can vary greatly in content across time and geography. Also, archetypal representations can become reified over time, acquiring a life of their own, and oftentimes be the object of conflicting interpretations within a particular culture where outdated myths and stories are still used for justifying present-day expectations (Durand 1996; Monneyron 2016). A classic military example of an archetypal representation is to construe officers as honorable knights from an idealized and unhistorical view of the Middle Ages.

To make matters a bit more complicated, Jung also changed his views regarding archetypes *as-such*. In his early writings, he noted that "in principle, it [the archetype] can be named and has an invariable nucleus of meaning--but always only in principle, never as regards its concrete manifestation" (Jung 1959, 80). Yet, in later writings, he suggested that archetypes *as-such* are beyond description (Jung 1969). This last notion has been challenged since in the post-Jungian literature based on the simple fact that if in a clinical context, the goal is to identify which archetypes are activated, or need to be activated, in a patient's own mental universe, then the analyst must have an idea of what to look for, and hence to have some sort of heuristic description of archetypes *as-such* (Smythe and Baydala 2012, 69; Mills 2013, 34). In this light, exploring what could constitute the warrior archetype *as-such*, rather than remaining at the level of the more superficial and conflicting archetypal representations of the warrior may help shed light on a central force behind the military culture.

1.2. The warrior archetype

Jung, unfortunately, never described the warrior archetype and makes only a handful of mentions of it in his texts. Furthermore, and as noted above, most of the literature on the warrior archetype does not explain in any depth what an archetype is, and how it operates as an unconscious force throughout an organization. A notable exception can be found in Pearson (1986), who took a clear and deliberate Jungian perspective to discuss how various archetypes can be activated in making one's life more meaningful, including the warrior archetype. She identifies some of the basic elements underlying the warrior archetype such as seeking feelings of strength and avoiding feelings of weakness, but without offering much explanation of how these elements were selected (Pearson 1986, 21).

It is in this intellectual context that a deeper look at the warrior archetype is found necessary. To do so, one has to go back to Jung's fundamental questions related to the universal function of archetypes, and how it plays an important role in the life of a group so that it becomes a universally found feature. Hence, the first question ought to be why there is such a thing that could be called the warrior archetype. Starting with Pearson, if bridging over fear through feelings of strength is the fundamental function of the warrior archetype, then what are the generic sources of such fear?

One can posit that there are at least two distinct but interrelated universal sources of fear in group life. The first one could be described generically as the "unknown," however one defines it beyond the simple duality of known and unknown. The "unknown" can be a source of fear, as it can possibly bring chaos and misery, especially when construed as unknown by the group. The second source could be described as "them," other groups of humans distinct from "us," whose intentions towards "us" can be malignant or at least unknown. Humans have been and continue to be, unfortunately, a significant threat to other humans. All security institutions, pre-modern and modern, are based on this simple notion.

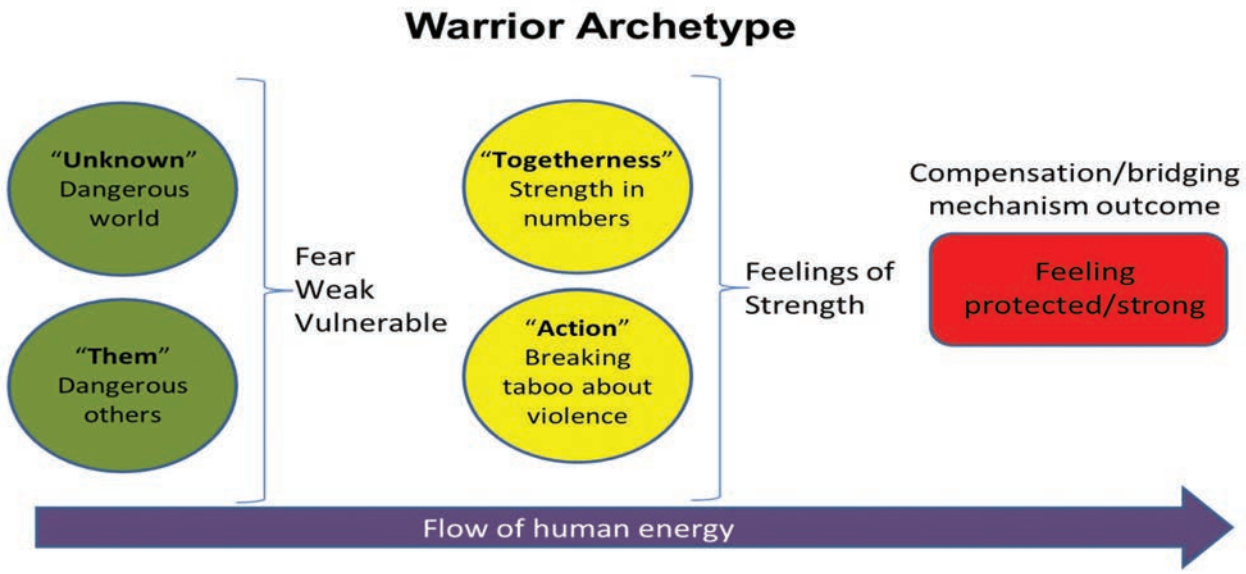
The second set of questions, logically, is related to what generically brings feelings of strength in a group context, which can bridge over or compensate for feelings of weakness or vulnerability emanating from fear of the "unknown" and of "them"? Once again, one can posit that there are at least two fundamental building blocks, or principles, to the warrior archetype. The first one could be termed as "togetherness" in the sense that there are feelings of strength and safety in numbers. This is a pervasive, if not ubiquitous, notion that has been studied since the early days of social psychology (McDougall 1908) and continues to produce an abundant literature (Park and Hinsz 2006). Given its widespread reality, it is probably safe to see strength in numbers as a universal group experience.

The second building block of the warrior archetype could be defined as "unrestrained action," implying that one feels empowered when one can act without restrictions to deal with the issue at hand. However, it carries a particular complexity, as it also includes the potential use of violence. In this context, a full feeling of psychological empowerment is possible through one's own group lifting social restrictions on the use of violence. The social sciences literature on violence is also quite vast and the particular importance of sanctioned forms of violence was identified in its early days, particularly in the work of pioneer sociologist Max Weber (1919). What constitutes legitimate forms of violence, who should legitimize it, and in what circumstances are still hotly debated questions today, but the tremendous empowering effect of socially sanctioned violence has been well-known for a long time in social sciences (Milgram 1974).

The combination of "togetherness" producing feelings of strength in numbers with "unrestrained action" producing feelings of empowerment by the potential of using sanctioned violence, if necessary, creates a powerful release of psychical energy that can compensate fears emanating from the "unknown" and from "them." This constitutes a heuristic description of the warrior archetype being activated. The activation of the archetype does not necessarily need the use of violence to exist, as it is fundamentally a psychological compensating mechanism. It can be seen in its more ostentatious form in fictional representations in television shows like the *Sons of Anarchy*, where the main characters go to "war" against another bikers' gang. The gang has sanctioned the use of violence, based on an informal bikers' code, and the vast energy release is clearly shown in their eagerness to fight. But the warrior

archetype is also activated when a group of kids are adventuring in a wooden area less familiar to them; they go as a gang and usually, a few will instinctively pick up a wooden stick. A last example, from personal experience, was at a daycare picking up my daughter early and watching the all-female staff rushing to the door ready to handle a stranger woman verbally angry at the daycare, for some unclear reasons. The selection of these examples is to highlight that the activation of the warrior archetype *as-such* is not military or paramilitary-specific, nor is it gender-specific, and does not require the actual use of violence but only its potential. Hence, this description of the warrior archetype seems to have all the potential to pass Jung's universality test. Graphically, it can be represented as in Figure 1.

Figure 1



1.3. Activating the warrior archetype as a cultural practice

If we accept that the fundamental function of the warrior archetype is to produce a significant amount of psychical energy through "togetherness" and "unrestrained action" to handle an "unknown" world where dangerous "them" can be found, then one can posit that past and present military institutions, and their cultural dynamics, are fundamentally designed to "harvest" or "mobilize" this powerful source of human energy on an ongoing basis. This energy is in turn used to get things done in the face of violent adversity, physical stress, deprivation, and all the other challenges that war brings. In other words, permanently activating the warrior archetype in military personnel, to continuously mobilize such psychical energy, is the central dynamic of any military culture ancient or contemporary, whether there is an actual war to wage or in preparation for a known or unknown potential future war.

If the profound and fundamental mobilizing effect of the archetype *as-such* is not at the center of any study of military culture, then it will miss the central issue at stake. For instance, the seemingly irrational military obsession about creating conditions for team bonding on a nearly 24-hour basis, allegedly "proven" in promoting military

cohesion, even if a given personnel is working together all the time anyway, has been described by some as "male" dominating cultural ways, and seen as problematic in itself (Pendlebury 2020). Yet, this explanation is superficial at best, as such a social and cultural practice in the military only makes sense if one understands that it is fundamentally supporting an unconscious dynamics geared towards channeling on an ongoing basis the energy of an activated warrior archetype, especially through the "togetherness" component. Togetherness is not particularly male or female, even if the ways it is practiced may follow particular gendered cultural practices. The actual impact on military effectiveness and desirability of such permanent bonding is unconsciously assumed as valid because it is so deeply coherent with activating the warrior archetype, and therefore conscious and rational explanations to prove the need for such perpetual bonding very rarely occur in a military context; it is taken for granted.

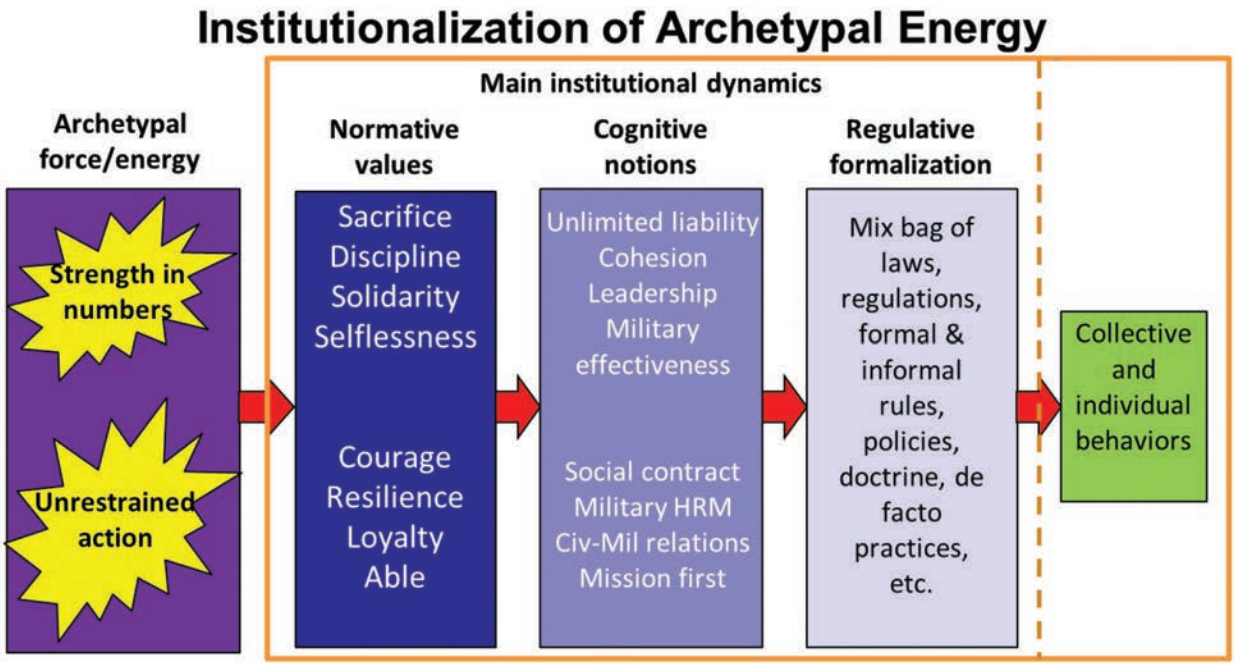
This lack of awareness and understanding of how central unconscious forces operate puts military organizations in a disadvantageous position in the face of those outside the military demanding change, as it is a pain to explain what seems so obvious. Furthermore, significant challenges in getting buy-in for changing ways of bonding in the military become suddenly quite explainable, especially if what is proposed as an alternative to bonding does not seek to continue activating the warrior archetype among the personnel. An approach to culture change incorporating the warrior archetype, however, would state and seek to find other ways where togetherness can be activated to the same degree but in manners where both men and women in uniform can feel safe. Unfortunately, the tendency has been rather to condemn such military practices as "male domination," as a blanket accusation (Duncanson 2015), without providing any credible alternative. Experience has shown that in such situations informal practices to reinforce togetherness emerge, and they tend to be far more dysfunctional and make buy-in even more difficult to achieve (Maaranen and Tienari 2020).

2. Warrior archetype and military institutional dynamics

The ongoing mobilization of psychical energy through the activation of the warrior archetype has been institutionalized in all militaries, and through this institutionalization, one can see cultural dynamics emerging. It is found in official doctrines and military history and numerous apocryphal narratives, which link back directly to the archetypal building block of "togetherness" in discipline, teamwork, solidarity, selflessness, sacrifice, etc. Other officially espoused normative values can be linked back to "unrestrained action" through sanctioned violence in courage, resilience, loyalty, ability (or fitness), etc. In turn, these normative notions have their counterparts in the cognitive realm through various formal concepts in military literature and practices such as unlimited liability, leadership, cohesion, military effectiveness, civil-military relations, social contract, mission first, the universality of

service, and the many criteria used in military human resources management. At the regulatory level, all these find themselves formalized in one way or another through a mixed bag of laws, regulations, permanent orders, policies, formal and informal rules, de facto practices, etc. The complexity of these arrangements is certainly staggering, but they all have unconscious and implicit golden threads going back to the warrior archetype *as-such*, providing them with foundational unconscious legitimacy. This deep unconscious legitimacy, in turn, is what allows psychical energy to be effectively "mobilized" permanently through those arrangements by continuously activating the warrior archetype. Graphically, it can be represented as in Figure 2.

Figure 2



To be fair, the warrior archetype is certainly not the only one being active in military institutions. One can think of the king archetype (group governance), where loyalty to the state creates particular conditions in decision-making; the magician archetype (those with special knowledge) where strategists and technologists have usually special privileges in the military, or the merchant archetype (making the most of the group's resources, oftentimes taking the form of managerialism in the modern world) can produce a conflict with military ethos, etc. Yet, the warrior archetype remains the single most important one in a military institution.

Any directed military culture changes based on altering on an ad hoc basis these institutional arrangements are at risk of failure if they are not done through a coherent effort deliberately congruent with the warrior archetype. A classic example was the unsuccessful American policy described as "don't ask, don't tell" regarding gay and lesbian people serving in the military (The White House 2021). If in theory, one's personal life should not be of interest to the military institution, collectively

mobilizing on an ongoing basis the psychical energy of individuals in uniform requires comprehensive "togetherness" to create feelings of strength in numbers. Past military practices have led to the exclusion of gays and lesbians formally and/or informally because their presence was seen as undermining togetherness, and "don't ask, don't tell" implicitly maintained such an approach. More recent policies focusing holistically on what an individual brings to the group, as a first step towards togetherness through individual commitment, are far more likely to succeed. This is because they remain aligned with the warrior archetype while altering how togetherness is construed from a general individual blanket contribution to the group's safety towards a skill and ability-based contribution to the group's safety. On the flip side, however, doctrinarian and academic-influenced proposals published in recent years where any form of togetherness is constantly criticized as attempts at domination, while seeking complete individual autonomy, if not sovereignty, for individual military members are going completely against the warrior archetype and are, in time, bound to fail.

2.1. Shadow and Warrior Archetype

When Jung presented his concept of the archetype, he also introduced the notion of the mythological realm, which is made of values, notions, rules, stories, myths, and symbols that are not universal, as they are always situated in time and space, in social and cultural practices. As discussed above, it is the realm of the archetypal representations. Yet, this realm is not static, things change whether it is because of natural crises, human affairs, new technologies, etc., and this leads to making aspects of the mythological realm out of phase with new realities over time. For Jung, it is an important aspect of analytic psychology, because many mental illnesses arise when an individual's deep beliefs become out-of-phase with reality, which could lead ultimately to psychosis (i.e., one living in his/her own mental world disconnected from social reality). The classic example can be found in overbearing parents towards their adult children, not accepting that they are autonomous adults now.

In these situations, individuals regress, and a shadow or negative archetype gets activated (Jung 1959, 20-21). The activation of the shadow archetype has for effect of redirecting life-force energy through a modified pattern, acting as a defense mechanism that tends to be very dysfunctional (Jung 1969, 96). Usually, it can be observed by hanging on older beliefs (i.e. values, notions, rules, etc.). The shadow archetype is also a bridging or compensating mechanism, and when activated it seeks to protect the internal unconscious psychological balance of an individual caused by the significant discrepancy between one's inner world and the outer reality. Also, a significant amount of physical energy is produced, and where the nasty side of one's personality can be observed. But for Jung, the shadow is not something to be rejected or to be belittled, instead, it is a part of one's personality to acknowledge and understand so that a genuine change and adaptive process can be launched.

Jung provided also a collective-level use of his archetypal concept of the shadow through his study of the rise of Nazism in Germany; hence shadow archetypal

configurations have demonstrated analogs at the collective level (Lewin 2009). More generally speaking, in the case of groups "the collective shadow is derived from the influence of broader social, cultural and religious factors that make certain qualities and characteristics of the personalities of persons belonging to the same group, nation or culture incompatible with a prevailing ethos or worldview" (Hennelly 1988, 222-223). The most common symptoms of a collective shadow being activated can be found when a group is developing a fixation on other "[…] groups which do not match the definition laid down by the cultural canon: aliens, inferiors, criminals, etc. Second, it consists of the negative projections by the dominant group upon the subordinate groups" (Gray 1996, 274). In other words, whoever does not "fit" into an older worldview is deemed the source of the group's problems, and ought to be dealt with.

This brings us to the heart of the matter regarding contemporary military culture change debates. There is very little doubt that 21st-century liberal views create conditions for the emergence of shadow warrior archetypal configuration in the military. The world changes but some militaries do not. If we go back to the case of the Canadian military, despite what recruits, trainees, and overall personnel are told by the senior leadership, they are working in an institution that faces significant contradictions. One should not underestimate the profound and negative impact on personnel of repeated stories and events such as the cancellation of the maritime helicopter project by a click of the fingers in 1993, the so-called "decade of darkness from 1992 to 2002 where the military faced deep budget cuts, the ongoing present lack of commitment to reach the 2% of GDP on military budget, the lack of high-end equipment to send to Ukraine, the interminable saga of the F-18 replacement, the ongoing societal narrative that the Canadian military should only be doing peacekeeping, etc. All these narratives send powerful and essentially permanent signals to the effect that the necessity of having armed forces in Canada is construed as questionable, as an expansive optional institution. This perception is also confirmed in a growing literature in security studies about Canada's seriously out-of-phase defence and foreign policies (Juneau et al. 2020). In this kind of environment, the central compensating function of the warrior archetype appears as being not necessary. To put it in Jungian terms, the social signal is that there is no need or desire to deal with the dangerous "them" out there and that the world does not have significant "unknowns" to worry about. The fundamental problem, however, is the military institution and its leadership remain actively dedicated to mobilizing the energy of an activated warrior archetype, through training, planning, and preparing for the eventuality of armed conflicts. The discrepancy between what the outer world is saying and what is going on in the inner world of the institution is significant.

2.2. Activation of the shadow warrior archetype as a cultural practice

2.2.1. Inward validation

If a society rejects a particular sub-group, then such sub-group will develop its own internal validation process to compensate. This is a well-known phenomenon

observed among minority groups, and there is a substantive and long-standing literature in social sciences about the centrality of social validation (Festinger 1954; Becker 1962; Berger and Luckmann 1966). In a military context, internal validation can go as far as seeking to self-appropriate legitimacy in the use of violence, which can become a critical element in understanding rogue behaviors. In more extreme cases, research has shown that social "disengagement factors can assist in enhancing the moral acceptability of killing, and in turn, make killing easier and less distressing (Aquino et al. 2007; Castano, Leidner and Slawuta 2008; Coman et al. 2014; Maoz and McCauley 2008; McAlister, Bandura and Owen 2006; Webber et al. 2013, 471). Similarly, veterans returning from conflict zones oftentimes face substantive challenges in reintegrating into civilian life, as the nature of social validation changes significantly (Demers 2011). In other words, to find back the empowering effect of "unrestrained action," some in the military will redesign on their own accord how the sanction of violence ought to be, with all the problems and issues that it entails for the institution.

The literature in organization studies also emphasizes how social validation produces cultural meaning and shapes identities, especially for newcomers in organizations (Smith et al. 2013). Yet, those cultural meanings are always open for challenge and are routinely resistant in organizations (Prasad and Prasad 2000; Mumby 2005; Burnes 2015), especially when new values sought after do not align with existing values within the personnel (Burnes and Jackson 2011). In these cases, resistance is not necessarily obvious and can be quite subtle, if not unconscious in nature (Schein 1984). It often takes the form of front-stage compliance while effectively engaging in backstage resistance, where a different set of values are adhered to (Ybema and Horvers 2017). This research literature, if enriched with the notion of the warrior archetype, shows that if on one hand the permanent activation of the archetype is sought after by the military institution, but the implicit sanction of using violence and even the existence of a dangerous world and "them" is denied on the other hand, one can only see that inward validation being the only way to maintain a collective internal psychical balance, to maintain in one's own eyes the legitimacy and value of one's own profession.

2.2.2. Negative projection against the "weak"

As the warrior archetype is also about bringing feelings of strength through togetherness, if older ways of producing togetherness are also denied, and more importantly not clearly replaced by new ones seen as legitimate, while the institution still seeks to mobilize the psychical energy by permanently activating the archetype, then the formation of a shadow version would be also the obvious result.

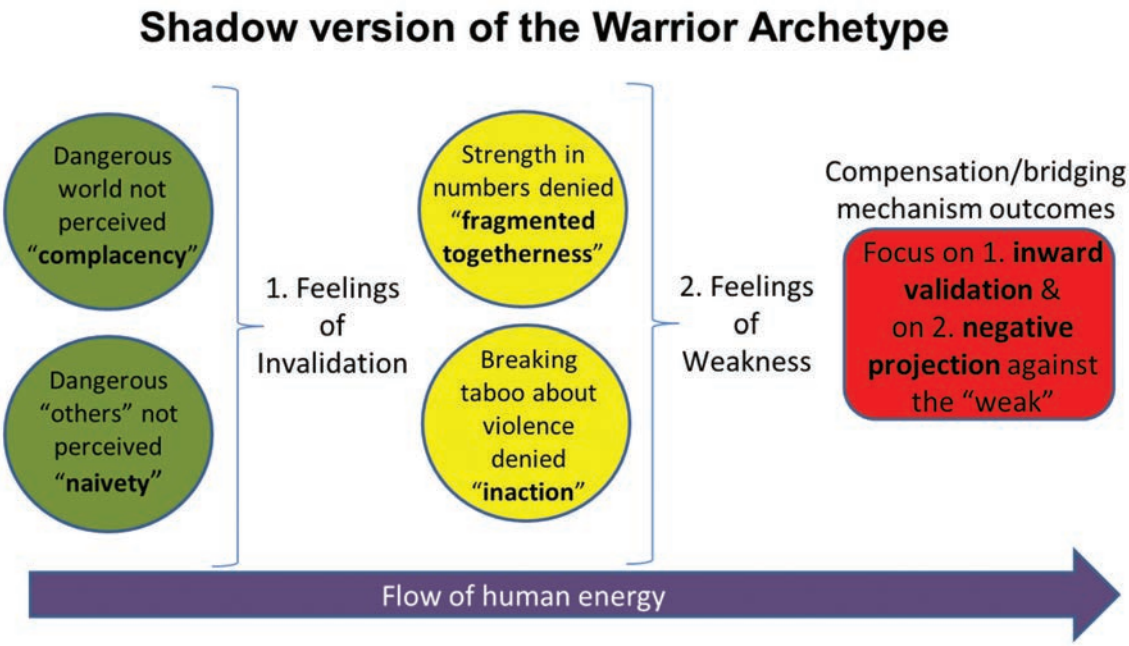
There is a vast literature about discriminatory attitudes and behaviors in social sciences, and it would be beyond the scope of this paper to review it all. For the purpose of this article, the notion of projection from analytical psychology will be used to shed light on how a dysfunctional compensation process is put in place to maintain feelings of togetherness. The notion of projection in psychology is a classic

one and can be defined as "ascribing of one's own motivations, feelings, and behavior to other persons" (Murstein 1957). The study of racism, for instance, has been and continues to be informed by the concept of projection (Clark 1999; Samuels 2020). Projection, in such contexts, means that individuals, who are psychologically challenged in their identity, ego, or self-concept, will project towards others the feelings causing their challenge. In the case of racism, racist projections are these individuals' own feelings of inferiority, of lack of self-esteem, of destitution that are projected towards groups who are visibly different from them, and who are usually under-privileged because of pre-existing social inequalities. According to this approach, racism is built in many ways on the foundation of an unconscious shadow and dysfunctional compensation mechanism.

When it comes to the modern military, if feelings of weakness are not compensated by feelings of strength through togetherness, then military members are at risk of projecting their feelings of weakness towards those who could be ascribed as the "source" of what is undermining togetherness. Given that historically military organizations have defined and cultivated the source of effective togetherness through homogeneity, then it should be expected that anyone undermining homogeneity can become a target for projection, namely women, minorities, non-heterosexuals, and even individuals coming from different social class origins.

Such a projection does not necessarily take the form of collective violent actions, but it can take the form of conscious and deliberate activities to encourage the "weak" to leave the organization. Yet, the most common forms in today's military are likely to be found in individual aggressions, micro-aggressions, and deliberate passive attitudes toward unhealthy work climate. Graphically, the overall shadow version of the warrior archetype could be represented in Figure 3.

Figure 3



3. Strategic-level way forward in light of the warrior archetype

This section proposes some high-level or strategic considerations for a way forward for culture change efforts in a military context, and to inform *the spirit* in which future policies and programs should be built to improve probabilities of success in implementing positive and durable cultural change. If one accepts that a shadow version of the warrior archetype is undermining the establishment of a healthier organizational culture, then addressing the core reasons as to why a shadow archetype has emerged should be the first order of business. As an illustration, the Canadian military case is used here once again.

3.1. Revalidating CAF personnel by acknowledging reality

In the early 2000s, the then Chief of Defence Staff General Rick Hillier was fully engaged in revalidating the CAF personnel after the so-called "decade of darkness" of the 1990s, marked by significant budget cuts and public criticism about personnel misconduct (Galloway 2007). Newly found energy and enthusiasm could be observed in many quarters of the military at the time (Thorne 2005). His focus was on getting back pride in the military profession, by engaging positively with the personnel and the general population and restoring effective military capabilities. These activities were described as a "transformation" effort (Jeffery 2010). Of course, the active Canadian engagement in the Afghan conflict coincided with his various strategic transformation activities. The CAF, at the time, had a clear dangerous "them" to deal with, and both the government and society showed significant solidarity towards this engagement. The era of focusing on peacekeeping was gone, "real" combat was the norm (Fletcher and Hove 2012). The point here is not about duplicating approaches taken during that era, but rather to illustrate what revalidating CAF personnel looks like in concrete terms.

Unfortunately, there are some structural issues that are beyond the CAF leadership control, and many of the issues faced by Hiller have resurfaced, even if in a different guise. Successive governments in Canada, and society in general, have only passing support for the military (Leuprecht and Sokolsky 2015). Once the engagement in the Afghan conflict subsided, a return to the "normality" of limited solidarity reinstated itself rather quickly. For instance, Canada's military spending reached a historical low of 0.99% of GDP in 2014 (Statista.com 2024). The CAF is a small military, almost always in a catching-up mode with respect to military equipment and technology, implicitly (or by neglect) not designed for high-end military engagements, etc., are all outcomes of the Canadian strategic culture (Massie and Vucetic 2019). This broader societal culture has shown no sign that will evolve in the foreseeable future either (The Economist 2023). As another clear illustration, through a leak to the *Washington Post* (Coletta 2023), it was discovered that Prime Minister Trudeau informed NATO allies that he had no intention to ever reach the 2% of GDP allocated to defense spending, something he never denied. It is in this context the CAF senior leadership needs to have an honest, frank, and ongoing discussion with its personnel

about what it really means to be part of the CAF today; namely, despite growing threats brought by Russia, the People's Republic of China, Iran, disinformation, etc., the Canadian military is not at par with our allies, and it will likely never be (Charron and Ferguson 2019). Canada does what it can, beyond symbolic gestures, but with limited will to do so. In other words, starting with the leadership, a non-complacent reality check is much needed, and it has already started to some extent. As Canada's Chief of Defence Staff General Eyre noted recently "Our people see the degrading declining security situation around the world and so trying to explain this [latest round of budget cuts] to them is very difficult…" (Tumilty 2023).

Revalidation needs to be based on a more sober and very public assessment of the CAF's overall situation and context. Courageous truth speaking to political power will likely be required as well. The overall objective for the CAF senior leadership is to create a self-concept based on reality rather than fantasy, and this will not be an easy task, but it is a necessary one. As noted in the organization studies literature, aligning lived values with espoused values is a critical task, but at times it is the espoused values that need to be seriously revisited (Bourne and Jenkins 2013; Jonsen et al. 2015; O'Brien 2020). The outcome of this is to adjust the ongoing mobilization of psychical energy through the activation of the warrior archetype in a manner that is consistent with what can be actually expected of the military institution. Unrealistic espoused values can have deep damaging effects, as discussed in organization studies (Smollan and Sayers 2009; Inabinett and Ballaro 2014). To put it in other words, there are some serious institutional "delusions of grandeur" in the belief that Canada can have an all-purpose force, high-end and combat capable in all-spectrum military conflict. This issue is not uniquely Canadian, and has been noted elsewhere (Carpenter 1997; Coyne 2011; Porter 2023). This will not create a high level of energy as observed in Hillier's time, but it will create better channeled "quiet energy" to change what is dysfunctional and start undoing inward validation, removing frustrations, and bringing expectations in line with reality. This would lead also to taking ownership of change, by regaining internal control over a narrative that would be far more honest and aligned with reality. Once again, the importance of internally owning such alignment has been underlined in organization studies (Balogun and Jenkins 2003; He and Baruch 2009; Karasvirta and Teerikangas 2022). The Canadian military did have great historical moments, but they fully belong to history. This is the difficult part that the senior military leadership needs to address to bring real buy-in to culture change and deactivate the shadow archetype.

3.2. Changing the meaning of strength and weakness

The second macro-level task would be to change how creating strength is construed within the CAF. There are already useful precedents based on the notion that diversity is a source of strength (Chuang, Church and Zikic 2004; Ashikali and Groeneveld 2015; Taylor, Santiago and Hynes 2019). Such a notion is certainly not antithetical to military affairs either. The synergetic effects of using the different combat arms,

logistics, intelligence, etc., in the Army, the notions of jointness, and force multipliers are all examples of strength through diversity. The key challenge is to bring this view of strength through diversity at the individual level, not just at the unit and sub-unit level (Resteigne and Manigart 2021). From a warrior archetype perspective, what brings strength in numbers is not defined in its content. Hence, any initiative that is built and sincerely perceived as growing the strength will be necessarily aligned with the warrior archetype and therefore would be much easier to legitimize and to get buy-in (Hubbart 2022). The key is for the CAF to own such an initiative through well well-calibrated and honest narrative about strength through diversity as something worth pursuing in its own right, rather than just being reactive to the government, societal expectations, and externally imposed narratives (Duval-Lantoine 2023).

In parallel, the definition of "weakness" needs also to be redefined publically, as it is central to the activation of the shadow warrior archetype. Research has shown that inequality leads to mistrust and lack of cohesion, acting therefore against togetherness (Helkama 2012). And yet, this has to reach the primary cohesion level not just the institutional one (Siebold 2007), which is where many culture change exercises fail in getting genuine buy-in. Again, there are also useful precedents to work with. For instance, Lt. Gen David Morrison, commander of the Australian Army made a famous video in 2013, if looked through the lenses of the warrior archetype, he essentially conveyed the sentiment that those who cannot accept diversity and who are sticking to the old ways are now a source of weakness, and they should get out of the military immediately; they are not needed as they are a liability. Such messaging, which was directed to every individual soldier, is also fully aligned with the warrior archetype because it is about building strength through togetherness. Such direct leadership activity can then, in turn, give personnel the possibility to own for themselves the change narrative (Dalpiaz and Di Stefano 2018). It appears, according to many accounts, that it was a successful approach (BBC News 2016).

It is not to say that the military of old ages is to be disgraced, quite to the contrary, it needs to continue to be honored for what it did at the time and within the social context in which it operated. The key is to convey the message that times have changed and what brings strength has changed too, and so the military needs to change to remain strong. This also means that all the discourses and narratives from influential people outside the military that are implicitly or unconsciously built on a notion of "evangelizing the barbarians" need to be kept at bay, as all it achieves is undermining trust and buy-in, as noted recently in Canada (Hopper 2024). Such messaging is profoundly counter-productive if one is seeking to build strength, get buy-in, and ultimately produce real and long-lasting change.

Conclusion

This paper seeks to introduce the notion of archetype, and more specifically the warrior archetype, to shed some light on military culture and its deep dynamics in

an attempt to fill some void in the literature. This notion provides a valid anchoring to understand military culture, especially when it is defined as a series of narratives, implicit norms, practices, and symbolisms geared towards mobilizing on an ongoing basis the psychical energy of an activated warrior archetype. It also provides a deeper understanding of why a military culture can become dysfunctional when shadow forms of the warrior archetype are active. A second objective was to provide some high-level illustrations of the difficulties of culture change in a military context. Any policy or program that cannot build a golden thread back to the warrior archetype *as such* is likely to be doomed to fail in the long run.

It also opens conversations about resistance to culture change where resistance is actually construed as a normal compensating mechanism that should not be ignored nor belittled as normative aberrations. People who resist are not stupid; rather they and the deeper reasons behind their resistance need to be understood from *their* perspective. When there is significant organizational resistance, the onus is always on the ones seeking change to provide better legitimate, and acceptable solutions. In the final analysis, seeking the reasons behind behaviors and attitudes fueled by a shadow version of the warrior archetype, and addressing them for what they are, is a far more productive approach than preaching a particular version of "Truth and Virtue" as an imperative.

References

Aquino, Karl, Americus Reed, Stefan Thau and Dan Freeman. 2007. "A Grotesque and Dark Beauty: How Moral Identity and Mechanisms of Moral Disengagement Influence Cognitive and Emotional Reactions to War." *Journal of Experimental Social Psychology* 43 (3): 385-392.

Ashikali, Tanachia and Sandra Groeneveld. 2015. "Diversity management for all? An empirical analysis of diversity management outcomes across groups." *Personnel Review* 44 (5): 757-780.

Aurelio, Jeanne L. 1995. "Using Jungian Archetypes to Explore Deeper Levels of Organizational Culture: Facing our organization's psyche." *Journal of Management Inquiry* 4 (4): 347-368.

Balogun, Julia and Mark Jenkins. 2003. "Re-conceiving change management: A knowledge-based perspective." *European Management Journal* 21 (2): 247-257.

BBC News. 2016. "Australian of the Year is equality activist Gen David Morrison." *British Broadcasting Corporation.* https://www.bbc.com/news/world-australia-35378881.

Becker, David V. and Steven L. Neuberg. 2019a. "Archetypes Reconsidered as Emergent Outcomes of Cognitive Complexity and Evolved Motivational Systems." *Psychological Inquiry* 30 (2): 59–75.

__. 2019b. "Pushing Archetypal Representational Systems Further." *Psychological Inquiry* 30 (2): 103-109.

Becker, Ernest. 1962. *The Birth and Death of Meaning*. New York: Free Press.

Berger, Peter L. and Thomas Luckmann. 1966. *The Social Construction of Reality: A treatise in the sociology of knowledge*. New York: Anchor.

Bloeser, Katharine and Heliana Ramirez. 2019. "Queering the Warrior Archetype: LGBTQ Servicewomen." In *Invisible Veterans: What Happens when Military Women Become Civilians again*, edited by Kate Hendricks Thomas and Kyleanne Hunter, 113-131. Santa Barbara: Praeger.

Bourne, Humphrey and Mark Jenkins. 2013. "Organizational values: A dynamic perspective." *Organization studies* 34 (4): 495-514.

Bowles, Martin L. 1993. "The Gods and Goddesses: Personifying Social Life in the Age of Organization." *Organization Studies* 14 (3): 395–418.

Brown, Mary Louise, Seonaidh McDonald and Fiona Smith. 2013. "Jungian Archetypes and Dreams of Social Enterprise." *Journal of Organizational Change Management* 26 (4): 670-688.

Burnes, Bernard. 2015. "Understanding Resistance to Change – Building on Coch and French." *Journal of Change Management* 15 (2): 92-116.

Bernard Burnes and Philip Jackson. 2011. "Success and Failure in Organizational Change: An Exploration of the Role of Values." *Journal of Change Management* 11 (2): 133-162.

Campbell, Joseph. 1991. *The Power of Myth*. New York: Anchor Books.

Carlsen, Arne. 2016. "On the tacit side of organizational identity: Narrative unconscious and figured practice." *Culture and Organization* 22(2): 107-135.

Carpenter, Ted Galen ed. 1997. *Delusions of Grandeur: The United Nations and Global Intervention*. Washington: Cato Institute.

Charron, Andrea and Jim Ferguson. 2019. "Canada and Defence Against Help: The Wrong Theory for the Wrong Country at the Wrong Time." In *Canadian Defence Policy in Theory and Practice*, edited by Thomas Juneau, Philippe Lagassé, and Srdjan Vucetic, 99–115. Cham: Palgrave Macmillan.

Castano, Emanuele, Benhard Leidner and Patrycja Slawuta. 2008. "Social identification processes, group dynamics and the behaviour of combatants." *International Review of the Red Cross* 90 (870): 259-271.

Chen, Rongxin Roger and Narasimhan, Rangapriya Priya Kannan. 2015. "Formal Integration Archetypes in Ambidextrous Organizations." *R&D Management* 45 (3): 267–286.

Chuang, You-Ta, Robin Church and Jelena Zikic. 2004. "Organizational culture, group diversity and intra-group conflict." *Team Performance Management: An International Journal* 10 (no. 1/2): 26-34.

Cloud, Doug. 2019. "The Rise of the Gay Warrior: Rhetorical Archetypes and the Transformation of Identity Categories." *Discourse & Communication* 13 (1): 26–47.

Coletta, Amanda. 2023. "Trudeau told NATO that Canada will never meet spending goal, Discord leak shows." *Washington Post.* https://www.washingtonpost.com/national-security/2023/04/19/canada-military-trudeau-leaked-documents/.

Coman, Alin, Charles B. Stone, Emanuele Castano and William Hirst. 2014. "Justifying Atrocities: The Effect of Moral-Disengagement Strategies on Socially Shared Retrieval-Induced Forgetting." *Psychological Science* 25 (6): 1281–1285.

Coyne, Christopher J. 2011. "Delusions of Grandeur: On the Creeping Militarization of U.S. Foreign Policy." *GMU Working Paper in Economics*, no. 11-03. https://ssrn.com/abstract=1753318.

Dalpiaz, Elena and Giada Di Stefano. 2018. "A universe of stories: Mobilizing narrative practices during transformative change." *Journal of Strategic Management* 39 (3): 664-696.

Demers, Anne. 2011. "When Veterans Return: The Role of Community in Reintegration." *Journal of Loss and Trauma* 16 (2): 160-179.

Diamond, Michael A. 2007. "Organizational Change and the Analytic Third: Locating and Attending to Unconscious Organizational Psychodynamics." *Psychoanalysis, Culture & Society* 12 (2): 142-164.

Duncanson, Claire. 2015. "Hegemonic Masculinity and the Possibility of Change in Gender Relations." *Men and Masculinities* 18 (2): 231-248.

Durand, Gilbert. 1996. *Introduction à la mythodologie*. Paris: Albin Michel.

Duval-Lantoine, Charlotte. 2023. "Culture Change Beyond Misconduct: Addressing Systemic Barriers." *Canadian Global Affairs Institute*. Policy Perspective paper. https://www.cgai.ca/culture_change_beyond_misconduct_addressing_systemic_barriers.

Enns, Carolyn Zerbe. 1994. "Archtypes and gender: Goddesses, warriors, and psychological health." *Journal of Counseling and Development* 73 (2): 127-133.

Erwin, Dennis G. and Andrew N. Garman. 2010. "Resistance to organizational change: Linking research and practice." *Leadership & Organization Development Journal* 31(1): 39–56.

Festinger, Leon. 1954. "A theory of social comparison processes." *Human Relationships* 1: 117-140.

Fletcher, Joseph F. and Jennifer Hove. 2012. "Emotional Determinants of Support for the Canadian Mission in Afghanistan: A View from the Bridge." *Canadian Journal of Political Science* 45 (1): 33–62.

Galloway, Gloria. 2007. "Hillier decries military 'decade of darkness.'" *Globe and Mail.* https://www.theglobeandmail.com/news/national/hillier-decries-militarys-decade-of-darkness/article20393158/.

Geisler, David. 2001. "Bottom-feeders: People who reject change." *Executive Excellence* 18 (12): 19.

Gover, Laura, Michael Halinski and Linda Duxbury. 2016. "Is it Just Me? Exploring Perceptions of Organizational Culture Change." *British Journal of Management* 27: 567–582.

Government of Canada. 2023a. *Canadian Military Journal* 23. Vol. 23, no. 3. http://www.journal.forces.gc.ca/cmj-23.3-toc-en.html.

__. 2023b. *Conduct and culture change progress tracker*. Ottawa: Department of National Defence. https://www.canada.ca/en/department-national-defence/services/conduct-and-culture/conduct-and-culture-tracker.html#2022-2023.

Gray, Richard. 1996. *Archetypal Explorations: An integrative approach to human behavior*. London: Routledge.

Grey, Chris. 2017. *A Very Short, Fairly Interesting and Reasonably Cheap Book about Studying Organizations*, London: Sage Publications Ltd.

He, Hongwei and Yehuda Baruch. 2009. "Transforming organizational identity under institutional change." *Journal of Organizational Change Management* 22 (6): 575-599.

Helkama, Klaus. 2012. "Equality, Trust, Fairness, and Cohesion." In *The Science of Unit Cohesion – Its Characteristics and Impacts*, edited by Mikael Salo, and Risto Sinkko. Finish National Defence University, Department of Behavioural Sciences, Series 1 (Number 1): 109-113.

Hennelly, R. Kevin. 1988. "The Psychological Roots of Political and Ideological Violence: A Jungian Perspective." *Alternatives* 13: 219-252.

Hopper, Tristin. 2024. "The Canadian military's all-in embrace of far-left 'anti-oppression' dogma." *National Post.* https://nationalpost.com/opinion/first-reading-the-canadian-militarys-all-in-embrace-of-far-left-anti-oppression-dogma.

Hubbart, Jason A. 2022. "Organizational change: considering truth and buy-in." *Administrative Sciences* 13 (1). https://www.mdpi.com/2076-3387/13/1/3.

Hughes, Mark. 2022. "Reflections: How Studying Organizational Change Lost Its Way." *Journal of Change Management* 22 (1): 8-25.

Hunt, Harry T. 2012. "A collective unconscious reconsidered: Jung's archetypal imagination in the light of contemporary psychology and social science." *Journal of Analytical Psychology* 57: 76-98.

Inabinett, Jean M. and Julie M. Ballaro. 2014. "Developing an Organization by Predicting Employee Retention by Matching Corporate Culture with Employee's Values: A Correlation Study." *Organization Development Journal* 32 (1): 55-74.

Jeffery, Michael. 2010. "Inside Canadian Forces Transformation." *Canadian Military Journal* 10 (2): 9-18.

Jonsen, Karsten, Charles Galunic, John Weeks and Tania Braga. 2015. "Evaluating espoused values: Does articulating values pay off?." *European Management Journal* 33 (5): 332-340.

Jones, Jenni, Janet Firth, Claire Hannibal and Michael Ogunseyin. 2019. "Factors contributing to organizational change success or failure: a qualitative meta-analysis of 200 reflective case studies." In *Evidence-based initiatives for organizational change and development*, edited by Robert G. Hamlin, Andrea D. Ellinger, and Jenni Jones, 155-178. Hershey: IGI Global.

Juneau, Thomas, Philippe Lagassé and Srdjan Vucetic eds. 2020. *Canadian defence policy in theory and practice*. Cham: Palgrave Macmillan.

Jung, Carl. 1959. *The Archetypes and the Collective Unconscious*. Princeton: Princeton University Press.

__. 1969. "On the nature of the psyche." *Jung Collected Work, volume 8*, 159-234. Princeton: Princeton University Press, 1969.

Karasvirta, Saara and Satu Teerikangas. 2022. "Change organizations in planned change–A closer look." *Journal of Change Management* 22 (2): 163-201.

Kociatkiewicz, Jerzy and Monika Kostera. 2010. "Experiencing the Shadow: Organizational Exclusion and Denial within Experience Economy." *Organization* 17 (2): 257–282.

Leuprecht, Christian and Joel J. Sokolsky. 2015. "Defense Policy 'Walmart Style': Canadian Lessons in 'not-so-grand' Grand Strategy." *Armed Forces & Society* 41(3): 541-562.

Lewin, Nicholas. 2009. *Jung on War, Politics and Nazi Germany: Exploring the theory of archetypes and the collective unconscious*. London: Karnac.

Long, Susan. 2019. "The unconscious won't go away-especially in organisations." *Organisational and Social Dynamics* 19 (2): 218-229, 289-290.

Maaranen, Anna and Tienari Janne. 2020. "Social media and hyper-masculine work cultures." *Gender, Work & Organization* 27: 1127-1144.

Maloney, Marcus and Scott Doidge. 2021. "Homegrown Heroes and New War Warriors: Post-9/11 Depictions of Warfare in Call of Duty." In *Militarization and the Global Rise of Paramilitary Culture: Post-heroic reimagining of the warrior*, edited by West, Brad and Thomas Crosbie, 57-74. Singapore: Springer.

Marion, James and John Lewis. 2020. *How to Fail at Change Management: A Manager's Guide to the Pitfalls of Managing Change*. Lowell: Business Expert Press.

Massie, Justin and Srdjan Vucetic. 2019. "Canadian Strategic Cultures: From Confederation to Trump." In Canadian Defence Policy in Theory and Practice, edited by Thomas Juneau, Philippe Lagassé, and Srdjan Vucetic, 29-44. Cham: Palgrave Macmillan.

Maurer, Rick. 1996. *Beyond the wall of resistance: Unconventional strategies that build support for change*. Austin: Bard Books.

McDougall, William. 1908. *An introduction to social psychology*. London: Methuen.

Milgram, Stanley. 1974. *Obedience to authority*. New York: Harper and Row.

Mills, Jon. 2013. "Jung's metaphysics." *International Journal of Jungian Studies* 5 (1): 19-43.

Mitroff, Ian I. 1983. "Archetypal Social System Analysis: On the deeper structure of human systems." *Academy of Management Review* 8 (3): 387-397.

Monneyron, Frédéric. 2014. "Gilbert Durand et l'étude des mythes." *Sociétés*, no. 123: 41-49.

Moore, Robert and Douglas Gillette. 1990. *King, Warrior, Magician, Lover: Rediscovering the archetypes of the mature masculine*. New York: HarperCollins.

Moxnes, Paul. 2013. "The Hero's dream and other primordial patterns of imagery: Archetypal influences on organisational fantasies and ideations." *Journal of Organizational Change Management* 26 (4): 638-653.

Mumby, Dennis K. 2005. "Theorizing resistance in organization studies: A dialectical approach." *Management Communication Quarterly* 19 (1): 19-44.

Murstein, Bernard I. 1957. "Studies in projection: a critique." *Journal of projective techniques* 21 (2): 129-136.

O'Brien, John. 2020. "Corporate Complex: Diagnostic and Application". In *The Professional Practice of Jungian Coaching: Corporate Analytical Psychology*, edited by Nora O'Brien, and John O'Brien, 127-133. London: Routledge.

O'Donovan, Gabrielle. 2018. *Making Organizational Change Stick: How to Create a Culture of Partnership Between Project and Change Management*. New York: Routledge.

Oreg, Shaul. 2006. "Personality, context, and resistance to organizational change." *European Journal of Work and Organizational Psychology* 15 (1): 73–101.

Pardo-del-Val, Manuela and Clara Martínez-Fuentes. 2003. "Resistance to change: A literature review and empirical study." *Management Decision* 41 (4): 148–155.

Park, Ernest S. and Verlin B. Hinsz. 2006. "Strength and safety in numbers: A theoretical perspective on group influences on approach and avoidance motivation." *Motivation and Emotion* 30 (2): 135-142.

Pearson, Carol. 1986. *The Hero Within: Six archetypes to live by*. San Francisco: Harper and Row.

Pendlebury, Jarrod. 2020. "'This Is a Man's Job:' Challenging the Masculine 'Warrior Culture' at the U.S. Air Force Academy. *Armed Forces & Society* 46 (1): 163-184.

Pisch, Anita. 2016. *Stalin in Soviet Posters, 1929–1953: Archetypes, Inventions & Fabrications*. Canberra: Australian National University Press.

Porter, Bernard. 2023. *Britain, Europe and the world 1850-1986: Delusions of grandeur*. London: Taylor and Francis.

Prasad, Pushkala and Anshuman Prasad. 2000. "Stretching the iron cage: The constitution and implications of routine workplace resistance." *Organization Science* 11: 387- 403.

Prince, Melvin and James Forr. 2021. "Metaphor elicitation: A new way to assess organizational culture." *The Psychologist-Manager Journal* 24 (4): 199-219.

Rafferty, Alannah Eileen, Nerina L. Jimmieson and Achilles A. Armenakis. 2013. "Change readiness: A multilevel review." *Journal of Management* 39 (1): 110–135.

Resteigne, Delphine and Philippe Manigart. 2021. "The Different Soldiers: A Look at Diversity and Inclusion in Military Organizations". In *Yin-Yang Military: Ambidextrous Perspectives on Change in Military Organizations*, edited by Jacqueline Heeren-Bogers, René Moelker, Esmeralda Kleinreesink, Jan Van der Meulen, Joseph Soeters, and Robert Beeres, 125-139. Springer: Cham.

Roesler, Christian. 2012. "Are archetypes transmitted more by culture than biology? Questions arising from conceptualizations of the archetype." *Journal of Analytical Psychology* 57: 223–246.

Statista.com. 2024. "Canada: Ratio of military spending to gross domestic product (GDP) from 2012 to 2022". https://www.statista.com/statistics/810367/ratio-of-military-expenditure-to-gross-domestic-product-gdp-canada/.

Samuels, Robert. 2020. "Simon Clarke and the Politics and Psychoanalysis of Racism." *Psychoanalysis, Culture & Society* 25 (1): 108-112.

Schein, Edgar H. 1984. "Coming to a New Awareness of Organizational Culture." *Sloan Management Review* 25 (2): 3-16.

Siebold, Guy L. 2007. "The essence of military group cohesion." *Armed Forces & Society* 33 (2): 286-295.

Smollan, Roy K. and Janet G. Sayers. 2009. "Organizational culture, change and emotions: A qualitative study." *Journal of change management* 9 (4): 435-457.

Starr-Glass, David. 2004. "Exploring Organizational Culture: Teaching notes on metaphor, totem and archetypal images." *Journal of Management Education* 28 (3): 356-371.

Smith, Laura G. E., Catherine E. Amiot, Joanne R. Smith, Victor J. Callan and Deborah J. Terry. 2013. "The Social Validation and Coping Model of Organizational Identity Development: A Longitudinal Test." *Journal of Management* 39 (7): 1952–1978.

Smythe, William E. and Angelina Baydala. 2012. "The hermeneutic background of C. G. Jung." *Journal of Analytical Psychology* 57: 57–75.

Szitanyi, Stephanie. 2020. *Gender Trouble in the U.S. Military*. Cham: Palgrave MacMillan.

Tallman, Bruce. 2003. "The Organization Leader as King, Warrior, Magician and Lover: How Jungian Archetypes Affect the Way Men Lead Organizations." *Organization Development Journal* 21 (3): 19-30.

Taylor, Andrea, Felix Santiago and Rilla Hynes. 2019. "Relationships Among Leadership, Organizational Culture, and Support for Innovation". In *Effective and Creative Leadership in Diverse Workforces*, edited by Bethany K. Mickahail, and Carlos Tasso Eira de Aquino, 11-42. Cham: Palgrave Macmillan.

The Economist. 2023. "Canada's miserly defence spending is increasingly embarrassing". https://www.economist.com/the-americas/2023/07/24/canadas-miserly-defence-spending-is-increasingly-embarrassing.

The White House. 2021. "Statement by President Joe Biden on the Tenth Anniversary of the Repeal of Don't Ask, Don't Tell". https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/20/statement-by-president-joe-biden-on-the-tenth-anniversary-of-the-repeal-of-dont-ask-dont-tell/.

Thorne, Stephen. 2005. "Rick Hillier". *International Journal* 60 (3): 824-830.

Tumilty, Ryan. 2023. "Defence budget facing nearly $1 billion in cuts, Chief of Defence staff says". *National Post.* https://nationalpost.com/news/politics/chief-of-defence-staff-military-budget.

Turner, Stephen P. 1977. "Complex organizations as savage tribes." *Journal for the Theory of Social Behaviour* 7: 99-125.

Waddell, Dianne and Amrik S. 1998. Sohal. "Resistance: A constructive tool for change management." *Management Decision* 36 (8): 543–548.

Webber, David, Jeff Schimel, Andy Martens, Joseph Hayes and Erik H. Faucher. 2013. "Using a Bug-Killing Paradigm to Understand How Social Validation and Invalidation Affect the Distress of Killing." *Personality and Social Psychology Bulletin* 39 (4): 470–481.

Weber, Max. 1919. *From Max Weber: Essays in Sociology*. Oxford: Oxford University Press.

Ybema, Sierk and Martha Horvers. 2017. "Resistance Through Compliance: The Strategic and Subversive Potential of Frontstage and Backstage Resistance." *Organization Studies* 38 (9): 1233–1251.

Young-Eisendrath, Polly and Terence Dawson eds. 1997. *The Cambridge Companion to Jung*. Cambridge: Cambridge University Press.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Possibilities of using virtual reality technology in skills development

Colonel Imre NÉGYESI, Ph.D.*

*Head of Department of Information Technology
University of Public Service, Budapest, Hungary
e-mail: negyesi.imre@UNI-NKE.hu

Abstract

With changing threats and rapid technological progress, society is facing significant changes and challenges. Ensuring that people have the skills and capabilities to meet these challenges is key. One 'tool' for this could be the use of virtual reality (VR). The VR research community is becoming increasingly active in the search for solutions. In this article, we have tried to summarize the concepts related to VR education and training, followed by the challenges of using VR technology and the solutions already implemented through examples from the US, France and China. We then concluded the article by outlining possible future concepts that will need to be developed to implement VR training, with a particular focus on the issues of military training.

Keywords:
metaverse; virtual reality; military training; skill development; VR-technology; VR training courses.

Article info
Received: 2 February 2024; Revised: 26 February 2024; Accepted: 18 March 2024; Available online: 5 April 2024

Citation: Négyesi, I. 2024. "Possibilities of using virtual reality technology in skills development." *Bulletin of "Carol I" National Defence University*, 13(1): 31-43. https://doi.org/10.53477/2284-9378-24-02

Virtual Reality (VR) has emerged as a new field of multidisciplinary research. In the last ' few years, its scope has expanded beyond academic research and industry is investing heavily in this field, both for research and for the development of various VR-based products. Various industrial sectors such as information technology, biomedical engineering, structural design and the technology sector for training aids are investing in this technology. The military industry, always looking for new ideas, is slowly becoming one of the main investors in VR. Like many other scientific discoveries, VR is rooted in science fiction novels and essays and is therefore a centuries-old concept, but in the past, the concept was defined differently. Many generations ago, the Greek philosopher Plato (427-347 BC) offered the rulers of the day a perspective on political decision-making, and in doing so, he promoted a concept similar to that of virtual reality in his day. He urged them to make political decisions strictly based on certain knowledge and insights, not on intuition. Over the years, the concept of virtual reality has evolved considerably. In particular, important developments in the information technology sector have revolutionized the definition of virtual reality considerably.

1. VR and related concepts

Before starting to analyze the topic indicated in the abstract, i.e. the possibilities for military use, let us first consider what the terms used mean. The topic under consideration is relatively new and therefore lacks a universal definition, the phenomenon has been approached in many different ways and, of course, each has had a different view of what is important. Linda Jacobson[1] and Steve Tice[2] defined the term as follows: 'In our view, "virtual reality" refers to technologies or environments that provide realistic cues to some or all of the senses sufficient to induce a willing suspension of disbelief in the participant. A successful VR application provides quality content and experience; thus, virtual reality essentially represents an evolution in user interface studies and human factors-based application design." (Tice and Jacobson 1991)

To clarify the concepts, let us look at the difference between Augmented Reality (AR) and Virtual Reality (VR), because these two concepts are sometimes erroneously referred to together, mainly because of the similarities between the two technologies. AR, as the name suggests, adds (extends) information to the actual reality. But the essence of VR is that it takes the user out of reality and places him or her in an artificial space. The aim of VR is therefore to make the virtual space as plausible as possible by using visual elements, sound effects and a variety of accessories. However, life is more complex than that, as there is also the concept of Mixed Reality (MR). MR combines elements of AR and VR by adding digital objects to the real space and allowing these now virtual elements to interact with reality. To conclude the clarification of the concepts, we should also

[1] Commercial VR hardware and software development, operation and implementation specialist. Since 29 August 22, J2022, he has been the Director of Marketing at HaptX, a leading supplier of realistic VR and robotic gloves in the US.
[2] Manager, currently Sr. Manager Product Engineering at Texas Metropolitan Area.

mention Augmented Reality (XR), where 'X' refers to the variables that the above technologies will include in the future.

The picture can be further nuanced by looking at the fact that the aforementioned Linda Jacobson, in her book "Cyberarts: Exploring Art & Technology" (Jacobson 1995), distinguishes between four different virtual realities:

- Perpetual virtual reality;
- Desktop virtual reality;
- Projected virtual reality;
- Desktop Virtual Reality; Desktop Virtual Reality; Simulation Virtual Reality.

However, there are other types of virtual reality, so let us look at an extended list:

- Perpetual, first-person singular virtual reality (e.g. head-mounted displays (helmets), fibre-optic cable gloves, position tracking devices and surround sound systems).
- Augmented reality, which creates a transparent layer of computer graphics that highlights elements of reality and aids understanding.
- Virtual reality is viewed through a window, where you can view the virtual three-dimensional world through a monitor and navigate using tools such as a mouse.
- The mirrored world allows a second-person experience, where the viewer is outside the imaginary world but can communicate with persons or objects in the projected world.
- Waldo World (virtual persons) is a blend of digital puppetry and real-time computer animation.
- A relatively small-scale projected virtual reality theatre controlled by a number of computers.
- A car simulator environment is essentially an evolution of a traditional simulator.
- Cyberspace is an artificial reality on a global scale that can be viewed by multiple people at the same time via a computer network.
- Remote Presence/Teleoperation appears as if you are in a place that is different from your real location.
- A viewing dome is an immersive, multi-user, single-projection virtual reality environment, where the user enters a "viewing dome" and finds themselves in a hemispherical space that provides complete immersiveness.
- The Experiential Learning System, which aims to provide the military with a high-fidelity system based on virtual reality and artificial intelligence to ensure realistic military exercises.

The definition of the term is therefore quite broad. In the first part of this article, we will look at the areas where VR can be used to help with workforce training. Traditionally, training took place in classrooms or laboratories through presentations and practical exercises. However, it has now been shown that VR can drastically reduce the cost of training while improving the effectiveness of training. (This is why we will compare the two forms of training, focusing on military training.)

https://doi.org/10.53477/2284-9378-24-02

2. Traditional training or VR

Since all comparisons are subject to errors of subjective judgement, we will keep the comparison of the two types of training at a general level and use only listed facts to support our arguments, rather than a deeper analysis. Let us first look at some of the possible disadvantages of traditional education:

- Getting to the training sites can be time-consuming and involve extra costs.
- It can be more expensive to produce training materials.
- Allowances for trainers may be an extra cost.
- Less effective training due to less attractive and unintuitive visuals in classrooms (e.g. lack of 3D animations)
- Some skills cannot be taught in a real-world classroom environment (e.g. emergency procedures)

Of course, VR training does not automatically guarantee lower costs, but the benefits that these systems bring to trainees can justify the investment. VR also reduces training costs by increasing the number of training scenarios. This is possible because VR training scenarios are mainly computer-generated 3D graphics, VR developers can easily create different scenarios from existing 3D assets that can be used repeatedly to train different people. A particular advantage is that the scenarios available online are convenient and inexpensive. At the same time, VR technology also allows students to learn in their own homes, which further reduces additional costs (electricity, water, heating, etc.). Another feature of VR training is that it allows students who otherwise have difficulty coping with teacher supervision and the presence of observers to do well. There are, of course, training situations that need to take place in the presence of the instructors, because it is necessary to warn students of any problems they may be experiencing and to draw their attention to negative trends in their performance. VR also allows training to be carried out safely in situations that could lead to a fundamental hazard (fire, explosion, etc.).

The scope of this publication is limited to VR training. Accordingly, training in other augmented reality domains (e.g. augmented and mixed reality) will not be considered. VR training can be evaluated from a myriad of perspectives: from software selection to software development, from graphical fidelity to runtime efficiency, and from interaction techniques to interaction realism. The VR training creation process can be divided into three stages:

1. task analysis (hierarchical[3], cognitive[4]);
2. preparation of a training scenario[5];
3. implementation.

The main difference between traditional and VR training is the implementation. Traditional training methods are usually based on

[3] HTA (Hierarchical Task Analysis): describing goals that are made up of different units.
[4] CTA (Cognitive Task Anlysis): focuses on dealing with unexpected situations.
[5] The work on the development of efficient and comprehensive representations of training scenarios not only provides a general framework and new ideas for the design of new VR training applications, but also offers a theoretical basis for the development of procedural approaches for the automatic generation of virtual training environments.

technical manuals or multimedia resources, whereas the implementation of VR training is nowadays based on modelling and simulations, which are essential components of VR training software.

2.1. VR training in military training

It is undeniable that military training can be dangerous. Many soldiers die every year from non-combat causes or accidents. Technology is constantly evolving. We can now simulate different environmental conditions, such as day and night, and take into account different types of weather and other scenarios. NATO was quick to recognize the potential of VR technology. Already in February 2003, the NATO Research and Technology Organization (RTO) published a technical report entitled "Virtual Reality: the state of military research and applications in member countries". (RTO/NATO 2003) The military has started to use simulation software and serious games as training tools, so it has started to exploit the potential of virtual reality. The United States, for example, has developed the Flooding Control Trainer (FTC) to train recruits in the US Navy in various skills. US Aviation has begun experimenting with VR training through the Aviator Training Next (ATN) program to supplement traditional hands-on training. Their preliminary results suggested that VR training produced pilots of similar quality and competency as pilots trained in "real" aircraft. One of the main drivers for these improvements was precisely the fact that traditional training methods are often limited by the real training environment and some specialized tools or equipment. VR training provides a safe, controlled virtual environment at a relatively low cost for soldiers to practice their technical skills and develop their cognitive functions.

Another thing that can be said about military training is that many traditional training methods require a specific location or equipment.[6] As examples, let us look at some VR training already in operation. One of the main training tools used to train all Landing Signal Officers (LSOs) for several decades is the 2H111. This simulator is located in Oceana, Virginia, and the device itself is housed in a two-story room and consists of several large screens and physical displays of actual equipment used by LSOs in their operational environment. Young officers serving in this speciality typically encounter this system only during a short formal training period (six one-hour sessions), leaving more dead time in training. While the 2H111 experience is extremely valuable for any LSO officer, the time spent using the training tool is undeniably too short. The need to provide LSOs with an unlimited number of training opportunities that are not constrained by space and time, coupled with recent advances in commercially available immersive technologies, has provided an ideal platform to create an easy training solution that fills these gaps and goes beyond the options currently offered in the 2H111 simulator. The main objective of the 2H111 training capabilities is to ensure that the

[6] These field and portable devices can be a starting point for further developments. (See previous articles by the author.)

new prototype system is mapped to support the main training objectives of 2H111, the design and development of the prototype training system. The results achieved so far show that it is definitely time to renew the LSO training to take the leap towards immersive VR and provide an ideal platform to create a lightweight training solution that addresses the training gaps and goes beyond the capabilities currently offered in the 2H111 simulator.

Another such training tool, which is also not new, in which VR has greatly improved the quality and condition of training compared to traditional methods and which helps French Army infantrymen master the calibration procedure for infrared sensors is the 21st-century combat system called FELIN[7]. In order to practice on the actual FELIN system, soldiers have to practice several times on the conventional software until they get it wrong.

FELIN is a system developed by the French Army's Infantry Soldier Modernization Programme. The complete system was developed by a consortium led by Sagem as integrator. FELIN combines the modified FAMAS[8] machine rifle with a range of other electronics, clothing, helmets and body armor. The portable electronic platform (PEP) is the core of the system. All the electronic equipment of the system is connected to the PEP. These are the tactical radio, the weapon and helmet mounted and handheld optics, the commander's battle management system (BMS) terminal and the batteries. The PEP includes a wearable computer that uses a USB 2.0 interface for data communication with the communication and navigation unit. The suit contains two wired networks. One transmits electrical power to all systems. The other provides the data connection. The system's communication device is the Thales TRC-9100 voice and data radio. The radio has an integrated GPS receiver. A SitComdé tactical terminal in the commander's kit connects to the SITEL combat management system installed on the combat vehicle. The device with color touch screen allows the driver to manage the tactical situation, with integrated messaging and friend/enemy situation display. The handheld optics is the JIM LR (long range) portable multifunction infrared telescope, a member of the Sagem JIM modular optics family. These devices can also be equipped with optional features and functions to meet requirements. The biggest improvement is that while the conventional system only provides soldiers with a 2D program to practice the calibration procedure, the new VR method allows them to practice in a virtual environment with a 3D-printed rifle model, which provides similar control and feel of use as its real-life counterpart. An ad hoc study was carried out on a group of French soldiers to compare these two methods. The results showed that the VR method greatly improved the soldiers' learning efficiency and their intrinsic motivation to perform training tasks. The US and French training tools using this VR technology illustrate the ambitions of both countries. All of the developments already implemented have already

[7] Fantassin à Équipements et Liaisons Intégrés, Infantry soldier with integrated equipment and links.
[8] FAMAS: Fusil Automatique vagy Fusil d'Assault, MAS – Manufacture d'Armes St. Étienne, Automatic rifle from the St Etienne arms factory.

been incorporated into training exercises in order to reduce the number of accidents during training. With these training tools, it may be possible in the future to minimise the risks during training operations.

2.2. VR and military equipment training

In the next section, we looked at the possibilities related to the training of weapons and other military equipment, in short, military equipment. The training of military equipment has its own notable feature, namely the need to train troops in the equipment to be used in combat before deployment. It is also a specialty that the training concerns the actual equipment of the army, ensuring that VR technologies will also meet specific requirements. In general, however, the educational equipment of military training sites (academies, universities, university faculties, training centres) is not in line with the training equipment of the troops and often lags behind the pace of renewal of the troops' equipment. Therefore, a common problem in current military college and university equipment training is that the equipment is incomplete and outdated, the instructional layout of practical operations training is more prominent in equipment instruction than actual deployment, causing students to lack practical proficiency in the equipment, and the teaching effect of practical operations is generally unsatisfactory. The main reason for this is the lack of effective teaching resources, according to a summary of traditional practical training, the following problems mainly arise. Even if the problem of financial expenditure is not taken into account, due to the strict management of actual combat equipment and the fact that military equipment used in education and training is not usually active military equipment, it is true that the production of a model of military equipment for educational purposes can significantly increase the cost of procurement.

In the field of security and defence, training is considered by all forces to be one of the key factors in developing soldiers' skills in tactical operations. Advances in technology and communications have enabled the development of new technological tools to be efficient and at significantly lower operating costs. This section presents the design of a virtual firing range for one of the key training tasks, simulating an open polygon that includes the recreation of real scenarios, 3D objects, silhouettes, targets and weapons from each region of the country. The soldier performing the individual firing task is modeled as a 3D object, positioned relative to the virtual environment on the firing range. The VR environment could include multiple virtual environments (e.g., jungle, urban, rural, coastal, mountainous, etc.). Preliminary published results in usability showed that participants perceived realism in the scenarios and the 3D objects that comprised them. Evaluations of the tools used showed that virtual reality goggles and VR weapon controllers facilitated the visualization and interaction of virtual scenarios during training. Based on

this, it can be said that the virtual shooting range mentioned as an example can be a useful and complementary tool for training military personnel and developing the skills needed to carry out tactical operations. It could be a cheap technological alternative, reducing risk, and increasing the time and number of training sessions.

After building each feature module of virtual training software, a full debugging of the software should be performed on the Unity 3D platform to find software loopholes and optimize the software locally and globally to underpin the final software release. Software debugging mainly includes the following aspects:

- Does the graphical interface adequately represent the real operational steps?
- Is the animation composition smooth and correct?
- Is the background information included correctly?
- Is the operation of each function smooth and correct?

To summarize, in the case of software running on the Unity 3D platform, the exercises carried out so far have demonstrated that virtual training software can be a good complement to the teaching and training of military equipment and has good prospects for military education and training.

3. What could the future hold? The metaverse and the army

In this chapter, we look at what the future might hold for us. As VR technology continues to evolve and its use becomes more diverse, we have selected an area where recent research and future prospects may be worth exploring from a military perspective. The first area under consideration is image fusion, which is currently being widely used as an important branch of multi-sensory information fusion. This area may also be worth exploring because the development of existing image processing software is conducive to further analysis of images, but today, many problems still face operators in developing image processing technology.

The NUKE software was "arbitrarily" used for the analysis, mainly because it does not require a specific hardware platform (x86-64 processor, 5.70 GB free disk space, 8 GB RAM, 1280X1024 pixel resolution and 24-bit color, graphics card with 512 MB memory and driver support for OpenGL 2. 0), support for all major operating systems (operating systems already tested: macOS Big Sur 11.x, macOS 12.x Monterey, Windows 10 or 11, CentOS 7.6), while providing users with flexibility, efficiency and full functionality. The latest version of the NUKE 3D system (14.0) has enabled users to work more efficiently with modern 3D scenes by introducing a new USD-based beta system. Nuke also integrates the famous Primatte[9], Uimatte and Keylight encoding plug-ins by

[9] Primatte Studio is the world's best software-based key solution that not only includes Primatte 3D key cutting technology, but also includes a custom on-screen toolbar that guides users through the key cutting process, ensuring a perfect key every time.

default, giving unlimited possibilities for post-coding work. Based on the software's powerful image processing function, it performs experiments and analysis on image fusion algorithm, and in the proposed image fusion algorithm, it provides the experimental basis and images for research of the proposal and application. From these technical specifications alone, it is clear that NUKE, although primarily designed for artists, can be effectively used in education, including military education and training.

After analyzing this example, let us return to the general issues of metaverse and educational innovation and the development of metaverse educational applications and their impact on military training. This section also starts with a definition of the basic concept, namely metaverse. In the simplest terms, a metaverse is the concept of an online, 3D universe that combines several different virtual spaces. It can also be thought of as a future version of the internet. However, the metaverse does not yet exist, but some platforms already include "metaverse-like" elements. In more concrete terms, "The metaverse is a post-reality universe, a persistent and real multi-user environment that combines physical reality with digital virtuality." (Mystakidis 2022)

Whatever the definition of the metaverse, it is now clear that China, which is also at the forefront of artificial intelligence research, is aiming to play a leading role in all the related technology industries that will serve as the backbone of this emerging technology. China's role is also worth examining because most talk of the metaverse is about civilian applications, but there is growing debate in China about its potential military applications. As a starting point, it is argued that although the metaverse is still in its infancy, the downgrading or disabling of the metaverse could have serious consequences as society and even the military become increasingly integrated and reliant on this technology. The importance of its military use has already been published in several scientific analyses, already referred to under the new name of "battlefield technology" and aimed at finding possible methods of attack on the adversary's own metaverse. A study by the prestigious New Media Research Centre at Tsinghua University has already identified security concerns that could be significant for military use. A study by the China Institute of Contemporary International Relations (CCIR) has already identified generalized national security risks. The study identified three areas of concern:

1. Technological hegemony, i.e. that some countries develop metaverse technology faster, can cause instability in capabilities and access.
2. Cyber and data security, as relying on and using the metaverse, will make data sharing more sensitive and is considered a category of critical infrastructure.
3. How metaverse will change a country's politics, economy and society.

February 2022, the People's Liberation Army (PLA) joined the enthusiasm for the metaverse and celebrated Chinese New Year with a Spring Festival on the military network in virtual space. The event was hosted by avatars and broadcast live. The

description of the event boasted, "Participants using HTML 5 were guided by the integration of artificial intelligence, image recognition, semantic analysis, holographic imaging and other technologies." (Qingxiu, Shiyang and Chenxu 2022) The attachment to the metaverse is also reflected in China's "National and Cyberspace Security Strategy", which focuses on the importance of sovereignty, the digital economy, norm formation, and the cultural impact of cyberspace. The authors write, "Cyberspace has become a new field of human activity with the same significance as land, sea, air, and space, national sovereignty has been extended to cyberspace, and cyberspace sovereignty has become an important part of national sovereignty." (China Copyright and Media 2016)

Since the metaverse represents the new frontier of cyberspace, it is logical that the Chinese Communist Party would want to invest heavily and take a leading role in technology to better defend its own sovereignty, rather than have another nation take on this role. From an economic perspective, China considers that taking the lead in metaverse technology will have a significant positive impact on their already rapidly expanding digital economy. The authors write in their start-up paper that the internet has "spurred an adjustment of economic structures and a transformation of economic development methods, giving a new impetus to the economy and society." Harnessing this momentum and leading a meta-digital transformation could have an incredible impact on China's economy. If the metaverse is the next phase of the internet, then whoever leads it could reap huge benefits from the billions of potential users.

4. Realized "battlespace"[10]!

[10] or battlefield

It is clear from the previous chapters that China's leadership in the application of artificial intelligence is unquestionable, so it may be worth looking at their specific views on the potential for military use of the metaverse. In an article entitled "Looking Forward to Battleverse" in the late January 2022 edition of PLA Daily, the term "Battleverse" has already appeared in the article to emphasize the importance of military applications. In addition to emphasizing the potential for training use, an important fact is that there is no mention of further necessary technological breakthroughs. The predicted scenarios all use current VR/AR/MR and digital technology. Let us take a point-by-point look at the technical conditions needed to make the "battlefield" work:

- independent network;
- independent communication;
- authentication security (strict access filtering process, recording of all operations of the elevators);
- assignment of user levels (trainers, examiners, staff officers, system operators and maintenance staff, etc.) to access;

- artificial intelligence bots to assist individual users;
- realistic simulation performance (aiming to reproduce the functional performance of real weapons and weapon systems);
- creation of a realistic environment (geographic, electromagnetic, meteorological and hydrological environment).

The combination of these conditions can provide an opportunity to make better use of virtual space in military training. A summary of the potential benefits for military training and military-style education:

- The „battle room" will play an important role in centralized military education, allowing free communication with teachers and students regardless of location. Virtual teaching tools will also improve teachers' ability to explain new concepts.
- The „battlefield" can be able to fully meet the actual combat requirements of a large-scale operation. Repeated training and assessment help to improve tactical cooperation and combat morale of soldiers.
- The new weapons can be tested in simulations to assess performance, compatibility and overall combat effectiveness. (This can also increase the life span of conventional weapons.)
- The „metaverse" coordinates expert resources regardless of their physical location. A platform for remote extraction and control of new equipment and innovation in tactics. Conduct continuous analysis and acquire vast data sets for analysis and research objectives.
- If the usual means of command communications are destroyed in a confrontation, the „battle space" can even act as a backup communications system.

An important form of use of the „battleverse" is therefore the training of soldiers in actual combat conditions, for which virtual reality simulations are used. This is cost-effective and allows for significantly more training. Let us look at a Chinese example of the latest application of this type of training. The Chinese People's Liberation Army (PLA) has introduced a VR parachute training system for new paratroopers. The program uses spatial positioning, virtual simulation and other technologies to build a realistic skydiving environment, allowing new skydivers to detect various aerial emergencies, thereby reducing the risks of actual skydiving. All VR jump data is collected to help teams train most effectively. The result is that the simulation improves the training level of paratroopers, while also providing them with a platform to experience new paratrooper types, unfamiliar environments and new training subjects, which can greatly help paratroopers adapt to different battlefield demands and improve their skills.

Of course, the competition between the United States and China can be traced not only in the field of artificial intelligence but also in the application of VR. Although the US does not use the word „battleverse", it is clear that it has similar views on the

benefits of a military metaverse. The idea of using virtual worlds to prepare soldiers for war can be traced back to the 1980s with SIMNET, a large-scale network of various vehicle simulators and displays for real-time distributed combat simulations. (Tanks, helicopters, and planes on a virtual battlefield.) In recent decades, the standard for distributed interactive simulation and high-level architecture to perform real-time, platform-level wargaming has been developed on multiple hosts. Since SIMNET was a network simulation, each simulation station needed its own representation of the shared virtual environment. The demonstration stations themselves were mock-ups of certain tank and aircraft control simulators and were set up to simulate the conditions of an actual combat vehicle. Tank simulators, for example, can accommodate a full crew of four to increase the effectiveness of training. The network is designed to support hundreds of users simultaneously. The fidelity of the simulation was such that it could be used for training for mission scenarios and for tactical rehearsals of operations during US operations. SIMNET was actively used by the US Army for training primarily at Fort Benning, Fort Rucker and Fort Knox.

The SIMNET-D (Developmental) program used the simulation systems developed in the SIMNET program to conduct experiments related to weapon systems, concepts, and tactics. This became the Advanced Simulation Technology Demonstration (ADST) program. In the military branches, this type of technology is used to prepare soldiers for combat. Recently, the US military's newest branch, the Space Force (USSF), has described investment in the metaverse as key to their success. Recently appointed Space Force Chief Technology and Innovation Officer Lisa A. Costa stated on the first day of the Armed Forces Communications and Electronics Association (AFCEA) "Space Force Information Technology Day" in February 2022 that the USSF must "take advantage of what industry has of the investments made in the metaverse. These technologies could be used for training and operations, and when integrated into the digital engineering ecosystem, operator feedback could be used to automatically improve the product during the next iteration."

Conclusions

The metaverse is an emerging technology, so it is difficult to gauge how it will affect society, politics, economics, international norms, national security, and society as a whole. We are on the brink of a technology that can touch billions of users simultaneously, transforming how society consumes media and interacts with each other. In this article, we have summarized the concepts that will come to the fore when we examine the possibilities of military use of VR technology. Of course, we do not yet know what the future will bring. However, it is certainly worth further investigating the role of the metaverse in military training and education - the article primarily deals with this area - since it cannot be a coincidence that the two leading superpowers in artificial intelligence research (China, USA) also provide significant resources for virtual " battlefield" for research.

References

Binxiong, Dai and Xiong Sunhao. 2022. "Uncovering the Metaverse." *PLA Daily.* http://www.81.cn/jfjbmap/content/2021-11/26/content_303934.htm.

China Copyright and Media. 2016. *National Cyberspace Security Strategy.* https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/.

Jacobson, Linda. 1995. *Cyberarts: Exploring Art & Technology.* San Francisco: Miller Freeman Inc. .

Mystakidis, Stylianos. 2022. "Metaverse." *Encyclopedia* 2 (1): 486-497. https://doi.org/10.3390/encyclopedia2010031.

Négyesi, Imre. 2009a. "Die vision der tragbaren informations-technologiegeräte." *Military engineer* (Issue 4): 173-179.

__. 2009b. "Tagbare und feldinformatik-geräte I." *Military engineer* (Issue 2): 333-339.

__. 2009c. "Tagbare und feldinformatik-geräte II." *Military engineer* (Issue 3): 355-362.

Qingxiu, Sun, Liu Shiyang and Wang Chenxu. 2022. *Zero Distance! Gathering in the Metaverse, Have You Ever Seen Such a Spring Festival Gala?* http://www.81.cn/2022zt/2022-02/03/content_10134595.htm.

RTO/NATO [The Research and Technology Organisation of NATO]. 2003. "Virtual Reality: State of Military Research and Applications in Member Countries - AC/323(HFM-021) TP/18." https://apps.dtic.mil/sti/pdfs/ADA411978.pdf.

Tice, Steve and Linda Jacobson. 1991. "Definitions of Virtual Reality." In *Cyberarts: The Art of Building Virtual Realities*. San Francisco. http://switch.sjsu.edu/archive/switch/SwitchV1N2/Jacobson/vrdef.html.

Zhongo, Wang. 2022. "Informatization Wings for Army Party Building." *PLA Daily.* http://www.81.cn/jfjbmap/content/2022-03/28/content_312404.htm.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

The need for an integrated model of smart warfare

Matei BLĂNARU, Ph.D. Candidate*

*Doctoral School of Sociology of the University of Bucharest
e-mail: matei.h.blanaru@gmail.com

Abstract

Unfortunately, the war in Ukraine and many other events or processes taking place all over the world show us that perhaps there can be no smart peace unless we are ready to fight a smart war. Both against conventional or unconventional enemies, both regarding symmetrical or asymmetrical warfare. And if we are beginning to see our society in terms of smart governance, smart education, smart economy or smart people, which means we see it in terms of smart peace and smart society, then there is definitely the need to see war and conflict in an integrated, compact vision of smart war. We use observation to point out how a large series of contemporary events and processes, starting from cybersecurity issues, aerial, terrestrial, or maritime drones, electronic warfare equipment meant to counter these drones, propaganda, and disinformation easily spread through rapid smart means of worldwide mass communication, and of course, Artificial Intelligence, microprocessors, or fledgling space warfare where satellites can be used to attack rival satellites, need to be addressed in an inclusive, integrated conceptual approach of smart warfare focused on the future and not as separate events or developments patched up upon conventional warfare equipment or thinking. We need to understand that "smartness" is all about peace, but all about war as well, if we want a smart peace to last or if we want to be able to defend it, as Romania has a definitely defensive strategy. We are building a smart peace, but we have to prepare for a smart war as well.

Keywords:
smart war; threats; society; cyber; AI.

Article info
Received: 30 January 2024; Revised: 19 February 2024; Accepted: 14 March 2024; Available online: 5 April 2024

Citation: Blănaru, M. 2023. "The need for an integrated model of smart warfare".
Bulletin of "Carol I" National Defence University, 13(1): 44-62. https://doi.org/10.53477/2284-9378-24-03

Introduction

Obviously, as civilians, war is something we would rather not think about. We would rather think about smart living, smart peace, about a smart society, or smart education for our children, than anything else but war. Modern ideologies and recent history, where war has mostly avoided Western societies for well over half a century, play an important part in this public perception as well. But, as we see in Ukraine or Israel, this way of thinking does not mean that war is not here. On the contrary, war is here to stay, but maybe in the new shape of *smart war*. So how is a *smart war* waged or what is it?

Well, the way our society is changing and the war in Ukraine are giving us many hints in that direction. Smart governance, smart leadership, smart living, smart education, and so on, all of them address societal concerns and they mean an integrative approach to such concerns, with a significant impact of the new technologies. But if a societal future is depicted in such a way, then why should war be any different in the future and why should we not adapt rather sooner than later to the *smart war*? We are not saying that modern warfare is not incorporating or even generating the most up-to-date technologies, war has always done so throughout history, but what we are saying is that our way of thinking about war has not kept in touch with these new realities. Our way of thinking can be a vulnerability in front of new threats or hostile actors. And that needs to change. Thus, we definitely need the concept of a *"smart war"*.

1. Prior work on the topic of Smart Warfare

At the time we are writing this paper (October, 2023), we could not find a concept of *smart war* named as such in modern scientific literature, in the way we mean to address it - which is similar to a *smart education*, *smart governance* or *society*, which means that *taking advantage of all technological innovations in an inclusive, integrated strategical perspective is a must*. There is, however, a similar concept of "intelligent warfare" developed in particular by Chinese researchers.

Regarding the "smart war" concept, most of the accounts available to the public online refer to the "smart war" as being equivalent to an "intelligent war," waged in an intelligent manner regarding mental capability, or they are referring to the gaming industry. Other accounts refer to the so-called "smart war" policy of the US administration at various moments between 2002 and 2015 or so, which ultimately also meant "intelligent" from the mental capability point of view. In US policies and strategies, there was something called "the smart war" as opposed to a "dumb war", a difference first outlined by Obama in a 2002 speech (Thrush 2011). But again, it only meant a sort of warfare conducted intelligently. Which also reportedly failed in Afghanistan. In 2002, US Defence Secretary Donald Rumsfeld also devised a "smart war" strategy meant for the invasion of Iraq and the overthrowing of Saddam

Hussein. However, despite the use of "smart bombs", the "smart war" devised by Rumsfeld's strategy only meant a sort of war waged intelligently too.

There is another very interesting mention of "smart war" in an analysis, even though again it uses "smart" as meaning an intelligent mental capacity. The article *"Soft War = Smart War? Think Again"* criticizes overly confident reliance on *soft power* in order to pursue security goals, probably referring as well to the new concepts of "smart power": *"In light of this, tying our long-term security to the notion that we can out-manipulate and out-spin others in the realm of cross-cultural persuasion, and thus wage some sort of soft, smart war seems especially imprudent."* (Simons 2012) We agree with this conclusion. Soft war is extremely important, but only employed in conjunction with hard power. Technologically advanced soft war abilities and technologically advanced military capabilities make up part of the concept of smart war we mean to describe. It will be clearer when we point out the features we would ascribe to a smart war, below. However, there should be no confusion between the concept of "smart power" and what we are trying to analyze as "smart war". The war in Ukraine has proven the importance of employing *smart power* (Danylenko et al. 2022), but ultimately, *smart power* is simply a combination of *hard power* and *soft power* (Dargiel 2009). But *smart war* should mean much more than that, and in different ways. *Smart war* foremost means thinking outside of the box, a revolution in traditional military thinking. For example, all the technologies to build and use maritime drones were here already. But nobody had thought about using them to the extent Ukraine is now using them, inflicting huge damage to the Russian Navy. And this is only the beginning. Soon, huge ships and airplane carriers may start losing their dominant role in the seas.

Back in 2011, then Secretary General of NATO Anders Fogh Rasmussen spoke of a concept of a "smart defence" strategy that would have meant *"the idea of creating more European capabilities with less money"* (Eugénio 2013) and lessening the financial and operational burden on the US regarding NATO. So, it too regarded "smart" as a mental capacity. NATO does not seem to operate with the concepts of "smart war" or "intelligent war", but in 2021 it adopted its first AI strategy, acknowledging that: *"Artificial Intelligence (AI) is changing the global defence and security environment. It offers an unprecedented opportunity to strengthen our technological edge but will also escalate the speed of the threats we face. This foundational technology will likely affect the full spectrum of activities undertaken by the Alliance in support of its three core tasks: collective defence, crisis management, and cooperative security."* (NATO 2021) Acknowledging the speed of new threats and the fact that new technologies (not just AI, in our opinion) will fully affect all the Alliance´s activities, are one of our main arguments in this analysis as well.

However, the "smart war" concept used in a slightly similar manner to the one we mean to address is being felt at ground level. A mention of *smart war* in a slightly similar way to what we mean to analyse here (even though they employ it more

concerning smart *equals* the intelligent ability of thinking), did not come from academics, but from ground level, from a rather unexpected provenance – the Wagner mercenaries in Ukraine who complained in 2022 that Ukraine was waging a *smart war* against them, while they were still stuck in a conventional military mindset (Comisarul 2022).

Even very recent trademark volumes, that deal with *"An international and interdisciplinary perspective on the adoption and governance of artificial intelligence (AI) and machine learning (ML) in defence and military innovation by major and middle powers."* (Raska and Bitzinger 2023, iii) do not devise an integrated approach and definition of the "smart war" in the way we mean to. For example, in what is perhaps the most recent such volume, *The AI Wave In Defence Innovation. Assessing Military Artificial Intelligence Strategies, Capabilities, and Trajectories*, edited by Michael Raska and Richard A. Bitzinger and from which we cited above, published at Routledge in 2023, we could not find the concept of "smart war" named as such. But, to its defence, that was neither the purpose of the volume in the first place. It deals with a very important aspect of "smart war", even essential, which is AI and machine learning (ML), but it did not devise the greater picture comprising of all features and integrated approaches to a smart war that we will briefly point out below.

Things, however, as the aforementioned volume proves, differ to a certain degree when it comes down to China and The People's Liberation Army (PLA) who have been using for quite some time the concept of "intelligent warfare". For example, there is a thorough 2021 analysis written by the US *Center for Naval Analyses (CNA),* named *The PLA and Intelligent Warfare: A Preliminary Analysis*, which tries to investigate the Chinese meaning and strategy of "intelligent warfare", and the results are somehow intriguing and surprising. It rightfully states that *"The widespread adoption of artificial intelligence (AI) and autonomous weapon systems portends a new revolution in military affairs."* (Pollpeter and Kerrigan 2021, i), which is a very important part of what we are saying in this paper, and it also says that *"The People's Liberation Army (PLA) is now conceptualizing a future battlefield environment dominated by AI and autonomy, which it calls "intelligent warfare."* (Pollpeter and Kerrigan 2021, i), which is a warning for the future, from a geopolitical and strategical perspective.

There was a very interesting remark in a 2021 analysis, stating that Chinese analysts made *"Assessments that AI and autonomy will enable weaker militaries to defeat stronger militaries suggest that writers may view AI and autonomy as new technologies that could play a significant role in defeating the US military."* (Pollpeter and Kerrigan 2021, iv) We are not quite there yet regarding AI and autonomous systems, but we can see how the almost non-existent Ukrainian Navy managed to defeat the powerful Russian Black Sea Fleet by using just a few smart war devices, that is naval drones.

As regards the features of this "intelligent warfare" described by the Chinese and PLA, the CNA analysis points out that *"Most PRC writers do not explicitly define*

intelligent warfare, but describe it as follows: • A new and advanced stage of warfare based on AI and autonomy; • A combination of human and machine intelligence; • The extensive use of AI in all military applications." (Pollpeter and Kerrigan 2021, i) Also, Chinese analysts have rightfully emphasized the importance of data, algorithms, and computing power to what they call "intelligent warfare" (Pollpeter and Kerrigan 2021, i). As regarding who will be in control of these "intelligent warfare" capabilities, most Chinese analysts predicted that, at least at a strategic level, humans will be in control, and overall there will be a hybrid control system made up of humans and machines. A minority predict that in time machines will completely replace humans in that respect too.

From an official point of view, the 2019 White Paper on China's National Defense in the New Era describes briefly what they mean by " intelligent warfare": *"There is a prevailing trend to develop long-range precision, intelligent, stealthy or unmanned weaponry and equipment. War is evolving in form towards informationized warfare, and intelligent warfare is on the horizon.*" (State Council of The People's Republic of China 2019).

One of the key recent works regarding "intelligent warfare" in the Chinese understanding of the concept is *"Intelligent Warfare. Prospects of Military Development in the Age of AI"* by Mingxi Wu, a Chinese researcher, who argues that: *"Intelligent warfare may take on diversified forms, most notably cognitive confrontations with AI at their core and integrated operations utilizing "intelligence+" and "+intelligence." (...) Intelligent technologies such as AI, big data, cloud computing, interdisciplinary biology, unmanned systems, and parallel training are advancing at a breakneck pace and becoming increasingly integrated with established technologies, altering humans' epistemology, methodology, and operational mechanisms and enhancing humans' ability to transform the world. Following mechanization and informatization, intelligentization will be the third stage of human civilization.*" (Wu 2023, xv) We thoroughly agree with all of the above that the Chinese researcher has said, but again, that is in the relatively distant future. However, things will never be the same again regarding warfare and we would better accept that rather sooner than later. He goes on by saying that *"Whoever controls the advantage of intelligence will have the initiative in future warfare.*" (Wu 2023, xvi) This seems to be the Chinese main focus regarding possible future confrontation with the US.

2. Features and meaning of Smart War

The *smart war*, of course, is a concept in the process of being drafted and there can be many more dimensions added to it (some of which may have not been innovated yet), but we want to point out in the following paragraphs some of its main *sine qua non* features. The objective of this analysis is not to thoroughly investigate the following features or components of what we describe as *smart war*, but merely to

enumerate some of the most important of them. As we have just mentioned, the list is not closed, but, just like the smart war, it is continuously evolving and open to innovation and new features.

2.1. Drones (unmanned vehicles). One of the main features of any smart war, in current understanding, would mean relying heavily on large numbers of relatively cheap modern drones (Trofimov 2023). Whether human-operated or by AI, autonomous systems. The war in Ukraine, just as well as the Hamas terrorist attack against Israel, underlines this statement. Just as Oleksii Reznikov, former Defence Minister of Ukraine, said about the Russians: *"We have no serious fleet or naval capability. But we can hit them with drones"* (Harding 2023). And then there is the cost of their maritime drones, ranging from 10 to 100 thousand US dollars, compared to the cost of Russian Fleet vessels, which cost hundreds of millions of US dollars (Harding 2023). We conclude that smart war does pay.

This dimension is currently changing, developing very fast, and investing in home development and manufacture of cheap drones would be the best choice. We remember that at the start of the war in Ukraine, the Turkish Bayraktar drones were making headlines all over the world. Now, we can hardly ever hear of them. This means that Russia has been employing effective counter measures. From the perspective of a smart war, perhaps one could argue that just as things changed, the Romanian Army will receive outdated relatively expensive Bayraktar drones worth hundreds of millions of US dollars, instead of having started developing their own capacities worth all that money for the future. Choosing where and how much to invest is definitely an attribute of any good strategy of *smart war*.

2.2. Communication and public diplomacy. Another essential dimension of any current smart war would be a very active and good communication and diplomatic campaign, which are *soft power capabilities*. Considering the current state of globalization, the importance of public opinion, narratives and justification, especially for Western societies, cannot be underestimated. We can see how for Israel it is increasingly difficult to wage confrontation, manage narratives and justify war in this domain of communication and public perception, even for the home public, although Israel did not start the war with Hamas.
Communication has always been essential to winning a war. But there is communication inside the military chain of command, extremely important, essential, and communication towards the civilian society, both at home and abroad, that is the narratives employed and public diplomacy.

A very comprehensive analysis of the importance of current public diplomacy in the war in Ukraine is the paper *Public Diplomacy during Military International Conflicts. The Ukraine war case*, which argues that *"public diplomacy itself transformed"* and *"the battle between the Ukrainian and Russian military for image and legitimacy in the international public opinion" is increasingly important*", because *"In the information*

age in which we live, the activities and capabilities of public diplomacy can have a significant impact on how people, organizations, and governments perceive this war." (Hlihor 2023, 19)

2.3. Soft power. It is an essential part of any present confrontation and it will be as such for a while to come. Joseph Nye Jr. first developed the concept in 1990, and in his iconic volume of 2004, he said: *"Soft power rests on some shared values. That is why exchanges are often more effective than mere broadcasting. By definition, soft power means getting others to want the same outcomes you want, and that requires understanding how they are hearing your messages, and fine-tuning it accordingly. It is crucial to understand the target audience."* (Nye 2004, 111) It seems to us that we now need more than ever to understand *"the others"*, whomever they may be. Thus, *soft power* also means employment of culture, mutual understanding and respect for other cultures, economy, moral values, reliability, trust, and other aspects. Chinese analysts tend to minimize the importance of *soft power* when they talk about the "intelligent war", while sometimes Western researchers and practitioners tend to overestimate and over-rely on *soft power*. Or, just like it happened in Afghanistan, they may implement it in a faulty manner (for example, they relied on corrupt local elements that eventually estranged the local population despite huge American *soft power* and financial investments).

2.4. Information Warfare. We briefly mentioned earlier the importance of communication and public diplomacy, which brings us to the importance of information warfare in this age of smart technological development: *"Information Warfare (IW), the complex set of new phenomena associated with the use of Information and Communications Technologies (ICTs) in fighting scenarios. IW is redefining how war is waged. (...) Nowadays, IW indicates a heterogeneous phenomenon concerning the deployment of robotic weapons, cyber weapons, and the use of ICTs to foster coordination among militaries on the battlefield and for propaganda, the so-called C4ISR (integrated command, control, communications, computers, intelligence, surveillance, and reconnaissance)."* (Taddeo and Floridi 2014, v)

2.5. Societal Approach. If we mentioned the importance of public diplomacy and information warfare for the smart war, then we would definitely have to mention the importance of societal threats. A societal approach to smart war would imply nation and cohesion building internally and public diplomacy, drawing public attention and public support on an international level. To a certain degree, exactly what Ukraine has been doing since it was invaded by Russia.

A societal approach and support to war has always been deemed and recognized as important, but current means and methods have changed just as well as the technological and military ones have. Having learned their lessons from the past, modern societal warfare is much more powerful and hard to counteract. Especially with an ever-growing lack of trust in institutions and politicians (which may be the exact result a societal

warfare campaign would aim to achieve in a target society). There is a Chinese *"PLA's Strategic Support Force, which has responsibilities for outer space, cyber, electronic warfare, and psychological warfare operations"* (Pollpeter and Kerrigan 2021, v).

2.6. Psychological and cognitive warfare. Specific side domains of the societal approach to smart warfare are *psychological* and *cognitive warfare*. In this field, the Chinese PLA has been increasingly conducting research trying to see how modern technologies, like AI, can offer key advantages in a modern confrontation. There is a comprehensive volume on this issue, *"Chinese Next-Generation Psychological Warfare: The Military Applications of Emerging Technologies and Implications for the United States"*, which states that *"In brief, China views psychological warfare, centered on the manipulation of information to influence adversary decisionmaking and behavior, as one of several key components of modern warfare. Chinese psychological warfare has evolved, driven in part by technological progress that brought new opportunities and in part by lessons learned from other militaries, but the core principles and objectives have remained relatively constant. The importance placed on psychological warfare is increasingly linked to Chinese military assessments that the cognitive domain will be a key domain of future warfare."* (Beauchamp-Mustafaga 2023, iv-v) About the modern technologies that can be used to this end, the same volume states that: *"The PLA psychological warfare community has discussed a range of technologies that it envisions leveraging for future operations, including three broad categories of technologies: advanced computing, especially big data and information processing; brain science, especially brain imaging; and a raft of legacy proposals that remain of interest, including sonic weapons, laser weapons, subliminal messaging, and holograms."* (Beauchamp-Mustafaga 2023, v)

About propaganda and disinformation and their importance today, corroborated with the advantage of modern technologies, the CNA analysis we cited earlier states that *"The PLA may emphasize cognitive warfare as it integrates AI into warfighting. • Some PRC writers argue that cognitive warfare can enable the PRC to achieve the Sun Tzu maxim of "winning without fighting" by sapping the morale and will of adversaries. • The PLA may increase efforts to influence competitors and potential adversaries in the cognitive domain by spreading propaganda and disinformation."* (Pollpeter and Kerrigan 2021, v) This shows just how important societal components are for current smart warfare.
NATO operates as well with the concept of *cognitive warfare* and it offers a definition: *"Cognitive Warfare includes activities conducted in synchronization with other Instruments of Power, to affect attitudes and behaviours, by influencing, protecting, or disrupting individual, group, or population level cognition, to gain an advantage over an adversary. Designed to modify perceptions of reality, whole-of-society manipulation has become a new norm, with human cognition shaping to be a critical realm of warfare."* (NATO n.d.)

2.7. Satellites and Starlink. The current war in Ukraine has just proven again just how important is to a modern smart war the key feature of satellites, space exploration, and even the Elon Musk satellite system of Starlink.

2.8. Space warfare. Even though the pandemic may have delayed some processes regarding space militarization and exploration, the main trend is that: *"Space is becoming a less stable environment, even as it holds the promise of becoming a new source of human prosperity."* (Nagashima 2020) The US Space Command announced some time ago, in 2020, that they had evidence that Russia had recently conducted tests of anti-satellite weapons (Patel 2020). There are pleas for more regulation in space, for cooperation instead of competition or dominance, but that is more like wishful thinking, especially considering the current international situation. The US has a military force called the Space Force: *"As a military service, the Space Force has responsibilities under Title 10 of the U.S. Code to organize, train, equip prepare, and maintain forces. In a conflict, those forces would be assigned to a combatant command."* (Erwin 2020) As regards China and Russia, it seems they already have arsenals designed to be used to destroy opponent satellites in space: *"Nations around the world - notably China and Russia - are building arsenals of weapons that can destroy or disrupt satellites in orbit."* (Erwin 2021) So, whether we like it or not, the smart war is already present in space too, and it will be ever more important.

2.9. Electronic Warfare (EW). There are multiple accounts about the importance and the development of effective Electronic Warfare equipment employed in the war in Ukraine. The Russian Federation seems to have an edge over other adversaries regarding similar capabilities at the moment.

2.10. Cyber Warfare. No need to stress the huge importance of cyber warfare for any smart war. Hacking, cyber attacks and cyber war (for example, a quite recent event where CISA – The US Cybersecurity And Infrastructure Security Agency issued a warning about a China state-sponsored cyber actor whose *"activity affects networks across U.S. critical infrastructure sectors"*(CISA 2023) will always be an essential part of any strategy for any kind of war from now on, but especially for a smart war. The smart war simply cannot be defined without cyber attack and cyber defence capabilities.

2.11. Semiconductors/Chips. Any future military war or conflict would depend upon the ability to supply or manufacture the appropriate amounts and types of advanced microchips for its own military capabilities, AI and ML instruments. There are multiple accounts in this regard (Hawkins 2023).

One of the latest and most comprehensive analyses on the topic is the volume *Chip War. The Fight for The World's Most Critical Technology.* The author stresses that the world's supply of computing power is in peril if even one of the steps involved in the semiconductor production process is interrupted. We can easily imagine its impact on AI, drones, cyber capabilities, even smart bombs, aircraft, essentially everything that makes a smart society, a smart peace or a smart war. The author continues by saying that if many people consider nowadays data to be the new oil, it is actually the processing power of computers depending on semiconductors that is most

important and which is in limited amount, and not the data, which seems limitless (Miller 2022). Needless to argue the essential importance of semiconductors/chips for any war of today.

2.12. Artificial Intelligence (AI). We have mentioned earlier two of the most recent and important volumes regarding just how essential AI is deemed to be for future wars (and peace as well). *The AI Wave In Defence Innovation. Assessing Military Artificial Intelligence Strategies, Capabilities, and Trajectories* and *The PLA and Intelligent Warfare: A Preliminary Analysis* try to describe the immense possibilities (and risks as well) presented by AI technologies. It depends on a lot of factors, but in the long term, AI may be the *single* most critical issue in future smart wars.

However, an aspect we have to take into consideration is over-reliance on AI, especially at this early stage of AI development. Because if AI failures can now have catastrophic consequences at an *individual* level (for example, in China, if an individual is designated as "suspect", "dangerous" or of a particular "race", according to face recognition and surveillance AI systems, AI analysis of surveillance camera images, and he/she may be innocent), AI failures can have catastrophic consequences at *a collective, even national level*, if they are faulty, vulnerable, and adopted prematurely in extensive military use.

2.13. Internet of Things (IoT) for military purposes. According to an analysis, *"The Internet of Things (IoT) describes the concept of connecting any device to the internet, resulting in a gargantuan network of objects and people that collect and share data. (...) Another defining characteristic of the Internet of Things is that the objects can "talk" to each other, like the sensors in a smart home or factory that share information to control lights, temperature or inventory levels."* (Mail.com 2023) The same analysis goes on by saying that: *"The Internet of Things is made up of "smart" devices – objects with built-in microchips and sensors that are connected to an internet-based platform with data collection and processing capabilities."* (Mail.com 2023) The US Army has been researching military use of IoT, but not very convincingly and not in a resolute manner. However, it did create the Internet of Battlefield Things (IoBT) project and in 2017 the US Army created a project called the Internet of Battlefield Things Collaborative Research Alliance (IoBT-CRA) meant to invite civil academics to bring contributions to IoBT. This is exactly the collaboration that we deem to be of great importance: academics, practitioners and education.

2.14. Building an appropriate industrial base and securing a constant unhindered supply of necessary materials. Their essential importance for the future is being noticed, we only point out that the European Union has provisionally adopted a European Critical Raw Materials Act, *"as demand for rare earths is expected to increase exponentially in the coming years"* (European Council 2023). In Romania as well it seems that domestic models of drones are being developed, they will be essential in the wars of tomorrow, and we hope that there will be even more domestic

programmes, such as the one undertaken by the Romanian Research Agency for Military Technique and Technologies (ACTTM) (Dumitrache 2023).

2.15. A change in current military structure and command. The changes that are currently taking place all over our society, both technologically, and at a deep societal level, need to be properly addressed in the future by military decision-makers. Current military command and execution structures seem to be struggling to keep pace with technological innovations in the war in Ukraine.

To sum up, the smart war would mean not just a new way of conducting warfare, but also a whole new strategy based on an integrated, dynamic, innovative and interdisciplinary approach to all the new technological and societal developments, plus at least all of the above-mentioned features, as well as a dramatic change of mentality regarding warfare, more future-orientated. And we can actually start "smart warfare" by acting now in the light of the changes that we can already see happening in our society, the keyword is "integrated".

3. Differences between our concept of "smart war" and the Chinese concept of "intelligent warfare" or other similar concepts

First of all, the Chinese view tends to see "intelligent war" as something in the future, while we see "smart war" as something that can be done right now. From a technological point of view, we already have the necessary capabilities, from a conceptual and organizational point of view, we do not. At the same time, pressured by politics, economic considerations, public opinion, wages, jobs, lobbying and huge contracts, Western views tend to see "smart war" as something that can be slowly grafted onto the old and current traditional way to wage war, as it is happening in the US. But, to cite US Admiral Selby, this is simply not good enough (Lipton 2023).

Secondly, we do not see "smart war" as only a specific way of waging war, only as an act limited in time, means, consequences, and scope, as analysts tend to perceive "intelligent war" in China, but we look at it as a whole societal process going on in all dimensions of society, as a part of society. If we talk about "smart administration", "smart economy", "smart city", "smart society", etc., how can we not talk about "smart war" in the same terms of profound radical change in our society? Of course, people's concerns, not a few, associated with this future must be addressed as thoroughly as possible, they are very serious. But we need to talk about them and start building not only technologically, but also conceptually the future framework of "smart war", with an emphasis on defense. From this point of view, the strategy of waging and conceptualizing war lagged far behind the development of society. Many researchers are already talking about the third stage of human civilization, as we have shown above, and this also applies to war.

Third, current military command, execution, and communication structures seem unable to keep pace with technological development. So, we have to seriously think about innovation regarding command and execution structures in the military field as well, if we want the human factor and decision to prevail over AI in the future. This aspect does not seem to be seriously addressed either by the Western side or by the Chinese side that innovates "intelligent warfare," but we see it as an indispensable part of "smart warfare" in the future. Again, there is an indissoluble connection of "smart war" with the societal dimension, because the human structures of command and execution are also part of society. Considering the rigidity of the current military command structures, perhaps this change is also one of the most difficult things to do. But that does not mean that it must be done immediately, it means that we have to start thinking about it today.

Another key difference between what we mean by "smart war" and other similar concepts is the importance given to *soft power*. Chinese researchers focus more on psychological and cognitive operations, far too little on *soft power*, perhaps knowing their shortcomings in this area compared to the West (although, rather late, Chinese researchers began to realize their mistake in neglecting this essential area of current international relations, in their case, regarding China-Central Asia relationship (Toma and Ghinea 2023), while Western concepts tend to rely too much on *soft power*, attracting criticisms like the one we cited at the beginning of our analysis. Soft power is an essential and very important part of what we mean by "smart war", but in a balanced formula - not too little, as in the case of China, not too much or deeply misapplied, as it was done by the West in Afghanistan - and taking into account local particularities. Maybe few people realize it, but even Romania has a huge soft power potential in a very vast region, stretching from Greece to Croatia, Poland and the Czech Republic, which is not being exploited at all. We will point out in a future analysis some essential elements of such a soft power strategy for Romania.

Last but not least, we must not think of "smart war" as something optional, or conjunctural, or something we can leave for later. We need to think of "smart war" as something mandatory, something that needs to be done right now, and something that should be considered whenever we make new purchases, in any new human and technological development programs, etc. So, a whole strategy for "smart war" is needed starting now. And this strategy, as we have shown, is not only limited to technological progress, but also to how we incorporate this technological progress conceptually, theoretically, in the way our society is organized and functions, and especially in the defense forces of our society.

It is about how we shape all our present actions in order to meet the future, as we can interpret it to be based on what is already happening concretely today. This is what an integrated model of "smart warfare" is about.

4. Obstacles to implementing an integrated model of Smart Warfare

Why is *smart war* not being developed and implemented faster? One of the main obstacles to innovation and to this integrated approach of *smart war* that we are advocating for, actually derives from political considerations and from different individuals or entities in the current civil or military establishment, as various military purchases made by Romanian officials prove it, and which is also definitely proven in the US as well by an explicit analysis cited below.

So, a few of the reasons why *smart war* is not currently conceptualized, analysed, developed and deployed, not even in some of the world's most powerful military, are the same as the reasons depicted in this New York Times analysis, written by Eric Lipton, regarding the US Navy and its efforts to modernize. Ken Perry, who is a former US nuclear submarine captain and *„who is now an executive at ThayerMahan, a Connecticut-based company that has invented an unmanned device that tracks enemy submarines at a fraction of the cost of the large vessels the Navy uses" bluntly summarizes that "They refuse to take money from the legacy programs (…) The Navy, big industry and other key stakeholders are vested in the current shipbuilding enterprise.*" (Lipton 2023) Multiple contractors for the US Army and Navy are waiting for big contracts for unmanned vehicles developed by them, but this is just not happening. *Not yet.*

The author also draws the sensible conclusion that *"A new generation of cheaper and more flexible vessels could be vital in any conflict with China, but the Navy remains lashed to big shipbuilding programs driven by tradition, political influence and jobs.*" (Lipton 2023) He also stresses that the obstacles to implementing these new technologies and ways of military thinking are that: *"the Navy, analysts and current and former officials say, remains lashed to political and economic forces that have produced jobs-driven procurement policies that yield powerful but cumbersome warships that may not be ideally suited for the mission it is facing. An aversion to risk-taking — and the breaking of traditions — mixed with bravado and confidence in the power of the traditional fleet has severely hampered the Navy's progress, several recently departed high-ranking Navy and Pentagon officials told The New York Times.*" (Lipton 2023) These are the obstacles to the smart war that we are analyzing.

A high-ranking US officer, Admiral Selby, tried to implement these new technologies more radically in the US Navy, and *"He proposed that the Navy create a new high-ranking officer who would have the authority and funding to build a so-called hybrid fleet in which the new generation of unmanned vehicles would operate in conjunction with traditional warships.*" (Lipton 2023) It is a formidable idea, that we should consider implementing as well.

However, he was turned down, which made him conclude that *"You now run up against the machine — the people who just want to kind of continue to do what we've always done (…) The budgeting process, the congressional process, the industrial lobbying efforts. It is all designed to continue to produce what we've already got and make it a little better. But that is not good enough."* (Lipton 2023)
This is exactly what we are stressing in this analysis: only adapting modern technologies to conventional warfare equipment and way of thinking *is just not good enough* to stay ahead of what is to come. We have to develop an integrated vision and strategy about what the future *smart war* will be and start implementing it. Any purchase, innovation, development, or industrial capacity that we make from now on must be considered and valued according to the elements within a strategy frame that we must have for the *smart war*.

5. Why a Smart War would be a very good choice for Romania's defensive capabilities

First of all, the military capabilities of Romania are behind for what is needed at this very moment for a confident defence and presence at the Black Sea. Romania cannot afford the large amounts of money needed for updating old equipment and for purchasing the large amounts of conventional military equipment needed in order to build a powerful defence military force. Converting the focus to smart military capabilities may mean spending less while staying ahead in the development and implementation of top modern smart warfare equipment. *If we are so far behind, it means we have to think ahead.*

In this regard, Eric Lipton, the author of the NY Times analysis cited earlier, also stresses the big difference in cost between the conventional warfare of today and the smart war of tomorrow, which is one of our key arguments too*: "Operating on a budget that was less than the cost of fuel for one of the Navy's big ships, Navy personnel and contractors had pieced together drone boats, unmanned submersible vessels and aerial vehicles capable of monitoring and intercepting threats over hundreds of miles of the Persian Gulf, like Iranian fast boats looking to hijack oil tankers."* (Lipton 2023)

Secondly, Romania benefits from a considerable large number of people involved in the innovative field of IT research, programming, and cybersecurity, so, it has the human capital needed. Another good reason for Romania to implement a smart war would be that it seems to be paying off on the battlefield, especially for weaker or smaller armies against larger opponents. Ukraine has managed to resist and even counterattack the Russian Army using a complex mix of smart war features, not conceptualized in this manner, but ranging from very good public diplomacy to innovation and the efficient use of naval drones which culminated in a defeat for the Russian Black Sea Fleet.

With all of the above, by no means do we mean that conventional arms and ammunition should not be purchased, manufactured, or used anymore, or that they are not important. Of course, they are still very important, and there should be an investment in conventional weapons, ammunition manufacture, and purchase, and especially gunpowder manufacturing facilities. However, we should gradually shift perspective towards the smart war that will follow, and significant investments, financially but especially in time and effort, should be made with that in mind, envisaging what is to come.

Romania has a unique opportunity in that respect, similar to the development of the internet infrastructure in Romania a while ago. Since our country had no previous internet infrastructure, when this infrastructure was implemented in Romania, the most up-to-date technologies and equipment were used and therefore we now have one of the most reliable, fastest and cheapest internet connections in the world (Dumitrescu 2022). *We should do exactly the same thing with our current warfare abilities and equipment - since we lack sufficient conventional warfare defensive equipment, we should skip a few steps and invest big in the newest and most effective smart war equipment, which is the future (and is often cheaper).* The war in Ukraine could not be clearer in that respect.

From the perspective of future wars, perhaps the one example of falling behind both regarding strategic thinking and equipment would be the purchase for the Romanian Navy of 2 second-hand demining vessels from the UK, which is replacing them with maritime drones (Jipa 2023). It is hard to explain why this is happening, why the purchase of such old equipment, considering the fact that even before the war in Ukraine there were explicit pleas from Romanian professionals regarding the importance of investing, developing, implementing maritime and aerial drones with various tasks (Eremia 2020). Perhaps, just one example of a lack of strategy regarding the new *smart war*.

Another example would be the very expensive purchase of second-hand F16 aircraft from Norway and already outdated Bayraktar drones from Turkey. Of course, Romania definitely needs modern aircraft and in even larger numbers than today, but the Romanian officials perhaps should have focused on purchasing more technologically advanced aircraft (and why not new?) and drones. There are more and more voices arguing that even the F35s are deemed to be one of the last fighter jets. Despite his eccentricities, Elon Musk does have a certain vision for the future and at an Air Warfare Symposium in 2020 in the US he plainly said in front of high US Airforce commanders that *"The fighter jet era has passed."* and that *"Locally autonomous drone warfare is where the future will be."* (Cohen 2020) He could not have been any clearer than that. Not to mention the amount of time and resources needed for the training of a single aircraft pilot, for example, compared to the training and resources needed for the training of a drone pilot.

His words actually made US Air Combat Command Gen. Mike Holmes ponder and he reportedly said *"The next decision point I have is when … the Block 30 and older F-16s, when they need to be replaced, what am I going to replace them with? I want to work to do the experimentation to answer that* question," *Holmes said. "Will I still want to replace them all with F-35s or will I start cutting in something else, like Elon talked about, or like [Air Force acquisition chief] Will Roper and I are discussing?"* (Cohen 2020) This is what everybody should be seriously wondering before adopting smart war real strategies for the future. Which is exactly what Romania should do.

Conclusions

We understand the complex issues behind important and powerful traditional defence companies, the political issues, jobs and people issues, just like the New York Times article debated, but when we are talking about security and modern warfare, recalibrating to a *smart war* is a must. We can see how the Chinese are already doing that. And recalibrating to a different way of thinking is a must too. Ukraine is learning this the hard way. We should be smart, learn it the easy way and get ready beforehand for whatever may come. Investing big in domestic drone manufacturing and research, as well as electronic warfare capabilities, instead of outdated (or soon to be outdated) and very expensive massive equipment, should be a must for Romania's national security strategy, which has always been a defensive one. That would be "smart" thinking.

Waging a successful smart war must not be regarded as individual separate smart technologies employed within different arms and in different ways, because that will not be enough. Modern smart war needs to be conceptualized in a comprehensive, integrated and interdisciplinary manner, incorporating input from both military and civilian professionals, meant to provide maybe that very leap in technology and thinking that Ukrainian General Zaluzhnyi recently deplored it missing.

References

Beauchamp-Mustafaga, Nathan. 2023. *Chinese Next-Generation Psychological Warfare: The Military Applications of Emerging Technologies and Implications for the United States.* Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/research_reports/RRA853-1.html.

CISA [The Cybersecurity and Infrastructure Security Agency]. 2023. "People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection." https://www.cisa.gov/news-events/cybersecurity-advisories/aa23- 144a#_Toc135639517.

Cohen, Rachel S. 2020. "The Fighter Jet Era Has Passed." *Air and Space Forces Magazine.* https://www.airandspaceforces.com/article/the-fighter-jet-era-has-passed/.

Comisarul. 2022. „Ucrainenii duc un „smart war", iar noi ne ghidăm după hărți/Furie in randul Mercenarilor Wagner față de generalii ruși." ("The Ukrainians are waging a "smart war", and we are guided by maps/Anger among the Wagner Mercenaries towards the Russian generals"). *Comisarul.* https://www.comisarul.ro/articol/ucrainenii-duc-un-smart-war-iar-noi-ne-ghidam-dupa_1370939.html.

Danylenko, Serhiy, Nina Averianova, Tatiana Voropayeva and Mykola Drobotenko. 2022. "The Strategy of "Smart Power" As a Key Prerequisite For Ukraine's Victory in The Russian-Ukrainian Neo-Imperial War." *Almanac of Ukrainian Studies* 30: 43-53. doi:10.17721/2520-2626/2022.30.6.

Dargiel, Jessica. 2009. "'Smart Power': A change in U.S. diplomacy strategy." *E-International Relations.* https://www.e-ir.info/2009/06/21/smart-power-a-change-in-us-diplomacy-strategy/.

Dumitrache, Ciprian. 2023. "În plin război al dronelor, Armata română va avea un UAV de concepție proprie. La anul ajung și primele drone Bayraktar TB2." ("In the midst of the drone war, the Romanian Army will have a UAV of its own design. The first Bayraktar TB2 drones also arrive next year"). *Defense Romania.* https://m.defenseromania.ro/in-plin-razboi-al-dronelor-romania-anunta-cand-ajung-in-tara-primele-bayraktar-bonus-mapn-lucreaza-la-prima-drona-de-conceptie-proprie_624823.html#google_vignette.

Dumitrescu, Radu. 2022. "Romania among EU countries with highest internet speed for households." *Romania Insider.* https://www.romania-insider.com/romania-eu-countries-highest-internet-speed-households.

Eremia, Cristian. 2020. „A sosit timpul marilor investiții în drone navale militare." ("The time has come for big investments in military naval drones"). *Monitorul Apărării și Securității.* https://monitorulapararii.ro/a-sosit-timpul-marilor-investitii-in-drone-navale-militare-1-33035.

Erwin, Sandra. 2021. "Report: Space weapons are a fact of life, but there are many ways to counter them." *Space News.* https://spacenews.com/report-space-weapons-are-a-fact-of-life-but-there-are-many-ways-to-counter-them/.

—. 2020. "U.S. Space Force to expand presence inside the Pentagon." *Space News.* https://spacenews.com/u-s-space-force-to-expand-presence-inside-the-pentagon/.

Eugénio, António. 2013. "Smart Defense: Overcoming Hurdles and Passing Batons." *Marshall Center Occasional Paper* (no. 25). https://www.marshallcenter.org/en/publications/occasional-papers/smart-defense-overcoming-hurdles-and-passing-batons.

European Council. 2023. *Infographic - An EU critical raw materials act for the future of EU supply chains.* https://www.consilium.europa.eu/en/infographics/critical-raw-materials/.

Harding, Luke. 2023. "A new form of warfare':how Ukraine reclaimed the Black Sea from Russian forces." *The Guardian.* https://www.theguardian.com/world/2023/oct/05/how- ukraine-reclaimed-black-sea-from-russian-forces.

Hawkins, Amy. 2023. "China's war chest: how the fight for semiconductors reveals the outlines of a future conflict." *The Guardian.* https://www.theguardian.com/world/2023/may/22/chinas-war-chest-how-the-fight-for-semiconductors-reveals-the-outlines-of-a-future-conflict.

Hlihor, Ecaterina. 2023. "Public diplomacy during military international conflicts. The Ukraine war case." *Bulletin of "Carol I" National Defence University* no. 1. https://revista.unap.ro/index.php/bulletin/article/download/1672/1623/5597.

Jipa, Florin. 2023. "România a cumpărat două nave «vânător de mine» britanice, la mâna a doua, HMS Blyth şi HMS Pembroke. Preţul este trecut la «secret comercial»". ("Romania bought two second-hand British «mine hunters», HMS Blyth and HMS Pembroke. The price is classified as a «trade secret»") *Monitorul Apărării şi Securităţii.* https://monitorulapararii.ro/romania-a-cumparat-doua-nave-vanator-de-mine-britanice-la-mana-a-doua-hms-blyth-si-hms-pembroke-pretul-este-trecut-la-secret-comercial-1-51693?fbclid=IwAR1kNJliuHZIcP0GD_JQXefbM8-hfKZS1qoUjJBtQx5JlEvAwC51M2MDy04.

Lipton, Eric. 2023. "Faced With Evolving Threats, U.S. Navy Struggles to Change." *The New York Times.* https://www.nytimes.com/2023/09/04/us/politics/us-navy-ships.html.

Mail.com. 2023. *What is the Internet of Things (IoT)?* https://www.mail.com/blog/posts/the-internet-of-things/75/#.7518-stage-mmmm2-2.

Miller, Chris. 2022. *Chip War: The Fight for the world's Most Critical Technology.* Scribner Books Co.

Nagashima, Jun. 2020. "The Militarization of Space and its Transformation into a Warfighting Domain." *The Sasakawa Peace Foundation.* https://www.spf.org/iina/en/articles/nagashima_02.html.

NATO. n.d. "Cognitive Warfare." *Strategic Warfare Development Command.* https://www.act.nato.int/activities/cognitive-warfare/.

—. 2021. *Summary of the NATO Artificial Intelligence Strategy.* https://www.nato.int/cps/en/natohq/official_texts_187617.htm.

Nye, Joseph S., Jr. 2005. *Soft Power: The Means to Success in World Politics.* New York: PublicAffairs Books.

Patel, V. Neel. 2020. "The US says Russia just tested an "anti-satellite weapon" in orbit." *MIT Technology Review.* https://www.technologyreview.com/2020/07/23/1005568/us-space-command-russia-test-anti-satellite-weapon-orbit-kosmos-2543/.

Pollpeter, Kevin and Amanda Kerrigan. 2021. "The PLA and Intelligent Warfare: A Preliminary Analysis." *Center for Naval Analyses (CNA).* https://www.cna.org/reports/2021/10/The-PLA-and-Intelligent-Warfare-A-Preliminary-Analysis.pdf.

Raska, Michael and Richard A. Bitzinger. 2023. *The AI Wave In Defence Innovation. Assessing Military Artificial Intelligence Strategies, Capabilities, and Trajectories.* New York: Routledge.

Simons, Anna. 2012. "Soft War = Smart War? Think Again." *Foreign Policy Research Institute.* https://www.researchgate.net/publication/286929221_Soft_War_Smart_War_Think_Again.

State Council of The People's Republic of China. 2019. *China's National Defense in the New Era.* https://english.www.gov.cn/archive/whitepaper/201907/24/content_WS5d3941ddc6d08408f502283d.html.

Taddeo, Mariarosaria and Luciano Floridi. 2014. *The Ethics of Information Warfare.* Springer.

Thrush, Glenn. 2011. "'Smart' war loses logic for Obama." *Politico.* https://www.politico.com/story/2011/06/smart-war-loses-logic-for-obama-057603.

Toma, Paula and Diana Ghinea. 2023. "Strategia Chinei pentru Asia Centrală (II). China la zi (China´s Strategy for Central Asia (II). China update)." *Centrul de Studii Sino-Ruse Ruse (Center for Sino-Russian Studies) - CSSR. Adevărul.* https://adevarul.ro/blogurile-adevarul/strategia-chinei-pentru-asia-centrala-ii-china-2311194.html.

Trofimov, Yaroslav. 2023. "Drones Everywhere: How the Technological Revolution on Ukraine Battlefields Is Reshaping Modern Warfare." *The Wall Street Journal.* https://www.wsj.com/world/drones-everywhere-how-the-technological-revolution-on-ukraine-battlefields-is-reshaping-modern-warfare-bf5d531b.

Wu, Mingxi. 2023. *Intelligent Warfare. Prospects of Military Development in the Age of AI.* New York: Routledge.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

SSSCIP's Perspective on the cyber-attacks unfolded in the context of the military conflict between Russia and Ukraine (January 2022 – January 2024)

Mihai OLTEANU, Ph.D. Student*

*"Carol I" National Defence University, Bucharest
e-mail: mihaiolteanu48@yahoo.com

Abstract

This paper evaluates the reports of the SSSCIP regarding cyber-attacks carried out against Ukraine from January 2022 to January 2024. From the exploitation of the CaddyWiper malware, attributed by SSSCIP to APT SANDWORM, to the sophisticated campaigns of the FSB and the cyber-attack on Kyivstar, the paper provides an insight into Russian-origin cyber-attacks against Ukraine, as reported by the main Ukrainian authority in the field, SSSCIP.

The purpose of the article is to identify how SSSCIP reported cyber-attacks on Ukrainian IT&C infrastructures, the completeness of the published data, and the way the campaigns are presented. To achieve this goal, all SSSCIP reports from the reference period were evaluated, and only those that materialized and affected IT&C infrastructures were included in the study. In conclusion, the paper will primarily highlight the limitations of SSSCIP reports and, secondarily, SSSCIP's perspective on the domains most frequently targeted by cyber-attacks and the capabilities of Russian actors.

Keywords:

SSSCIP; Ukraine; APT; cyber security; Russia; military conflict.

Article info

Received: 1 February 2024; Revised: 26 February 2024; Accepted: 13 March 2024; Available online: 5 April 2024

Citation: Olteanu, M. 2024. "SSSCIP's Perspective on the cyber-attacks unfolded in the context of the military conflict between Russia and Ukraine (January 2022 – January 2024). *Bulletin of "Carol I" National Defence University*, 13(1): 63-79. https://doi.org/10.53477/2284-9378-24-04

Over the past decades, the continuous evolution of technology and the significant expansion of digitization processes at the state and private company levels have led to a constant increase in the importance of the field of cybersecurity. This growth has brought about substantial changes in the most crucial sectors of society, particularly in political, economic, and military domains. Simultaneously, cyber threats have become more complex, with a broader range of targets, offering financial, political, and military opportunities upon compromise (Furstenau, Sott et al. 2020).

In the political context, cyber-attacks have emerged as a primary concern for states and international organizations, given that compromising IT&C infrastructures can lead to strategic disadvantages. Aspects such as influencing electoral processes, manipulating political decisions, and undermining the stability of governmental institutions have evolved into threats to the political domain. The use of cyber-attacks has been solidified as a strategic means to achieve geopolitical objectives, both for state and non-state actors (Visvizi and Lytras 2020). An example in this regard is the cyber actor APT28, which, according to reports from cybersecurity industry companies, operates to support the interests of the Russian Federation (RUS). It has successfully compromised strategic targets in various states (such as Georgia, Poland, and Hungary) and organizations (including NATO and OSCE) (Mcwhorter 2014).

In the economic sphere, extensive business digitization has inherently introduced cyber threats affecting not only information confidentiality but also financial integrity and organizational reputation. Data theft, industrial espionage, and various forms of cyber extortion pose risks to both public and private sectors, impacting the smooth functioning of economic entities (Hernandez-Castro and Cartwright 2020). Prominent incidents, such as the WannaCry[1] cyber campaign, have illustrated the destructive potential of cyber threats, directly impacting economic and industrial sectors (Hernandez-Castro, Cartwright and Stepanova 2017).

The military sphere, reliant on advanced information systems, faces significant cybersecurity risks due to increased interconnectivity between communication and control systems. Modern military operations' complexity has heightened vulnerabilities to cyberattacks, often employed as instruments in state conflicts, such as the ongoing conflict between RUS and Ukraine (UA) since February 2022. Existing literature offers specific analyses of cyberattacks in certain domains, yet comprehensive assessments of major cyber campaigns against UA, irrespective of their targets, starting from 2022, remain scarce. In this context, the purpose of this study is to analyze the official reports issued by Ukrainian authorities regarding the most significant

[1] WannaCry represented a ransomware cyber campaign that occurred in May 2017. Upon infecting a system, WannaCry encrypted user files and demanded payment in the virtual currency Bitcoin for their release. The attack had a global impact, affecting major organizations, including the healthcare system in the United Kingdom and companies in the energy and financial sectors, highlighting the relevance of vulnerabilities in critical infrastructures to cyber threats. (Mohurle and Patil 2017).

cyberattacks spanning from January 2022 to January 2024, impacting various sectors. Following this analysis, conclusions will be drawn, primarily focusing on the reporting practices of SSSCIP and, secondarily, on SSSCIP view of cyberattacks during the conflict between RUS and UA.

For the conduct of this study, particular emphasis will be placed on the reports issued by SSSCIP UA[2], the primary Ukrainian cyber security service under the control of the President. This agency is engaged in activities related to policy formulation in the field of safeguarding IT&C infrastructures, including classified networks within UA (Cyber Security Intelligence 2022). Additionally, it engages in interventions in the event of cyber-attacks, conducted through CERT-UA (Temple-Raston 2023).

[2] Державна служба спеціального зв'язку та захисту інформації України – The State Service of Special Communications and Information Protection.

It is important to underline the fact that the cyberattacks included in SSSCIP's reports are characterized by different levels of complexity and relevance, from two perspectives: (1) the impact that these attacks produced against the targeted infrastructures and (2) the level of technical capabilities of the attackers (Agrafiotis et al. 2018). Therefore, it is relevant that one of the most common types of cyberattacks is based on phishing, a technique grounded in social engineering which aims to persuade the target into accessing the malicious attachment (Khonji, Iraqi and Jones 2013). Most of the phishing attempts are unsuccessful, an outcome determined by multiple factors such as the lack of capabilities of the attackers, the use of phishing attempts insufficiently documented or easily detected by cybersecurity software (Patil et al. 2022). Thus, from a methodological point of view, in order for this paper to be more relevant, it will not take into consideration the SSSCIP reports focused only on unsuccessful phishing campaigns, without a real impact on the targeted infrastructures. Furthermore, it is relevant that between January 2022 and January 2024, SSSCIP published 435 reports. Still, after conducting an initial analysis, it has been concluded that 394 of these were strictly focused on phishing campaigns, without having a real impact against the Ukrainian infrastructures. Taking these facts into consideration, 41 articles have been selected, which will be presented and evaluated with the aim of underlining some conclusions regarding the cybersecurity component as a part of the conflict between RUS and UA.

Literature review

Regarding the analysis of cyber-attacks in the context of the conflict between RUS and UA, existing works focus on the impact of attacks on specific sectors or in short time frames. Davydiuk and Zubok evaluate the resilience of UA's energy sector to cyber-attacks and the potential for cascading effects on other industries, providing insights into the disadvantages faced by UA in the conflict (Davydiuk and Zubok 2023). Similar analyses have been

published, including on Ukraine's financial sector, focusing on the characteristics of cyber-attacks and cyber threats in the context of the RUS-UA conflict. The studies delve into the trends of cyber-attacks targeting the financial industry, highlighting the active use of SMS messages and emails containing links or malware codes (Kloba and Kloba 2022). CERT-EU has consistently released assessments on cyber-attacks conducted against UA, identified by various public and private entities (CERT-EU 2023). However, these works adopt a perspective focused solely on specific sectors (such as those centered on the energy and financial sectors) or aim for an assessment from the viewpoint of external entities in the conflict. In comparison, this study exclusively focuses on the reports made by UA through its competent institution.

Marcus Willet published an analysis on the possibility of escalating the conflict between RUS and UA at the international level, involving NATO (based on international law), as a result of broader cyber-attacks (Willett 2022). The evolution of the conflict from the perspective of cybersecurity is analyzed, taking into account the involvement of unexpected non-state actors in February 2022, which played a significant role (Lonergan, Smith and Mueller 2023). Wilson and Fitz suggest in their work the possibility that cyber-attacks in the context of the RUS-UA conflict could lead to the triggering of events of a nuclear nature, either intentionally or incidentally (Wilson and Fitz 2023). There are also works that have attempted to construct a cybersecurity strategy to ensure resilience, concluding that the improvement of the UA cybersecurity system is in its early stages (Tarasenko, et al. 2022).

The literature includes several works regarding the involvement of non-state entities in the conflict between RUS and UA, particularly the entity named Ukraine IT Army, created by the authorities in Kiev to gather experts regardless of their location to help UA combat cyber-attacks (Soesanto 2023). Similarly, Smith and Dean evaluate the effectiveness of the Ukraine IT Army and its ability to manage around 200,000 volunteer experts who have chosen to join the entity (Smith and Dean 2023). There are works that assess the involvement of external entities in supporting UA, such as major technology companies (e.g., Google, Microsoft, Meta, Apple, and Amazon), and the impact generated by this aspect (Matania and Sommer 2023). Alongside private companies, there have also been states or international organizations (such as the EU) that have sent teams to support UA in ensuring cybersecurity (Sullivan 2023).

The cyber-attacks reported by SSSCIP through the year 2022

Throughout 2022, a significant number of cybersecurity attacks targeted the IT&C infrastructure within UA, with the most notable incidents including:

- On the night of January 13-14, 2022, several public organizations' websites in UA were targeted in a cyber-attack. According to SSSCIP, the attack involved in some cases the display of provocative images and data encryption or deletion. (SSSCIP 2022a). The attack was considered to be premeditated

and involved various types of malware, including a destructive one named WhisperKill, aiming to incapacitate infrastructures (CERT-UA 2022a). SSSCIP did not provide data regarding the potential attribution of the attack campaign to a state or non-state entity. According to Microsoft, the targets included both governmental and non-governmental organizations, among which private companies (Microsoft 2022).

➢ On February 15, 2022, a significant Distributed Denial of Service (DDoS) attack aimed to compromise IT&C infrastructures belonging to both public organizations (including the Ministry of Defense and the Armed Forces websites) and private entities (such as Privatbank and Oschadbank, both of which were compromised) (SSSCIP 2022e). According to Ukrainian authorities, the same cyber-attack campaign was identified on the evening of February 23, 2022, one day before the RUS invasion of UA. This time, the cyber-attacks intensified, targeting the websites of the Cabinet of Ministers, Verkhovna Rada (the Ukrainian Parliament), the Ministry of Foreign Affairs, and the Security Service. On the same day, SSSCIP reported an escalation in malware distribution campaigns, attempts to penetrate public and private IT&C infrastructures, and data destruction attempts. This time, SSSCIP specified that it is clear these campaigns are carried out by the "*aggressor state*" (SSSCIP 2022r).

The relevance in this context lies in the synchronization of the intensified cyber-attacks with the onset of the conflict, creating the conditions for coordinated actions by the RUS against UA (Lewis 2022).

➢ On March 6, 2022, SSSCIP released statistics announcing a record number of cyber-attacks, reaching 2800. Additionally, a record number of 271 DDoS attacks within 24 hours were recorded. These actions are attributed entirely to the RUS, with the Ukrainian authority asserting that they complement attacks from air, water, and land (SSSCIP 2022q). Furthermore, on March 25, SSSCIP announced that in the week of March 15-22 alone, it recorded 60 cyber-attacks, including 11 targeting local and central authorities, 8 against the defense sector, 6 on the financial sector, 6 on commercial organizations, 4 on the telecommunications sector, 2 on the energy sector, and the remaining attacks targeted other public and private entities (SSSCIP 2022p).

➢ On March 15, 2022, SSSCIP released information about a new malware, known in the industry as CaddyWiper, designed to erase data from compromised systems. It is noteworthy that this is the first instance where SSSCIP cites two private companies, Eset and Microsoft, regarding the identification of this malware (SSSCIP 2022b). The campaign targeted entities in the energy sector with the objective of disrupting the electricity supply in UA, and it has been attributed to the Russian cyber actor APT SANDWORM (CERT-UA 2022b).

It is noteworthy that APT SANDWORM was the attributed attacker in the 2015 cyber campaign targeting UA, specifically aimed at the national energy grid (Paverman 2019).

➢ On April 6, 2022, SSSCIP reported a cyber-attack targeting the infrastructure of UKRTELECOM, Ukraine's largest mobile phone company. The attack, characterized by a high level of complexity, originated from territories occupied by RUS at that time, aiming to take control of the communication infrastructure. UKRTELECOM had to reduce infrastructure capacity to 13% to prevent the attackers' intentions. Restoration efforts were successful, though attribution to a specific attacker remains inconclusive according to UKRTELECOM and SSSCIP (SSSCIP 2022c).

➢ On April 11, 2022, an announcement highlighted challenges in maintaining mobile communications in UA. SSSCIP consistently worked to sustain Internet and telecommunication providers, such as Vodafone. At that time, only 65% of the telecom infrastructure remained operational, impacting citizens' communication capabilities within UA (SSSCIP 2022i).

➢ On April 12, 2022, SSSCIP announced efforts to prevent a new cyber campaign by APT SANDWORM, targeting the disruption of electricity supply in UA by compromising network equipment used by private enterprises. Similar to the March 15, 2022 incident, SSSCIP reported collaboration with ESET and MICROSOFT to prevent the cyber-attack. UA maintained cooperation with European states, exchanging information on this cyber threat. However, SSSCIP emphasized that the goal of cooperation was to identify any other compromised energy infrastructure within UA by APT SANDWORM (SSSCIP 2022h).

➢ The following day, on April 13, 2022, SSSCIP reported receiving information from international partners regarding the compromise of an electricity distribution company by the Russian actor APT SANDWORM. The objective was to disrupt the electricity supply for a significant portion of UA. At the time of the intervention, the cyber-attack was underway, successfully compromising some resources but without achieving its final intent. Furthermore, SSSCIP announced a continued increase in the number of cyber-attacks, especially DDoS attacks, with approximately 25 times more incidents identified compared to the entire previous year (SSSCIP 2022l).

➢ Subsequently, on April 16, 2022, SSSCIP reported a new DDoS cyber-attack campaign targeting the websites of public authorities, resulting in their temporary unavailability. Following technical interventions, the websites were restored to operation (SSSCIP 2022n).

➢ Throughout May 2022, attempts to disrupt communications persisted, with attackers successfully permanently disabling them in the Kherson region, occupied by RUS. Residents lost access to mobile and internet communications, and SSSCIP announced its inability to intervene due to military occupation and controlled equipment. Simultaneously, Ukrainian authorities reported that in the absence of communication means, RUS soldiers patrolled and transmitted propagandistic news through audio systems to influence citizens without communication access outside the area. Furthermore, SSSCIP estimated that citizens in the Kherson region would be

granted access to RUS's state-controlled telecom network (SSSCIP 2022m). At the end of the year, in November 2022, SSSCIP announced the successful restoration of access to Ukrainian television and radio stations in Kherson with the assistance of the Polish company Emitel SA (SSSCIP 2022t).

➢ On June 6, 2022, SSSCIP reported an ongoing cyber campaign accompanied by propaganda actions, resulting in the compromise of Ukraine's major television networks. During this incident, Russian news was broadcast while Ukrainian television was airing the national football team's World Cup qualification match. The attackers likely gained access to a TV communication node, enabling the transmission of altered content (SSSCIP 2022j).

By the end of 2022, SSSCIP had not reported additional cyberattacks, although private industry sources, such as MANDIANT, disclosed campaigns, including power outages during October 10-12, 2022 (Proska et al. 2023). Furthermore, SSSCIP did not release a report regarding the campaign against VIASAT KA-band satellite modems, which were rendered inoperable in Ukraine and several European countries, including Poland, the UK, and France, as a secondary effect (Boschetti, Gordon and Falco 2022). Nevertheless, multiple European states attributed this cyber campaign to RUS throughout the year 2022 (Steinbrecher 2022). The only mention of this campaign by SSSCIP was on July 2, 2022, when it stated that UA utilizes the STARLINK satellite infrastructure provided by Elon Musk to ensure backup communications in the event of a cyber-attack on the main infrastructure (SSSCIP 2022o).

Throughout 2022, there were additional statistical reports on the intensity of cyber-attacks, which were three times higher than the previous year (SSSCIP 2022u). The targeted sectors were primarily telecommunications, medical, and governmental (SSSCIP 2022g), with attackers consisting mainly of ideologically motivated groups and state actors (SSSCIP 2022d). However, an interesting aspect is a report from May 1, 2022, when SSSCIP announced that existing indicators suggested that the intensity of Russian cyber-attacks against UA had reached a maximum level. The Ukrainian service estimated that there would be no stronger cyber operations (SSSCIP 2022k). This aspect may indicate an attempt to increase social confidence and maintain an offensive attitude towards RUS at a high level, similar to the period preceding the military conflict (Paniotto 2020). On the other hand, it is possible that UA may have acted to promote a strong image against the aggressor state, aiming to weaken the support of the Russian population for the military actions conducted by RUS, which was at 60% in 2022 (Kizilova 2022). The initiative was supported two months later when SSSCIP announced that the intensity of cyber-attacks continued to remain at the same high level, but their quality was on a declining trend (SSSCIP 2022f).

Another aspect indicating a distinct approach from SSSCIP is revealed in a statement from May 1, 2022, in which Ukraine states that Russian cyber-attacks directed against its infrastructure are also a potential attack on other partner states. As an example, SSSCIP mentions that in 2014, Ukrainian elections were targeted by cyber-

attacks of Russian origin, and two years later, the same modus operandi was observed in the electoral processes in the United States (SSSCIP 2022s). Thus, considering the precedents in terms of cyber security, UA indirectly reiterates the need for support throughout the conflict, emphasizing that it is not only of interest to the two participating states (Ratten 2022).

The cyber-attacks reported by SSSCIP through the year 2023

During the year 2023, SSSCIP published a reduced number of statements regarding cyber-attacks against its own networks and information systems. The most notable ones include:

- On January 1, 2023, a statement was released attributing the cyber-attacks carried out through the CaddyWiper malware in January 2022 to the Russian cyber actor APT SANDWORM (SSSCIP 2023l), publicly attributed towards the RUS military intelligence service (Akimenko and Giles 2020).
- On January 18, 2023, SSSCIP published an analysis regarding a cyber campaign targeting the compromise of media entities, particularly the news agency UKRINFORM. The statement emphasized Russia's attempts to compromise information sources for the population, with the main goal being the disinformation of citizens and subsequent influence (SSSCIP 2023a).
- On February 1, 2023, a series of technical investigations were published concerning cyber campaigns carried out by the Russian FSB against information infrastructures within Ukraine. It was specified that the activity is conducted through cyber-attacks with a high level of complexity and precision, in contrast to DDoS attack campaigns. Furthermore, SSSCIP stated that these types of operations conducted by the FSB represent the most significant cyber threat identified during the military conflict (SSSCIP 2023k).
- One day later, SSSCIP released information about a watering hole cyber-attack[3], which involved creating a website using the image of the Ukrainian Ministry of Foreign Affairs to give the appearance of a legitimate site. Once accessed, the website offered visitors a program to be downloaded, disguised as an application that could identify whether the user's system was compromised. However, the application contained malware that would infect the visitor's computer if installed (SSSCIP 2023f). The campaign is the only one of its kind reported by SSSCIP and was based on exploiting citizens' desire to be informed about the status of the conflict, using a trusted government source.
- On July 1, 2023, an analysis was published regarding the increase in the number of cyber-attacks targeting companies in the IT&C sector

[3] Watering hole – A cyber-attack that relies on identifying websites frequently used by the target group and cloning or modifying them to compromise visitors to that domain (Krithika 2017).

in UA. The stated purpose of these attacks was to compromise these companies to gain control over the software products sold in Ukraine and, subsequently, over the users of these solutions. Additionally, SSSCIP mentions that the private sector assesses its ability to handle this type of threat independently, but recent examples indicate that major companies in the field have been compromised (SSSCIP 2023c).

➢ On July 5, 2023, SSSCIP reported on a cyber campaign that successfully compromised the Facebook page used by the National Statistics Service of Ukraine. Attackers posted on this page claiming that the institution's infrastructure had also been compromised, thereby disrupting access to economic and social statistical data. According to SSSCIP, the attackers only managed to compromise the Facebook page without gaining access to the National Statistics Service's infrastructure, and the message posted in the institution's name was false (SSSCIP 2023e). It is possible that the purpose of these actions was to destabilize public trust in the official statistics published by UA. Such propaganda actions have been consistently carried out by RUS throughout the conflict with UA, aiming to reduce society's trust in the governmental authorities (Geissler et al. 2023).

➢ On July 19, 2023, SSSCIP published a technical investigation into two highly sophisticated malware applications named CAPIBAR and KAZUAR. These were utilized by APT TURLA, attributed to the FSB intelligence service of the Russian Federation. The purpose of these applications was to compromise targets within Ukraine. SSSCIP highlighted that it shared all technical investigation results, including with the private sector in the cybersecurity industry (SSSCIP 2023j).

➢ On December 13, 2023, SSSCIP reported that the IT&C infrastructure of the telecommunications operator Kyivstar was compromised the day before, leading to the disruption of specific services for approximately 24 million customers for several days (Balmforth 2024). In order to successfully restore the operator's functionality, SSSCIP recommended temporarily suspending the provision of roaming services, resulting in customers being unable to communicate outside Ukrainian territory for a limited period (SSSCIP 2023d). It is relevant to note that SSSCIP did not announce the impact of the cyber-attack on the official website. However, additional statements provided by the director of the institution to European publications revealed that the IT&C infrastructure of Kyivstar was fully affected, with the malware used successfully deleting most of the data (Gatlan 2024), while the cyber-attack was being characterized as the greatest in the history of telecom (Sapuppo 2023).

➢ The latest cyber-attack published by SSSCIP during the reference period involves a campaign conducted by the Russian cyber actor APT28. This campaign targeted not only entities within Ukraine but also networks and information systems in Poland. SSSCIP thus conveys the message that cyber-attacks on UA are not geographically isolated incidents but can also impact member states of the EU or NATO (SSSCIP 2023i).

It is noteworthy that, throughout 2023, SSSCIP has had a series of statistical reports regarding the most targeted domains by cyber attackers, thus listing commercial organizations, the telecom industry, software developers, government institutions, the industry and defense sector, as well as local authorities (SSSCIP 2023h). Furthermore, SSSCIP specifies that, starting from September 2022, it has been monitoring at least seven cyber actors consistently targeting Ukrainian infrastructures, all of them being associated with the Russian government (SSSCIP 2023g), as well as 23 groups known as hacktivists (SSSCIP 2023b).
Additionally, it is important to note that until the end of January 2024, no new reports have been published regarding other cyber-attacks targeting the IT&C infrastructure in UA.

Conclusions

From a methodological standpoint, this article initially aimed to select and present the 41 reports issued by SSSCIP between January 2022 and January 2024 concerning cyberattacks of high complexity levels that managed to impact Ukrainian IT&C infrastructures, thereby excluding phishing cyber campaigns. After the presentation of the reports by SSSCIP, several noteworthy aspects emerge regarding the functioning of the institution, its reporting on cyber-attacks against Ukrainian IT&C infrastructure, and the operating methods of Russian cyber actors.

First and foremost, it is notable that the most targeted sectors in cyber campaigns were those related to communications and energy. This can be explained by the fact that the energy sector is a critical resource for both the attacked state, ensuring its basic functioning (Kozak, Klaban and Šlajs 2023), and for the aggressor state, representing a factor that can induce panic among the population once compromised (Lee 2022). As for the telecommunications sector, its main roles are determined by informing the population about the conflict's status (especially through TV and radio stations) and enabling citizens to communicate with each other for safety reasons or to reach individuals outside the state (Bratich 2020). The impact is particularly noticeable in the Kherson region, where Russian forces have acted to restrict access to Ukrainian information and the ability to communicate with individuals outside the area. Regarding hacktivist groups, their goal was to compromise the websites of public authorities, both to decrease trust in public institutions and to create a sense of panic among civilians who, even if not directly involved in the conflict, could realize its effects (Hupperich 2023). An example highlighted in this regard is the compromise of the Facebook page of the National Statistics Service of Ukraine, an action that, although not affecting the institution's data, aimed to decrease public trust in the information published by the agency.
Regarding the capabilities of Russian-origin cyber actors, it is noteworthy that they exhibited a wide range, ranging from destructive attacks, such as the one carried out through the CaddyWiper malware, to DDoS cyber campaigns aimed at temporary

resource unavailability (Liedekerke and Frankenthal 2023). According to SSSCIP reports, the identified Russian services were primarily the FSB and GRU, with the cyber actor APT SANDWORM being highlighted, attributed to the military intelligence service (McFail, Hanna and Rebori-Carretero 2021). Additionally, a level of synchronization between military forces and cyber capabilities can be noted, considering the SSSCIP report that announced a cyber campaign a day before the invasion of Ukraine, likely aimed at supporting the military forces of RUS in the upcoming conflict (Radu 2022). Furthermore, it is noteworthy the significant increase in the number of cyber-attacks, leading to the conclusion that the cyber segment played a significant role in the unfolding of the conflict from January 2022 through January 2024. Regarding the functioning of SSSCIP and the institution's reporting on cyber campaigns, it is notable that initially, cyber-attacks were not attributed with a high degree of confidence to the RUS, a situation that changed over time. However, SSSCIP did not publish sufficient technical data to prove these public attribution actions, suggesting that the reports had strategic political foundations rather than technical ones. Thus, the rhetoric in the reports shifted towards expressions emphasizing that the aggressor state undoubtedly carried out the attacks. Furthermore, over time, SSSCIP increasingly emphasized in its reports that the level of cooperation with the private sector in the IT&C field is high, specifically naming companies such as ESET and MICROSOFT. This aspect could aim to highlight the existence of developed cooperation that supports UA in preventing and countering cyber-attacks (Lilly et al. 2023). Another aspect repeatedly emphasized by SSSCIP is that the impact of offensive cyber actions is not only felt within UA but also affects partners, regardless of their location. Thus, it is possible that SSSCIP aimed to increase solidarity with UA in the conflict with RUS.

Another important aspect to note is that in the two years of analysis, no cyber-attacks were presented as being associated or attributed to entities other than Russian. SSSCIP did not report cyber-attacks of Chinese, Iranian, or North Korean origin, even though cyber actors associated with these states typically exhibit a high level of activity (Assoudeh 2020). Thus, a hypothesis in this regard could be that SSSCIP aimed to construct a rhetoric focused entirely on RUS (rather than on the authentic presentation of facts), in which case it avoided publishing reports that would have shown that there are other entities seeking to compromise networks and systems in UA.

Finally, it is necessary to emphasize that SSSCIP reports have proven in some instances to be incomplete or lacking. A relevant example in this regard is the cyber campaign against the VIASAT satellite infrastructure, not fully reported by SSSCIP, especially from a technical standpoint. Another example is related to the report dated December 13, 2023, regarding the cyber-attack on the Kyivstar operator, which did not specify the extent of the impact of the cyber-attack on UA infrastructure. These aspects lead to two possible conclusions: (1) the decision to report incidents incompletely or not at all was a strategic one to avoid a decrease in public trust, or (2) the high rate of cyber-attacks generated communication errors, and SSSCIP was unable to maintain the reporting pace aligned with the number of cyber-attacks.

References

Agrafiotis, Ioannis, Jason R.C. Nurse, Michael Goldsmith, Sadie Creese and David Upton. 2018. "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate." *Journal of Cybersecurity* 4 (1). https://doi.org/10.1093/cybsec/tyy006.

Akimenko, Valeriy and Keir Giles. 2020. "Russia's Cyber and Information Warfare." *Asia Policy, National Bureau of Asian Research* 27 (2): 67-75. doi:10.1353/asp.2020.0014.

Assoudeh, Mitra. 2020. "Shaping Cybersecurity Strategy: China, Iran, and Russia in a Comparative Perspective." *Reno ProQuest Dissertations Publishing.* http://hdl.handle.net/11714/7624.

Balmforth, Tom. 2024. "Exclusive: Russian hackers were inside Ukraine telecoms giant for months". https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/.

Boschetti, Nicolò, Nathaniel G. Gordon and Gregory Falco. 2022. "Space Cybersecurity Lessons Learned from the ViaSat Cyberattack." https://doi.org/10.2514/6.2022-4380.

Bratich, Jack. 2020. "Civil Society Must Be Defended: Misinformation, Moral Panics, and Wars of Restoration." *Communication, Culture and Critique* 13 (3): 311-332. https://doi.org/10.1093/ccc/tcz041.

CERT-EU. 2023. "Russia's war on Ukraine: one year of cyber operations". https://cert.europa.eu/static/threat-intelligence/TLP-CLEAR-CERT-EU-1YUA-CyberOps.pdf.

CERT-UA. 2022a. "Fragment of the study of cyberattacks 14.01.2022". https://cert.gov.ua/article/18101.

—. 2022b. "Sandworm Group Cyberattack (UAC-0082) on Ukrainian energy objects using INDUSTROYER2 and CADDYWIPER malware (CERT-UA#4435)". https://cert.gov.ua/article/39518.

Cyber Security Intelligence. 2022. "State Service of Special Communications & Information Protection of Ukraine (SSSCIP)". https://www.cybersecurityintelligence.com/state-service-of-special-communications-and-information-protection-of-ukraine-ssscip-7222.html.

Davydiuk, Andrii and Vitalii Zubok. 2023. "Analytical Review of the Resilience of Ukraine's Critical Energy Infrastructure to Cyber Threats in Times of War." *15th International Conference on Cyber Conflict: Meeting Reality (CyCon).* Tallinn, ESTONIA: IEEE. 121-139. doi:10.23919/CyCon58705.2023.10181813.

Furstenau, Leonardo Bertolin, Michele Kremer Sott, Andrio Jonas Ouriques Homrich and Liane Mahlmann Kipper. 2020. "20 Years of Scientific Evolution of Cyber Security: a Science Mapping." *International Conference on Industrial Engineering and Operations Management.* Dubai, UAE: IEOM Society International. https://www.researchgate.net/publication/340413661_20_Years_of_Scientific_Evolution_of_Cyber_Security_a_Science_Mapping.

Gatlan, Sergiu. 2024. *"Russian hackers wiped thousands of systems in KyivStar attack"*. https://www.bleepingcomputer.com/news/security/russian-hackers-wiped-thousands-of-systems-in-kyivstar-attack/.

Geissler, Dominique, Dominik Bär, Nicolas Pröllochs and Stefan Feuerriegel. 2023. "Russian propaganda on social media during the 2022 invasion of Ukraine." *EPJ Data Science* 12 (1). doi:10.1140/epjds/s13688-023-00414-5.

Hernandez-Castro, Julio, Edward Cartwright and Anna Stepanova. 2017. "Economic Analysis of Ransomware." https://ssrn.com/abstract=2937641.

Hernandez-Castro, Julio andEdward Cartwright. 2020. "An economic analysis of ransomware and its welfare consequences." *The Royal Society Open Science.*

Hupperich, Thomas. 2023. "On DDoS Attacks as an Expression of Digital Protest in the Russo-Ukrainian War 2022." *2023 International Symposium on Networks, Computers and Communications.* Doha, Qatar: IEEE. doi:10.1109/ISNCC58260.2023.10323968.

Khonji, Mahmoud, Youssef Iraqi and Andrew Jones. 2013. "Phishing Detection: A Literature Survey." *IEEE Communications Surveys & Tutorials* 15 (4): 2091 - 2121. doi:10.1109/SURV.2013.032213.00009.

Kizilova, Kseniya. 2022. "Assessing Russian Public Opinion on the Ukraine War." *Social Science Open Access Repository* 2-5. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-86994-6.

Kloba, Lev andTaras Kloba. 2022. "Cyber threats of the banking sector in the conditions of the war in Ukraine." *Financial and Credit Activity - Problems of Theory and Practice* 5 (46): 19-28. doi:10.55643/fcaptp.5.46.2022.3883.

Kozak, Pavel, Ivo Klaban and Tomáš Šlajs. 2023. "Industroyer cyber-attacks on Ukraine's critical infrastructure." *2023 International Conference on Military Technologies (ICMT).* Brno, Czech Republic: IEEE. 1-6. doi:10.1109/ICMT58149.2023.10171308.

Krithika, N. 2017. "A study on wha (watering hole attack)–the most dangerous threat to the organisation." *International Journal of innovations in Scientific and Engineering Research (IJISER)* 4 (8): 196-198. https://web.archive.org/web/20180421102442id_/http://www.ijiser.com/paper/2017/vol4issue8/Aug2017p101.1.pdf.

Lee, Chia-yi. 2022. "Why do terrorists target the energy industry? A review of kidnapping, violence and attacks against energy infrastructur." *Energy Research & Social Science* 87 (8): 102459. doi:10.1016/j.erss.2021.102459.

Lewis, James A. 2022. "Cyber War and Ukraine." https://www.csis.org/analysis/cyber-war-and-ukraine.

Liedekerke, Arthur de and Kira Frankenthal. 2023. "The Cyber Dimension in Russia's War of Aggression." doi:10.5771/9783748917205-239.

Lilly, Bilyana, Kenneth Geers, Greg Rattray and Robert Koch. 2023. "Business@War: The IT Companies Helping to Defend Ukraine." *15th International Conference on Cyber Conflict: Meeting Reality (CyCon)* (IEEE) 71-83. doi:10.23919/CyCon58705.2023.10181980.

Lonergan, Erica D, Margaret W Smith and Grace B. Mueller. 2023. "Evaluating Assumptions About the Role of Cyberspace in Warfighting: Evidence from Ukraine." *15th International Conference on Cyber Conflict (CyCon).* Tallinn, ESTONIA: IEEE. 85-102. https://doi.org/10.23919/CyCon58705.2023.10182101.

Matania, Eviata and Udi Sommer. 2023. "Tech titans, cyber commons and the war in Ukraine: An incipient shift in international relations." https://doi.org/10.1177/00471178231211500.

McFail, Michael, Jordan Hanna and Daniel Rebori-Carretero. 2021. "Detection Engineering in Industrial Control Systems. Ukraine 2016 Attack: Sandworm Team and Industroyer Case Study." *The MITRE Corporation* 2-3. https://www.mitre.org/sites/default/files/2022-04/pr-22-0094-detection-engineering-in-industrial-control-systems-ukraine-2016-attack-case-study.pdf.

Mcwhorter, Dan. 2014. "APT28 Malware: A Window into Russia's Cyber Espionage Operations?". https://www.mandiant.com/resources/blog/apt28-a-window-into-russias-cyber-espionage-operations.

Microsoft. 2022. "Destructive malware targeting Ukrainian organizations". https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/.

Mohurle, Savita and Manisha Patil. 2017. "A brief study of Wannacry Threat: Ransomware Attack 2017." *International Journal of Advanced Research in Computer Science* 8 (5). https://www.ijarcs.info/index.php/Ijarcs/article/view/4021.

Paniotto, Volodymyr. 2020. "The Attitude of Ukraine's Population to Russia and Russia's Population to Ukraine (2008–2020)." *NaUKMA Research Papers Sociology* 3: 3-14. doi:10.18523/2617-9067.2020.3.3-14.

Patil, Dharmaraj, Tareek Pattewar, Shailendra Pardeshi, Vipul Punjabi and Rajnikant Wagh. 2022. "Learning to Detect Phishing Web Pages Using Lexical and String Complexity Analysis." https://eudl.eu/doi/10.4108/eai.20-4-2022.173950.

Paverman, Joseph Herbert. 2019. "An Examination of Cyber-Attacks Carried Out by Russia to Perpetuate Expansion." *Utica College ProQuest Dissertations Publishing.* https://www.proquest.com/openview/a0cb326bdab5e2f4c65f0baca4d2ab47/1?pq-origsite=gscholar&cbl=18750&diss=y.

Proska, Ken, John Wolfram, Jared Wilson, Dan Black, Keith Lunden, Daniel Kapellmann Zafra, Nathan Brubaker, Tyler Mclellan and Chris Sistrunk. 2023. "Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology". https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology.

Radu, Claudiu-Cosmin. 2022. "Russia's approach to cyberspace." *International Scientific Conference Strategies XXI. Volume XVIII.* București: "Carol I" National Defence University Publishing House. 533-544. https://doi.org/10.53477/2971-8813-22-61.

Ratten, Vanessa. 2022. "The Ukraine/Russia conflict: Geopolitical and international business strategies." *Thunderbird - International Business Review* 65 (2): 265-271. https://doi.org/10.1002/tie.22319.

Sapuppo, Mercedes. 2023. "Ukrainian telecoms hack highlights cyber dangers of Russia's invasion". https://www.atlanticcouncil.org/blogs/ukrainealert/ukrainian-telecoms-hack-highlights-cyber-dangers-of-russias-invasion/.

Smith, Margaret W. and Thomas Dean. 2023. "The Irregulars: Third-Party Cyber Actors and Digital Resistance Movements in the Ukraine Conflict." *15th International Conference on Cyber Conflict: Meeting Reality (CyCon)* 103-119. doi:10.23919/CyCon58705.2023.10182061.

Soesanto, Stefan. 2023. "Ukraine's IT Army." *Global Politics and Strategy* 65 (2): 93-106. https://doi.org/10.1080/00396338.2023.2218701.

SSSCIP. 2022a. "A fragment of the January 14 cyber attack investigation has been published". https://www.cip.gov.ua/en/news/opublikovano-fragment-doslidzhennya-kiberatak-14-sichnya.

—. 2022b. "A new program erasing data from computers has been detected". https://www.cip.gov.ua/en/news/viyavleno-novu-programu-yaka-stiraye-dani-z-komp-yuteriv.

—. 2022c. "Cyberattack against Ukrtelecom on March 28: the details". https://www.cip.gov.ua/en/news/kiberataka-na-ukrtelekom-28-bereznya-detali.

—. 2022d. "Cyberattacks against Ukraine are carried out by Russian military hackers". https://www.cip.gov.ua/en/news/cyberattacks-against-ukraine-are-carried-out-by-russian-military-hackers.

—. 2022e. "Cyberattacks on the sites of military structures and state banks". https://www.cip.gov.ua/en/news/shodo-kiberataki-na-saiti-viiskovikh-struktur-ta-derzhavnikh-bankiv.

—. 2022f. "Four Months of War: Cyberattack Statistic". https://www.cip.gov.ua/en/news/chotiri-misyaci-viini-statistika-kiberatak.

—. 2022g. "Hackers mainly attack state institutions, telecommunication operators, local authorities, logistics companies and medical resources of Ukraine". https://www.cip.gov.ua/en/news/khakeri-atakuyut-perevazhno-derzhavni-ustanovi-operatoriv-zv-yazku-miscevi-organi-vladi-logistichni-kompaniyi-ta-mediaresursi-ukrayini.

—. 2022h. "Heavy cyberattack on Ukraine's energy sector prevented. https://www.cip.gov.ua/en/news/poperedzhena-masshtabna-kiberataka-na-energetichnii-sektor-ukrayini.

—. 2022i. "Latest update on networks operation in Ukraine as of April 11, 15:00". https://www.cip.gov.ua/en/news/operativna-informaciya-derzhspeczv-yazku-pro-robotu-mobilnogo-zv-yazku-internetu-ta-cifrovogo-telebachennya-v-ukrayini-stanom-na-15-00-11-kvitnya-2022-roku.

—. 2022j. "Russian cyberattack on the OLL.TV service". https://www.cip.gov.ua/en/news/kiberataka-rosiyi-na-servis-oll-tv.

—. 2022k. "Russian cyberwarfare against Ukraine seem to have reached its peak". https://www.cip.gov.ua/en/news/rosiiski-kibernastupalni-operaciyi-na-ukrayinu-imovirno-dosyagli-svogo-maksimalnogo-potencialu.

—. 2022l. "Russian hackers attempted to cut electricity supply to many Ukrainians". https://www.cip.gov.ua/en/news/rosiiski-khakeri-namagalisya-pozbaviti-dostupu-do-elektroenergiyi-znachnu-kilkist-ukrayinciv.

—. 2022m. "Russian Invaders Disabled Communication Services in the South of Ukraine". https://www.cip.gov.ua/en/news/rosiiski-okupanti-vidklyuchili-zv-yazok-na-pivdni-ukrayini.

—. 2022n. "SSSCIP's State Centre of Cybersecurity has neutralized an attack on public authorities' websites". https://www.cip.gov.ua/en/news/derzhavnii-centr-kiberzakhistu-derzhspeczv-yazku-neitralizuvav-ataku-na-saiti-derzhavnikh-organiv.

—. 2022o. "Starlink in Ukraine: How Elon Musk's Satellite Internet is Helping Now and What the Prospects Are". https://www.cip.gov.ua/en/news/starlink-v-ukrayini-yak-suputnikovii-internet-vid-ilona-maska-dopomagaye-zaraz-ta-yaki-perspektivi.

—. 2022p. *"Statistics of Cyber Attacks on Ukrainian Critical Information Infrastructure: 15-22 March"*. https://www.cip.gov.ua/en/news/statistika-kiberatak-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-15-22-bereznya.

—. 2022q. "The war continues not only on land, in the air and at sea. Cyberspace has also become an arena for hostilities". https://www.cip.gov.ua/en/news/the-war-continues-not-only-on-land-in-the-air-and-at-sea-cyberspace-has-also-become-an-arena-for-hostilities.

—. 2022r. "Today's attacks are a continuation of the attacks that took place on February 15". https://www.cip.gov.ua/en/news/23-lyutogo-2022-roku-stavsya-chergovii-akt-kiberagresiyi-proti-ukrayini.

—. 2022s. "Ukraine is not the only target for russian hackers, but a major one". https://www.cip.gov.ua/en/news/ukrayina-ne-yedina-cil-rosiiskikh-khakeriv-prote-odna-z-golovnikh.

—. 2022t. "Ukrainian television and radio are back in Kherson". https://www.cip.gov.ua/en/news/do-khersona-povernulosya-ukrayinske-telebachennya-i-radio.

—. 2022u. "Within a month of war, there were already three times more hacker attacks than during the same period last year". https://www.cip.gov.ua/en/news/za-misyac-viini-vzhe-stalosya-maizhe-vtrichi-bilshe-khakerskikh-atak-riznogo-vidu-nizh-za-analogichnii-period-minulogo-roku.

—. 2023a. "A Cyberattack Failed to Disrupt Ukrinform News Agency". https://www.cip.gov.ua/en/news/kiberataka-ne-zmogla-zupiniti-robotu-informaciinogo-agentstva-ukrinform.

—. 2023b. "At least 23 russian cyber terrorist groups act against Ukraine". https://www.cip.gov.ua/en/news/proti-ukrayini-pracyuyut-shonaimenshe-23-rosiiski-kiberteroristichni-khakerski-grupi.

—. 2023c. "Attacks against IT companies and specialized software developers as a threat to critical infrastructure". https://www.cip.gov.ua/en/news/ataki-na-it-kompaniyi-ta-specializovanikh-rozrobnikiv-pz-yak-zagroza-kritichnii-infrastrukturi.

—. 2023d. "CERT-UA experts are investigating a cyberattack against Kyivstar telecom operator's network". https://www.cip.gov.ua/en/news/fakhivci-cert-ua-doslidzhuyut-kiberataku-na-merezhu-telekom-operatora-kiyivstar.

—. 2023e. "Cyberattack on the State Statistics of Ukraine: the enemy reports another non-existent «victory»". https://www.cip.gov.ua/en/news/kiberataka-na-derzhstat-ukrayini-vorog-ukotre-prozvituvav-pro-peremogu-yakoyi-ne-bulo.

—. 2023f. "Cybercriminals tried to steal data, disguising themselves as Ukrainian MFA". https://www.cip.gov.ua/en/news/kiberzlovmisniki-namagalisya-vikradati-dani-maskuyuchis-pid-ukrayinske-mzs.

—. 2023g. "How russian and pro-russian hackers attack Ukraine". https://www.cip.gov.ua/en/news/yaki-rosiiski-ta-prorosiiski-khakeri-atakuyut-ukrayinu.

—. 2023h. "Local public authorities are among the key targets for russian hackers". https://www.cip.gov.ua/en/news/miscevi-organi-vladi-odna-z-osnovnikh-mishenei-rosiiskikh-khakeriv.

—. 2023i. "Russian hackers attacked users in Ukraine and Poland once again: this time they used emails containing links to «documents»". https://www.cip.gov.ua/en/news/rosiiski-khakeri-vchergove-atakuvali-koristuvachiv-ukrayini-ta-polshi-cogo-razu-za-dopomogoyu-elektronnikh-listiv-z-posilannyami-na-dokumenti.

—. 2023j. "Russian hacking group Turla attacks defense forces using CAPIBAR and KAZUAR malware — CERT-UA investigation". https://www.cip.gov.ua/en/news/rosiiske-ugrupuvannya-turla-spryamovuye-ataki-proti-sil-oboroni-vikoristovuyuchi-shkidlivi-programi-capibar-ta-kazuar-doslidzhennya-cert-ua.

—. 2023k. "Targeted cyberattacks remain among the major cyber threats posed by the FSB hackers — Report". https://www.cip.gov.ua/en/news/targetovani-kiberataki-zalishayutsya-odniyeyu-z-osnovnikh-kiberzagroz-vid-khakeriv-iz-fsb-zvit.

—. 2023l. "The attack on Ukrinform might have been carried out by the Sandworm hacking group, associated with russian GRU: preliminary results of CERT-UA investigation". https://www.cip.gov.ua/en/news/ukrinform-mogli-atakuvati-khakeri-z-ugrupuvannya-sandworm-pov-yazanogo-z-rosiiskim-gru-poperedni-dani-doslidzhennya-cert-ua.

Steinbrecher, Dominique. 2022. "Viasat KA-SAT attack (2022)". https://cyberlaw.ccdcoe.org/wiki/Viasat_KA-SAT_attack_(2022).

Sullivan, Scott. 2023. "Unpacking Cyber Neutrality." *15th International Conference on Cyber Conflict (CyCon).* Talinn, ESTONIA: IEEE. 9-23. https://www.ccdcoe.org/uploads/doc/CyCon_2023_book_print.pdf.

Tarasenko, Oleh, Dmytro Mirkovets, Artem Shevchyshen, Oleksandr Nahorniuk-Danyliuk and Yurii Yermakov. 2022. "Cyber security as the basis for the national security of Ukraine." *Cuestiones Politicas* 40 (73): 583-599. https://doi.org/10.46398/cuestpol.4073.33.

Temple-Raston, Dina. 2023. "In recent interview, ousted Ukrainian cyber official spoke about new Russian attacks, long-term plans". https://therecord.media/victor-zhora-interview-click-here-ousted.

Visvizi, Anna and Miltiadis D. Lytras. 2020. "Government at risk: between distributed risks and threats and effective policy-responses." *Transforming Government: People, Process and Policy* 14 (3): 333-336. https://doi.org/10.1108/TG-06-2020-0137.

Willett, Marcus. 2022. "The Cyber Dimension of the Russia–Ukraine War." *Global Politics and Strategy* 64 (5): 7-26. https://doi.org/10.1080/00396338.2022.2126193.

Wilson, Richard L. and Alexia Fitz. 2023. "Nuclear Weapons, Cyber Warfare, and Cyber Security: Ethical and Anticipated Ethical Issues." *Proceedings of the 18th International Conference on Cyber Warfare and Security Vol. 18 No. 1.* Baltimore, MD: Towson University. 440-448. https://doi.org/10.34190/iccws.18.1.1050.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Travel Intelligence: Enhancing Counterterrorism and National Security

Anastasios-Nikolaos KANELLOPOULOS, Ph.D. Candidate*
Dimitrios STAVROPOULOS, M.Sc.**

*Department of Business Administration, Athens University of Economics and Business, Greece
e-mail: ankanell@aueb.gr
** Department of Informatics and Telematics, Harokopio University of Athens, Greece

Abstract

In the contemporary landscape of global security challenges, addressing the intricate dynamics of Counterterrorism and National Security is paramount. This paper emphasizes the pivotal role of Travel Intelligence (TRAVINT) in enhancing Counterterrorism (CT) strategy and improving security measures.
Eventually, through a comparative analysis between theoretical frameworks and practical applications, supplemented by case studies of Hezbollah and Hamas, the study examines the significance of TRAVINT, in proactively identifying and preventing potential Terrorism and National Security.

Keywords:
Travel Intelligence; TRAVINT; Counterterrorism; National Security; Hezbollah; Hamas.

Article info
Received: 19 January 2024; Revised: 4 February 2024; Accepted: 1 March 2024; Available online: 5 April 2024

Citation: Kanellopoulos, A.N. and D. Stavropoulos. 2024. "Travel Intelligence: Enhancing Counterterrorism and National Security". *Bulletin of "Carol I" National Defence University*, 13(1): 80-93. https://doi.org/10.53477/2284-9378-24-05

In the intricate and dynamically evolving sphere of global security challenges, an imperative exists for a thorough exploration of Counterterrorism (CT) theory and practice to effectively confront the multifaceted nature of contemporary threats. This scholarly endeavor, embarks on a broad trajectory, encompassing both theoretical foundations and pragmatic applications that constitute the bedrock of efficacious CT measures. Commencing with an exhaustive review of seminal works in CT theory, it offers an emphasis on the strategic nature of terrorism and the imperative to address root causes and establishes a robust theoretical framework, providing insights into the intricate landscape of contemporary security challenges.

Effectively transitioning from theory to practice, the paper focalizes on the pivotal role of Travel Intelligence (TRAVINT) in fortifying National Security and ensuring border control measures. TRAVINT, constituting the systematic collection, analysis, and application of travel-related information, emerges as a cornerstone in contemporary CT strategies. Delving into historical developments within the European Union and the United States, where institutions such as the Europol Travel Intelligence Center and agencies like the Transportation Security Administration actively engage in the gathering of travel-related data, the paper accentuates the escalating recognition of TRAVINT's significance.

Moreover, by synthesizing theoretical insights with practical applications, this academic inquiry posits TRAVINT as a paradigm shift in the tactical and operational approaches employed to secure nations against the evolving challenges posed by contemporary terrorism. Systematically examining the interplay between theory and practice, it contributes to a holistic comprehension of CT dynamics, underscoring the imperative for adaptive and effective strategies.

Furthermore, the paper incorporates two case studies, scrutinizing the travel patterns and operational methods of Hezbollah and Hamas terrorist organizations, providing concrete insights into their activities, and offering potential strategies for leveraging travel intelligence in CT efforts.

Counterterrorism Theory and Practice

The dynamic and multifaceted nature of global security challenges demands a thorough exploration of CT theory and practice. This comprehensive review delves into the theoretical foundations that guide the development of strategic frameworks, drawing insights from seminal academic papers that have significantly contributed to the discourse.

One pivotal aspect of CT theory is the understanding of motivations driving acts of terrorism. Robert Pape's (2013) influential work, "The Strategic Logic of Suicide Terrorism" , searches through the *strategic calculations that underpin suicide*

terrorism, shedding light on the rational decision-making processes of individuals engaged in such acts. This influential piece has profoundly shaped the theoretical discourse by highlighting the strategic underpinnings of terrorism and stressing the critical need to address its root causes for effective counterterrorism measures. By meticulously dissecting the strategic calculations behind suicide terrorism, Pape's work underscores the necessity of understanding the underlying motivations driving such acts. In due course, by recognizing the complex interplay of socio-political, economic, and ideological factors contributing to radicalization and extremist violence, Pape's insights advocate for holistic approaches aimed at mitigating these underlying grievances and conditions.

Expanding on the sociological aspects, the work of Mark S. Hamm and Ramón Spaaij (2017) in "The Age of Lone Wolf Terrorism" provides valuable insights into the phenomenon of *lone-wolf attacks*. Understanding the motivations, radicalization processes, and unique challenges posed by individuals acting alone adds a layer of complexity to CT Theory, necessitating adaptive strategies in practice.

Moreover, theoretical frameworks must also encompass a broader perspective that considers the psychological dimensions of *radicalization*. "Radicalization in the West: The Homegrown Threat" by Mitchell D. Silber and Arvin Bhatt (2007) is an influential work that explores the various factors contributing to radicalization, emphasizing the need for a multidisciplinary approach. As the theoretical foundation informs practical measures, intelligence agencies play a pivotal role in gathering and analyzing information critical to identifying potential threats. J. M. Berger's (2015) research on "The ISIS Twitter Census" underscores the significance of *technological advancements in intelligence gathering*, particularly the role of social media in the dissemination of extremist ideologies. This work highlights the need for CT practitioners to remain technologically savvy and adapt their strategies to the evolving online landscape.

In addition, the practical application of intelligence, however, comes with ethical considerations. Issues of surveillance, privacy rights, and data protection are explored in Didier Bigo's (2008) work, "Security, Exception, Ban and Surveillance: A Critical Sociology of the War on Terror". Bigo's examination of the ethical challenges associated with CT practices calls for an extensive approach that balances security imperatives with respect for individual rights.

Summing up, this academic inquiry into CT theory and practice underscores the importance of integrating insights from various disciplines. Important works ranging from strategic analyses of terrorism to sociological and psychological examinations of radicalization contribute to a holistic understanding. The symbiotic relationship between theory and practice remains crucial, with academic research informing the development of adaptive and effective CT strategies that address the complexities of the contemporary security landscape (Shepherd 2022).

Defining Travel Intelligence

The role of Travel Intelligence (TRAVINT) in bolstering national security and ensuring effective border control is instrumental, offering valuable insights into potential threats, risks, and suspicious activities tied to individuals and materials in transition. TRAVINT involves the systematic collection, analysis, and utilization of travel-related information and intelligence, enhancing security measures and law enforcement efforts. Focusing on data generated by passenger travel, including Passenger Name Record (PNR), Advance Passenger Information (API), and the European Travel Information and Authorization System (ETIAS), TRAVINT serves as a cornerstone in contemporary CT strategies (National Counterterrorism Center 2013; European Parliament 2016; Romanian Parliament 2019; Priestley and Beauvais 2022; Wagner 2021; Namazov 2022; Frizberg 2023).

The historical trajectory of TRAVINT in the European Union (EU) and the United States reflects a growing recognition of the need for enhanced security measures. In the EU, the establishment of the Europol Travel Intelligence Center (ETIC) in 2019, as part of Europol's horizontal operational services, signifies a concerted effort to utilize travel-related data in combating security threats within the EU (Frontex, 2020; Romanian Parliament, 2019). This development aligns with the EU's commitment to collecting and sharing travel data, as outlined in the EU PNR directive 2016/681 (Priestley and Beauvais, 2022). Similarly, in the United States, organizations like the Transportation Security Administration (TSA) and the Department of Homeland Security (DHS) actively gather travel-related data for security and border protection purposes, recognizing the pivotal role of TRAVINT in national and regional security strategies. (National Counterterrorism Center 2013; US Department of Homeland Security Privacy Office 2015, 2017).

Eventually, TRAVINT aids in the identification of individuals or groups posing a threat to national security by monitoring travel patterns and analyzing passenger data (National Counterterrorism Center 2013). It also provides insights for assessing potential risks associated with destinations, travel routes, or transportation modes, allowing authorities to determine the appropriate level of security measures required (US Department of Homeland Security Privacy Office 2015). In responding to emerging threats, TRAVINT enables authorities to adjust their security strategies promptly by continuously monitoring and analyzing travel-related information (National Counterterrorism Center 2013). Moreover, it facilitates watchlist management, helping border security agencies identify and screen individuals who pose security risks (US Department of Homeland Security Privacy Office 2015, 2017).

Specifically referring to Passenger Name Record (PNR), it is a comprehensive record containing information about a passenger's travel arrangements. PNR data, collected by airlines and travel agencies during the booking process, includes details such as the passenger's name, contact information, travel itinerary, ticket information, seat

assignments, and other relevant data (Glouftsios and Leese 2022). The analysis and use of PNR data for intelligence and security purposes within the framework of TRAVINT involve detecting anomalies or red flags indicating suspicious or illicit activity, such as travel to high-risk destinations or patterns warranting further investigation (Namazov 2022).

Subsequently, despite the critical role of PNR in TRAVINT, the collection and use of PNR data for intelligence purposes necessitate adherence to legal and regulatory frameworks, considering potential privacy implications (De Hert and Papakonstantinou 2010). Nevertheless, the analysis of PNR data within the TRAVINT context contributes significantly to enhancing security, preventing terrorism, combating human trafficking, and supporting law enforcement efforts (Rudner 2014; Barnea 2019; Shepherd 2022).

Discussion over Travel Intelligence Use in Counterterrorism Efforts

CT is inherently concerned with thwarting the activities of terrorist actors and organizations, and it involves, among other actions, intelligence gathering, analysis, and the implementation of measures to prevent acts of terrorism. This includes activities such as monitoring travel patterns, conducting background checks, and analyzing passenger data, all crucial components in identifying individuals with connections to terrorism (National Counterterrorism Center 2013; US Department of Homeland Security Privacy Office 2015, 2017).

In due course, TRAVINT emerges as a linchpin in the complex and dynamic landscape of CT, offering a sophisticated and multifaceted approach that combines tactical and operational methodologies. At the tactical level, the strategic utilization of Pattern Intelligence Analysis proves indispensable. This involves a meticulous analysis of Passenger Name Record (PNR) data, allowing the identification of anomalies or suspicious activities that may indicate potential security risks. The scrutiny extends to the examination of unusual travel itineraries, frequent changes in travel plans, and connections to known terrorism organizations' hotspots (European Commission 2023; Frontex 2020, 1–10). This comprehensive approach to pattern analysis not only aids in threat detection but also provides granular insights into the modus operandi of potential threats (Shepherd 2022).

Thereafter, complementing Pattern Intelligence Analysis, Social Network Analysis adds depth to the tactical arsenal by conducting link analysis on PNR data. This methodology unveils connections between individuals or groups engaged in terrorism activities. By dissecting shared travel patterns, common contacts, and other indicators of collaboration, Social Network Analysis contributes to a comprehensive understanding of the collaborative efforts within the terrorist network

(Shulsky and Schmitt 2009, 11–18). This strategic approach transcends individual analysis, delving into the interconnectivity that defines modern terrorism and allows for a more targeted and effective response (Shepherd 2022).

Moreover, Travel Behavioral Analysis represents another critical component of the tactical repertoire within travel intelligence. Examining the behavior of individuals or groups in PNR data provides unique insights into potential terrorism activities. This behavioral scrutiny encompasses an analysis of social behaviors, travel patterns, unusual booking behavior, and other indicators of suspicious activity (European Commission 2023; Frontex 2020, 1–10). By understanding the behavioral nuances embedded in travel data, law enforcement agencies can refine their threat assessments and proactively identify potential risks (Shepherd 2022).

On the operational front, TRAVINT unfolds as a comprehensive and adaptive strategy that extends beyond analysis to continuous monitoring and assessment. The integration of PNR data with other intelligence sources becomes imperative for a more holistic CT strategy. By merging PNR data with diverse intelligence sources, such as open-source intelligence (OSINT) and human intelligence (HUMINT), law enforcement agencies gain a more comprehensive and contextualized picture of potential terrorist activities. This collaborative approach not only corroborates findings but also provides additional context, ensuring a robust and validated understanding of potential threats (European Commission 2023; Frontex 2020, 1–10).

The implementation of these tactical and operational approaches necessitates a strategic policy framework that fosters collaboration, investment in advanced technologies, and a balance between security imperatives and individual privacy rights. International collaboration is paramount, with the establishment of robust information-sharing mechanisms globally and the fostering of bilateral agreements and joint task forces for intelligence exchange. Standardizing protocols ensures coordinated responses to emerging threats on a global scale. Investing in advanced data analytics and artificial intelligence capabilities enhances the tactical approach, enabling accurate pattern recognition and anomaly detection in travel data. Real-time monitoring requires substantial technological investments, but the benefits of early threat detection and response make it a worthwhile endeavor. Additionally, adopting a risk-based approach to CT ensures that resources are allocated efficiently, focusing efforts on high-risk travelers without causing undue disruptions (Government Publishing Office 2011).

Summarizing, TRAVINT represents a paradigm shift in the tactical and operational approaches employed in CT efforts. From pattern analysis and social network scrutiny to comprehensive operational strategies involving the integration of various intelligence sources and real-time monitoring, travel intelligence offers a multi-faceted approach to identifying and countering security threats. By embracing these approaches and implementing the suggested policy proposals, nations can foster a

more secure and resilient global landscape, proactively addressing the challenges posed by contemporary terrorism (Shepherd 2022).

Case Studies

The Case of Hezbollah

Hezbollah, a Shiite Islamist organization with a global footprint, poses a distinctive challenge in monitoring the travel patterns and *modus operandi* of its members. This case study explores wide scenarios, and travel intelligence considerations imperative for comprehending and countering Hezbollah's activities on a global scale.

Hezbollah's modus operandi is a multifaceted amalgamation of covert operations, guerrilla tactics, and recruitment strategies. Searching through the intricacies of their methods is paramount for devising effective CT strategies.

- Exploiting Lebanon and Syria International Diaspora: Hezbollah strategically capitalizes on the international diaspora originating from Lebanon and Syria, particularly in regions such as the European Union, South America, and Canada. The organization adeptly taps into these diaspora networks to gain support by engaging in fundraising activities, and potentially recruiting sympathizers. The utilization of diaspora communities provides Hezbollah with a global reach, enabling the establishment of transnational connections and alliances. Understanding the dynamics of Hezbollah's engagement with its international diaspora, especially in regions with significant Lebanese and Syrian communities, is pivotal for developing comprehensive CT strategies that address this facet of their modus operandi (Haddad 2005; Levitt 2015; Avon et al. 2012; Dionigi 2015; Kızılkaya 2019).

- Employing Coordinated Networks: Hezbollah members operate within highly coordinated networks, relying on encrypted communication channels to communicate and execute plans clandestinely. This interconnected web enhances their ability to avoid detection and facilitates seamless coordination on a global scale. The establishment of coordinated networks underscores Hezbollah's organizational sophistication. By leveraging encrypted communication, they create a resilient infrastructure that adapts to the challenges posed by modern CT measures, emphasizing the need for law enforcement agencies to stay ahead in the technological arms race (Avon et al. 2012; Dionigi 2015; Levitt 2015; Koss 2018; Kızılkaya 2019).

- Harnessing Legitimate Businesses: A distinctive facet of Hezbollah's approach involves exploiting legitimate businesses to finance their activities. This tactic blurs the lines between legal and illicit transactions, making it intricate for authorities to discern between routine economic engagements and those that fund the organization's operations. Hezbollah's incorporation of legitimate

businesses into its funding model showcases a shrewd understanding of financial systems. This dual-use strategy not only provides a stream of resources but also complicates efforts to trace and block financial support, demanding an extensive and adaptive approach from CT authorities (Levitt 2015; Avon et al. 2012; Dionigi 2015; Koss 2018; Kızılkaya 2019).

- Radicalization and Recruitment: The organization engages in systematic radicalization and recruitment efforts, often targeting diaspora communities. Identifying the patterns within these communities is pivotal for preemptive action against potential threats and serves as a key element in disrupting Hezbollah's operational capabilities. The emphasis on radicalization and recruitment within diaspora communities highlights Hezbollah's efforts to exploit existing social structures. Understanding and countering these patterns are essential not only for preventing the recruitment of new members but also for dismantling existing networks and mitigating the organization's global influence (Levitt 2015; Avon et al. 2012; Dionigi 2015; Koss 2018; Kızılkaya 2019).

The Case of Hamas

Hamas, recognized as a terrorist organization by numerous countries, operates within a multifaceted environment shaped by political, religious, and socio-economic factors. Comprehensive knowledge of the travel patterns and operational methods of Hamas members is imperative for developing effective CT strategies. This case study aims to scrutinize these aspects and propose potential strategies for leveraging travel intelligence in CT efforts.

Hamas's operational methodology, much like Hezbollah's, comprises the same diverse combination of operational tactics and strategies. A comprehensive examination of the intricate details of these methods is essential for the formulation of effective CT strategies. Understanding the nuances of Hamas's modus operandi is crucial to developing informed and targeted approaches to mitigate the organization's activities.

- Using International Palestine Migrants and Minorities: Hamas strategically leverages international Palestinian migrants and sympathizers residing in regions such as the European Union, Canada, and the United States. By exploiting existing diaspora communities, the organization seeks to establish support networks, facilitate recruitment, and potentially utilize these connections for international operations. Understanding the dynamics of engagement with Palestine migrants and minorities in these regions is crucial for comprehending the global reach of Hamas and devising CT strategies that address this aspect of their modus operandi (Shadid 1988; Dunning 2015; Sen 2015; Flamer 2022).

- Manning Covert Operations: Hamas employs covert operations, deploying clandestine networks for recruitment, fundraising, and communication. Members adeptly navigate beneath the radar, exploiting vulnerabilities in border

control systems and employing clandestine channels to move undetected and avoid surveillance (Shadid 1988; Uslu and Karatas 2020).

- Exploiting Social and Cultural Ties: Hamas members leverage extensively the social and cultural ties within the Palestinian territories. This involves exploiting familial connections, community relationships, and shared ideologies to facilitate recruitment and movement. The intertwining of social and cultural networks serves as a foundation for the organization's resilience and operational effectiveness (Shadid 1988; Dunning 2015; Sen 2015; Flamer 2022).

- Financial Networks: Hamas strategically employs financial networks, often relying on illicit funding sources to support its operations. This includes money laundering, exploitation of informal financial systems, and clandestine transactions that contribute to the organization's financial resilience (Shadid 1988; Berti 2015; Uslu and Karatas 2020; Alsoos 2021).

Hezbollah and Hamas members' Travel Patterns

Hezbollah and Hamas's members exhibit a remarkable ability to conceal their movements, employing a mix of legal and illicit means for international travel. The potential travel patterns encompass a spectrum of strategies.

- Disguised Tourism: Members adeptly disguise their activities as ordinary tourists, leveraging legitimate travel documents to seamlessly blend in with the regular flow of travelers. This tactic enables them to operate discreetly while avoiding unnecessary attention from authorities. The skillful use of disguised tourism by Hezbollah and Hamas members highlights the adaptability and resourcefulness of the organizations. By seamlessly integrating into crowds of genuine tourists, they exploit the anonymity that travel affords, complicating efforts to identify and track their movements (Dionigi 2015; Uslu and Karatas 2020).

- Business Cover: Hezbollah and Hamas operatives frequently utilize business-related travel as a cover for their activities. Engaging in seemingly legitimate ventures, these members manage to mask their true objectives behind a façade of routine business dealings, making it challenging for authorities to discern their clandestine motives. The adoption of business cover demonstrates Hezbollah and Hamas's strategic thinking, utilizing the guise of legitimate enterprises to shield their true intentions. This approach not only provides operational cover but also adds an additional layer of complexity for law enforcement agencies attempting to distinguish between lawful business activities and potential threats (Shadid 1988; Dionigi 2015; Koss 2018; Flamer 2022).

- Multiple Transit Points: Hezbollah and Hamas members employ sophisticated travel itineraries with multiple transit points. This deliberate complexity serves to obfuscate their final destinations and the overarching purpose of their travels, adding an extra

layer of intricacy to efforts aimed at deciphering their global movements. By weaving intricate travel routes, members exploit the vastness of international travel networks, making it arduous for law enforcement agencies to pinpoint their ultimate objectives and connections (Shadid 1988; Dionigi 2015; Koss 2018).

- Regional Mobility: Hamas members display significant regional mobility, frequently traversing the Palestinian territories, encompassing the Gaza Strip and West Bank. Additionally, some members may embark on cross-border journeys to countries like Egypt and Jordan. Understanding these regional movements is vital for monitoring and disrupting the organization's activities (Shadid 1988; Dionigi 2015; Koss 2018; Kızılkaya 2019; Flamer 2022).

- International Connections: While Hamas primarily operates within the Palestinian territories, its members may establish connections with sympathetic entities abroad. Travel to nations like Iran, Turkey, or other regions supportive of their cause may transpire, leading to the formation of alliances and the acquisition of external support. Similarly, Hezbollah members, primarily operating within Lebanese territories, are known to establish connections with sympathetic entities abroad, engaging in travel to nations such as Iran, Syria, or other regions that align with their cause. This international outreach facilitates the formation of alliances and provides external support, contributing to the organization's resilience and operational capabilities. The connections established beyond Lebanese borders underscore Hezbollah's transnational influence and highlight the importance of monitoring these international ties for effective CT efforts (Shadid 1988; Dionigi 2015; Koss 2018; Flamer 2022).

CT Measures Utilizing TRAVINT Against Hezbollah and Hamas

In the ever-evolving landscape of CT, the need for sophisticated strategies to combat organizations like Hezbollah and Hamas is paramount. A key aspect of such an approach involves leveraging TRAVINT to monitor and thwart the movements of Hezbollah and Hamas members. Specifically:

- API and PNR Analysis: To effectively counter the travel patterns of Hezbollah and Hamas members, governments and law enforcement agencies can employ Advanced Passenger Information (API) and Passenger Name Record (PNR) analysis. By collecting and scrutinizing data related to individuals' travel details, authorities can identify suspicious patterns and connections to known members of these organizations. This method provides a proactive means of preventing potential threats before they materialize by flagging individuals associated with Hezbollah or Hamas attempting to cross borders (Frontex 2020; European Commission 2023).

- Technological Surveillance: Incorporating advanced technologies into CT measures is essential for monitoring the travel of Hezbollah and Hamas

members. Facial recognition, biometric scanning, and sophisticated surveillance systems at border crossings and airports play a pivotal role in enhancing travel intelligence. These tools can aid in the identification of individuals associated with Hezbollah and Hamas, helping security forces detect irregular travel patterns and strengthening overall security measures (Government Publishing Office 2011; Oliveira Martins et al. 2022, 10-14).

- Infiltration of Clandestine Networks: Penetrating the clandestine networks utilized by Hezbollah and Hamas is a challenging but effective CT strategy. Law enforcement agencies can deploy agents with specialized training to infiltrate these networks, gathering critical information on travel routes, safe houses, and communication channels. Such on-the-ground intelligence provides actionable insights, enabling authorities to disrupt the logistical and operational foundations of these organizations (Shulsky and Schmitt 2009; Government Publishing Office 2011; Frontex 2020; European Commission 2023).

- Continuous Risk Assessment: Maintaining a dynamic and continuously evolving risk assessment system is crucial for adapting CT measures to the changing tactics of Hezbollah and Hamas. Regularly updating watchlists, refining intelligence-sharing protocols, and incorporating emerging technologies ensure that CT efforts remain effective and responsive to the evolving strategies of these designated terrorist organizations (Frontex 2012a, 2012b, 2013; Liu et al. 2018).

- International Collaboration: Given the transnational nature of Hezbollah and Hamas, collaboration with international partners is critical. Countries facing the threat of these organizations must share information on watchlists, known associates, and travel histories. This collaborative effort enables a more comprehensive tracking of the movements of Hezbollah and Hamas members across borders. The exchange of intelligence on a global scale contributes to a more robust defense against the international activities of these groups (U.S. Government Publishing Office 2011; Frontex 2012a, 2012b, 2013; Priestley and Beauvais 2022).

Conclusions

In conclusion, this research paper underscored the paramount importance of understanding Counterterrorism Theory and its practical applications in navigating the complexities of contemporary security challenges. With a focus on Travel Intelligence (TRAVINT), the paper highlighted its pivotal role in fortifying National Security and improving border control measures. The incorporation of two sets of results from the case studies on Hezbollah and Hamas offered concrete insights into the operational and traveling methods of these terrorist organizations, contributing

to a wider comprehension of Counterterrorism dynamics. This comprehensive inquiry advocates for adaptive and effective strategies, emphasizing the symbiotic relationship between theory and practice in the ongoing efforts to secure nations against the evolving challenges posed by contemporary terrorism. Eventually, leveraging Travel Intelligence (TRAVINT) becomes essential, employing new intelligence inputs, such as Advanced Passenger Information (API) and Passenger Name Record (PNR), and new analytical approaches like Security Risk Analysis and Backlisting. This approach enables governments and law enforcement agencies, to proactively identify and prevent potential threats by scrutinizing travel patterns and connections to known members of these organizations.

References

Alsoos, I. 2021. "From jihad to resistance: The evolution of Hamas's discourse in the framework of Mobilization". *Middle Eastern Studies*, 57(5): 833–856. https://doi.org/10.1080/00263206.2021.1897006.

Avon, D., Khatchadourian, A.T. and Todd, J. M. 2012. Hezbollah: A history of the "party of god", Cambridge, MA: Harvard University Press.

Barnea, A. 2019. "Big Data and counterintelligence in western countries". *International Journal of Intelligence and Counterintelligence*, 32(3): 433–447. https://doi:10.1080/08850607.2019.1605804.

Berger, J.M. and Morgan J. 2015. "The ISIS Twitter Census", The Brookings Project on U.S. Relations with the Islamic World, no.20.

Berti, B. 2015. "Non-state actors as providers of governance: The Hamas government in Gaza between effective sovereignty, centralized authority, and resistance". *The Middle East Journal*, 69(1): 9–31. https://doi.org/10.3751/69.1.11.

De Hert, P. and Papakonstantinou, V. 2010. "The EU PNR framework decision proposal: Towards completion of the PNR processing scene in Europe", *Computer Law &; Security Review*, 26(4): 368–376. https://doi:10.1016/j.clsr.2010.05.008.

Didier, Bigo. 2006. "Security, Exception, Ban and Surveillance." *King's College London - War Studies*.

Dionigi, F. 2015. *Hezbollah, Islamist Politics, and International Society*. Palgrave Macmillan.

Dunning, T. 2015. "Islam and resistance: Hamas, ideology and Islamic values in Palestine". *Critical Studies on Terrorism*, 8(2): 284–305. https://doi.org/10.1080/17539153.2015.1042304.

European Commission. 2023. Passenger name record (PNR). https://home-affairs.ec.europa.eu/policies/law-enforcement-cooperation/passenger-data_en.

European Parliament. 2016. *Regulation establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624*.

Flamer, N. 2022. "Hezbollah and Hamas's main platforms for recruiting and handling of human sources after 2006". *Middle Eastern Studies*, 59(5): 842–854. https://doi.org/10.1080/00263206.2022.2126835.

Frizberg, D. 2023. Advance passenger information (API): Revising the rules, European Parliament. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2023)747429.

Frontex. 2012a. *Common Integrated Risk Analysis Model a comprehensive update*. Warsaw.

__. 2012b. *Guidelines for risk analysis units: Structure and tools for the application of CIRAM version 2.0*. Warsaw.

__. 2013. *Border Control in the Information Age*. https://frontex.europa.eu/media-centre/news/focus/border-control-in-the-information-age-udh57L.

__. 2020. Future Group on Travel Intelligence and Border Management. https://www.europol.europa.eu/publications-events/publications/future-group-travel-intelligence-and-border-management#downloads.

Glouftsios, G. and Leese, M. 2022. "Epistemic fusion: Passenger information units and the making of international security", *Review of International Studies*, 49(1): 125–142. https://doi:10.1017/s0260210522000365.

Haddad, S. 2005. "A survey of Lebanese Shi'i attitudes towards Hezbollah," *Small Wars & Insurgencies*, 16(3): 317–333. https://doi:10.1080/09592310500221286.

Hamm, M. and Spaaij, R. 2017. "Introduction: The age of Lone Wolf terrorism", *The Age of Lone Wolf Terrorism*. https://doi:10.7312/hamm18174-002.

Kızılkaya, Z. 2019. "Morality of Hezbollah's conflicts with Israel," *Critical Studies on Terrorism*, 12(3). https://doi:10.1080/17539153.2019.1573037.

Koss, M. 2018. "The Lebanese Hezbollah," *Resistance, Power, and Conceptions of Political Order in Islamist Organizations*. https://doi:10.4324/9781315104867-3.

Levitt, M. 2015. *Hezbollah the global footprint of Lebanon's party of god*, Washington: Georgetown University Press.

Liu, X., Portney, K. E., Mumpower, J. L. and Vedlitz, A. 2018. "Terrorism risk assessment, recollection bias, and public support for counterterrorism policy and spending". *Risk Analysis*, 39(3): 553–570. https://doi.org/10.1111/risa.13203.

Namazov, R. 2022. Application of Advance Passenger Information (API) and Passenger Name Record (PNR) security systems by using travel information. State Customs Committee of Azerbaijan and Kanazawa University of Japan. https://www.border-security-report.com/wp-content/uploads/2022/07/API-PNR-Namazov-research.pdf.

National Counterterrorism Center. 2013. Watch listing Guidance. https://www.eff.org/files/2014/07/24/2013-watchlist-guidance_1.pdf.

Oliveira Martins, B., Lidén, K. and Jumbert, M.G. 2022. 'Border Security and the digitalisation of sovereignty: Insights from EU Borderwork', *European Security*, 31(3): 475–494. https://doi.org/doi:10.1080/09662839.2022.2101884.

Pape, R. 2013. "The strategic logic of suicide terrorism", *Terrorism Studies*, 282–310. https://doi:10.4324/9780203717622-29.

Priestley, A. and Beauvais, M. 2022. "*International experience and good practices in API/PNR, OSCE*". https://www.osce.org/project-coordinator-in-ukraine/510575.

Romanian Parliament. 2019. *IPEX | the Platform for EU Interparliamentary Exchange*. https://secure.ipex.eu/IPEXL-WEB/download/file/082dbcc568e94e7e0168eba5046a0223. https://ipexl.secure.europarl.europa.eu/IPEXL-WEB/

Rudner, M. 2014. "Intelligence-led air transport security: Pre-screening for watch-lists, no-fly lists to forestall terrorist threats", *International Journal of Intelligence and CounterIntelligence*, 28(1): 38–63. doi:10.1080/08850607.2014.962352.

Sen, S. 2015. Bringing back the Palestinian state: Hamas between government and resistance. *Middle East Critique*, 24(2): 211–225. https://doi.org/10.1080/19436149.2015.1017969.

Shadid, M. K. 1988. "The Muslim Brotherhood movement in the West Bank and Gaza". *Third World Quarterly*, 10(2): 658–682. https://doi.org/10.1080/01436598808420076.

Shepherd, A.J.K. 2022. "EU counterterrorism, collective securitization, and the internal-external security nexus", *Collective Securitization and Crisification of EU Policy Change*, 117–133. https://doi.org/doi:10.4324/9781003291374-8.

Shulsky, A.N. and Schmitt, G.J. 2009. *Silent warfare: Understanding the world of Intelligence*. Washington: Potomac Books, Inc.

Silber, Mitchell, and Arvin Bhatt. 2007. *Radicalization in the west: The homegrown threat*. New York, NY: NY Police Dept.

U.S. Department of Homeland Security Privacy Office. 2015. A Report on the Use and Transfer of Passenger Name Records between the European Union and the United States. U.S. Department of Homeland Security Privacy Office.

__. 2017. Privacy Impact Assessment Update for the Automated Targeting System DHS/CBP/PIA-006(e). U.S. Department of Homeland Security Privacy Office.

U.S. Government Publishing Office. 2011. Intelligence sharing and terrorist travel: How DHS addresses the mission of providing security, facilitating commerce, and protecting privacy for passengers engaged in International Travel. https://www.govinfo.gov/content/pkg/CHRG-112hhrg73736/html/CHRG-112hhrg73736.htm.

Uslu, N. and Karatas, I. 2020. Evaluating Hamas' struggle in Palestine. *Insight Turkey*, 109–124. https://doi.org/10.25253/99.2020221.08.

Wagner, J. 2021. *Border Management in transformation: Transnational threats and security policies of European states*. Springer.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

The integration of multi-domain capabilities in land forces units combined arms operations

Major, superior instructor Petru–Marian VEREȘ, Ph.D. Student*

*"Carol I" National Defence University, Bucharest, Romania
e-mail: verespetrumarian@gmail.com

Abstract

Current conflicts, ongoing across the globe, have highlighted the need for a new form of warfare that reduces the number of casualties and the degree of destruction and, at the same time, mitigates the effects of hybrid means, ubiquitous in the doctrine of all actors. This new approach to warfare utilizes multi-domain operations as a means of achieving success. Although multi-domain operations have been conducted in the past, the concept that encompasses the process of these operations is novel, and there are still significant adjustments that need to be made to make it operational for all actors. This article aims to study the integration of multi-domain operations into land operations by identifying the strengths and limitations of their development process, the conditions and principles of their integration at the land forces level, resulting from a comparative analysis of US and Russian Federation approaches, as well as from lessons learned from current conflicts.

Keywords:
combined arms combat; domain; effects; simultaneous and synchronized engagement of arms; multi-domain operations; capabilities.

Article info
Received: 26 January 2024; Revised: 18 February 2024; Accepted: 6 March 2024; Available online: 5 April 2024

Citation: Vereș, P.M. 2024. "The integration of multi-domain capabilities in land forces units combined arms operations". *Bulletin of "Carol I" National Defence University*, 13(1): 94-109. https://doi.org/10.53477/2284-9378-24-06

The evolution of operational art, over time, can be regarded as an effect of the great military campaigns, fundamental for the level of evolution that war and the different military doctrines that were applied during military operations. In the last century, military doctrine has undergone a massive evolution, often moving from one concept to another, or from one approach to tactics, to another, during the same campaign. Common to all conflicts of the 20th century was that land forces were the main instrument of winning the war and consequently were always supported by other force components. This habit that nations had, has been perpetuated, with few exceptions, to this day. This fact also results from the low level of development of capabilities in other domains achieved, such as air, naval, space, or cyber (NATO Standard AJP-01 2022), capabilities that are complex, difficult to produce, and expensive.

The doctrine of land forces, applied in World War I, involved the use of trenches to protect troops against direct and indirect infantry and artillery fire. This tactic led to numerous periods of stalemate, in which neither side had any solutions to defeat its opponent, and major maneuvers were often futile and with significant loss of life. It was not until 1916, right after the integration of the tank into the land forces operations, that an efficient combination of infantry maneuver, with artillery fire support and frontal tank strikes, was possible, which led to the Entente forces' success on the Western Front, in breaking the German defenses, and the consolidation of conquered objectives by means of the engineer troops. Most military historians regard World War I as a turning point and as an event of major change, which laid the foundation for contemporary combined arms warfare (Simoens 2022).

World War 2, on the other hand, practically forced the participating armies to integrate all available weapons, including at battalion level, a moment in which when the combined arms battalion appeared on the battlefield, thus configured, more evident than ever before. In the early years of the war, Germany implemented the „blitzkrieg" doctrine, meaning „lightning war", which involved the rapid and coordinated engagement of infantry, tanks, and artillery with close air support. This configuration of tactical units constituted a major leap, from the idea of massing tanks or infantry into division-level units, to the creation of mechanized combined arms units, starting from the battalion level. At the same time, the need to counter these German units forced the opposing sides to build their units in the same way, and, moreover, to create small forces with anti-tank capabilities, which significantly hampered armored and mechanized units' penetration through defensive positions.

The emergence and use of the atomic bomb provoked military theorists to consider the possibility that conventional ground warfare might be outdated and that a concentration of ground forces across a small area would be particularly risky. Moreover, the need to wage national liberation campaigns gave rise to guerrilla warfare and unconventional operations, fundamentally changing the doctrine of the first half of the 20th century. Concepts such as guerrilla warfare and

counterinsurgency, especially noticeable in the Vietnam War, led Western states to abandon the development of new-generation conventional mechanized and armored capabilities and to reinvest in light infantry units with enhanced mobility and constant air support (House 1984, 141).

The year 1990 is marked by an event that radically changed the way great military campaigns are planned, prepared, and executed. The Iraqi invasion of Kuwait and the inability of the small state to defend itself against Iraq prompted the US and Saudi Arabia to intervene with military power as well. Operation „Desert Shield" 1990-1991, involved the strategic deployment of US armed forces on the territory of Saudi Arabia, together with the involvement of European or other world allies in this campaign, produced the largest build-up of armed forces in the last 20 years (Hooton and Cooper 2019, 65). The second phase of this major campaign was Operation "Desert Storm", which meant attacking and defeating invading Iraqi forces in order to liberate Kuwait by employing a major joint air-land-naval operation.

The US lead coalition's intervention in Iraq, signified the last war of the 20th century, in which large masses of conventional capabilities, tanks, artillery, infantry, engineers, logistics, air assault, and aviation were involved (Hooton and Cooper 2019, 67), again highlighting the importance of configuring large tactical units of ground forces, according to combined arms principles, to enable maneuver over wide spaces and across great distances in order to avoid the enemy's strengths and occupy advantageous positions.

Currently, conventional warfare has become a component of hybrid warfare, in which military operations are conducted in all 5 domains of the battlespace, and do not use kinetic effects as a primary form of gaining success, but combine lethal and non-lethal effects, advanced technology, behavior-centric approaches on the target audience, and philosophies of leadership or execution, in a harmony designed to orchestrate fighting power as effectively as possible.

The strong evolution of military capabilities and doctrine, accelerated especially after the events of Russia's invasion of Ukraine and annexation of the Crimean Peninsula in 2014, leading to the development of concepts and terms such as „4th generation warfare" or even 5th generation, multi-domain operations, information warfare, hybrid threat or artificial intelligence, placing a traditional and important concept such as combined arms warfare in a shaded area, where the danger of being forgotten by the scientific community is increasing, despite its proven importance throughout history. It should not be forgotten that, as Murat Caliskan says in his article *Hybrid warfare through the lens of strategic theory*, published in *Defense and Security Analysis, "concepts shape our military understanding and consequently the armed forces"* (Caliskan 2019), and therefore, the possibility of eliminating coherent and effective approaches exists, when we try to implement, with possible limited success, the more modern concepts, but which do not yet have full validation.

However, combined arms warfare has not yet disappeared from the doctrine of The North Atlantic Treaty Organization (NATO) member states, and this article is meant to reinforce the importance of land forces combined arms units in operations, in the context of the current security environment. The concept of combined arms warfare has been the subject of many scientific articles, but most of them have been oriented towards presenting its peculiarities during various campaigns or wars throughout history. Some of the articles focus on placing the concept in the context of security environments governed by approaches that are currently either not relevant or outdated. What is special about this article is that it analyzes the importance of land forces' combined arms units in the context of multi-domain operations. This analysis is crucial for military theorists, providing support in developing knowledge regarding the place and role of land forces in multi-domain operations and offering a possible tool for use in initiatives aimed at configuring tactical units.

The article addresses 3 main research directions, which materialized as the paper's chapters. In the first chapter, the study addresses the configuration of tactical land units according to the combined arms principle and their place within multi-domain operations. This chapter highlights the critical condition necessary for any tactical unit, namely to have a combined arms configuration in order to have the possibility of integrating capabilities that allow it to act in all the domains of the battlespace and to generate effects in the operational environment. The chapter will also discuss the US' and the Russian Federation's way of configuring tactical combined arms units. In the 2nd chapter, the article presents the possible limitations and challenges arising from the integration of multi-domain capabilities into land forces operations as well as possible methods to mitigate them. Finally, the paper assesses the performance of the Russian Federation's Battalion Tactical Groups (BTGs) in the Ukraine conflict and presents relevant aspects arising from their integration into multi-domain operations conducted in this war.

The role of land forces combined arms units in multi-domain operations

The great armed conflicts of history have been, for the military science community, a good source of information about the actors involved, of observing the tactics used in warfare, an opportunity to evaluate the performance of the utilized units and capabilities, and definitely of lessons learned. Similarly, Russia's invasion of Ukraine, which began in 2014, is an important source of information, from which theorists also built the concept of *multi-domain operations.* The Allied Doctrine AJP-1 defines multi-domain operation as the "*orchestration of military activities, across all domains and environments, synchronized with non-military activities, to enable the Alliance to deliver converging effects at the speed of relevance*" (NATO Standard AJP-01 2022, 3). On the other hand, the US military doctrine, *FM 3-0 Operations,* defines multi-domain operations as "*combined arms employment of all joint and*

Army capabilities to create and exploit relative advantages that achieve objectives, defeat enemy forces, and consolidate gains on behalf of joint force commanders" (Department of the Army 2022, 3-1). The difference between the two main approaches to the concept is clearly visible, but it is also determined by the Alliance's need to create standards applicable and implementable at the level of all member states, in contrast to the American doctrine, which develops military doctrine to train its own forces.

By analyzing these two forms of defining multi-domain operations, we can agree that they represent those actions that armed forces take by means of capabilities in all domains of the battlespace, which are aimed at achieving success in the most effective way. Although differences in approach do not radically change the nature of multi-domain operations, it should be noted that US doctrine describes actions as a combined arms employment of capabilities across all domains. This approach is an indicator of the importance of a combined arms configuration of units, to enable the employment of capabilities in multiple domains and specially to generate effects in multiple domains.

Military operations that produce multi-domain effects require compliant, resilient, high-tech capabilities and tactical units, characterized by flexibility and versatility, increased combat power, extended operational range, and the ability to enable the execution of joint operations across all domains. These characteristics of land forces tactical units are reflected in the synergistic joining of several arms, services, or components, synchronizing their employment in armed combat, so that countering one of these elements will make the enemy vulnerable to another. With this in mind, we can easily deduce that a combined arms approach to multi-domain operations is not just a good method, but an absolutely necessary one.

The combined arms character of a unit is defined in US doctrine as *"the simultaneous and synchronized application of arms, to achieve an effect greater than that achieved by using each element separately or sequentially"* (Department of the Army 2019, 3-9), and this is also reflected in the configuration of tactical units, especially brigade, division, and corps level.

Throughout the continuum of competition (NATO Standard AJP-01 2022, 7) – cooperation, rivalry, confrontation and armed conflict – the corps, as a large tactical unit, integrates capabilities from all domains, at the appropriate tactical echelon, and employs divisions in battle in order to conquer the objectives of the joint force land component. The divisions, supported by the army corps, defeat the enemy by combining the maneuver and fire of their brigades and subordinate arms structures, control the conquered terrain, and consolidate the success of the joint operation. This integration of multi-domain capabilities and their engagement in an armed conflict, filled with uncertainty, ever-degraded communication, and fleeting windows of opportunity, is only possible by developing a culture in which tactical unit commanders exercise disciplined initiatives and accept calculated risks, within the mission command leadership philosophy.

Considering these aspects, we can define the role of land forces tactical units in multi-domain operations, as a role of integration and employment of multi-domain capabilities in armed combat, in order to outperform the enemy in all respects and preserve the combat power of the unit.

In US military doctrine, the corps and division provide the joint force with flexible and mission-adaptable combined arms formations and commands, capable of crisis management as well as executing large-scale ground operations, while army-level commands integrate and coordinate multiple capabilities to conduct large-scale operations within the joint operation. Corps or armies may assume multiple roles, of tactical leadership (land component headquarters) or operational leadership (joint force grouping command). These tactical echelons provide combatant commanders with forces that possess the technical and tactical capabilities necessary to conduct operations across the entire spectrum of military operations (Department of the Army 2021, 1-1).

On the other hand, Russian tactics emphasize the combined arms army and the armored army (tanks) as the main echelon between the operational or strategic leadership of the armed forces and tactical land echelons. These tactical echelons are organized, for the most part, by combined arms brigades, but major changes in the equipment of the armed forces, corroborated with a rushed technological advance caused by the war with Ukraine, portend a reorganization of these armies on divisions and even army corps (Grau and Bartles 2016, 30). These tactical units have a strong combined arms character; however, they have certain limitations, in terms of multi-domain capabilities, which are retained at operational and strategic echelons, but can conduct multi-domain cyber and air-land operations.

American combined arms units have logical consistency in their organization. The command of a US army corps primarily integrates 3 to 5 combined arms divisions, arms brigades and services, ISR (Intelligence, Surveillance, Reconnaissance), engineer, CBRN defense (Chemical, Biological, Radiological, Nuclear), air defense, artillery and missiles, military police, logistics and other specialized units, with related capabilities. For their part, U.S. divisions have a similar structure to the corps, integrating warfighting brigades, arms, and service battalions, but differing in their capability, in terms of the effects they produce. Analyzing both tactical echelons and their effects, we concluded that corps effects begin where division effects end, in the multi-domain battlespace, with the corps tasked with shaping the battlespace inaccessible to divisions in order to enable divisions to conduct unhindered action in their operating environment. More specifically, the robust combat units of division- or corps-level tactical combined arms structures receive combat or service support constantly, enhancing their maneuver execution and extending their operational range.

In contrast, the Russian combined arms army, organized on divisions, brigades, or regiments in smaller cases, as it showed in the Battle of Kiev of 2022, involved

generating *battalion-level tactical groups (BTGs),* from the organic structures of the brigades, which were logistically supported by the division and led by the combined arms army (Zabrodskyi et al. 2022, 45). These formations had the combat composition of a reinforced battalion, and their combined arms character was enhanced by the integration of several combat support capabilities, artillery, and missiles in particular, but with reduced infantry combat power. Within these BTGs, the role of infantry consisted of occupying and maintaining defensive positions as well as supporting tank structures.

The differences between the two approaches, American and Russian, are obvious. In the American concept, emphasis is placed on supporting combat units to ensure the success of their maneuver, consolidating conquered objectives and executing tactical actions without interruptions for a long time. The Russian method of engaging tactical combined arms structures relies more on an intense action of combat support structures and their effects, especially those of direct and indirect fire with artillery shells or missiles, followed by the action of combat forces. This method has a visible inclination towards attrition warfare, limited in the maneuvering of combat units and based on the effects of other means, especially hybrid, to defeat the enemy. The American and, by extension, allied approach focuses on integrating multi-domain capabilities into the combined arms operations of tactical structures, to enhance their maneuver and to shape the battlespace so that, through maneuver, the decisive points and centers of gravity of the enemy are exploited, in order to reduce the loss of human lives or capabilities, in both sides.

Many of these limitations of Russia's combined arms concept have led to the return of outdated tactics, by engaging in combat those small teams of „sacrificial" infantrymen, usually recruited from Luhansk or Donetsk provinces, from among prisoners or detainees, or from among mobilized and poorly trained soldiers, who, according to the Ukrainian military, attack under the influence of narcotics or coercion of commanders, usually until they are shot down by defensive fire, or are executed by their own comrades when they retreat. This tactic of attacking in „human waves", aims to expose opposing defensive positions, depleting resources and creating acceptable conditions for a new attack (Watling and Raynolds 2023, 5).

Challenges arising from the integration of multi-domain capabilities in land force operations and possible methods of mitigating them

The military strategy of the future is conceived and created following the path from cooperation to armed conflict, along the continuum of competition. The North Atlantic Alliance, through the strategic concept adopted at the Madrid Summit on June 29, 2022, orients the main line of effort from crisis prevention and management to its deterrence and defence function (NATO 2022). This reorientation is mainly

caused by the evolution of the main threat to the Alliance, the Russian Federation, and by the new physiognomy of the war as identified in the Russian-Ukrainian conflict.

The new war employs multi-domain capabilities in tactical operations, and combat philosophies such as the Russian one, are relentlessly developing A2/AD (Anti Access/Area Denial) capabilities and means of engaging direct and indirect fire as destructive and performant as possible. Countering Russia's threat, in the Alliance's view, involves deterring armed aggression, and if this strategy fails, defeating the enemy by overcoming it in all domains. As in most cases, the US took the initiative in 2018 to develop a land forces concept for multi-domain operations, in a context in which the other member states of the Alliance did not have the same capacity.

The American concept has as its central idea, the execution of multi-domain operations by land forces, as an element of the joint force in order to achieve success during the competition; when needed, ground forces penetrate and disintegrate enemy A2/AD systems and exploit the resulting freedom of maneuver to conquer strategic objectives and force a return to competition on favorable terms (TRADOC Pamphlet 525-3-1 2018, 7). The U.S. plans to reach full multi-domain operational capability by 2035.

The US has allocated a 773 billion US dollar budget for defense (US DoD 2022, 1-3), ranking number one in the world in 2023. Given the gigantic budget allocated by the US and the estimated time projection at this time, we clearly deduce that the main limitation to having full multi-domain capability is the high cost and long time needed to operationalize it. Among the other NATO member states, Germany and the United Kingdom are next ranked, both with a budget of over $ 65 billion allocated in 2021, according to a press release of the Alliance (NATO 2023, 7), budgets significantly lower than the American one. This further highlights the inability of NATO member states to achieve an acceptable level of multi-domain capability. Russia does not appear to be close to that capability either, with a defense spending of just over $351 billion in 2023, according to an article published by Reuters (Reuters 2023a), but improvements have been seen in various defense segments, especially for the development of long-range ballistic missile systems. Also, China, a confirmed adversary that can challenge the US in military power, had defense spending worth $ 224 billion in 2023 (Reuters 2023b), but most of the spending is focused on the acquisition of more modern equipment for land and naval forces, and not necessarily for multi-domain capabilities. For now, from the present data, only the US has a solid concept of achieving a complete multi-domain capability and allocates enough resources in this regard, but acquiring this capability will take at least 10 years.

From a tactical point of view, integrating multi-domain capabilities into ground forces operations generates unique challenges. During experimentation with multi-domain capabilities, analysts have found fluctuations in the availability of multi-domain capabilities. Each domain has concrete limitations such as the speed of

satellites in orbit, closed cybernetic networks that require effective penetration, or the times of refueling, repairing, and rearming aircraft in the air, land or sea environment (Skates 2021, 70). These constraints lead to a temporary availability of all capabilities and can create dilemmas for commanders regarding their allocation.

A principle of multi-domain operations, introduced in American doctrine and mentioned in FM 3-0 Operations, is *"convergence",* which according to this field manual, is the result created by the concentrated engagement of capabilities across multiple domains and echelons against a combination of decisive points in any domain, to create effects on a system, formation, decision-maker, or geographic area (Department of the Army 2022, 3-3). As mentioned earlier, multi-domain capabilities are, in the American view, retained at the corps level and employed to shape the division's combat. From this point of view, we can see that the division, as a fundamental echelon for combined arms operations, has limitations in multi-domain engagement, having significant effects in the ground and air environment and reduced in the other three areas. This involves major efforts to coordinate and synchronize the actions of the division and the corps to achieve convergence. Moreover, high-tech cosmic and cyber capabilities are expensive and often insufficient, being retained by operational and strategic echelons, limiting their availability also at corps level, which can only make it difficult to comply with this tenant.

However, if we imagine the effects of a successful convergence, in a multi-domain operation, the enemy will probably suffer multiple neutralizations of strong points, denying the execution of a coherent operation with chances of success, even from the first phases of the operation. For a successful convergence, its planning and preparation are crucial. We infer from the conditions of successful convergence that the synchronization of actions is the most difficult challenge. According to the military decision-making process (MDMP), the identification of critical points of the enemy depends on the quality of its evaluation outcomes. These outcomes are built through integrative processes related to MDMP, such as the *Intelligence Preparation of the Operational Environment (IPOE)* and *Joint Targeting (JT).*

IPOE identifies the elements of the enemy, related to its capabilities, its center of gravity, and doctrine applied in combat, integrating lessons learned from combat history as well as probable courses of action of the enemy (NATO Standard AJP 3-9 2016, 2-17). Also, through JT, those High-Value Targets (*HVT*), High Payoff Targets (HPT), Time-Sensitive Targets (TST*),* or other enemy targets are identified and prioritized, in order to establish their appropriate engagement in order to obtain effects consistent with the commander's intention and operation objectives (NATO Standard AJP 3-9 2021, 1-1). The overlapping of products resulting from the 3 processes, MDMP, IPOE, and JT, reveals the enemy's critical points.
Further, the commander of the large tactical unit will direct the staff on how to engage those critical points. It will aim to synchronize the engagement of capabilities in all domains to deliver simultaneous strikes to the enemy and produce decisive

effects for the entire operation from its inception. As a rule, the General Staff will provide the commander with tools that facilitate the synchronization of actions, through which he will be able to direct the actions of the combined arms unit that he leads.

Challenges of integrating multi-domain capabilities into combined arms units of land forces also arise from the need to configure structures that can integrate and engage these capabilities. Combined arms tactical units, traditionally, are configured to conduct combined arms warfare. The setup of a multi-domain engagement tactical unit seeks to develop multi-domain operations, and currently, there are no tactical units that independently conduct this type of operations. Today's multi-domain engagement requires a joint effort, and capabilities are engaged and coordinated at the operational level.

However, in an article published by the US Land Forces Association, Charles McEnany offers us a variant of configuring a multi-domain structure (Fig. 1), with an operationalization horizon no later than 2035. The configuration of this structure follows 4 functions: effects, fires, protection, and support (McEnany 2022).

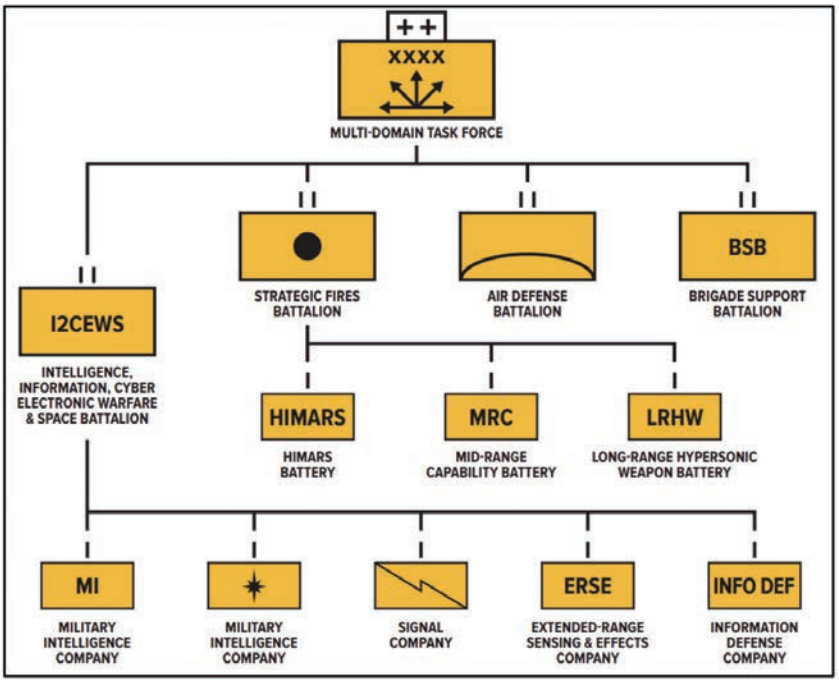


Figure 1 Multi-domain unit composition (McEnany 2022)

This structure has a similar composition to combined arms units, however, the capabilities of its microstructures differ significantly. If combined arms units were configured to effectively neutralize the combat power of the tactical enemy for the success of the operation, the multi-domain structure aims to engage A2/AD capabilities, to ensure freedom of action of the joint force, through synchronized employment of kinetic and non-kinetic effects (Chief of Staff Paper #1 2021). The long operationalization time of this type of structure, even for a nation with a

considerable advance in multi-domain operations, like the US, reveals the difficulty with which the force structure can engage multi-domain effects. Moreover, a possible conflict, assuming the need for such a structure, can accelerate the configuration and operationalization process, and this can have negative effects on its capability.

The Performance of Russian Land Forces in the Multi-domain Operations of the Russian-Ukrainian Conflict

After Russia's invasion of Ukraine and the annexation of Crimea, the Russian armed forces went through a process of reconfiguration, moving to a new look. Before this reform of the Russian ground forces, the Russian combined arms army was organized into combined arms divisions, which in turn were organized into regiments. For the most part, the combined arms character of these structures was not highlighted as it is today, and the combat or service support forces were retained under other commands, having coordinated actions at that level, leaving the divisions and regiments to be nothing more than a massing of tanks, mechanized infantry and motorized infantry, with little arms support.

As Charles Bartles and Lester Grau point out in the book „*The Russian Way of War - Force Structure, Tactics, and Modernization of the Russian Ground Forces*", the new physiognomy of the Russian ground forces, also applied in the Ukrainian conflict, has as tactical and operational echelon, the combined arms army, organized on brigades. The major change that reform brings involves generating those BTGs, within brigades, to project the combat power of a brigade (Grau and Bartles 2016, 37). Although this change was being implemented, in the initial phase of the war in Ukraine in 2022, the Russians attacked with large tactical units that were configured according to both variants: armies configured by divisions and regiments, but also by brigades. At the same time, the basis for building these large tactical units is the BTG, being Russia's choice in the Battle of Kiev and in the military operations in Donbass, to engage Ukraine's forces at the tactical level.

The BTG used in Ukraine was composed of well-trained personnel and the best readiness capability within a brigade, to create a „reinforced" battalion. The personnel problem faced by the battalion consisted in the fact that the soldiers, from all categories of personnel, did not know each other, did not train together, nor had they ever fought together. Moreover, tactical units in the ground forces faced an acute shortage of staff officers, and NCOs were not properly integrated into the BTG. To mitigate the shortcomings caused by the lack of personnel, the Russians resorted to detaching many of them from brigades or divisions higher up the hierarchical ladder, in order to create operationalized staff at the level of BTGs (Nistorescu 2022, 140). These limitations will, in most cases, create morale, cohesion, and even a significant impact on tactical actions executed by reducing the operational range of large brigade or division-level units. We cannot speak of an efficient war without

well-trained, prolific troops in the tactical field, generated by the development of a professional military institution (Stanciu 2018, 195).

Although battalions were well equipped with artillery and missile systems, often beyond the battalion commander's ability to manage them, these battle groups lacked surveillance, target acquisition, or electronic warfare systems. This has a major impact on their ability to counter enemy actions in the electromagnetic spectrum, with BTG soldiers resorting even to the use of the mobile phone network of Ukrainian citizens. Of course, this error allowed Ukrainian forces to obtain vital information about Russian plans and intentions. Moreover, this intelligence also revealed the current status of Russian troops, the state of morale, and the remaining combat power. Also, the lack of cyber defense systems has led to the interruption of the operation and systems of ISTAR, leading to the inability of Russian commanders to build a common understanding of the situation, to have a clear ground picture, or to have accurate estimates regarding ongoing operations.
However, although the Russian BTG lacked developed engineer support, it was observed that they had increased mobility in the tactical field, especially for crossing valleys or rivers, due to the constant support with assault bridges or fixed bridges, received from the echelon of the combined arms army (Watling and Raynolds 2023, 10).

Perhaps the most important aspect that affected the performance of the Russian ground forces was the transformation of the combined arms army command into a joint forces command, which would coordinate capabilities in several fields. Broadly speaking, the Ukrainian theater of operations had Russian land, air, and naval forces, with multiple cosmic and cyber capabilities, coordinated by commanders of ground forces. In this way, we infer that the Russian land forces constitute a category of supported forces, and the other categories have only a supporting role, limiting the benefits brought by the joint operation.

Thus, air operations, being coordinated by the ground command, had the operational range, in terms of time, space, or purpose, reduced to conquering the objectives set by the ground commander. Also, targets engaged through air force actions served the needs of ground forces to occupy critical infrastructure elements (Zabrodskyi et al. 2022, 45). Also, the air force, as the conflict progressed, was largely used to provide close air support to ground forces. By providing close support for soldiers in defensive or assault positions, it virtually nullified the modeling of enemy depth, to allow freedom of action for ground forces. As a result, with the air force largely focused on the advance directions of the ground forces, the depth, as a basic tenant of an operation, as written in *FM 3-0 Operations/2022,* was not extensive and was severely affected in the other areas as well. The ground component plays an important role in expanding depth, facilitating access to other capabilities in all domains, especially space and cyber, which improve the protection of tactical formations and neutralize enemy air defense systems (Department of the Army 2022, 3-7).
In general, the Russian ground forces that acted in the war in Ukraine had a poor

performance, which is also proven by the inability to achieve the main objective: the capture of Kiev and the defeat of the Ukrainian armed forces. The poor performance of the Russians results mainly from the lack of maximizing the effects of the joint operation, by limiting the use of multi-domain capabilities to supporting ground forces. Also, this method of waging war has considerably reduced the operational range of large tactical units in the ground forces by concentrating the effort on generating these BTGs with personnel and capabilities from higher tactical echelons, reducing their possibilities to execute major large-scale operations, and relying on the arms and logistical support of the army's echelon.

Perhaps, as the extensive and relevant study by Jack Watling and Nick Reynolds shows, the most important problem affecting Russia's military operations in Ukraine consisted in the lack of troop morale, lack of training and professionalism, and the lack of a philosophy of leadership and execution based on cohesion, trust, and competence.

Conclusions

The year 2024 began with major conflicts unfolding around the globe, characterized, first of all, by a large number of human casualties, mostly among civilians. The Russo-Ukrainian War, Israel's military operations to neutralize Hamas in the Gaza Strip or the Civil War in Yemen are examples of conflicts where the condition of not having a large number of human losses and a massive destruction of infrastructure is set by the ability of the armed forces to plan and execute multi-domain operations. From the images posted by the media or social networks, we realize that multi-domain operations cannot be discussed in these conflicts, the landscape of states where conflicts take place highlighting entire localities turned into rubble, humanitarian crises hard to imagine, and the lack of solutions to end the crises.

From the research carried out, it is deduced that multi-domain operations are oriented towards reducing the duration of conflicts, reducing casualties, reducing infrastructure destruction, and preserving the combat power of the actors involved. This goal of multi-domain operations cannot be achieved without a major investment of money, without considerable resources oriented towards research and development, necessary to build those capabilities that allow the military commander to have, at all times, a real and clear, comprehensive and constantly updated operational environment picture as well as the ability to engage the enemy's centers of gravity and critical points, regardless of their positioning in the battle space.

Thus, we find that the nations of the world are currently far from having operationalized multi-domain forces and capabilities. The US has a fairly large advance in terms of operationalizing a concept of multi-domain operations, but this does not mean that states such as China or Russia will not challenge the

Americans' position in the future, in any domain of the battlespace, by developing their own concepts and programs. However, the fact that the US is moving towards this objective, estimating an operationalization of the concept by 2035, has major benefits for NATO. Alliance member states should assume a participating role in the development of a multi-domain concept of operations, benefiting from the experience and progress of the US in this regard. In any case, Alliance members should at least participate in the development of the American concept in order to strengthen the European side's defence and threat deterrence capability and contribute to its implementation, collectively in Europe.

In another context, we deduce from studying the performance of the Russian Armed Forces in Ukraine that the land forces, engaged in a multi-domain operational environment, must be reconfigured so as to give up the character of supported component and start producing synchronized effects with the other four components, within the joint operation. The role of combined arms ground forces in multi-domain operations must include supporting the other components, which produce effects in other areas, because this extends the operational range of the grouping of joint forces, in scope, space and time, an element that is crucial for the success of large campaigns.

References

Caliskan, Murat. 2019. "Hybrid Warfare through the Lens of Strategic Theory." *Defense and Security Analysis* 35 (1): 40-58. doi:10.1080/14751798.2019.1565364.

Chief of Staff Paper #1. 2021. "Army Multi-Domain Transformation." https://api.army.mil/e2/c/downloads/2021/03/23/eeac3d01/20210319-csa-paper-1-signed-print-version.pdf.

Department of the Army. 2019. "Army Doctrine Publication 3-0 Operations." Washington. https://irp.fas.org/doddir/army/adp3_0.pdf.

__. 2021. "Field Manual 3-94 Army, Corps and Division Operations." Washington. https://irp.fas.org/doddir/army/fm3_94.pdf.

__. 2022. "Field Manual 3-0 Operations." Washington. https://irp.fas.org/doddir/army/fm3-0.pdf.

Grau, Lester W. and Charles K. Bartles. 2016. *The Russian Way of War – Force Structure, Tactics, and Modernization of the Russian Ground Forces.* Fort Leavenworth, Kansas, SUA: Foreign Military Studies Office. https://www.armyupress.army.mil/Portals/7/Hot%20Spots/Documents/Russia/2017-07-The-Russian-Way-of-War-Grau-Bartles.pdf.

Hooton, Ernest A. and Tom Cooper. 2019. *Desert Storm. Volume I: The Iraqi Invasion of Kuwait and Operation Desert Sheild 1990-1991.* Helion & Company Limited.

House, Jonathan M. 1984. *Toward Combined Arms Warfare: A Survey of 20th-Century Tactics, Doctrine, and Organization.* US Army Command and General Staff College. https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/house.pdf.

McEnany, Charles. 2022. "Multi-Domain Task Forces A Glimpse at the Army of 2035." *The Association of The United States Army.* https://www.ausa.org/publications/multi-domain-task-forces-glimpse-army-2035.

NATO. 2022. "NATO 2022 Strategic Concept." Adopted at Madrid Summit on 29 June 2022. https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf.

__. 2023. "Defence Expenditure of NATO Countries (2014-2023)." https://www.nato.int/nato_static_fl2014/assets/pdf/2023/7/pdf/230707-def-exp-2023-en.pdf.

NATO Standard AJP 3-9. 2016. *Allied Joint Doctrine for Intelligence Procedures.* Edition B, Version 1, NATO Standardization Office.

__. 2021. *Allied Joint Doctrine for Joint Targetting.* Edition B, version 1, NATO Standardization Office.

NATO Standard AJP-01. 2022. *Allied Joint Doctrine.* edition F, version 1, NATO Standardization Office. https://assets.publishing.service.gov.uk/media/659ea238e96df5000df843f3/AJP_01_EdF_with_UK_elements.pdf.

Nistorescu, Claudiu Valer. 2022. "The Battle of Kyiv – Considerations on the conduct of military operations at the tactical level." *"Romanian Military Thinking" Conference.* Bucharest: The Defence Staff.

Reuters. 2023a. *Russian budget expenditure in 2023 to total $351 bln - finance minister.* https://www.reuters.com/markets/europe/russian-budget-expenditure-2023-total-351-bln-finance-minister-2023-12-27/.

__. 2023b. *China plans 7.2% defence spending rise this year, faster than GDP target.* https://www.reuters.com/world/china/china-says-armed-forces-should-boost-combat-preparedness-2023-03-05/.

Simoens, Tom. 2022. "Combined Arms Warfare As The Key To Success On The Contemporary Battlefield?" *The Defense Horizon Journal.* https://tdhj.org/blog/post/combined-arms-warfare-success-battlefield/.

Skates, Jesse L. 2021. "Multi-Domain Operations at Division and Below." *Military Review - The Proffesional Journal of the U.S. Army* (Army University Press). https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2021/Skates-Multi-Domain-Ops/.

Stanciu, Cristian-Octavian. 2018. "War – A Complex Social Phenomenon." *International Scientific Conference "Strategies XXI", Technologies - Military Applications, Simulations And Resources* . Bucharest: "Carol I" National Defense University.

TRADOC Pamphlet 525-3-1. 2018. "The U.S. Army in Multi-Domain Operations 2028." Department of The Army, Training and Doctrine Command, USA, Fort Eustis, Virginia. https://adminpubs.tradoc.army.mil/pamphlets/TP525-3-1.pdf.

US DoD [United States Department of Defense]. 2022. *Defense Budget Owerview.* Office Of The Under Secretary Of Defense (Comptroller)/Chief Financial Officer. https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2023/FY2023_Budget_Request_Overview_Book.pdf.

Watling, Jack and Nick Raynolds. 2023. *Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine.* Special Report, London: Royal United Services Institute for Defence and Security Studies. https://static.rusi.org/403-SR-Russian-Tactics-web-final.pdf.

Zabrodskyi, Mykhaylo, Jack Watling, Oleksandr V. Danylyuk and Nick Reynolds. 2022. *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022.* London: Royal United Services Institute for Defence and Security Studies. https://static.rusi.org/359-SR-Ukraine-Preliminary-Lessons-Feb-July-2022-web-final.pdf.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Modeling rifle section reconnaissance patrol formation

Lieutenant Colonel Assistant Professor Vinko ŽNIDARŠIČ, Ph.D.*
Colonel Velibor PAVLOVIĆ**,
Lieutenant Colonel Aleksandar VARGA***

* University of Defence, Belgrade, Republic of Serbia; Assistant Professor in the Military Academy University of Defence, Republic of Serbia
e-mail: vinko.znidarsic@gmail.com
** Serbian Armed Forces, Republic of Serbia
*** Serbian Armed Forces, Republic of Serbia

Abstract

The successful execution of reconnaissance patrols by rifle section commanders hinges on their ability to adeptly organize their soldiers into effective formations. These formations must ensure both the safety and efficacy of the soldiers and the mission at hand. Inefficient utilization of human and material resources within rifle sections assuming the role of reconnaissance patrols can detrimentally impact the combat readiness of higher echelon units. This paper aims to explore the optimization of rifle section organizational structures by aligning them with regulations and effectively balancing capabilities with requirements. By comparing prescribed protocols in the Serbian Armed Forces with commanders' practical insights and utilizing scientific methodologies to evaluate various scenarios, this research endeavors to distill one or several generalized rifle section reconnaissance formations applicable across a spectrum of situations.

Keywords:
rifle section (rifle squad); formation; reconnaissance patrol; command and control; scenario-based method.

Article info
Received: 12 January 2024; Revised: 9 February 2024; Accepted: 1 March 2024; Available online: 5 April 2024

Citation: Žnidaršič, V., V. Pavlović and A. Varga. 2024. "Modeling rifle section reconnaissance patrol formation". *Bulletin of "Carol I" National Defence University*, 13(1): 110-127. https://doi.org/10.53477/2284-9378-24-07

An informal survey conducted through a series of interviews with the Serbian Armed Forces members in 2018 showed that Serbian Armed Forces rifle section commanders have trouble forming a reconnaissance patrol formation from available rifle section soldiers. They stated that they were not able to conduct all reconnaissance patrol formations according to the Serbian Armed Forces "Rule of infantry soldier–section" (2016).
That finding raised attention and became a problem of research in the next two years. During that period, the subject of research was the capabilities of rifle sections associated with the type and number of weapons, equipment, and specialities of rifle section soldiers when they conduct reconnaissance patrols.

The hypothesis at the beginning of the research was that the rifle section could form an effective reconnaissance patrol formation but not in all prescribed variants. The aim of the research was to discover one or several prescribed variants of formations which could raise the capability of the Serbian Armed Forces rifle section to safely and effectively conduct reconnaissance patrol without changing a weapon and equipment. The main research method was content analysis of regulations, scenario-based analysis, interviews, and brainstorming. The aim was to form one or several general variants of formations applicable for most situations in full compliance with the regulation and with reality in performance taking into consideration the real capabilities of the weapons and equipment of the troops.

Basics of reconnaissance patrol and rifle section

To be able to determine the best routes for a force to approach its objective, or secure the flanks of main forces, a commander orders reconnaissance actions so that the route, area, or zone can be checked for enemy forces, and how the weather and other factors have affected terrain. Reconnaissance is traditionally a job for small units organised as patrols in team, group, section, or platoon size. A reconnaissance patrol is not only conducted by specialized units like special forces, it is also conducted by more ordinary, general-purpose units like rifle units (Colton 2008, 54). In the Serbian Armed Forces, reconnaissance patrols are formed from units of all branches and services depending on the situation. In the Infantry battalion, the biggest infantry unit in the Serbian Armed Forces, the most commonly used unit for reconnaissance patrol is the rifle section. When the rifle section gets the task to form and conduct a reconnaissance patrol, basic rifle organization changes into a reconnaissance organisation.

At that point the problem becomes visible. The reconnaissance units are specially equipped, trained and focused on reconnaissance missions, but rifle units are not. The rifle section soldiers are generally trained for combat and reconnaissance, but they are not primarily specialized for all reconnaissance activity, especially those behind enemy lines. For rifle section commanders organizing their soldiers to perform reconnaissance patrols is very important to be able to conduct the given task

with minimum risk for soldiers and the mission. This command organization will be able to cover the general structure and the structures of its individual elements: personal, technical and organizational, as well as the appropriate transformation of these structures (Wrzosek 2022, 38).
The Serbian Armed Forces conduct a reconnaissance patrol to collect intelligence on the enemy, combat area, and meteorological conditions in a certain area. A reconnaissance patrol is a temporarily formed reconnaissance unit from a company or platoon. The strength and composition of the reconnaissance patrol can be a reconnaissance section which depends on the task, strength, activity and distance of the enemy, the type of combat actions, speed of movement of the majority of own forces, characteristics of the land, meteorological conditions and others (II Uprava GŠ JNA 1977).

In other larger armed forces reconnaissance patrols have identical tasks and roles. In the United States Army patrols are missions to gather information or conduct combat (Headquarters 2013). Reconnaissance patrols are conducted before executing operations to find the enemy and determine his strength and dispositions (Headquarters 2001). They avoid combat except for self-protection or to take advantage of an unusual opportunity (Headquarters US. Marine Corps 2000, 12-1). In Russian Ground Forces reconnaissance patrols are typically platoon-sized elements, reinforced with engineers and other specialists (Grau and Bartles 2016, 43,276). The mission of the patrol is to provide intelligence data on the enemy's strength, composition, and direction of movement. The patrol attempts to penetrate and report on the enemy's main body. The patrol also reports information on routes, the radiological and chemical situation, and the nature of the terrain (Headquarters 1984).

One brigade can have 2 infantry battalions, with 3 infantry companies each (Engelbrecht 1998, 31), with 3 rifle platoons each, with 3 rifle sections each (Headquarters 2006, 1-3). If each infantry company organizes one reconnaissance patrol with the strength of one rifle section, this would mean that at the brigade level, 54 rifle sections should be ready to carry out 6 reconnaissance patrols. Since all rifle sections periodically change in the role of a reconnaissance patrol, this means that all sections must be familiar with the possibility of using their resources to perform this task. Suppose each of the 6 rifle sections in the role of a reconnaissance patrol does not use its human and material resources effectively. In that case, it can in part affect the combat capabilities of the entire brigade.

Organization of rifle section and reconnaissance patrol

The Serbian Armed Forces "Rule of infantry soldier–section" from 2016, regulates that organizational structure of rifle section consists of nine members: the rifle section commander („komandir odeljenja", abbreviated as "KO"), machine gunner-1 („prvi nišandžija", abbreviated as "N-1"), assistant machine gunner-1 („pomoćnik nišandžije-1",

"Po-1"), machine gunner-2 („drugi nišandžija", "N-2"), assistant machine gunner-2 („pomoćnik nišandžije-2", "Po-2"), rifleman-1 („prvi strelac", "S-1"), rifleman-2 („drugi strelac", "S-2"), rifleman-3 („treći strelac", "S-3") and sniper („snajperista", "Sn"). The rifle section personnel are armed with four 7,62 mm M70 automatic rifles (or 5,56 mm M21 automatic rifles), two 7,62 mm M84 machine guns, and one 7,9 mm M76 semi-automatic sniper rifle (Žnidaršič, Stojadinović and Slađan 2021, 162) (Figure 1).

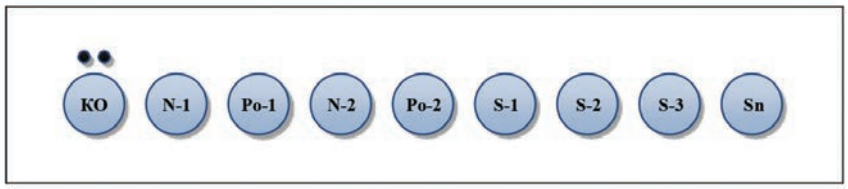


Figure 1 Organizational structure of the rifle section (KzO GŠ VS MORS 2016)

Determination of the basic organizational structure of the rifle section was the first step. The next step was to identify the variants of rifle section reconnaissance patrol formations in Serbian Armed Forces regulations.

The variants of rifle section reconnaissance patrol formations in Serbian Armed Forces regulations

To be able to determine the best routes for The Serbian Armed Forces, "Rule of infantry soldier–section" regulates that the rifle section is sent as the reconnaissance patrol by a company commander or battalion commander and that they can give the task of moving in the grip of the lead, in their area or in the area of the enemy, in the attack, defence, rest, march, fighting in the fight surrounded by enemy, pursuit, retreat and other activities and operations, reconnoiter the enemy, terrain, and important objects, at a distance determined for each specific situation (KzO GŠ VS MORS 2016, point 193, 194, 197).

The regulation specifies that all reconnaissance patrol activities take place around the core. The core leads the rifle section commander as reconnaissance patrol commander („komandir izviđačke patrole", "KIP") or his deputy (when rifle section commander moves with the lead scouts) (KzO GŠ VS MORS 2016, point 200). The reconnaissance patrol is moving generally in a column formation. In the lead of the core, two to three soldiers were designated to be the lead scouts („čelni izviđači", "ČI") (Figure 2) (KzO GŠ VS MORS 2016, point 198).

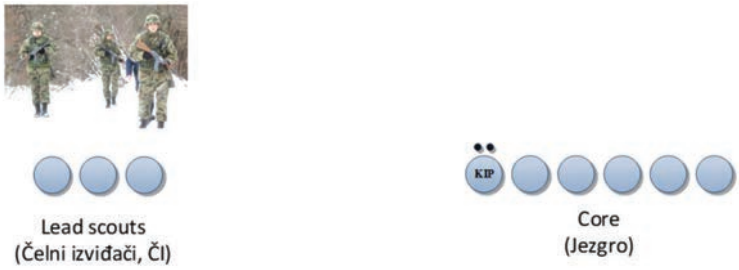


Figure 2 Lead scouts of rifle section reconnaissance patrol (Stamenković 2019, 132)

If necessary, to prevent surprises from the side of a reconnaissance patrol, the rifle section commander as reconnaissance patrol commander, designates side scouts („bočni izviđači", "BI") (KzO GŠ VS MORS 2016) (Figure 3).

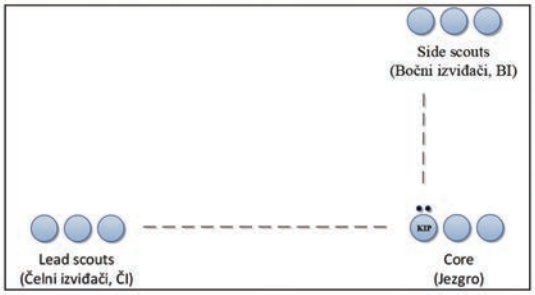


Figure 3 Lead and side scouts and core of rifle section reconnaissance patrol

For monitoring the movement and the actions of the scouts, the rifle section commander as reconnaissance patrol commander designates observers at the core („osmatrači čelnih i bočnih izviđača", "OČI" and "OBI"). Observers move inside the core or outside of the core (Figure 4). The lead and side scouts are occasionally replaced, as they move, especially when reconnaissance is carried out in difficult weather conditions (KzO GŠ VS MORS 2016, 198-200).

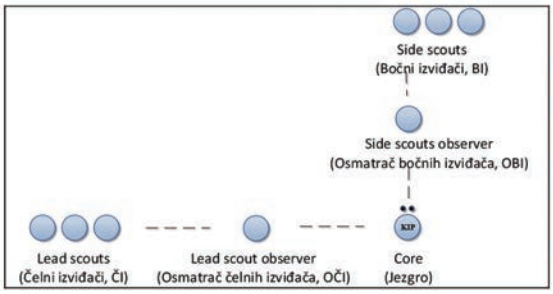


Figure 4 Observers of lead and side scouts of rifle section reconnaissance patrol

When in the reconnaissance area they are isolated and important objects are outside the direction of movement of the lead or side scouts, rifle section commander as reconnaissance patrol commander designates additional scouts („dopunski izviđači", "DI") (KzO GŠ VS MORS 2016, point 199) (Figure 5).

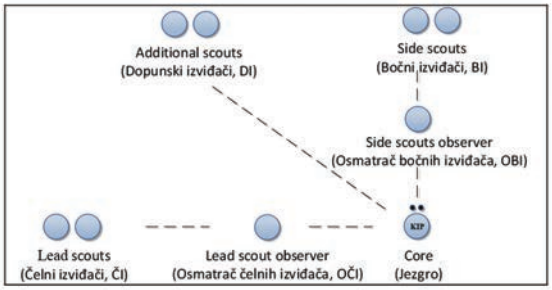


Figure 5 Additional scouts as an element of the rifle section in reconnaissance patrol formation

All scouts move at a distance that secures the core of the reconnaissance patrol from surprise and enables visual connection and signalling, with the task of detecting the enemy in a timely manner, performing reconnaissance on a particular object and reporting to the commander and directly securing the core of patrol (KzO GŠ VS MORS 2016, point 201).
In this variant, it becomes clear that all soldiers scout outside the core and that core is only one man. This is in coordination with the Rule, but it becomes clear that the reconnaissance patrol is maximally engaged outside and that the commander is that one man. This is acceptable for standing position but not for movement. Commanders have just too many scouts to control and coordinate.

In Figure 5 it is clear that the problem is the lack of soldiers in the rifle section to conduct all variants of reconnaissance patrol formation. Maximizing the engagement of all rifle section soldiers could be a short-term option with a lack of control and safety. Here it is also visible that it is crucial that general military training should prepare all platoon commanders regardless of service in order to define the necessary behaviour to perform their fighter roles, one of which is reconnaissance patrol (Petcu 2016, 47).
To perform a detailed analysis, it was necessary to know all possible regulated variants of formation. The third step was to determine all possible variants of the rifle section formation in the reconnaissance patrol and determine criteria to select those that are effective.

Variants of the rifle section formation in the reconnaissance patrol

The basis for creating scenarios of all variants of formations were two primary criteria: 1) the number of soldiers in the reconnaissance patrol and 2) the elements of the reconnaissance patrol.

For the first criterion found in the Serbian Armed Forces, "Rule of infantry section – soldier" indicated that the rifle section is a unit of nine soldiers. For the second criterion, it is established that rifle section reconnaissance patrol formation could have six elements: lead scouts (ČI), lead scouts observer (OČI), side scouts (BI), side scouts observer (OBI), additional scouts (DI) and core (jezgro) (Table 1). Back scouts („začelni izviđači"), although determined in reconnaissance units, in rifle section regulations are not a mandatory element of the rifle section reconnaissance patrol formation (Figure 5). For that, no explanation was given but was accepted as a regulated fact in the research. All elements of the rifle section reconnaissance patrol formation are shown in the columns. It is listed in the lines the number of soldiers who can make up each element (Table 1).

TABLE 1 Elements of rifle section reconnaissance patrol formation

	Lead scout	Lead scouts observer	Side scouts	Side scouts observer	Additional scout	Core
	(ČI)	(OČI)	(BI)	(OBI)	(DI)	(Jezgro)
1	3 soldiers	1 soldier	3 soldiers	1 soldier	3 soldiers	1 soldier: Section commander
2	2 soldiers		2 soldiers		2 soldiers	2 soldiers: Section commander + 1 soldier
3	1 soldier		1 soldier		1 soldier	3 soldiers: Section commander + 2 soldiers
4						4 soldiers: Section commander + 3 soldiers
5						5 soldiers: Section commander + 4 soldiers
6						6 soldiers: Section commander + 5 soldiers
7						7 soldiers: Section commander + 6 soldiers
8						8 soldiers: Section commander + 7 soldiers
9						9 soldiers: Section commander + 8 soldiers

By combining all columns (elements) and rows (numbers of soldiers) from Table 1, all possible variants of rifle section reconnaissance patrol formation were created. The variants had to have nine soldiers in total and all soldiers were seen as equal as if they were the same speciality (Table 2).

TABLE 2 List of scenarios that represent variants of the rifle section reconnaissance patrol considered as all soldiers were of the same speciality (Žnidaršič 2022)

Variant number	Lead scouts	Lead scouts observer	Side scouts	Side scouts observer	Additional scouts	The core
	(ČI)	(OČI)	(BI)	(OBI)	(DI)	(Jezgro)
1						9: KO + 8
2	3					6: KO + 5
3	2					7: KO + 6
4	1					8: KO + 7
5			3			6: KO + 5
6			2			7: KO + 6
7			1			8: KO + 7
8	3	1				5: KO + 4
9	2	1				6: KO + 5
10	1	1				7: KO + 6
11			3	1		5: KO + 4
12			2	1		6: KO + 5
13			1	1		7: KO + 6
14	3		3			3: KO + 2
15	3		2			4: KO + 3
• • •						
150	1	1	3	1	2	1: KO
151	1	1	3	1	1	2: KO + 1
152	1	1	2	1	3	1: KO
153	1	1	2	1	2	2: KO + 1
154	1	1	2	1	1	3: KO + 2
155	1	1	1	1	3	2: KO + 1
156	1	1	1	1	2	3: KO + 2
157	1	1	1	1	1	4: KO + 3

For a better understanding of Table 2, invariant number 1 (marked raw 1), the scenario is: that all nine soldiers are in the core. In variant 2 (marked raw 2), the scenario is: 3 soldiers are lead scouts and 6 soldiers are in the core. In variant number

8 (marked raw 8), the scenario is: 3 soldiers are lead scouts, 1 soldier is lead scouts observer and 5 soldiers are in the core.

The result of combining data from Table 1 is Table 2 in which 157 scenario-based variants of rifle section reconnaissance patrol column formation where all soldiers are presumed to have identical roles and specialities. But all soldiers in the rifle section are not of the same specialty and that is something that in the next step has to be taken into consideration.

Variants of the rifle section reconnaissance patrol formation balanced by soldier specialities

Soldiers of the rifle section are armed with six automatic rifles, one sniper rifle, and two machine guns and carry two complete kits of equipment to service machine guns. A machine gun 7,62 mm M84 crew consists of a machine gunner and an assistant of a machine gunner. The machine gunner is armed with a weapon that weighs 10 kg without the weight of ammunition. With two small ammunition boxes and 200 bullets in the ranks under the weight of his weapons and equipment could not be audible and concentrated on covert, careful and quiet movement in order to avoid being spotted by the enemy (Figure 6). The assistant of a machine gunner is armed with an automatic rifle, but he is limited in moves because he carries two large ammunition boxes with a total of 500 bullets. Carrying these large ammunition boxes, whether in his hands or on a combat vest, makes it difficult for him to move, even if he is relieved of unnecessary equipment in preparation for the task. It is also difficult to ensure that he remains silent and careful after a long movement.

In case it is necessary to open fast and persistent fire, members of the machinegun crew should be very close to each other. In a reconnaissance patrol, they are more likely to need to engage for the purpose of fire support for the withdrawal of lead, side or additional scouts.

Figure 6 Machine gunner and rifleman in scouting (Subotić 2014)

The sniper is armed with a 7,9 mm M79 semi-automatic sniper rifle, a long-barreled rifle that masks well but is less suitable for covert movement than an automatic rifle. The optics on the rifle are not suitable for observation in the role of scouts at short distances. Ten bullets in a rifle magazine is a small firepower that could protect or

neutralize the enemy in case of encountering him. In almost half of the interviews, commanders thought that the sniper could be used as a lead, side or scout observer, but the prevailing view in this stage of research is that it would be more useful in the core than outside it in the event of sudden combat contact with the enemy.

In the organization prescribed by the "Rule of infantry soldier–section" relative restrictions are given in point 202, that snipers and machine gunners are not assigned to lead and side scouts in principle. Although the restriction is not stated for the machine gun assistant, he should stay with the machine gunner in order for both of them to service the machine gun as successfully as possible. So, in such a determination, only riflemen can be determined as scouts.

For all the above reasons, two machine gun crew consists of two marksmen and two assistants, as one sniper and the rifle section commander are marked as not eligible for scouting. The core is the only organisational structure where they fit. Based on those criteria, all variants with less than six soldiers in the core are rejected as inadequate. That resulted in the rejection of 138 variants and the remaining 19 variants (Table 3). In all 19 variants, it is very obvious that 3 riflemen could not perform all scout duties all the time. In some moments they need rest and replacement with other riflemen but there is no additional rifleman in the rifle section to replace only 3 riflemen.

TABLE 3 Variants of rifle section reconnaissance patrol formation

	Variant number	Lead scouts	Lead scouts observer	Side scouts	Side scouts observer	Additional scouts	The core
		(ČI)	(OČI)	(BI)	(OBI)	(DI)	(Jezgro)
1.	2	3					6: KO + 5
2.	5			3			6: KO + 5
3.	12	2	1				6: KO + 5
4.	15			2	1		6: KO + 5
5.	22	2		1			6: KO + 5
6.	24	1		2			6: KO + 5
7.	52	1		1		1	6: KO + 5
8.	61	1	1	1			6: KO + 5
9.	67	2		1			6: KO + 5
10.	69	1		2			6: KO + 5
11.	3	2					7: KO + 6
12.	6			2			7: KO + 6
13.	13	1	1				7: KO + 6
14.	16			1	1		7: KO + 6
15.	25	1		1			7: KO + 6
16.	70	1		1			7: KO + 6
17.	4	1					8: KO + 7
18.	7			1			8: KO + 7
19.	1						9: KO + 8

This conclusion from Table 3 pushed the following analysis in research.

Variants of the rifle section formation in the reconnaissance patrol for most situations

Findings from Table 3 that 3 riflemen are suitable to perform all scout duties and that the rest of the rifle section could be in the core of reconnaissance patrol are simplified for research purposes. Lead, side and additional scouts are gathered as leading scouts. (Table 4, Figure 7)

TABLE 4 Reconnaissance patrol when soldiers are assigned to non-specialized positions

	Variant number	Lead scout	Lead scout observer	Side scout	Side scout observer	Additional scout	The core
		(ČI)	(OČI)	(BI)	(OBI)	(DI)	(Jezgro)
1.	2	3					6: KO + 5

In the picture, it would be seen like in Figure 7.

Figure 7 Assignment of soldiers in rifle section reconnaissance patrol formation

In this analysis, as interviewers, there were included infantry section and platoon commanders, instructors and specialists of the infantry and reconnaissance speciality at the Serbian Armed Forces, as well as teachers who conduct training with cadets of the infantry at the Military Academy of the University of Defence in Belgrade.

Interviewers in the research were tasked with examining each variant presented in Table 3, Table 4, and Figure 7. They were instructed to provide observations on both positive and negative characteristics they identified, as well as to propose changes aimed at enhancing performance or suggesting solutions that could facilitate the rifle section's successful execution of a reconnaissance patrol.

Comments and suggestions made by the interviewers during the research agree that the continuous engagement of all three riflemen on the duties of lead, side and additional scouts, as well as on the duties of observers of the lead and side scouts, meant a lot of stress for the three men during the execution of these activities. The duty of a scout is difficult and involves periodical changes in order to maintain the degree of their attention in perceiving a possible enemy and space.

All observations were gathered, leading to the conclusion that, while there may be occasions where all three riflemen could be assigned roles such as lead, side, additional, or scout observers due to reconnaissance needs, such arrangements should be avoided. This is because they would likely result in significant fatigue among the riflemen, increasing the risk of lapses in attention that could endanger the entire rifle section (reconnaissance patrol). This approach has been deemed unsustainable over the long term, as it compromises the safety of the rifle section during reconnaissance patrols.

By comparing the proposed advantages and disadvantages of the variants given by the interviewers, it was concluded that it is safe and efficient to engage one rifleman as a lead scout (Figure 8).

Figure 8 Variant of formation chosen by interviewers

Such a variant of formation would place the least burden on riflemen who are suitable to engage in scout's duties, because of characteristics of their weapons and equipment. This formation will enable all riflemen to have equal engagement on demanding scout duty.

Subjects in research proposed that this variant be the basic formation of the rifle section as the reconnaissance patrol, but interviewed commanders from mostly reconnaissance specialty also concluded that it was necessary to appoint an observer of the lead scouts who would move between the man and the core. They insisted that there was a problem in maintaining a visual connection between the core and the lead scout on curved paths, in the woods and other "closed" poorly visible spaces with many obstacles. In those spaces and situations, the lead scout is more likely to be forced to move more slowly so that the core can follow him. When the core stops, it takes some time for the solder in the core to start moving again. This slows movement and disrupts security due to frequent gathering.

This problem is in all cases being successfully resolved by appointing an observer to move between the core and the lead scout (Figure 9).

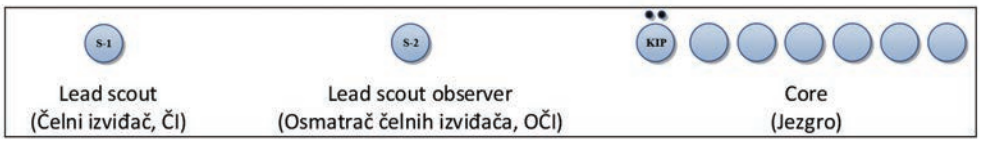


Figure 9 Less optimal, but more effective rifle section reconnaissance patrol formation

This led to a modification of the optimal formation variant from Figure 8 in which riflemen are evenly distributed on critical duties, on less optimal, but more effective rifle section reconnaissance patrol formation in Figure 9.

Formation variants in the core of the rifle section reconnaissance patrol

The determination of optimal and effective modules of rifle section reconnaissance patrol formation was a major success but formation within the core itself is the next step to complete research.

Since the Serbian Armed Forces "Rule of infantry soldier–section" stipulates that soldiers in the core generally move in a column (KzO GŠ VS MORS 2016, point 175), and it is not described elsewhere which other formations may be applied, only line formation was taken into consideration. Other formations for the movement of the rifle sections exist in literature like: line, file (column), staggered column, wedge, vee, echelon-left, echelon-right, box, diamond, Y and T (Žnidaršič and Bakos 2018) but in this study, it was initially limited to column formation as the only one listed in the legally accepted rule.

For easier data processing, machine gunner and assistant machine gunner were considered as a single entity (MGC-1 and MGC-2). They are crew and separating their members would reduce fire efficiency. The reconnaissance patrol (rifle section) commander is determined to be at the head of the patrol in all variants, i.e. at Position-1. Because it is the best position from where the reconnaissance patrol (rifle section) commander can affect the movement of the lead, side or additional scouts and core (Table 5).

TABLE 5 Variants of positions of solders in rifle section reconnaissance patrol (Žnidaršič 2022)

Variant number	Lead scouts (ČI)	Core					
		Position-1	Position-2	Position-3	Position-4	Position-5	Position-6
1	S-1	KO	MGC-1	MGC-2	S-2	S-3	Sn
2	S-1	KO	MGC-1	MGC-2	S-2	Sn	S-3
3	S-1	KO	MGC-1	MGC-2	S-3	S-2	Sn
4	S-1	KO	MGC-1	MGC-2	S-3	Sn	S-2
5	S-1	KO	MGC-1	MGC-2	Sn	S-2	S-3
6	S-1	KO	MGC-1	MGC-2	Sn	S-3	S-2
7	S-1	KO	MGC-1	S-2	MGC-2	S-3	Sn
8	S-1	KO	MGC-1	S-2	MGC-2	Sn	S-3
9	S-1	KO	MGC-1	S-2	S-3	MGC-2	Sn
10	S-1	KO	MGC-1	S-2	S-3	Sn	MGC-2
•				•			
•				•			
•				•			
109	S-1	KO	Sn	S-2	MGC-1	MGC-2	S-3
110	S-1	KO	Sn	S-2	MGC-1	S-3	MGC-2
111	S-1	KO	Sn	S-2	MGC-2	MGC-1	S-3
112	S-1	KO	Sn	S-2	MGC-2	S-3	MGC-1
113	S-1	KO	Sn	S-2	S-3	MGC-1	MGC-2
114	S-1	KO	Sn	S-2	S-3	MGC-2	MGC-1
115	S-1	KO	Sn	S-3	MGC-1	MGC-2	S-2
116	S-1	KO	Sn	S-3	MGC-1	S-2	MGC-2
117	S-1	KO	Sn	S-3	MGC-2	MGC-1	S-2
118	S-1	KO	Sn	S-3	MGC-2	S-2	MGC-1
119	S-1	KO	Sn	S-3	S-2	MGC-1	MGC-2
120	S-1	KO	Sn	S-3	S-2	MGC-2	MGC-1

By logically placing the soldiers with different weapons and equipment, several conclusions were made:

• Two machine gun crews would be good to be positioned so that they can use their heavy fire to protect the rifle section from any direction. This means that it would be good to place the first crew at the lead of the column and the second at its back.

• The rifleman or riflemen should be positioned closer to the section commander so that they are close enough to be able to replace the soldier on the duty of lead scout.

• A sniper has less firepower but a greater effect on the enemy if he is accurate. To be able to reduce stress for better accuracy, he should be assigned to Place-6. There, his ability to observe at the rear is greater in relation to the machine gun crew members, so he can successfully be an element of the back security.

Applying selection based on the given remarks 114 variants have been reduced and 6 variants remain (Table 6).

TABLE 6 Reduced variants of positions of solder in rifle section reconnaissance patrol

Variant number	Lead scout (ČI)	Core					
		Position-1	Position-2	Position-3	Position-4	Position-5	Position-6
50	S-1	KO	S-2	S-3	MGC-2	MGC-1	Sn
54	S-1	KO	S-2	S-3	MGC-1	MGC-2	Sn
61	S-1	KO	S-2	MGC-1	S-3	MGC-2	Sn
65	S-1	KO	S-2	MGC-1	MGC-2	S-3	Sn
67	S-1	KO	S-2	MGC-2	S-3	MGC-1	Sn
71	S-1	KO	S-2	MGC-2	MGC-1	S-3	Sn

Analysis shows variants in which the scenarios are identical and where machine gun crew-1 and crew-2 can be switched (marked in Table 6). The acceptable variant is where crew-1 is at the place which is directed towards the lead of the core column and crew-2 towards the rear of the core column, and then the number of variants is reduced to 3 (Table 7).

TABLE 7 More reduced variants of positions of solder in rifle section reconnaissance patrol

Variant number	Lead scout (ČI)	Core					
		Position-1	Position-2	Position-3	Position-4	Position-5	Position-6
54	S-1	KO	S-2	S-3	MGC-1	MGC-2	Sn
61	S-1	KO	S-2	MGC-1	S-3	MGC-2	Sn
65	S-1	KO	S-2	MGC-1	MGC-2	S-3	Sn

In variant number 65 (marked in Table 7), the rifleman at Position-5 is recognized as an inadequate solution because it is necessary to be closer to the section commander in order to be able to follow the events at the lead of the column and be more familiar with the situation when he should be engaged as a lead or side scout. After the rejection of variant number 65, only two variants remained (Table 8).

TABLE 8 More reduced variants of positions of solder after rejection of variant number 65

Variant number	Lead scouts (ČI)	Core					
		Position-1	Position-2	Position-3	Position-4	Position-5	Position-6
54	S-1	KO	S-2	S-3	MGC-1	MGC-2	Sn
61	S-1	KO	S-2	MGC-1	S-3	MGC-2	Sn

The last dilemma was whether both riflemen were in Position-2 and -3, respectively closer to the section commander (Variant number-54), or that rifleman-3 was placed in Position-4 (Variant number-61).

In Variant number 54, both riflemen would be better acquainted with the situation when they need to be engaged as scouts, but machinegun crews would be grouped. In case of need the crews would not be able to open fire on the wider lead for the defence and thus keep the enemy while the scouts are withdrawing. Machinegun crews would be vulnerable to the concentrated, sudden and strong fire of the enemy at one point where they are placed.

In Variant number 61, Rifleman-3 would be positioned farther from the section commander but would also be part of a subgroup capable of confronting an enemy attacking the flank or rear of the reconnaissance patrol. In such a scenario, he could assume command of this subgroup and engage the enemy while the primary group maintains suppression fire. Core variant number 61, was more acceptable to most subjects in research (Table 9 and Figure 10).

TABLE 9 Core variant number 61, more acceptable to most subjects in research

Variant number	Lead scout (ČI)	Core					
		Position-1	Position-2	Position-3	Position-4	Position-5	Position-6
61	S-1	KO	S-2	MGC-1	S-3	MGC-2	Sn

In the picture, it would be like in Figure 10.

Figure 10 Spatial representation of Core variant number 61

In the further course of the research, in relation to an optimal variant (Table 9), the subjects in the research were asked to determine one rifleman less in the core to be an observer leading scout (Table 10).

TABLE 10 Who would be more suitable to be an observer leading scout from the core?

Variant number	Lead scout (ČI)	Lead scout observer (OČI)	Core					
			Position-1	Position-2	Position-3	Position-4	Position-5	Position-6
61	S-1	?	KO	S-2	MGC-1	S-3	MGC-2	Sn

In this case, they had to decide whether to keep the Rifleman-3 (S-3) in Position-2 or-4. The interviewers in the research agreed that in such a scenario it is best to be in Position-2. Because of the need for the rifleman to be closer to the reconnaissance patrol commander, in order to be better acquainted with the events. In that scenario, machinegun crews, have positions very close to each other, but the Rifleman-3 is much more prepared and effective for lead scouting in this variant.

Another question of a who could take turns with the lead scout observer drew the attention of everyone (interviewers) to the sniper. His position is traditionally at the end of the column, but no explanation for that was found in papers during the research. It is assumed that such a position dates back to the time when this rifle and duty were introduced in the rifle section and when other soldiers were riflemen.

It was concluded that there are no reasons why such a position could not be changed. After careful study, it was concluded that the place of a sniper (Sn) in the formation should remain at Position-5, but flexible. In addition to this, it was also concluded that Position-2 and Position-5 can take either rifleman-3 (S-3) or sniper (Sn), according to the assessment and need (Table 11, Figure 11 and Figure 12).

TABLE 11 Positions of rifleman and sniper

Variant number	Lead scout (ČI)	Lead scout observer (OČI)	Core				
			Position-1	Position-2	Position-3	Position-4	Position-5
61	S-1	S-2	KO	S-3	MGC-1	MGC-2	Sn

In that way in core will always be one solder at the end of the column on Position-5, who is not from the machinegun crew, and one on Position-2 who is ready to replace the lead scout or lead scout observer solder (Table 11 and Figure 11).

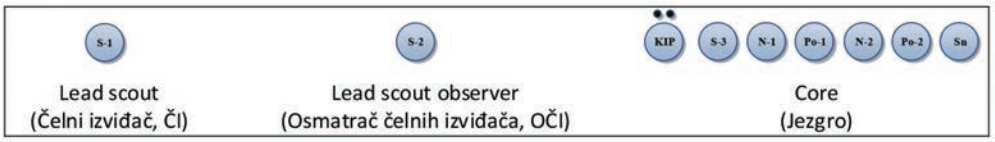


Figure 11 First variant of positions of solder and sniper during movement of reconnaissance patrol

As they move, the lead scout, rifleman-1 (S-1) and observer lead scout, rifleman-2 (S-2) could be occasionally replaced with rifleman-3 (S-3) and sniper (Sn) (Figure 12).

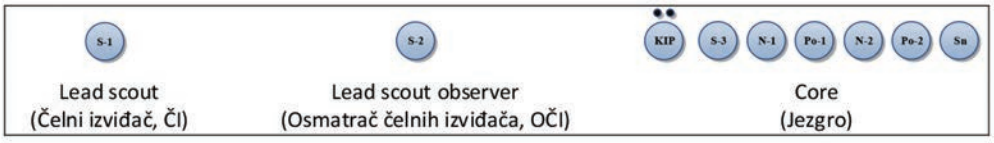


Figure 12 Second variant of positions of solder and sniper during movement of reconnaissance patrol

All other variants on riflemen and sniper positions are also acceptable.

Conclusions

In conclusion, this research presents an optimal and effective rifle section reconnaissance patrol formation suitable for a variety of common circumstances. While the rifle section is not inherently a reconnaissance unit, it possesses the capability to perform reconnaissance tasks in less hostile environments compared to specialized reconnaissance units. It is crucial to avoid overburdening the rifle section with all reconnaissance tasks, as this could jeopardize both safety and mission success. Instead, tasks must be optimized and aligned with the soldier and equipment capabilities within the rifle section, prioritizing achievable objectives over unrealistic options.

This end results variant deviates from the optimum for solders engagement to optimal for solders safety. By implementing the method of a scenario-based analysis, firstly it was determined that rifle section could be in 120 variants of the rifle section reconnaissance patrol, if all soldiers were seen as equal, as if they are the same specialty. By logically placing the solders, with different weapons and equipment, several conclusions were made and when they are implemented, the large number of variants (120) is reduced on 6, then 3, and in the end to 2 (Variant number-54 and 61). The final dilemma between those two variants was resolved by subjects in research which determined that core variant number 61 was more acceptable than variant number 54 (Table 9 and Figure 10).

In the further course of the research, in relation to an optimal variant (Table 9), the subjects in the research were asked to determine one rifleman less in the core to be an observer leading scout. It was concluded that there are no reasons why such a position could not be changed. As shown in Table 11 (Figure 11 and Figure 12), it was concluded that the place of a sniper in the formation should remain at Position-5, but flexible. In addition to this, it was also concluded that Position-2 and Position-5 can take either rifleman-3 or sniper, according to the assessment and need. As they move, the lead scout, rifleman-1 and observer lead scout, rifleman-2 could be occasionally replaced with rifleman-3 and sniper, and all other variants on riflemen and sniper positions are also acceptable.

It is important to note that the proposed variants of the rifle section reconnaissance patrol formation are not rigid prescriptions but rather flexible frameworks in line with both regulations and the practical constraints of the rifle section's organizational structure. While the rule provides a broad framework for reconnaissance patrols, it may prove overly demanding for a rifle section of nine soldiers. Practice shows that it is very rare to have a rifle section in a standard organization engaged in a reconnaissance patrol. For such tasks, the superior determines the most capable manpower and equips him with the best resources from the unit. The purpose of this research was to upgrade and balance the capabilities of the rifle section as a whole to perform specific missions such as reconnaissance patrol in an effective way.

Acknowledgements

This paper was written as a part of the scientific research project funded by the Ministry of Defence, Republic of Serbia, number: VA-DH/1/22-24 "Defence system capability development management model".

References

Headquarters US. Marine Corps [Headquarters United States Marine Corps - Department of The Navy]. 2000. *Scouting and Patrolling.* (MCWP) 3-11.3, Washington, DC: Marine Corps Warfighting Publication. https://www.marines.mil/Portals/1/Publications/MCTP%203-01A.pdf?ver=2020-08-04-074034-497.

Headquarters [Headquarters Department of the Army]. 1984. "The Soviet Army: Operations and Tactics." FM 100-2-1, Washington, DC, page 5-32. https://irp.fas.org/doddir/army/fm100-2-1.pdf.

__. 2001. "Infantry rifle platoon and squad." FM 7-8 C1, Washington, DC, point 2-5b. https://www.marines.mil/Portals/1/Publications/FM%207-8%20W%20CH%201.pdf.

__. 2006. "The Infantry Battalion ." Field Manual No. 3-21.20 (7-20), Washington, DC, Figure 1-1, page 1-3. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=04f51be4d36640dba632bfab06aff00eabbd597d.

__. 2013. "Reconnaissance Platoon, Army Techniques and Procedures." No. 3-20.98. ATP 3-20.98, Washington, DC., point 3-122. https://www.globalsecurity.org/military/library/policy/army/atp/atp3-20-98.pdf.

II Uprava GŠ JNA [II Uprava Generalštaba Jugoslovenske narodne armije Saveznog sekretarijata narodne odbrane]. 1977. *Pravilo izviđačka četa-vod u pešadijskim i oklopnim jedinicama.* II U-1, point 1. Belgrade, Vojnoizdavački zavod. https://dokumen.tips/documents/pravilo-izvidjacka-ceta-vod-u-pesadijskim-i-oklopnim-jedinicamapdf.html.

KzO GŠ VS MORS [Komanda za obuku Generalštaba Vojske Srbije Ministarstva odbrane Republike Srbije]. 2016. *Pravilo vojnik-odeljenje pešadije [Rule of infantry soldier–section].* point 193, 194, 197, 198, 199, 200, 201.

__. 2017. "Priručnik za vojnika - izviđača ." KzO-45. L 0-1.5.1., page 175. point 325.

Colton, Greg. 2008. "Enhancing operational capability: making infantry more deployable." *Australian Army Journal* 5 (1): 51-56. https://search.informit.org/doi/pdf/10.3316/ielapa.200806604.

Engelbrecht, Leon. 1998. "The infantry Battalion." *African Armed Forces* pp 31-35. https://www.defenceweb.co.za/wp-content/uploads/Repository/Editors-Archives/The-Infantry-Battalion-pt2-June-1998.pdf.

Grau, Lester W. and Charles K. Bartles. 2016. "The russian way of war: force structures, tactics, and modernization of the russian ground forces." *Foreign Military Studies Office* page 43, 276. https://www.researchgate.net/profile/Charles-Bartles/publication/329934215_The_Russian_Way_of_War_Force_Structure_Tactics_and_Modernization_of_the_Russian_Ground_Forces/links/5c245aee299bf12be39c2a4f/The-Russian-Way-of-War-Force-Structure-Tactics-and-Modernization-of-the-Russian-Ground-Forces.pdf.

Petcu, Vasile. 2016. "Professional Roles of The Basic Officer Course Graduates At The Army Level." *Bulletin of "Carol I" National Defence University* (no. 1): 43-48. https://www.ceeol.com/search/article-detail?id=415877.

Stamenković, Slađan. 2019. *Treća brigade kopnene vojske: monografija: 2007-2018.* Niš: Nais Print.

Subotić, Nemanja. 2014. *Reporteri "Novosti" u "ratnoj situaciji" sa Prvom brigadom VS.* https://www.novosti.rs/vesti/srbija.73.html:476583-Reporteri-.

Wrzosek, Marek. 2022. "Challenges of contemporary command and future military operations." *Scientific Journal of the Military University of Land Forces* 54 (1): 35-51. https://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-c5d8d300-2428-4980-a407-9a0f64269573/c/3_wrzosek_challenges_sjmulf_1_2022.pdf.

Žnidaršič, Vinko. 2022. *Modeling Rifle Section Reconnaissance Patrol Formation.* Mendeley Data, V1. doi: 10.17632/7ws2w4grh5.1.

Žnidaršič, Vinko and Csaba A. Bakos. 2018. "Formations variants analysis of four man infantry section fire team." *Vojno delo* vol. 70 (no. 8): 101. http://scindeks-clanci.ceon.rs/data/pdf/0042-8426/2018/0042-84261808097Z.pdf.

Žnidaršič, Vinko, Ivan Stojadinović and Veljković Slađan. 2021. "Serbian Armed Forces Rifle Platoon: Basic Models of Command Organisation." *International conference KNOWLEDGE-BASED ORGANIZATION.* vol. 27 (no.1): 161-167. https://doi.org/10.2478/kbo-2021-0025.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Crime Reporting Patterns and Frequencies in Print Media in Post-COVID Nigeria: A Security Approach

Tajudeen Yusuf ADEYINKA*
Musediq Olufemi LAWAL**
Olawale Olufemi AKINRINDE***
Remi Kasali ALATISE****

*Department of Criminology and Security Studies, National Open University of Nigeria
**Department of Sociology Osun State University, Osogbo, Nigeria
***University of Johannesburg, Johannesburg, South Africa
e-mail: oakinrinde@uj.ac.za
****Department of Sociology and Industrial Relations, Fountain University Osogbo, Nigeria

Abstract

This study systematically delves into the intricacies of crime reporting by mass media in post-COVID Nigeria, shedding light on its profound impact and intensity. Through meticulous archival methods, historical editions of The Guardian and Punch newspapers were analyzed over three years. The findings highlight a notable emphasis on crimes against individuals, such as murder and assault, compared to other categories like financial and drug-related crimes. Over 4,093 crime incidents were reported, with crimes against persons dominating in 2021 and 2022. The study underscores the need for nuanced crime reporting and advocates for substantive engagement through editorials and analyses. By fostering awareness and discourse, print media can play a pivotal role in shaping public understanding of crime dynamics and promoting societal well-being.

Keywords:
Crime; Crime rate; Security; Print media; Newspaper; Post-COVID; Nigeria.

Article info
Received: 2 February 2024; Revised: 27 February 2024; Accepted: 18 March 2024; Available online: 5 April 2024

Citation: Adeyinka, T.Y., M.O. Lawal, O.O. Akinrinde and R.K. Alatise. 2024. "Crime Reporting Patterns and Frequencies in Print Media in Post-COVID Nigeria: A Security Approach". *Bulletin of "Carol I" National Defence University*, 13(1): 128-137. https://doi.org/10.53477/2284-9378-24-08

In every society worldwide, there are distinct sets of problems and hurdles, and Nigeria is no exception. Being a developing nation, Nigeria encounters a range of social, political, economic, and cultural challenges that significantly impact the well-being of its people. Among the myriad issues plaguing the country, crime stands out as particularly pervasive, permeating all levels of society. Crime, a phenomenon experienced universally, varies only in intensity among different nations. In Nigeria, this issue is multifaceted and has the potential to undermine the nation's unity and efforts towards sustainable development. Various factors, including the escalating and uncontrolled crime rates, pose threats to Nigeria's corporate existence, especially given its historical and contemporary political landscape.

Over time, crime rates in Nigeria have risen, characterized by increased sophistication and efficiency in criminal activities, leading to the emergence of vigilante groups in certain regions to address the issue. Understanding the dynamics of crime is fundamental to combating criminal activities effectively. While crime is commonly perceived as a moral threat and detrimental to society, it is a global phenomenon, as evidenced by the International Crime Victim Survey's findings spanning different regions and time periods.

Nigeria, like many developing countries, grapples with a rising urban crime rate, posing significant social challenges. The concentration of violent crimes in urban centers reflects broader systemic issues and threatens lives, property, social order, and national security, thereby diminishing citizens' quality of life. The print media play a crucial role as society's watchdogs, shedding light on crime and security matters, although academic attention to complement media efforts remains insufficient.

In light of these considerations, this study aims to explore the patterns of crime reporting in Nigeria through a sociological lens, complementing existing data derived from the print media. Employing a descriptive research approach, the study extracted data from two national dailies, The Guardian and Punch, archived at the Kenneth Dike's Library, University of Ibadan. Information spanning from January 2021 to March 2023 was meticulously gathered and subjected to content analysis with a view to providing insights into crime reporting trends in Nigeria. The findings, presented through tables and supported by verbatim quotes from the newspapers, offer valuable contributions to understanding and addressing crime-related issues in the country.

Crime Rate as Reported by the Print Media

Table 1 illustrates the incidence and distribution of reported crimes by the print media during the period spanning January 2021 to December 2021. Within this timeframe, Punch newspaper documented a significant focus on crimes against persons, constituting 60% of their reported cases. Drug offenses accounted for 4.3%,

financial crimes for 13.5%, other crimes for 6.9%, and property crimes for 15.3%. The cumulative count of all reported crimes by Punch during this period amounted to 879 cases.

Similarly, The Guardian newspaper covered crimes reported from January to December 2021, with a notable emphasis on crimes against persons, comprising 63.4% of their reported incidents. Drug offenses constituted 5.6%, financial crimes 12.2%, property crimes 11.0%, and other crimes 7.6%. The total count of all reported crimes by The Guardian during this period summed up to 631 cases.

TABLE 1 Crimes reported between Jan 2021 – Dec 2021

Type of Crime	Punch	Guardian	Jan-December 2021
Crime against person	467 (60.0)	335 (63.4)	802
Drug offences	60 (4.3)	57 (5.6)	117
Financial crime	129 (13.5)	89 (12.2)	218
Others	81 (6.9)	67 (7.6)	148
Property crime	142 (15.3)	83 (11.0)	225
Total	**879**	**631**	**1510**

Source: Punch and Guardian Newspapers, 2021

The combined reportage from Punch and The Guardian accounted for a total of 802 cases of crimes, specifically offenses against persons. Additionally, the aggregated number of reported drug offenses by both newspapers amounted to 117 cases. Financial crimes were documented in a total of 218 cases. Conversely, under the category of 'others,' encompassing offenses like traffic acts, dog acts, perjury, and coining offenses, the Punch and The Guardian reported a combined total of 148 cases during the reviewed period. Property crimes, amounting to 225 cases, were also included in the overall tally, resulting in a cumulative count of 1,510 reported crimes.

TABLE 2 Crimes reported between Jan 2022 – Dec 2022

Type of Crime	Punch	Guardian	Jan –Dec, 2022
Crime against persons	475 (54.5)	325 (64.8)	800
Drug offences	112 (7.8)	80 (7.5)	192
Financial crime	175 (16.0)	92 (9.9)	267
Other	98 (6.1)	83 (7.7)	181
Property crime	169 (15.2)	94 (10.3)	263
Total	**1,029**	**674**	**1,703**

Source: Punch and Guardian Newspapers, 2022

Table 2 encompasses the data for the second year under examination. As per the presented data, Punch Newspaper reported a total of 1,029 cases. Among these, crimes against persons registered the highest frequency, accounting for 800 cases,

representing 54.5% of Punch Newspaper's reported instances. Other reported crimes included financial crime (16%), property crime (15.2%), and drug offenses (7.5%), while the remaining cases fell under the classification of 'others' (7.8%).

In a similar vein, the Guardian newspaper reported 325 cases of crimes against persons, making up 64.8% of their reported cases, followed by property crime (10.3%), financial crime (9.9%), 'others' (7.7%), and drug offenses (7.5%). The combined total of cases reported by both Punch and Guardian Newspapers during the period spanning January 2022 to December 2022 amounted to 1,703.

TABLE 3 Pattern of Crimes Reported January 2023 – March 2023

Type of Crime	Punch	Guardian	Jan-March 2023
Crime against persons	276 (54.1)	153 (41.4)	429
Drug offences	41 (8.0)	38 (10.3)	79
Financial crime	78 (15.3)	52 (14.0)	130
Other	45 (8.9)	61 (16.5)	106
Property crime	70 (13.7)	66 (17.8)	136
Total	**510**	**370**	**880**

Source: Punch and Guardian Newspapers, 2023

The table presented outlines the frequency and distribution of reported crimes by the print media during the period from January 2023 to March 2023. Punch newspaper documented a substantial focus on crimes against persons, constituting 54.1% of their reported cases. The reported rates of other crimes included financial crime (15.3%), property crime (13.7%), other forms of offenses (8.9%), and drug offenses (8%). During this timeframe, Punch reported a total of 510 crimes.

Contrastingly, the Guardian newspaper reported the occurrence of criminal activities from January to March 2023, with crimes against persons accounting for 41.4% of their reported cases. Property crime constituted 17.8%, 'other' offenses not classified herein comprised 16.5%, financial crime stood at 14%, and drug offenses at 10.3%. The total number of reported crimes by the Guardian during this period amounted to 370 cases. When combining the reported cases from both newspapers, the total number of reported crimes reached 880.

A comparison between the findings from the newspapers, as presented in Table 1, and the incidents of reported crimes at the national level, as shown in Tables 2 and 3, reveals a notable disparity in the number of crimes reported by the press and those reported by the police. Crimes against persons prominently featured in police-reported incidents. While the element of newsworthiness may have influenced these results, it raises concerns that the press might be presenting an inaccurate and distorted portrayal of the crime situation in the country.

Pattern of Crime Reported

The results indicated that the newspapers gave more coverage to violent crimes, such as murder and assaults, compared to other crime categories like financial, drug, and property crimes. Both Punch and Guardian newspapers reported on incidents involving gunmen attacks, Boko Haram issues, killings, fraud, and rape. Approximately 60% to 63% of the offenses reported in these newspapers fell under the classification of crimes against persons. The allure of crime and violence lies in their ability to attract attention and boost ratings for news programs and circulation figures for newspapers. Media owners, being profit-driven, find crime and violence stories appealing due to their sensational, dramatic, and sometimes colorful nature. This inclination is evident in the way media operators readily present gripping narratives of events such as rapes, commando-like bank robberies, murders, high-profile assassinations, or monumental frauds. In essence, crime and violence are not only captivating but also tempting to media operators (Dorfman and Thorson 1998).

TABLE 4 Crime reported within the years under review (2021 to 2023)

Pattern of Crime	2021	2022	2023	Total
Crime against persons	802 (53.1%)	800 (47.0%)	429 (48.8%)	2,031
Drug offences	117 (7.7%)	192 (11.3%)	79 (9.0%)	388
Financial crime	218 (14.4%)	267 (15.7%)	130 (14.8%)	615
Other offences	148 (9.8%)	181 (10.6%)	106 (12.0%)	435
Crime against property	225 (15.0%)	263 (15.4%)	136 (15.4%)	624
Total	**1,510**	**1,703**	**880**	**4,093**

Source: Punch and Guardian Newspapers, 2023

The above table shows the pattern and rate of crime reported by the print media from January 2021 to March 2023. These crimes were categorized under' crime against persons', 'drug offences', 'financial crime', 'crime against property', and 'other offences'. Using the model in Okunola (2009), the crimes classified above were highlighted to understand their dimensions below:

Crime Against Persons/Violent Crimes:

Trafficking, human trafficking, grievous bodily harm, child abuse, sexual offenses, and unnatural offenses were classified by Okunola (2009). Additionally, contemporary issues in Nigeria, such as kidnapping, hostage-taking, and banditry, were prevalent, although not explicitly covered by Okunola's classification. These newer elements received extensive coverage across print, electronic, and online news platforms.

Property Crime:

Property crimes include Stealing, Robbery, Extortion, Bunkering, Forgery, Vandalisation, Burglary, and Arson.

Economic/Financial Crime:
Cases in this form of crime include Fraud/false pretense and cheating, corruption, graft, embezzlement, fake currency, impersonation, smuggling, illegal mining, and Drug offenses.

Other offense/Local Acts:
These encompass perjury cases, offenses related to demand and menace, as well as related offenses, traffic acts, offenses against township acts, liquor acts, dog acts, and other related offenses.

Table 4 outlines crimes reported over three years (2021, 2022, and 2023), examining the crime rate monthly. According to the data, Punch and Guardian Newspapers reported a total of 4,093 cases across these years. Within this total, 2,031 were crimes against persons, 388 were drug offenses, 615 were financial crimes, 624 were crimes against property, and 435 were categorized as 'other offenses'. In 2021, crimes against persons comprised the highest percentage of reports (53.1%), followed by crimes against property (15%), financial crimes (14.4%), other offenses (9.8%), and drug offenses (7.7%). In 2022, both Punch and Guardian Newspapers reported 47% of crimes against persons, followed by financial crimes (15.7%), crimes against property (15.4%), drug offenses (11.3%), and other violations (10.6%). For the January to March 2023 period, 880 crime cases were reported in Punch and Guardian Newspapers, with crimes against persons still topping the list at 48.85%. Other trends included crimes against property (15.4%), financial crimes (14.8%), other offenses (12%), and drug offenses (9%).

In Northern Nigeria, reported crime cases largely reflected escalating socio-religious issues, primarily crimes against persons. A case from the Northeastern part mirrored events in Borno State three days prior, with a property crime case referred to court in Lagos. 'Other offenses/local act' cases attracted the attention of crime desks in print media. Newspapers in Nigeria also covered foreign-based criminal cases, often involving Nigerians, particularly those related to narcotic matters. The September 21st, 2021 edition of Punch Newspaper highlighted a phone crime case without providing details. The same paper reported on federal troops seizing guns, a pickup van, and ammunition boxes from Boko Haram insurgents in Kodunga, Borno State.

Geographical Spread of the Crimes Reported

The geographic location of a crime holds significant importance, encompassing elements such as law, offender, and target, as outlined in the dimensions of a criminal event by Brantingham and Brantingham (1991). Understanding the crime location and associated geographic information can offer insights into suspect identification, aid in devising prevention or apprehension strategies, facilitate program evaluation, and contribute to a better comprehension of environmental factors linked to crime (Christie 1982; Farrington 2002).

Print media reports highlight a considerable incidence of high crimes against persons in northern Nigeria, particularly involving events such as killings, bombings, and insurgency by groups like Boko Haram and Fulani herders. Examples from places like Kano, Yobe, Kogi, Borno, Plateau, etc., include incidents resembling bloodbaths, such as the suicide bomb attacks on motor parks in Kano and Potiskum. Notable casualties include 15 people killed and 53 others injured in the Potiskum, Yobe State attack, and 12 lives lost in the incident at the Kano line motor park on Zaria Road, Kano.

In eastern Nigeria, print media commonly cover crimes such as stealing, robberies, and killings in locations like Rivers, Anambra, Imo, Enugu, etc., often of a violent nature. Within the southwestern geopolitical zone of Nigeria, crimes reported during the review period include offenses against persons like manslaughter, attempted murder, suicide, rape, and indecent assault, as well as financial crimes like fraud/false pretense, cheating, corruption, graft, embezzlement, fake currency, impersonation, smuggling, illegal mining, and drug offenses. These cases were widespread in areas like Lagos, Osun, Ondo, and other states within the region.

Management Approach Towards Crime

Crimes often trigger responses and defensive actions from victims and potential victims. These reactions may involve the installation of alarm systems, avoiding nighttime outings, or steering clear of high-risk areas. As information about crime circulates, others may adopt similar defensive strategies. In due course, community groups and governments might implement neighborhood watch programs, enhance police surveillance in problematic areas, or introduce new legislation. The strategies employed by criminals and the counterstrategies implemented in response evolve in tandem, driven by various factors. Defensive counterstrategies, discussed below, prompt individuals seeking criminal opportunities to adapt by developing new crime strategies or transitioning to different types of crime (Cohen and Young 1981).

In a broader sense, higher crime rates often prompt the implementation of more stringent protective measures, initially causing a decline in crime rates. Conversely, lower crime rates may reduce barriers to crime as individuals and communities allocate limited resources to more urgent issues. Nonetheless, individuals with a development-focused orientation would always aspire for minimal crime rates. The reduction in crime rates may make criminal activities seem easier, less risky, and more attractive as a means to acquire resources, implying that crime is likely to persist at some level in society. As fewer individuals are drawn to crime, the potential rewards tend to increase, inevitably attracting someone. These dynamics, coupled with the tendency of defensive counterstrategies to initiate a cycle by provoking counter-counterstrategies from offenders, suggest that crime will likely persist at some level in society (Davis et al. 1997; Becker 1992; Simon and Feely 1995).

Understanding how counterstrategies address the root causes of crime is crucial for making criminological research relevant to public policy. Strikingly, in areas where brutal cases of crimes against persons were reported, there was a lack of proactive measures, and the common response after such incidents was people expressing 'lamentations.'

TABLE 5 Crime Cases and Their Treatment

Cases reported	2021	2022	2023	Total
Police investigation	512 (34.0%)	654 (38.4%)	373 (42.4%)	1,539
Judicial matter	643 (44.8%)	582 (34.2%)	298 (33.9%)	1,523
Neither police nor judicial matter	355 (21.2%)	467 (27.4%)	209 (23.7%)	1,031
Total	**1,510**	**1,703**	**880**	**4,093**

Source: Punch and Guardian Newspapers, 2021-2023

The presented table outlines crime cases reported by the print media from January 2021 to March 2023, categorizing them into three parts based on their treatment: police investigation and judicial matters, only police or judicial matters, and cases with neither police nor judicial involvement. In 2021, 34% of cases underwent police investigation, with 44.8% charged to court and attended to, and 21.2% neither treated by police nor judicial matters. In 2022, police investigation cases increased to 38.4%, judicial matters reduced to 34.2%, and cases with neither police nor judicial matters rose to 27.4%. Similarly, in 2023, police investigation cases further increased to 42.4%, judicial matters decreased to 33.9%, and cases with neither police nor judicial matters decreased to 23.7%.

During the study period, the Nigerian print media demonstrated very little or no pictorial representation of crime issues, which could have been a straightforward means of dissemination. Most analyses of media representations of crime have focused on newsprint and broadcast, with fewer studies on fiction. Crime and criminal justice have historically served as sources of popular spectacle and entertainment, illustrated by criminal biographies and pre-execution confessions prevalent in the seventeenth and eighteenth centuries. The police and criminal justice system are predominantly depicted positively in popular fiction as effective protectors against serious harm and violence. However, there has been increasing scrutiny of police success and integrity in recent times (Reiner, 2000). Notably, in the reviewed newspaper editions, a political analytical approach was adopted, while crime stories lacked a similar analytical treatment.

Conclusion

The study has delved deeply into the crime reports featured in Nigerian newspapers Punch and The Guardian, spanning from January 2021 to March 2023. It meticulously

detailed the occurrence and breakdown of reported crimes, classifying them into distinct categories such as crimes against persons, drug offenses, financial crimes, other offenses, and property crimes. Key observations include a consistent media focus on crimes against individuals, noticeable differences between media and police-reported incidents, and a preference for covering violent crimes in print media. The narrative extends to the geographical distribution of reported crimes, particularly highlighting patterns in northern Nigeria. Additionally, it explored the approach taken toward crime management, defensive counterstrategies, the handling of crime cases by law enforcement and the judiciary, and the absence of visual representation of crime issues in the print media. The study further observed that the selected media consistently and actively reported on crime, with crime against persons emerging as the most frequently covered deviant report throughout the three-year analysis. As a result, the front pages of the newspapers prominently featured the most significant and controversial crime stories. In terms of editorial bias, the study observed that a considerable portion of the stories adhered to reporting facts without undue favoritism. These items predominantly fell into the category of straight news stories, thereby necessitating a factual and balanced presentation of reports without bias.

Similar to other forms of mass media, it was observed that the print media demonstrated a degree of indifference towards actions taken against perpetrators of crime. Although, the media is expected to go beyond mere awareness creation or indifference and serve as a conscience of authority, encouraging further investigation, educating readers, and shedding light on legal processes to stimulate change from both authorities and citizens, the selected print media maintained and restricted themselves to their traditional role of report-making.

Since a heightened emphasis on editorials is essential, as they wield significant influence in shaping public policy and setting agendas, it is crucial to stress through editorials that crime is unacceptable, and anyone caught in the web of committing criminal acts would face the consequences. Hence, the potency of print news publications should not be underestimated and needs to be leveraged, especially in this age of information, where research trends are increasingly being concentrated on the rapidly evolving cyber technologies such as the Internet, visual media, films, and television, among several others.

References

Ackerman, W. and A.T. Murray. 2004. "Assessing Spatial Patterns of Crime In Lima, Ohio." *Cities* (Elsevier Ltd.) 21 (5): 423-437.

Aremu, M.A. and Y.A. Ahmed. 2011. "An Investigation of Security and Crime Management in Developing Society: The Implications for Nigeria Democratic Set-Up." *International Journal of Academic Research in Business and Social Sciences* 3 (1): 390-399.

Becker, H. 1992. *Outsiders.* New York: Free Press.

Brantingham, P.J. and P.L: Brantingham. 1991. *Environmental Criminology.* Prospect Heights, IL: Waveland Press.

Christie, N. 1982. *Limits to Pain* . Oxford : Martin Robertson & Company Ltd.

Cohen, S. and J. Young. 1981. "Mods and rockers: The inventory as manufactured news." In *The manufacture of news: Deviance, social problems, and the mass media* , by S. Cohen & J. Young (Eds.). California: Sage Publications.

Dambazau, A.B. 2007. *Criminology and Criminal Justice.* 2nd Edition. Ibadan: University Press.

—. 1994. *Law and Criminality in Nigeria.* Ibadan: University Press.

Davis, U.B., F. Simon, W. Farrington and G. Patterson. 1997. "1980 in ." In *The Oxford Handbook of Criminology, 2nd Edition*, by M. Maguire, R. Morgan, and R. Reiner (Eds). Oxford: Clarendon Press.

DeKeseredy, W.S. and M. Dragiewicz. 2011. *Handbook of Critical Criminology.* London: Routledge.

Dorfman, L. and E. Thorson. 1998. "Measuring the Effects of Changing the Way Violence is Reported ." *The Nigerian Foundation of Journalism at Harvard University* 52 (4).

Durston, G. 1997. *Moll Flanders: Analysis of 18th Century Criminal Biography.* Chichester: Barry Rose.

Fajemirokum, F.O., O. Adewale, T. Idowu, A. Oyewusi and B. Maiyegun. 2006. " A GIS Approach to Crime Mapping and Management in Nigeria: A Case Study of Victoria Island Lagos." *XXIII FIG Congress.* Munich, Germany.

Faller, L. 1987. *Turned to Account: The Forms and Functions of Criminal Biography in Late Seventeenth and Early Eighteenth-Century England.* Cambridge: Cambridge University Press.

Farrington, D.P. 2002. "Developmental Criminology and Risk Focused Prevention." In *The Oxford Handbook of Criminology, 3rd Edition*, by M. Maguire, R. Morgan and R. Reiner (Eds.). Oxford: Oxford University Press.

Okunola, R.A., J.A. Akintayo and J. Amzat. 2009. "The Presentation and Representation of Crime in Nigerian media." In *Justice, International Perspectives on Crime and Justice*, edited by K. Jaishankar, Chapter: Fifteenn. Cambridge Scholars Publishing.

Rawlings, P. 1992. *Drunks, Whores, and Idle Apprentices: Criminal Biographies of the Eighteenth Century.* London: Routledge.

Reiner, R. 2000. "Romantic Realism: Policing and the Media." In *Core Issues in Policing*, by B. Loveday, and S. Savage (eds) F. Leishman, 52-66. London: Longman.

Surette, R. 2007. *Media, Crime, and Criminal Justice: Images, Realities, and Policies.* 3rd ed. Belmont, CA: Thomson Wadsworth.

Tumber, H. 1982. *Television and the Riots.* London: British Film Institute.

Young, J. 1971. *The Drug-Takers.* London: Paladin.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Disinformation Dynamics Unveiling the Impact of Echo Chambers in Shaping Online Public Opinion

Ştefania-Elena STOICA, Ph.D. Student*

*"Carol I" National Defence University, Bucharest, Romania
e-mail: stoica.stefania@myunap.net

Abstract

The proliferation of misinformation and the emergence of echo chambers in the online environment pose significant challenges to modern democracies, directly impacting public opinion and social behaviors. This study focuses on the analysis of a Facebook group centered around a prominent Romanian political figure, boasting 93,800 members and averaging ten daily posts. Using advanced machine learning and AI-based hate speech detection, the study uncovers systematic echo chamber construction and the amplification of misinformation. The findings emphasize the influence of online echo chambers on public opinion and underscore the need to maintain information integrity in the media landscape and communication. This research has important implications for scholars, policymakers, and media practitioners, indicating the critical need to address the challenges posed by misinformation and echo chambers in the online environment.

Keywords:
disinformation; echo chamber; cognitive biases; filter bubble; polarizing; fake-news manipulation; social networks.

Article info
Received: 31 January 2024; Revised: 18 February 2024; Accepted: 18 March 2024; Available online: 5 April 2024

Citation: Stoica, Ş.E. 2024. "Disinformation Dynamics. Unveiling the Impact of Echo Chambers in Shaping Online Public Opinion". *Bulletin of "Carol I" National Defence University*, 13(1): 138-156. https://doi.org/10.53477/2284-9378-24-09

Background

In the digital information era, echo chambers formed on online social networks represent an environment conducive to group polarization through selective interaction of users with different people or information sources promoting a particular type of content. This describes how beliefs are amplified or reinforced through communication and repetition within a closed system (Ciampaglia, Menczer and TheConversationUs 2018). The entrenchment of misinformation is facilitated by exploiting cognitive biases, creating a self-reinforcing loop that perpetuates and amplifies misinformation and impedes critical thinking and informed discourse (Donis 2021).

Although the concept of the echo chamber is not a new phenomenon, and they do not only occur online, Eli Pariser also coined the term to describe the less-than-transparent process of data filtering by websites that "create a unique universe of information" customized for each individual (Pariser 2011, 10). One of the greatest dangers these filters pose is self-intoxication or indoctrination of users with their ideas through high consumption of familiar information material and exclusion of data that contradict individuals' beliefs (Pariser 2011, 13).

Misinformation often occurs in the echo chamber because these isolated environments provide fertile ground for deliberately disseminating false or misleading information to an audience less likely to question or critically examine it due to prevailing cognitive biases (Ceron and de-Lima-Santos 2023). According to a study by the American Psychological Association, misinformation campaigns manipulate cognitive biases to shape social perceptions by presenting information that aligns with people's existing beliefs, confirming their misconceptions and misjudgments. When false initial information (anchoring biases) is introduced, it becomes a reference point from which individuals find it challenging to move away. Furthermore, in the echo chamber, groupthink exacerbates the lack of critical control, as the unanimous group opinion suppresses dissent and encourages the acceptance of misinformation as truth (Nisbet and Kamenchuk 2019). Another Harvard Kennedy School Misinformation Review study found that misinformation campaigns can exploit cognitive biases such as confirmation bias, availability bias, and the illusory truth effect to manipulate public opinion (Murphy et al. 2023). In other words, in the echo chamber created in online environments, the seeds of misinformation can quickly take root by taking advantage of users' misguided beliefs, thereby validating their less-than-factual ideas.

Research

This research aims to investigate the extent to which social media algorithms facilitate the formation of echo chambers and how manipulative actors exploit these platforms to spread disinformation. The central hypothesis of this study posits

that social media algorithms play a significant role in creating echo chambers, which are then exploited by individuals or states for financial or political gain. These actors employ sophisticated techniques to use the cognitive biases of social groups, leading to a cycle where individuals seek affirmation and group identity and become complicit in propagating disinformation. Over time, these echo chambers are hypothesized to become self-sustaining as group members increasingly engage in selective information-seeking behaviors reinforcing their pre-existing beliefs. By identifying the mechanisms through which echo chambers are formed and exploited, this study aims to provide insights into how social media platforms can be redesigned to mitigate the spread of disinformation (Barberá 2020).

Purpose

The rise of extremist ideologies and the intensifying polarization within societies pose significant risks to the core values of democratic institutions, making this research highly relevant (Travierso 2021). The entrenchment of polarized viewpoints has been linked to the escalation of social tensions and the erosion of the common ground necessary for democratic discourse in contemporary society. By understanding the relationship between algorithm-driven content curation, echo chambers, and disinformation, this study aims to develop more robust counterstrategies to safeguard public discourse against the divisive effects of such phenomena (Travierso 2021).

The insights gained from this research are vital for policymakers, social media platforms, and civil society to mitigate the threats posed by disinformation to democratic processes, social cohesion, and the sanctity of factual debate. This research advances academic discussion in an era where the digital domain increasingly mirrors and influences the physical world. It is a critical resource for those endeavoring to preserve and enhance democratic engagement in the face of growing digital challenges (Travierso 2021).

Literature Review

The present study builds upon existing research on the echo chamber, misinformation, and cognitive bias to explore the manipulation of public opinion online through algorithmic personalization on social platforms. This study investigates Filter Bubble Theory (Pariser 2011) and the Law of Group Polarization (Sunstein 1999), as well as insights from "Networked Propaganda" (Benkler, Farris and Roberts 2018), to provide new perspectives on this topic.

Algorithmic personalization on social platforms reinforces echo chambers by creating feedback loops that perpetuate users' existing beliefs. This effect is further intensified by the design of online platform algorithms that aim to keep users

engaged. Ally Daskalopoulos et al. (2021) noted in the Detroit Regional Chamber Report that online news consumers often interact with fake news and spread unverified information, contributing to political polarization and misinformation. As a result, the echo chamber on digital platforms has significant implications for public discourse and societal polarization. They limit exposure to diverse viewpoints and undermine democratic processes (Garrett 2009; Woolley and Howard 2016; Lewandowsky, Ecker and Cook 2017).
While Axel Bruns (2019) suggests that users can interact with a broader range of content than Filter Bubble Theory assumes, indicating the existence of ideologically diverse social networks, most research emphasizes the role of selective exposure and confirmation bias in stimulating societal division into distinct groups (Cinelli et al. 2021).

The present study sheds light on how misinformation becomes ingrained in the human mind. Diaz Ruiz and Nilsson (2023) have shown that disinformation circulates through identity- and belief-based grievances. Their research focuses on the echo chamber formed on YouTube around the idea that the Earth is flat, illustrating how rhetoric plays a crucial role in spreading misinformation. Manipulative techniques appealing to beliefs and values related to cultural identity and religion are not the only ways to trap people in echo chambers with misinformation. Another study of US participants found that emotions generated by fake news headlines play a defining role in their redistribution and virality. Generally, study participants were more likely to give credence to news headlines aligning with their beliefs. At the same time, they were more tempted to dismiss news stories that elicited strong negative emotions and were not in line with their political values (Christy et al., 2021).
In sum, misinformation is constructed to reach the audience's emotional side, not only the cognitive component, taking advantage of the most used communication channels nowadays - the online environment.

The article examines the emotions influenced by misinformation, as per the research by Dag Wollebæk et al. (2019). It was found that fear and anger are the most powerful emotions associated with online misinformation, especially in the political context. The study surveyed Norway in 2017 and discovered that people who experience fear are more open to debate, both for and against their beliefs. This leads to an increase in the search for information, especially from opposing viewpoints, thereby improving the quality and quantity of information gathered. Fear and anxiety also prompt individuals to question specific facts and events. On the other hand, anger makes people rely on heuristic cues and existing routines, reducing the desire to seek new information. This leads to risk-seeking behavior and can worsen biased reasoning in the political arena, resulting in echo chambers.

The paper explores under-researched areas in the study of the echo chamber and misinformation, particularly in the Romanian social context. It highlights the need for more comprehensive research on how rapidly evolving topics in social media discourse influence user engagement and potentially lead to shifting beliefs

or values. The possibility of users experiencing cognitive shifts, especially in the context of misinformation, is noted as an area for further investigation. This includes examining how users may navigate between emotional and rational responses and factual and misleading information. The extent of research on these dynamics in the current literature warrants further exploration

Additionally, there is a phenomenon known as repetitive posting and the "flying monkey" effect, which has yet to receive adequate attention. This term, used metaphorically, describes the role of group members in echo chambers who contribute to amplifying and reinforcing misinformation. As a result, false narratives can go viral and persist despite their lack of accuracy.
Finally, there needs to be more understanding of the tangible impact of such digital phenomena on real-world scenarios, particularly regarding their negative consequences on Romanian society.

Data Collection

The present study aims to analyze a Facebook group in Romania, highlighting the phenomenon of extremism and division observed to be growing both in the countries of the European Union and globally. Online platforms, especially social media, have become fertile grounds for the spread of political extremism and polarization. This phenomenon is amplified by algorithms that personalize content according to user preferences, thus favoring the formation of echo chambers. In these spaces, individuals are isolated in informational bubbles, exposed only to information that reinforces their initial beliefs. According to organizations such as OpenDemocracy, in countries such as Romania, there has been an alarming increase in extremism and political polarization, a phenomenon that is becoming more and more visible in online echo chambers. This increase in polarization underscores a sharp ideological divide, reflected in the digital divide.

A relevant example of extremist tendencies in Romania is represented by an individual who has become notorious for their extremist rhetoric and behavior, especially during the pandemic. This person has expressed opposition to the COVID-19 restrictions and has taken a vocal anti-vaccination stance. With a strong presence on social media platforms like Facebook, where they actively participate in various groups or pages, this case highlights the manifestation of online extremism and its significant impact on Romanian society. The initial study explored Facebook groups that promoted perspectives associated with this person, with posts subsequently extracted through direct observation. The selection process aimed to identify the most significant and prominent groups, ultimately focusing on a single group with 93,800 members and an average of ten posts per day (the most relevant and current in terms of posts associated with this individual). Manual data collection took place over the course of a year, from January to December 2023, allowing for a detailed analysis of the group's

discourse and providing a deep understanding of the current situation, especially in the context of the anticipated elections in Romania in 2024.

Analyses methods

The study combines advanced computational methods such as **Latent Dirichlet Allocation (LDA), Natural Language Processing (NLP), Named Entity Recognition (NER), and machine learning** with manual analytical techniques to provide a comprehensive analysis of the echo chamber (Akhtar et al. 2023). The study employs a multifaceted approach to analyze the dynamics within an echo chamber, leveraging various methods to dissect the intricacies of language use, the spread of disinformation, and engagement patterns. The study begins with **topic modeling,** categorizing, and identifying the main themes and subjects in various social media posts. LDA or similar algorithms often drive this method and are crucial for understanding the dominant topics and narratives within the echo chamber. The study also includes a **feature extraction component,** where the mentions of specific people, places, and institutions are listed and analyzed. This is typically achieved through NER, a subfield of NLP, which helps identify and classify critical elements in the text.
Moreover, the study delves into the analysis of **emotional and manipulative language**. This involves examining the text for language that is designed to evoke emotional responses or manipulate perceptions, a process that can be enhanced by sentiment analysis algorithms and NLP tools (He, Hu and Pei 2023). Additionally, the study analyzes the **posts' frequency, engagement rates, and timing.** This involves statistical analysis and data visualization techniques to understand activity patterns and user engagement within the echo chamber.

In this study, I have developed a matrix for analyzing disinformation, drawing on extensive literature reviews, studies on disinformation, and my personal experience with multiple disinformation texts. It is important to note that while this matrix offers a structured framework for comprehensive and systematic examination, it could be better and remains a subject of ongoing research and optimization. The approach minimizes subjective interpretations by relying on predefined criteria, enhancing objectivity.

This structured approach is crucial for maintaining objectivity, as it relies on predefined criteria for evaluation, minimizing subjective interpretations. The consistency afforded by a standardized matrix is invaluable, as it allows for the replication of studies and comparison of findings, fundamental aspects of scholarly research. Moreover, disinformation is inherently multifaceted, and a matrix facilitates a multidimensional analysis, enabling researchers to delve into various elements such as language use, source credibility, and logical consistency. This comprehensive approach yields a deeper understanding of the complexities of disinformation.

Disinformation Criteria	Criteria Explanation
Emotionally and Sensationalist Language	Uses emotionally laden or sensational language to provoke emotional responses
Misrepresentation of Facts or Context	Presents facts inaccurately or out of context
Appeal to Fear and Urgency	It plays on fears and creates a sense of urgency.
Lack of Credible Evidence	Absence of backing from credible sources
Questionable Source Credibility	Relies on sources with dubious credibility
Factual Inconsistencies	Contradictions within the content or with facts
Contradiction of Established Understanding	Significantly deviates from widely accepted knowledge without substantial evidence.
Polarizing Us-vs-Them Rhetoric	Uses divisive language to create a sense of ingroup and outgroup
Overgeneralization and Stereotyping	Employs generalizations and stereotypes
Selective or Omitted Information	Leaves out critical information or selectively presents facts
Manipulation of Quotes or Sources	Alters quotes or sources to mislead
Lack of Transparency in Sourcing	Does not disclose sources, obscuring the origin of information
Inconsistent Logic or Argumentation	Arguments based on flawed reasoning or inconsistent logic
Use of Unverified or False Visuals	Relies on visuals that are unverified or proven false
Hyperbolic or Provocative Headlines	Uses headlines that are exaggerated or provocative
Opinion Presented as Fact	Presents opinions as if they were information
Anachronism	Refers to events or contexts inaccurately to mislead
Logical Fallacies	Employs reasoning that contains logical errors

Figure 1 **Disinformation matrix**

Findings

In the next phase, I conducted an in-depth analysis of the data extracted. This dataset included parameters like posting dates, message contents, user profiles, network contexts, likes, interaction rates, and unique identifiers. This comprehensive data collection enabled the identification of various narratives, hate speech instances, emotive language use, negative sentiments, and widespread amplification techniques within the echo chamber's discourse. However, while these parameters provide insights into the group's structure and dynamics, they might not directly reveal the nature of the narratives. To fully grasp the narratives, a qualitative examination of the message content is essential, looking at the themes, ideologies, and rhetorical strategies used in the posts.

a) ***Creating a Sense of Community and Belonging*** – I observed that using inclusive language was a powerful tool for fostering a sense of community and belonging. Phrases like "we," "together," and "us," along with hashtags such as #solidaritate (solidarity), #Împreună (together), #Comunitate (community), emphasize a shared identity among group members. Additionally, hashtags like #TradițiaNeDefinește (tradition defines us), #SchimbareaDeCareAvemNevoie (the change we need), #ErouAlNostru (our hero), #unire (unity), #RespectPentruCulturaNoastră (respect for our culture) further reinforce this sense of belonging and shared values. This language not only reinforces the feeling of being part of a distinct and cohesive group, appealing to those seeking

a sense of belonging but also plays a significant role in shaping social identity. Using such 'us/we' narratives taps into key psychological aspects like social identity, ingroup favoritism, and outgroup derogation. Social identity theory explains how an individual's self-concept is influenced by their membership in a social group. Ingroup favoritism, the preference for one's group, and outgroup derogation, the negative perception of other groups, are prevalent in such settings. In certain situations, spreading false information within an echo chamber can have severe consequences, such as exacerbating group polarization and reinforcing negative perceptions of outside groups. According to Sunstein (1999), social media platforms can often act as echo chambers, promoting a sense of group identity and encouraging users to seek information that aligns with their beliefs. This can lead to a lack of critical thinking and dismissing opposing viewpoints, ultimately exacerbating negative attitudes toward outside groups. This environment can also facilitate the spread of fake news and disinformation without being challenged.

b) Growth and repetitive messages – In the context of disinformation and the rapid expansion of echo chambers, the group I studied represents a relevant example. Established on October 25, 2021, it has consistently grown. In just the last week of the study period, the group expanded by 174 members, averaging a daily increase of around 130 members. This escalating growth rate indicates the group's burgeoning influence and reach. Significantly, within a single year, the group's posts elicited over 705,826 reactions (likes), reflecting a high level of engagement among its members. This pattern of rapid growth and increased engagement is characteristic of echo chambers, where repetitive messaging and targeted content can quickly attract and retain a growing audience, amplifying disinformation's spread and impact. Public activities, community outreach, and direct engagement in the physical world can also contribute to the group's online growth. The group can attract individuals who carry their interest and involvement into the online space by establishing a presence in the offline world through events, demonstrations, or local campaigns. This synergy between offline actions and online engagement helps expand the group's reach further and solidify its influence in the digital and the real worlds.

c) Reinforcing a Common Identity – Echo chambers often use language that strengthens the perception of a unified group identity, shifting focus from individuals to the collective. This common identity is built around shared beliefs, opinions, or ideologies, serving as a powerful unifying force within the group. For instance, the opinion leader talks about the group he represents and online supporters in a post like this: "our #patriotic spirit firmly stand in #war against the import attempts of foreign #customs that have no connection with our #national identity, (…)" clearly demonstrates this dynamic.

In this post, the assertion of national identity is evident, as it frames the situation as a "war" against foreign customs, emphasizing the importance of maintaining a

distinct Romanian identity. Although not explicitly stated in this specific portion, the overall message of the post advocates for celebrating Romanian traditions and rejecting foreign ones, reinforcing the idea that national customs are integral to the group's identity. The post positions the broadcaster as defender of national identity against foreign customs, creating a narrative of protection and resistance that strengthens group cohesion and unity. Using terms like "#war" and the emphasis on "our patriotic spirit" serves as a call to action for supporters to rally around the cause of preserving national identity, further solidifying the group's shared identity.

d) Reducing Receptivity to Opposing Viewpoints – In another post, the public figure states about another personality that she "*îi îndeamnă pe tineri să nu mai plece peste hotare: ‚Vă încurajez să vă proiectați un viitor în România'*" (Translation: „*urges young people not to go abroad: ‚I encourage you to design a future in Romania*'"), the comments of the group members predominantly indicate strong disapproval and cynicism compared to the encouragement of young people by another opinion former compared to the sympathetic one to stay in Romania. Many commenters view this as a disingenuous or manipulative gesture. This uniformity in sentiment and the lack of visible counterarguments or diverse perspectives suggest an echo chamber effect, where a single viewpoint predominates and dissenting opinions are either absent or dismissed. Some of the messages are:

- *Ristea D*: "Da stați în țara dragi tineri că au nevoie de carne de tun."* - *Translation: "Yes, stay in the country, dear young people, because they need cannon fodder."* This comment expresses cynicism towards young people staying in Romania, suggesting they are needed only as expendable resources, implying a lack of genuine concern for their well-being.
- *Monica P*: "Mars tradatorul! Vrei carne de tun?!"* - *Translation: "Go away, traitor! Do you want cannon fodder?!"* Echoing a similar sentiment, with this comment, the author labels the unloved public figure as a "traitor" and accuses him of wanting young people to be "cannon fodder", indicating a solid mistrust and negative perception.
- *Rodica I*: "Să îi trimiți în război nemernicule... Pupincuriști ai globaliștilor."* - *Translation: "Send them to war, you scoundrel... Bootlickers of the globalists."* This comment further intensifies the negative sentiment, accusing another public figure of sending young people to war and aligning himself with the globalists, reflecting deep-rooted mistrust and hostility.

When group identity becomes intertwined with specific beliefs or ideologies, any challenge to these beliefs feels like a personal attack on the group and, by extension, on the individual. This can result in a defensive stance against external information, further entrenching members in their existing beliefs. The strong sense of identity and belonging fostered by inclusive language leads to decreased openness to opposing viewpoints.

e) Frequent use of negative language – Utilizing the disinformation matrix analysis tool, I found that a significant portion of the language used in the echo chamber,

47,25% of the message, is harmful or manipulative. This high rate of negativity is crucial in echo chambers for several reasons. Firstly, it reinforces shared beliefs among group members, fostering a strong sense of unity against perceived outgroups or opposing ideas. This is often achieved by establishing a clear 'us versus them' dynamic. Secondly, negative language evokes stronger emotional reactions than neutral or positive language, leading to increased engagement within the echo chamber. This heightened emotional response can further entrench members' beliefs. Lastly, negativity in echo chambers contributes to the polarization and radicalization of opinions, as it increases members' resistance to outside information or alternative viewpoints. The significant presence of negative words, as revealed by our analysis, underscores the role of emotional and divisive language in shaping the dynamics within echo chambers.

f) Spontaneous Communication and Strong Emotion – In the analysis of the echo chamber's communication patterns, I encountered a notable use of manipulative language, with 2,076 instances identified across various posts. This manipulative language included words like: *'șocant (shocking),' 'brutală (brutal),' 'limitate (limited),' 'cenzură (censorship),' 'șocat (shocked),' 'devastatoare (devastating),' 'incendiară (incendiary),' 'limitărilor impuse (imposed limitations),' 'un eveniment pe care nu-l puteți rata (an event you can't miss),' 'mintit (lied),' 'manipulare totala (total manipulation),' 'arma (weapon),' 'profile false (false profiles),' 'stiri false (false news),' 'insultele (insults),' 'să nu mai îndrăzniți vreodată (never dare again),' 'haos (chaos),' 'tragedie (tragedy),' 'tristă (sad),' 'devastatoare (devastating),' 'suferă (suffer),' 'demisia (resignation),' 'esențială (essential),' 'vânzătorii (sellers),' 'gâtul nostru (our throat),' 'acuză (accuse)' and 'ăștia (these)'*. These manipulative words and expressions, filled with emotional triggers, are frequently used within the group to shape opinions and emotions. A closer examination of 825 posts reveals that, on average, each contained approximately 5.78 manipulative words, demonstrating the group's reliance on persuasive language to shape opinions and emotions. The identified manipulative words, as seen in phrases like 'DEMITEREA LUI ARAFAT, ARESTAREA SI CONDAMNAREA LUI PE VIATA PT GENOCID' (Arafat's resignation, arrest, and life sentence for genocide), 'PENTRU A NU SPUNE ADEVĂRUL, MI-AU INTERZIS SA VORBESC' (To prevent me from telling the truth, they prohibited me from speaking), and 'MANIPULAREA DNA, FILMARI PLATITE LA COMANDA SI SCOASE DIN CONTEXT' (DNA manipulation, paid-for videos on demand taken out of context), are designed to evoke strong emotional reactions and shape opinions. This underscores the use of emotionally charged language to influence and manipulate readers or the audience. Additionally, communication within these hyper partisan echo chambers is characterized by spontaneity and a high degree of emotional intensity. This is exemplified by the frequent use of swear words and exclamation marks, which act as markers of strong emotions and heightened arousal states. In such a polarized environment, these expressions of emotion are often indicative of either strong agreement or vehement disagreement with the shared beliefs and

biases prevalent within the group.

Additionally, the presence of swear words in the group's discourse indicates a less formal yet more impassioned and, at times, aggressive communication style (Wollebæk et al. 2019). In hyperpartisan settings, such usage of swear words often serves dual purposes: expressing intense emotions like anger or disdain, especially towards opposing views or groups, and reinforcing ingroup unity against perceived outgroups. This linguistic feature contributes to the echo chamber's charged and often contentious atmosphere. Similarly, using exclamation marks can amplify the emotional intensity of a message. It can indicate excitement, surprise, anger, or urgency. In hyperpartisan echo chambers, exclamation marks can enhance the emotional resonance of messages, making them more impactful and memorable.

g) ***A dynamic and strategic shifting of topics in the same echo chamber*** (see Figure 1) – This shifting serves multiple purposes: firstly, it hooks subjects from diverse backgrounds and with varying interests, and secondly, it plays a crucial role in altering perceptions. The analyzed echo chamber can effectively manipulate the perceptions of its members by rapidly transitioning from one topic to another, thereby shifting their emotional and cognitive states. This tactic is insidious as it does not allow the brain enough time to adjust from processing emotional content to rational thought.

The discussions cover a wide range of topics that cater to the diverse interests and beliefs of the audience. Categories such as Social Issues, Romanian Culture and Identity, Media and Communication, Politics, Nationalism, Religion, and Lifestyle serve as practical tools to keep members engaged and active within the echo chamber. However, it is essential to note the manipulative technique, where a neutral fact is validated before subtly transitioning into disinformation and hate speech. This seamless shift makes it difficult for members to discern the change in content integrity, resulting in an emotional response to manipulated or false data instead of a rational engagement with genuine information.

This tactic of topic shifting and blending information with disinformation keeps the members engaged and effectively alters their perceptions. Studies, such as one conducted by the Reuters Institute for the Study of Journalism, have shown that the constant oscillation between different topics and between emotional and rational states undermines the ability of individuals to critically evaluate the information being presented, leading to a gradual acceptance of disinformation as truth (Brennen 2019). This phenomenon highlights echo chambers' sophisticated strategies to manipulate opinions and beliefs. Another study conducted by the Harvard Kennedy School found that most regular internet users globally worry about misinformation, with young and low-income groups expressing the highest levels of concern (Knuutila, Neudert and Howard 2022).

The constant oscillation between different topics and between emotional and rational states undermines the ability of individuals to critically evaluate the information being presented, leading to a gradual acceptance of disinformation

as truth. This phenomenon highlights echo chambers' sophisticated strategies to manipulate opinions and beliefs.

Categories	Hashtags categorization – NLP modeling
Social Issues	#CopiiiSuntViitorul (Children are the future), #oameni (people), #parinti (parents), #Comunitate (community), #gradinita (kindergarten), #scoala (school), #sociale (social), #Împreună (together), #solidaritate (solidarity), #binele (goodness), #respect (respect), #drepturile (rights), #justitie (justice), #doaradevarul (only the truth), #drepturi (freedoms), #amintire (memory), #înțelegere (understanding), #recunoștință (gratitude), #adevar (truth), #toleranță (tolerance), #hotărâți (determined), #speciale (special), #TraficulDeDroguri (drug trafficking), #ConfidențialitateFinanciară (financial privacy), #LibertateEconomică (economic freedom), #SchimbareaDeCareAvemNevoie (the change we need), #pace (peace), #incompetenta (incompetence), #nurazboi (no war).
Romanian Culture and Identity	#decembrie (December), #TradițiaNeDefinește (Tradition defines us), #Datini (Customs), #istoric (historical), #OrașulCuInimăVeche (The city with an old heart), #tebea.
Media and Communication	#DezvaluiriCuImpact (Impactful revelations), #tiktok, #televiziuni (television), #socialmedia, #stiri (news), #facebook, #televiziune (television), #tipografie (printing), #dezvaluiri (revelations), #ziare (newspapers), #informatie (information), #actual (current), #live, #instagram, #vocea (voice), #dezbatare (debate), #Laudățium (praises).
Politics	#SchimbareaDeCareAvemNevoie (The change we need), #pace (peace), #incompetenta (incompetence), #nurazboi (no war), #sieusuntvoluntar (I am a volunteer), #DemisieArafat (Arafat resignation), #raedarafata (Arafat's resignation), #ResponsabilitateSauDemisie (Responsibility or Resignation), #uk (UK), #canada (Canada), #germania (Germany).
Nationalism	#Conștiență (consciousness), #bucovina (Bucovina), #RomâniaReală (Real Romania), #patriotism (patriotism), #tara (country), #națiune (nation), #patriot (patriot), #bunderomânia, #ErouAlNostru (Our hero), #roman (Romanian), #române (Romanian), #demnitate (dignity), #unirea (union), #istorie (history), #distrugă (destroy), #romania (Romania), #unire (union), #independent (independent).
Religion	#mihail (Michael), #sfint (saint), #ÎngeriiPăzitori (Guardian Angels), #cer (heaven).
Lifestyle	#iubire (love), #poet (poet), #carte (book), #simpozion (symposium), #viata (life), #cantece (songs), #dramaturg (playwright), #viitorul (future), #MoștenireLiterară (literary heritage), #RespectPentruCulturaNoastră (respect for our culture).

Figure 2 **Rapid shifting topics among multiple hate and conspiracy messages**

h) Utilizes a broad spectrum of negative themes to engage and influence its members – the wide range of categories used in the echo chamber's discourse reflects a sophisticated strategy to engage members across various emotional and intellectual levels. This strategy strengthens the echo chamber's internal cohesion and impacts broader societal dynamics, contributing to polarization, misinformation, and the erosion of healthy public discourse.

The prevalence of categories like *Negative Connotations and Slander*, *Discrimination and Bigotry*, and *Oppression and Coercion* indicates a deliberate strategy to invoke strong emotional reactions, often negative, to solidify group identity and beliefs. The presence of categories like *Solutions and Innovations*, *Support and Solidarity*, and *Hope and Aspiration* indicates that the echo chamber also uses positive and constructive themes. This dual approach of combining negative and positive narratives maintains engagement and bolsters the group's cohesive narrative. Moreover, categories such as *Legal and Ethical Issues*, *Social*

and Cultural Dynamics, and *Environmental and Ecological Awareness* show that the echo chamber does not shy away from complex and multifaceted issues. However, discussing these issues often needs more nuance and is framed within the echo chamber's ideological perspective.

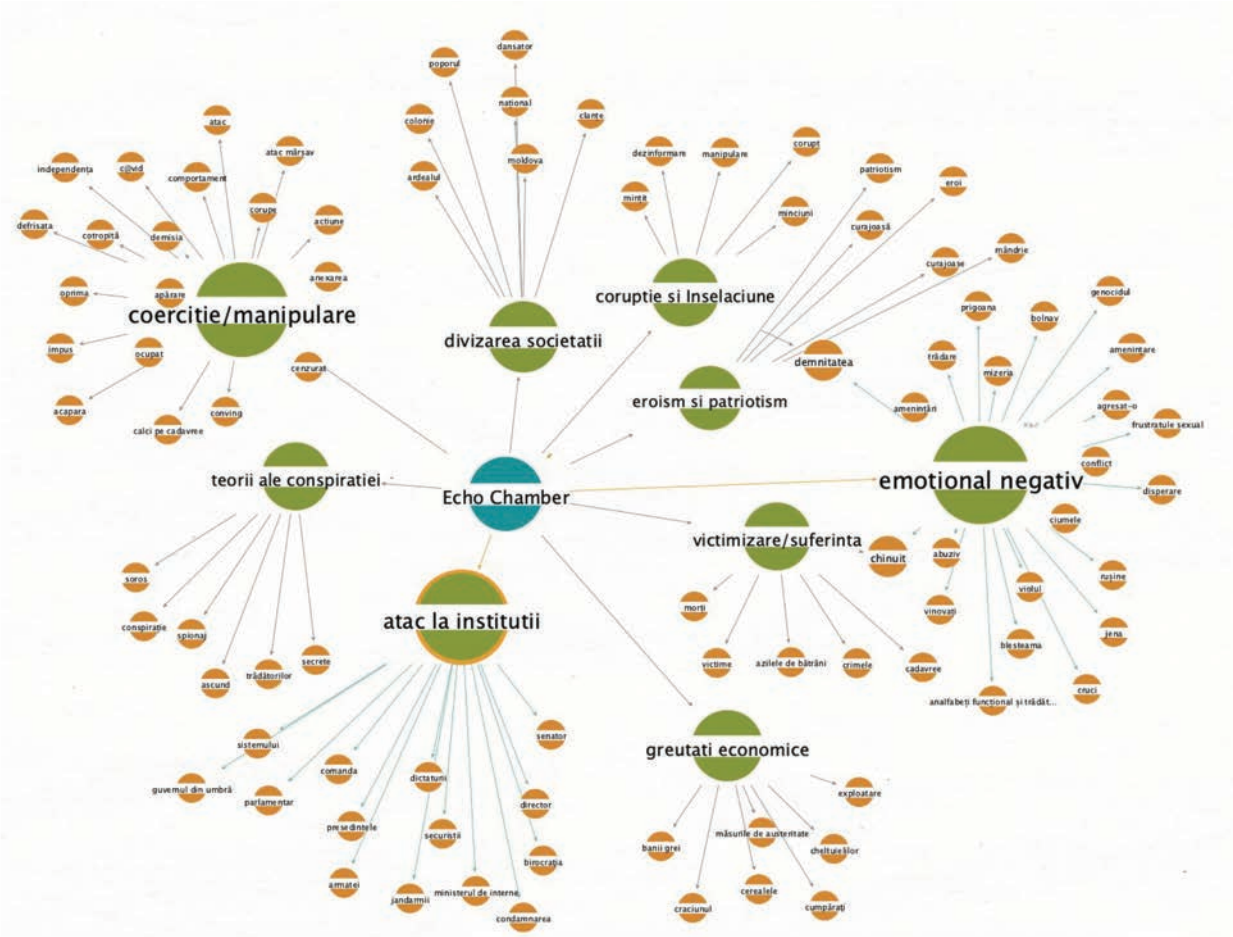


Figure 3 Topic modeling and clusterization on hateful, emotional, or negative content keywords found in the echo chamber

The keywords and topics in the echo chamber (see Figure 3) message suggest a complex and multifaceted approach to spreading disinformation and manipulating public opinion. Each set of keywords aligns with different aspects of disinformation strategies, aiming to influence perceptions, deepen societal divisions, undermine trust in institutions, and provoke emotional responses:

- **Coercion/Manipulation**: Keywords like "conving" (convincing), "calci pe cadavre" (stepping on corpses), "a acapara" (hoarding), "ocupa" (occupy), "impus" (impose), "oprima" (oppress), "defrișată" (deforestation), "cotropită" (invaded), "demisia" (resignation), "independența" (independence), "COVID" (COVID), "comportament" (behavior), "corupe" (corrupt), "atac" (attack), "atac mârșav" (malicious attack), "acțiune" (action), "anexare" (annexation), "cenzurat" (censored) suggest a narrative aimed at portraying forceful or deceitful actions,

possibly attributing them to specific groups or individuals to discredit them or justify aggressive or unethical behaviors.

- **Dividing Society**: Keywords such as "Ardealul" (Transylvania), "colonie" (colony), "poporul" (people), "trădător" (traitor), "Moldova" (Moldova) are likely used to exacerbate regional, ethnic, or national tensions, suggesting an effort to fragment societal unity by highlighting or fabricating divisions and fostering resentment among different communities.
- **Corruption and Deception**: Words like "mințit" (lied), "dezinformare" (disinformation), "manipulare" (manipulation), "corupție minciuni" (corruption lies) are typical in narratives aimed at undermining trust in individuals, organizations, or processes by accusing them of dishonest or fraudulent behavior, often without evidence.
- **Conspiracy Theories**: The mention of "conspirație" (conspiracy), "secrete" (secrets), "trădătorilor" (traitors), "ascund" (hide), "spionaj" (espionage), "Soros" (Soros) indicates the promotion of unfounded theories that claim shadowy forces are orchestrating events behind the scenes. These narratives often rely on prejudice, paranoia, or speculative connections to explain complex situations through simplified, misleading lenses.
- **Attacks on Institutions**: Keywords targeting "sistemului" (the system), "guvernul din umbră" (shadow government), "parlament" (parliament), "comandă" (command), "președintele" (president), "armatei" (army), "dictaturii" (dictatorship), "jandarmii" (police), "securiștii" (secret police), "ministrul de interne" (interior minister), "condamnare" (conviction), "birocrație" (bureaucracy), "director" (director), "senator" (senator) suggest an effort to erode confidence in governmental and societal institutions by portraying them as corrupt, oppressive, or illegitimate.
- **Economic Hardships**: Terms like "banii grei" (big money), "Crăciunul" (Christmas), "cerealele" (grains), "măsurile de austeritate" (austerity measures), "cumpărat" (bought), "cheltuielilor" (expenses), "exploatare" (exploitation) reflect concerns about economic conditions and policies, possibly twisting facts or context to incite anger or despair about the economic situation, attributing blame to specific entities or policies without a balanced perspective.
- **Victimization/Suffering**: With keywords such as "morți" (deaths), "victime" (victims), "azilele de bătrâni" (nursing homes), "crimele" (crimes), "cadavre" (corpses) the narrative focuses on highlighting real or imagined instances of suffering to elicit empathy, anger, or fear, often to sway opinion or justify radical viewpoints or actions.
- **Negative Emotional Appeals**: Phrases like "chinuit" (tortured), "abuziv" (abusive), "vinovați" (guilty), "analfabeți funcționali și trădători" (functional illiterates and traitors), "blestem" (curse), "viol" (rape), "cruci" (crosses), "rușine" (shame), "ciumele" (plagues), "disperare" (desperation), "conflict" (conflict), "frustrat sexual" (sexual frustration), "agresor" (aggressor), "amenințare" (threat), "genocid" (genocide), "bolnav" (sick), "mizerie" (filth), "prigoană" (persecution), "trădare" (betrayal) are designed to evoke strong negative emotions, aiming to

manipulate the audience's feelings to provoke outrage, fear, or hatred, bypassing rational analysis.

The goal is often to polarize society, distract from substantive issues, or consolidate power by creating an environment where rational discourse is overshadowed by fear, suspicion, and anger.

Discussion

Examining this echo chamber on Facebook yields valuable insights when contextualized within the cognitive biases and disinformation framework, thereby expanding our understanding of the phenomenon at hand. My observations were meticulously conducted by analyzing social categories and topic clustering inside the Facebook group. The diverse array of thematic orientations and manipulative tactics prevalent in the echo chamber is congruent with and leverages diverse cognitive biases. Biases like confirmation bias, where individuals favor information that confirms their pre-existing beliefs, are particularly evident. The echo chamber's targeted content reinforces these biases, continually exposing members to viewpoints that align with their own, thereby perpetuating a cycle of reinforced beliefs and misconceptions.

Echo chambers act as effective incubators of disinformation by creating an environment where only specific perspectives are presented and opposing views are omitted or discredited. These chambers create a fertile ground for disinformation to flourish. The emotional and manipulative language used further exacerbates this issue, as it is designed to evoke strong reactions and discourage critical thinking, making members more susceptible to accepting false information as truth.

The use of identity-based themes like nationalism and patriotism, coupled with negative portrayals of outgroups, contributes to group polarization. This polarization is compounded by groupthink, a phenomenon where the desire for harmony or conformity within the group results in irrational or dysfunctional decision-making. In such an environment, questioning or challenging the group's beliefs becomes increasingly complex, leading to a more homogeneous and extreme set of views.

Implications

The findings from our study on one possible echo chamber on the social Facebook platform have profound implications for understanding the nature of echo chambers more broadly and devising strategies to combat disinformation. The mechanisms identified – such as the use of emotionally charged and manipulative language, the formation of a strong sense of community, and the presence of spontaneous, emotionally intense communication – are not unique to the groups we studied. The

dynamics we observed reflect a broader, worldwide pattern where echo chambers, marked by manipulative techniques, are emerging across diverse contexts, highlighting the need for a global approach to address these challenges. These environments are particularly conducive to extremism, providing a platform where extreme ideas are amplified and normalized, potentially leading to the radicalization of individuals or masses, especially within vulnerable populations.

Moreover, the influence of echo chambers extends to democratic processes and societal stability, polarizing public opinion, eroding shared truths, and undermining healthy democratic discourse. This can result in real-world destabilization, driven by actions based on distorted perceptions and misinformation. Addressing these challenges requires understanding the mechanics of echo chambers to develop effective strategies for combating disinformation. This involves raising awareness, promoting media literacy, encouraging exposure to diverse viewpoints, and addressing the structural aspects of social media that contribute to forming these chambers.
Additionally, the implications for policymakers and regulators are significant. They need to be cognizant of the effects of echo chambers on social cohesion and democratic integrity, possibly requiring a reassessment of social media's role in public discourse, implementing regulations to curb disinformation, and supporting initiatives that foster critical thinking and fact-checking.

Limitations

It is essential to acknowledge some of the study's limitations by noting several vital constraints that may impact the generalizability and scope of the findings. First and foremost, the study covers only a tiny percentage of the potential echo chambers, focusing specifically on specific social segments within Romania. Given the unique cultural and historical context of Romania, the strategies adopted by the owners of these echo chambers and the nature of the discourse within them may not be fully representative of similar phenomena in other countries or cultures (Arguedas et al. 2022).

Furthermore, cognitive biases, which play a significant role in forming and sustaining echo chambers, can vary considerably from one population to another. These biases are influenced by a multitude of factors, including cultural background, social context, and historic periods, which means that the cognitive patterns observed in the study may not be universally applicable. Additionally, while the research provides valuable insights into the workings of echo chambers and their impact, it needs to be more comprehensive. Several external factors that might influence the dynamics within echo chambers, such as political restrictions, economic conditions, or external events like wars in neighboring countries, were not within the scope of the analysis. These factors can have a significant bearing on public opinion and the spread of disinformation but were not accounted for in the study.

In summary, while the study contributes essential findings to understanding echo chambers in a specific social and cultural context, these limitations should be considered when extrapolating the results to other contexts or broader populations. Future research could address these limitations by incorporating a more comprehensive range of echo chambers across different cultural and social contexts and considering various influencing factors.

Conclusions

The findings from this study on a potential echo chamber within the Facebook platform offer profound insights into the nature of such environments and suggest strategies to counter disinformation. This research indicates that the mechanisms identified, including emotionally charged language, cultivating a strong community sense, and emotionally intense communication, likely reflect a broader global trend in echo chambers.

These echo chambers provide fertile ground for extremism, amplifying extreme ideas and potentially leading to the radicalization of individuals or groups, particularly within vulnerable populations. Furthermore, they can significantly impact democratic processes and societal stability by polarizing public opinion and eroding shared truths, potentially leading to real-world destabilization fueled by misinformation. Addressing these issues necessitates understanding echo chamber mechanics and a comprehensive approach involving media literacy, exposure to diverse viewpoints, and structural changes in social media. Policymakers and regulators also play a crucial role and should be informed of these implications to develop effective policies and regulations.

References

Akhtar, P., A.M. Ghouri, H.U.R. Khan, M.A.U. Haq, U. Awan, N. Zahoor, Z. Khan and A. Ashraf. 2023. "Detecting fake news and disinformation using artificial intelligence and machine learning to avoid supply chain disruptions." *Annals of Operations Research* 327: 633-657. https://doi.org/10.1007/s10479-022-05015-5.

Arguedas, A.R., C.T. Robertson, R. Fletcher and R.K. Nielsen. 2022. "Echo chambers, filter bubbles, and polarisation: a literature review." *Reuters Institute.* doi:10.60625/risj-etxj-7k60.

Barberá, P. 2020. „Social Media, Echo Chambers and Political Polarization." In *Social media and democracy. The State of the Field, Prospects for Reform*, editors Nathaniel Persily and Joshua A. Tucker, 34-55. https://www.cambridge.org/core/books/social-media-and-democracy/social-media-echo-chambers-and-political-polarization/333A5B4DE1B67EFF7876261118CCFE19.

Benkler, Y., R. Farris and H. Roberts. 2018. *Network Propaganda.* Oxford University Press. https://doi.org/10.1093/oso/9780190923624.001.0001.

Braddock, K. 2022. "Vaccinating against hate: Using attitudinal inoculation to confer resistance to persuasion by extremist propaganda." *Terrorism and Political Violence* 34 (2): 240-262. https://doi.org/10.1080/09546553.2019.1693370.

Brennen, J.S. 2019. "Misinformation: The evidence on its scope, how we encounter it, and our perceptions of it." *Reuters Institute for the Study of Journalism.* https://reutersinstitute.politics.ox.ac.uk/news/misinformation-evidence-its-scope-how-we-encounter-it-and-our-perceptions-it.

Bruns, A. 2019. "Filter bubble." *Internet Policy Review* 8 (4). https://doi.org/10.14763/2019.4.1426.

Ceron, Wilson and Mathias-Felipe de-Lima-Santos. 2023. "Disinformation Echo Chambers on Facebook." In *Fighting Fake Facts*, 61-90. MDPI Books. https://doi.org/10.3390/books978-3-0365-1347-8-4.

Ciampaglia, G.L., F. Menczer and TheConversationUs. 2018. "Biases Make People Vulnerable to Misinformation Spread by Social Media." *Scientific American.* https://www.scientificamerican.com/article/biases-make-people-vulnerable-to-misinformation-spread-by-social-media/.

Cinelli, Matteo, Gianmarco De Francisci Morales, Alessandro Galeazzi and Michele Starnini. 2021. "The echo chamber effect on social media." *Proceedings of the National Academy of Sciences* 118 (9): e2023301118. https://doi.org/10.1073/pnas.2023301118.

Daskalopoulos, A., N. Hernandez, F. Jason, H. Jenvey, D. Gustafson, R. Mosley, C. Rodriguez, N. Schoonover and S. Townsend. 2021. "Thinking outside the bubble: Addressing polarization and disinformation on social media." *CSJS Journalism Bootcamp.* https://journalism.csis.org/thinking-outside-the-bubble-addressing-polarization-and-disinformation-on-social-media/.

Donis, L. 2021. „How to filter bubbles and echo chambers reinforce negative beliefs and spread misinformation through social media." *Debating Communities and Networks XII.* https://networkconference.netstudies.org/2021/2021/04/25/how-filter-bubbles-and-echo-chambers-reinforce-negative-beliefs-and-spread-misinformation-through-social-media/.

Garrett, R.K. 2009. "Echo chambers online?: Politically motivated selective exposure among Internet news users." *Journal of Computer-Mediated Communication* 14 (2): 265-285. https://doi.org/10.1111/j.1083-6101.2009.01440.x.

He, L., S. Hu and A. Pei. 2023. "Debunking Disinformation: Revolutionizing Truth with NLP in Fake News Detection." https://arxiv.org/abs/2308.16328.

Horner, G.C., D. Galletta, J. Crawford and A. Shirsat. 2021. "Emotions: The Unexplored Fuel of Fake News on Social Media." *Journal of Management Information Systems* 38 (4): 1039-1066. doi:10.1080/07421222.2021.1990610.

Knuutila, A., L.M. Neudert and P.N. Howard. 2022. "Who is afraid of fake news? Modeling risk perceptions of misinformation in 142 countries." *Misinformation Review, Harvard Kennedy School.* https://misinforeview.hks.harvard.edu/article/who-is-afraid-of-fake-news-modeling-risk-perceptions-of-misinformation-in-142-countries/.

Lewandowsky, S., U.K.H. Ecker and J. Cook. 2017. "Beyond Misinformation: Understanding and Coping with the "Post-Truth" Era." *Journal of Applied Research in Memory and Cognition* 6 (4): 353-369. https://doi.org/10.1016/j.jarmac.2017.07.008.

Murphy, G., C. De Saint Laurent, M. Reynolds, O. Aftab, K. Hegarty, Y. Sun and C.M. Greene. 2023. "What do we study when we study misinformation? A scoping review of experimental research (2016-2022)." *Harvard Kennedy School Misinformation Review.* https://misinforeview.hks.harvard.edu/article/what-do-we-study-when-we-study-misinformation-a-scoping-review-of-experimental-research-2016-2022/.

Nikolov, D., D.F.M. Oliveira, A A. Flammini and F. Menczer. 2015. "Measuring online social bubbles." *PeerJ Computer Science.* https://doi.org/10.7717/peerj-cs.38.

Nisbet, E.C. and O. Kamenchuk. 2019. "The Psychology of State-Sponsored Disinformation Campaigns and Implications for Public Diplomacy." *The Hague Journal of Diplomacy* 14 (2): 65-82. https://doi.org/10.1163/1871191X-11411019.

O'Shaughnessy, N. 2020. „From disinformation to fake news: forwards into the past." În *The SAGE Handbook of Propaganda*, pp. 55-70. SAGE Publications Ltd. https://doi.org/10.4135/9781526477170.

Pariser, E. 2011. *The Filter Bubble: What the Internet Is Hiding from You.* https://dl.acm.org/doi/10.5555/2029079.

Ruiz, C. Diaz and T. Nilsson. 2023. "Disinformation and Echo Chambers: How Disinformation Circulates on Social Media Through Identity-Driven Controversies." *Journal of Public Policy & Marketing* 42 (1): 18-35. https://doi.org/10.1177/074391562.

Sunstein, C.R. 1999. "The Law of Group Polarization." (John M. Olin Program in L. & Econ. Working Paper No. 91). https://dash.harvard.edu/bitstream/handle/1/13030952/The%20Law%20of%20Group%20Polarization.pdf.

Travierso, M. 2021. "Measuring magnetism: how social media creates echo chambers." *Nature Italy.* https://www.nature.com/articles/d43978-021-00019-4.

Vosoughi, S. and S. Arala. 2018. "The spread of true and false news online." *Science* 359 (6380): 1146-1151. https://doi.org/10.1126/science.aap9559.

Walter, S., M. Brüggemann and S. Engesser. 2018. "Echo Chambers of Denial: Explaining User Comments on Climate Change." *Environmental Communication* 12 (2): 204-217. https://doi.org/10.1080/17524032.2017.1394893.

Wollebæk, D., R. Karlsen, K. Steen-Johnsen and B. Enjolras. 2019. "Anger, Fear, and Echo Chambers: The Emotional Basis for Online Behavior." *Social Media + Society* 5 (2). https://doi.org/10.1177/2056305119829859.

Woolley, S.C. and P. Howard. 2016. "Automation, algorithms, and politics/ Political communication, computational propaganda, and autonomous agents – Introduction." *International Journal of Communication* (10). https://ijoc.org/index.php/ijoc/article/view/6298/1809.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY
https://buletinul.unap.ro/index.php/en/

Implications of the jihadist terrorism in cyberspace

Bianca Brandea, Ph.D. Candidate*

* University of Bucharest, Faculty of Foreign Languages and Literatures
"Languages and Cultural Identities" Doctoral School, Romania
e-mail: bianca.brandea@drd.unibuc.ro

Abstract

The terrorist attack on the 11th of September, 2001, marked the change in the West's perception of the Middle East and vice versa. Followed by the US military presence in the Middle East, this event contributed to the development of the means of terrorist actions around the world and the popularization of jihad. The hostile attitude of the West thus succeeded in maintaining the state of tension between the two spaces. Over time, jihadist and terrorist groups have been joined by members originating from the West who were convinced by the importance of the "missions" they later undertook. In the present paper, we will focus on the transposition and continuation of hostilities in both geographic and cyber spaces, with reference even to the current Israeli-Palestinian conflict.

Keywords:
terrorism; jihad; security; conflict; hacktivism; propaganda; defense; cyberterrorism.

Article info
Received: 12 February 2024; Revised: 28 February 2024; Accepted: 13 March 2024; Available online: 5 April 2024

Citation: Brandea, B. 2024. "Implications of the jihadist terrorism in cyberspace". *Bulletin of "Carol I" National Defence University*, 13(1): 157-165. https://doi.org/10.53477/2284-9378-24-10

The beginning of the 21st century brought major changes in the West's perception of the Middle East, a fact that contributed to the delimitation and segregation of the two spaces. Perpetual Western technological progress goes hand in hand with the evolution of Eastern attitudes and measures regarding Western supremacy. In this paper, we will analyze situations in which the interference of the two spaces was necessary for the performance of offensive and combative actions, from the physical environment to the virtual environment.

The international armed conflicts of the last decade – especially those in Eastern Europe and the Middle East[1] – have strengthened the rivalry between the US and Russia and reinstated negotiations on the positions of each other's allies. The conflict between Israel and Palestine is the most important one that we will consider, for which we will note some of its most important implications throughout history.

[1] The focus of our discourse herein pertains to the geographical domain commonly referred to by historians as the Near East, a constituent component encompassed within the broader expanse recognized as the Middle East.

In general, during international military tensions, the phenomenon of radicalization is becoming more common among civilians interested in actively supporting the cause of their belief. The unfettered access to the internet facilitates the circulation of materials designed to attract new followers who either already share the beliefs publicized or become interested or attracted to them. In the case of the radicalization of cyberspace attackers, the propaganda they are exposed to is intended to form invisible "troops" to contribute to hostilities from an invisible "front". It is notable that such "troops" are not only created through propaganda that is accessible on the internet, but they also include members who have extremist views gained from other sources, especially of a political nature.

The cyber environment is constantly exposed to threats both psychological and with repercussions in the physical environment. Therefore, in the context of the current armed conflicts in the proximity of Romania, the EU, and NATO, a high degree of alertness in cyberspace is necessary for attempting to meet and counter threats, attacks of various types, propaganda, and disinformation, taking into account the fact that such events have already taken place under the justification of contesting Romania's position.

Cyber-jihad or cyberterrorism?

Jihadist propaganda spread online by terrorist organizations such as Al-Qaida or ISIS is a manner of intimidating Westerners, but also a way of recruiting Muslims from both areas, namely encouraging non-Muslims to convert to Islam in order to join the jihad. It is important to state that, in such a context, Islam is used as a tool for manipulation and radicalization,

encouraging values that are not found in authentic Islam or that are even opposed to it, thus promoting an incomplete and incorrect image of religion (Toma 2013, 72).

For some jihadists, radicalization has meant adopting a new way of life, in which goals such as establishing a new Caliphate, killing those who do not follow the rules and values they consider to be Islamic, destroying or reshaping the West and especially the great powers, etc. (Leiken 2012, 142-144). Although all jihadist groups are divided by goals and ideologies, supporting the Palestinian cause represents a common ideal. For example, Al-Qaida's online approach is not only focused on insulting Israel but also involves incriminating Arab states that support Western perspectives on the conflict in Palestine. In addition, based on Europol's analysis of Al-Qaida's online propaganda in 2021, they claimed that jihad involves engaging every Muslim in support of the Palestinian cause while encouraging attacks against Israel, "Crusaders" and "Zionist" Arab states (Europol 2022, 39). By maintaining such beliefs, the information published by ISIS is intended to convince the audience that the jihadists are in fact the real Muslims (Frampton, Fisher and Prucha 2017, 24).

In another study published by Europol in 2017, cyber-jihad is described as "the global exploitation of the Internet by the Islamic State, which identifies itself as the Cyber Caliphate, through the specific discourse aimed at attracting hackers from around the world to engage in the media war against the "Crusaders" and join the United Cyber Caliphate" (Antinori 2017, 6).
These are just some of the concepts that underlie threats in the real world, but in the following lines, we will focus on the situation on the cyber "battlefield" and the common motivations identified at both levels.

Notably, jihad and terrorism are two distinct concepts. According to the *Dictionary of International Security*, jihad, although often translated as "holy war", is described as a central element in Islam, representing struggle, striving, or effort. Jihad can be offensive in order to spread Islam or defensive in situations where Islam is under attack (Robinson 2010, 119). Terrorism has not been given a precise definition, being described as a phenomenon that "consists of the illegal use of force by non-state actors with the aim of spreading terror among civilian populations and forcing governments to political concessions. The use of illegal violence is what distinguishes terrorism from normal political activity, legal/judicial violence, and conventional warfare" (Robinson 2010, 227).

As for the differentiation between cyber-jihad and cyberterrorism, it should be stated that information disseminated on behalf of a terrorist organization or a jihadist acting alone belongs to the cyber-jihad category. In contrast, cyberterrorism aims to carry out attacks with the aim of contributing to economic, political, and psychological conflicts (Babanoury 2014), and, in a strict sense, the usage of cyberspace as a tool for causing physical harm to individuals and objects (Torres 2016, 109).
Hence, placing the two concepts in the field of cyber security, we observe that jihadist

propaganda uses the religious pretext to attract followers, while Islam is actually the appearance of intentional political actions, while terrorism represents the tense state and attacks motivated by similar pretexts.

Terrorism abreast with cyber progress

In his study on the radicalization phenomenon of the second generation of Asian and African immigrants in Europe, Robert S. Leiken mentions the attraction of young extremists to the chosen identity, at the expense of the inherited one. Such an identity is shaped as a result of the failure of integration both among European natives and the lack of identification with the extended family and community of origin of the immigrant parents. Consequently, the justificatory discourse provided by terrorist groups together with the sense of belonging in a united community represents the ideal context for channeling their lifelong anger (Leiken 2012, 410).

Various specialists argue that terrorism associated with Islamist extremism is not technologically advanced enough to pose a major threat. Hunker (2010) notes that disruptive cyberattacks by terrorists are likely and possible, rather than serving to annoy the masses, cyber itself not being a weapon of terror (Hunker 2010, 12). Torres (2016) suggests that jihadists do not have the necessary technical training for cyber warfare, being rather prone to propaganda and hacktivism (Torres 2016, 108-9).

Interest in continuous technological progress and exposure to social networks where propagandistic materials and news of interest can be disseminated, along with the principle expounded by Leiken (2012) can establish a risk factor even for Romania's general and cyber security. According to the National Defense Strategy for 2020-2024, one of the listed risks includes "the intensification of global Islamist-jihadist propaganda that feeds the risks of radicalization on the national territory, including among Romanian citizens, conferring perspectives that are difficult to anticipate and counter" (Presidential Administration, 27).

From a general point of view, the attention of the Islamist terrorist organizations is mainly directed towards the states that support the US in the actions carried out in the Middle East. From this point of view, Romania could constitute a "legitimate" target, a fact that is also motivated by Romania's permanent involvement in international security councils and committees (Andreescu and Radu 2015, 273). "Indirectly exposed, through association with NATO, the EU, the USA, and the European states involved articulately in combating the scourge, our country remains a target of opportunity" (Presidential Administration, 25).

Romania has already been the target of DDoS attacks claimed by the pro-Russian hacker group Killnet and occasioned by the military and social support given to Ukraine as a result of the war started by Russia (Oancea 2022). The states that assist

Ukraine are still eligible as future targets for this type of attack, at least until the armed conflict has been finished (SRI 2022).

Hacking and hacktivism: the weapons of volunteers during armed conflict

Between hacktivism and cyber terrorism, there are similarities, but especially differences. Hacktivism involves a low level of disruption to the functionality of targets, with the main objectives being to humiliate them and gain visibility. In terms of cyber terrorism, perpetrators aim to remain undetected and the main goals are to undermine institutional security and public trust by attacking critical infrastructure and emergency services. Common features of the two concepts are the spread of propaganda, recruitment and fundraising intentions, and similar attack tools and techniques. In cases where hacktivists and cyber-terrorists have opposing visions, it is not out of the question that there will be cyber-attacks between the two types of groups (Baldi, Gelbstein and Kurbalija 2003, 18-19).

The involvement of the Killnet group in the conflict between Palestine and Israel does not represent the intention to support Palestine or the Hamas group with certainty, being rather an opportunity to launch cyberattacks against Israel. Their actions benefit the interests of other compatible groups around the world, as evidenced by their cooperation with Anonymous Sudan in the campaign against the "Israeli regime" (Hollingworth 2023). Although there is no accurate evidence that the members of the aforementioned groups belong to terrorist or jihadist organizations, we can identify two important elements that are part of the pattern of terrorist threats.

The first element is outlined by the choice of high-level targets. Successfully carrying out attacks on a government symbolizes the interaction between the attacker and the victim. In this way, the attacker has the certainty of delivering hostile messages and gains recognition of their destructive potential. Gaining control of government cyberspace means, as a result, the ability to control the security of the entire targeted state.

The second element is represented by the voluntary involvement of foreigners in supporting relevant causes and/or carrying out attacks. Analogous to non-Arabs and non-Muslims joining jihadist groups, we observe the motivation of pro-Russian and Sudanese groups to contribute to harming the Israeli government cyberspace.

On the other hand, radicalization is a key principle in the behavior and mentality of jihadists and terrorists. For hacktivists, radicalization is not necessarily a defining element, given that most high-profile attacks are carried out during periods of political tensions. Nevertheless, the extremist character is rather common to both hacktivists, hackers, and jihadists.

In addition, images of Palestinian civilians injured during the conflict – especially children – have over time contributed to the rise of jihadists and their desire to act against Israel in particular, but also against the Western states that support it. *Ways of cyberterrorism* cites the example of Nizar Trabelsi, a jihadist accused of planting a bomb in a military base in Belgium, who testified that images of a girl killed in the Gaza Strip encouraged him to become a member of Al-Qaeda in 2001 (Topor 2019, 87).

For better clarity on the current international tensions, it is relevant to recall some important aspects of the history of the last decades. In his study published in 1990 about the Arab-Israeli political tensions and the Cold War, Jerome Slater presents the conflict as caught up in the rivalry between the US and the Soviet Union, where the USSR would have pursued its expansionist ideology over the Middle East, eliminating US and NATO influences from the area and especially the energy independence of the West, Japan and the USA (Slater 1990, 557-9). In addition, Slater mentions the active support provided by the USSR for the establishment of the state of Israel, including the diplomatic recognition offered to Israel in 1948 within the UN council; certain historians justify the USSR's position during the named period as having the purpose of diminishing the British influence in the Middle East (Slater 1990, 562).

At the formal level, the evolution of the conflict broadly depends on the attitude of the "great powers" and the "superpower", respectively on the definition of the latter. According to Sarcinschi's study, the "superpower" status could be attributed to the United States of America, but during the latest decades, the decline of the power of the USA is taken into account, followed by the potential assignment of this rank to another state. As for the current "great powers", the states internationally recognized as having this status are the USA, Great Britain, China, France, Russia, Japan, and Germany (Sarcinschi 2010, 20-21). In the context where Israel plays the leading role in the conflict that started in 1948 and intensified in 2023, there are theories according to which Israel intends to become a superpower in the Middle East (Khashan 2020), at the global level (Kor 2021), in the field of technology (Forbes 2015), respectively of artificial intelligence for warfare (Williams 2023).

On the cyber "front", two defining aspects thus emerge for the perspectives of extremists on each of the opposing sides: the side allied to Israel seeks to achieve cyber and especially informational supremacy, while the side allied to Palestine opposes these operations, acting rather in response to Israel's continued offensives. In general, cyberattacks of a terrorist nature are classified as disruptive attacks by state and non-state actors, and cyber warfare is named as a special form of disruptive attack. A cyber war includes a disruptive attack on the space of one state by another state, which can be classified as an act of use of force (Hunker 2010, 2-4).

In an article on the cyber perspective of the conflict in the Gaza Strip, published by the Singaporean company Cyfirma, cyber security is particularly important not only

for the states involved, but also for their allies. This conclusion is based primarily on the conduct of cyber-attacks by hacktivist groups and threats from other types of actors in various regions that have targeted government websites, the education and media sectors, billboards, power plants, warning systems, and even sensitive military information. The article also mentions the possibility of Iran and its allies conducting "preemptive" actions in the near future as a result of Israeli attacks against Palestine (Cyfirma 2023).

In another Cyfirma article on hacker and hacktivist attacks in conflictual contexts of international relations, diplomatic intervention by governments is recommended in order to reduce geopolitical tensions. In such an approach, it is envisaged hacktivist activities can be prevented by eliminating their actual motivations (Cyfirma 2024).

Conclusions

The international conflicts in which the West and the Middle East are involved attract the engagement of civilians from both areas who, for this purpose, can carry out their offensive actions in the cyber environment. The conflict between Palestine and Israel is an opportunity for the intensification of jihadist and terrorist propaganda, which is joined by followers from both the Western and Eastern space.

The arguments applied to justify the hatred and the possible offensive position against the West are currently amplified as a result of the support provided by the West to Israel, a fact that may imply the increase in the number of terrorist threats in the cyber environment and outside it. Disagreement with the positions adopted by Western governments is also expressed among certain civilians originating in the West who, motivated by empathy and the belief that they can contribute to changing the international political landscape, adhere to an interpreted form of religion that gives the appearance of concordance with the ideologies that they generally guide themselves. Thus, an important part of the threats in conflict contexts is realized by exploiting the psychological factor both of the attackers who have the opportunity to satisfy their need for validation and of the targets among whom the state of terror is installed.

Romania is a potential target due to its presence in the EU and in treaties such as NATO, but precisely these memberships are crucial for maintaining and increasing the level of security, as well as cooperation in order to achieve these goals. In conclusion, complementary to military and logistical involvement in conflict zones, the resilience and defensive dimension of Romania's cyber environment remain extremely important regardless of the evolution of events.

References

Andreescu, Anghel and Nicolae Radu. 2015. *Jihadul islamic. De la „înfrângerea terorii" și „războiul sfânt" la „speranța libertății" [The Islamic Jihad. From "defeating terror" and "holy war" to "hope for freedom"].* București: RAO.

Antinori, Arije. 2017. *The "Jihadi Wolf" threat the evolution of terror narratives between the (cyber-)social ecosystem and self-radicalization "ego-system".* Hague: Europol Public Information.

Babanoury, Julien. 2014. *Cyber Jihad: The Internet's contribution to Jihad.* https://incyber.org/en/cyber-jihad-the-internets-contribution-to-jihad-par-julien-babanoury-ceis/.

Baldi, Stefano, Eduardo Gelbstein and Jovan Kurbalija. 2003. *Hacktivism, cyber-terrorism and cyberwar. The activities of the uncivil society in cyberspace.* Msida: DiploFoundation.

Cyfirma. 2023. *Israel Gaza conflict: the cyber perspective.* 18 October. https://www.cyfirma.com/outofband/israel-gaza-conflict-the-cyber-perspective/.

—. 2024. *Caught in the Crossfire : How International Relationships Generate Cyber Threats.* https://www.cyfirma.com/outofband/caught-in-the-crossfire-how-international-relationships-generate-cyber-threats/.

Cyware. 2019. *Flame 2.0 spyware found using strong encryption algorithm to avoid detection.* https://cyware.com/news/flame-20-spyware-found-using-strong-encryption-algorithm-to-avoid-detection-36939d76.

Europol. 2022. *Online Jihadist Propaganda 2021 in review.* Luxemburg: Publications Office of the European Union.

Forbes, Steve. 2015. *How The Small State Of Israel Is Becoming A High-Tech Superpower.* https://www.forbes.com/sites/steveforbes/2015/07/22/how-the-small-state-of-israel-is-becoming-a-high-tech-superpower/.

Frampton, Martyn, Ali Fisher and Nico Prucha. 2017. *The New Netwar: Countering Extremism Online.* London: Policy Exchange.

Hollingworth, David. 2023. *Killnet and Anonymous Sudan join forces to target Israel in widespread hacking campaign.* https://www.cyberdaily.au/security/9652-killnet-and-anonymous-sudan-join-forces-to-target-israel-in-widespread-hacking-campaign.

Hunker, Jeffrey. 2010. *Cyber war and cyber power: Issues for NATO doctrine.* Rome: NATO Defense College.

Khashan, Hilal. 2020. *Israel Becomes the Middle East's Superpower.* https://geopoliticalfutures.com/israel-becomes-the-middle-easts-superpower/.

Kor, Moira. 2021. *'I'm going to turn Israel into a world superpower'.* https://www.jns.org/im-going-to-turn-israel-into-a-world-superpower/.

Leiken, Robert S. 2012. *Islamiștii europeni. Revolta tinerei generații.* [*Europe's Angry Muslims. The Revolt of The Second Generation*]. Translated by Sorin Șerb. Bucharest: Corint Books.

Oancea, Dorin. 2022. *Grupul de hackeri pro-rus Killnet a revendicat atacul cibernetic ce a afectat mai multe site-uri ale instituțiilor din România [The pro-Russian hacker group Killnet claimed the cyberattack that affected several websites of Romania institutions].* https://www.mediafax.ro/externe/grupul-de-hackeri-pro-rus-killnet-a-revendicat-atacul-cibernetic-ce-a-afectat-mai-multe-site-uri-ale-institutiilor-din-romania-20782645.

Presidential Administration. 2020. "The Nationl Defence Strategy for 2020-2024." https://www.presidency.ro/files/userfiles/National_Defence_Strategy_2020_2024.pdf.

Robinson, Paul. 2010. *Dicționar de securitate internațională [The Dictionary of International Security].* Translated by Monica Neamț. Cluj-Napoca: CA Publishing.

Sarcinschi, Alexandra. 2010. *Rolul actorilor statali în configurarea mediului internațional de securitate [The role of state actors in shaping the international security environment].* Bucharest: Editura Universității Naționale de Apărare "Carol I".

Slater, Jerome. 1990. "The Superpowers and an Arab-Israeli Political Settlement: The Cold War Years." *Political Science Quarterly* 105 (4): pp. 557-577.

SRI. 2022. "Buletin Cyberint." II Semester. Accessed November 14, 2023. https://sri.ro/assets/files/publicatii/buletin-cyber-sem-2-2022-RO.pdf.

Toma, Gabriel. 2013. *Terorismul internațional. Reacții ale actorilor regionali și globali [International terrorism. Reactions of regional and global actors].* Iași: The European Institute.

Topor, Sorin. 2019. "Ways of cyberterrorism." *Bulletin of "Carol I" National Defence University*, September: pp. 82-90.

Torres, Manuel. 2016. "The limits of cyberterrorism." Edited by H. Giusto. *Daesh and the terrorist threat: from the Middle East to Europe* (Foundation for European Progressive Studies -Fondazione Italianieuropei) 108-114.

Williams, Dan. 2023. *Israel aims to be 'AI superpower', advance autonomous warfare.* https://www.reuters.com/world/middle-east/israel-aims-be-ai-superpower-advance-autonomous-warfare-2023-05-22/.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Narrative strategies in action – text, form, and context

Captain Anca CIORNEI, Ph.D. Student*
*"Carol I" National Defence University, Bucharest, Romania
e-mail: ciorneiancaelena91@gmail.com

Abstract

The major changes in the global security environment that took place at the end of the last millennium continue to deeply mark the first quarter of the 21st century, characterized by substantial changes in the classical instruments used in conducting a conflict. Also, the transformation of the informational environment has led to the emergence, development, adaptation, and contextualization of the use of strategic narratives with the aim of influencing people's perceptions of the actions of power states and producing effects in the sense desired by them.

The purpose of this article is to subject strategic narratives to attention, as part of contemporary hybrid confrontations, aiming to bring a better understanding of this subject, observing how they are used and with what effects, depending on the form in which they appear.

Moreover, the article proposes a multilevel conceptual delimitation, approaching strategic narratives from the perspectives of text, context, and form, as highlighted in the most recent research in the specialized field.

We will also consider their use in an allied context, with reference to working documents that NATO uses in strategic communication to influence target groups and audiences, both internal and external.

Keywords:
narrative strategies; strategic communication; cognitive warfare.

Article info
Received: 30 January 2024; Revised: 21 February 2024; Accepted: 15 March 2024; Available online: 5 April 2024

Citation: Ciornei, A. 2024. "Narrative strategies in action – text, form, and context". *Bulletin of "Carol I" National Defence University*, 13(1): 166-178. https://doi.org/10.53477/2284-9378-24-11

The beginning of the 21st century has brought into the spotlight little expected changes, with various effects, starting from the individual level and continuing to the societal one, in which both the great power states and numerous organizations are involved, having interests in directions such as industry, economy or other important fields with an impact on the population.
Moreover, if during the Cold War, we could talk about a certain symmetry in the relations between the two great political-military blocs, the USSR and the USA, today we are witnessing the emergence of multiple forms of asymmetry in contemporary conflicts, as a result of the differentiation between conventional war and new types of conflicts.

It can be said that the present is characterized by risks, opportunities, uncertainties, and threats, and all these elements can take various forms, depending on the rapid social, scientific, technological, geopolitical, or even climatic changes, in a time when globalization produces effects that are continuous and spread in unexpected directions.
If in the past we could categorize military action as land, air, sea, space, or cyber, each representing different domains, recently we have seen discussions about a cognitive dimension of warfare. This dimension involves influencing people's perceptions through various methods and means of manipulation, with the aim of achieving desired outcomes, such as altering perceptions of certain values.

At the same time, against the background of high interest in the research of new types of conflict, in a report published on the website of NATO's Allied Command Transformation (ACT), cognitive warfare is defined as *"the totality of activities carried out in close connection with other instruments of power with the aim of affecting attitudes and behaviors by influencing, protecting and/or disrupting individual and group knowledge in order to gain an advantage"* (NATO-ACT 2023).

In the same direction, in a report published on the *Innovation Hub* platform, Bernand Claverie and François du Cluzel put forward the following idea: *"The cognitive war is with us. The main challenge is given by the fact that it is invisible; all that can be seen is its impact, but by then...it is often too late"*. In other words, in conflicts where the battles are fought in people's minds, the effects of the actors' actions are visible as soon as the intentions have already reached their goal (Claverie and Du Cluzel 2022).

An approach that complements the above belongs to the current president of the Romanian Academy, Ioan Aurel Pop, who, as early as 2017, stated that *"information and communication are of enormous importance for historical research. It was said, until recently, that whoever controls the information controls the world. Today, something else is added - whoever masters communication can rule the world or can rule even wider communities. Much of the distortions at work in the world today had their theoretical foundations in history. In order to be able to compare and respond to*

these challenges, we need to cultivate our best-performing computer, the human brain" (Pop 2017).

If we are to debate about this new dimension, the informational one, in which the largest share is held by the cognitive side, then it is imperative to subject attention to the tools that are used for this purpose, to be able to wage war on such a territory. Undoubtedly, *strategic narratives* play a decisive role in generating and coordinating such hybrid confrontations.

From a methodological perspective, in order to achieve the objectives we propose in this article, we will approach the analysis of documents and specialized research, trying to deepen the concept of strategic narratives and that of narrative strategies, as well as the effects they have on the target audiences when they are implemented.

Regarding the structure of the article, it covers the theoretical approaches of strategic narratives, develops narrative strategies in terms of form, structure, and levels of action, and also presents their use in an allied context. All these elements aim to highlight the importance of strategic narratives and narrative strategies in a period characterized by major changes in the current security environment.
At the same time, by approaching these concepts, the work contributes to a better understanding of the cognitive dimension of current conflicts and identifies elements that can be found in the act of disinformation and manipulation of audiences, aspects that are increasingly present in hybrid confrontations.

Strategic narratives – theoretical approaches

The definition of the term *narration*, in general, starts from the neologism borrowed from the French language – *narration*, previously taken from the Latin language – *narration* with the meaning of *storytelling*. This term is, in fact, the mode of exposition by which facts and events are related, in a temporal sequence. Moreover, it is part of a discourse and presupposes the existence of the following elements: narrator, action, and characters, with an emphasis on the sequence and dynamism of events. In other words, as stated by Miskimmon, O'Loughlin and Roselle in 2014, *"narratives are formed and projected in a communication environment"* (Miskimmon, O'loughlin and Roselle 2014b).

Taking into account the fact that any narrative follows a grammatical line, then we must also bring into discussion the term *narratology*, proposed in 1969 by the French theorist Tzvetan Todorov, who speaks in his works about *thematic narratology*, in which the narrative contents are debated and the stories are delivered by the character or the narrator, and the formal one, which analyzes the narrative representation of the speech, the relationship between the narrator and the characters, as well as their positioning in relation to the narrative act (Todorov 1971). He also established, in the

work *"Categories of literary narrative"*, the two components of the narrative, viewed as a story – the logic of the actions and the relationships between the characters (Todorov 1966). From his perspective, the narration is entrusted directly to the characters or the narrator, both of which are difficult to identify in their pure state. Such an approach supports those who want to decode stories and who analyze how messages are presented by those involved in the narration, using the narrative act to nuance or direct the message in the desired meaning.

In the same line, in her work from 1999, entitled *"Semiotics, society, culture"*, Daniela Rovența-Frumușani talks about the creation of narratives and narrative structures as *"the strategy that allows us to make the world intelligible, being an essential model of data organization"* (Rovența-Frumușani 1999). In other words, by creating logical and well-structured narratives, effects can be obtained that can lead to the deciphering of the initial intentions and their interpretation, until the understanding of the meaning of the transmitted information. Moreover, she reviews and analyzes narrative structures, starting from Aristotle's *Poetica*, which talks about characters and actions, and following Propp's model, where narrative actions become fundamental, referring to introduction, realization, and conclusion. Such an approach is useful in realizing that narratives are consciously created, applied with a certain purpose, and adapted to the context so that the results obtained can be interpreted as clearly as possible.

Chronologically approached, numerous researchers, theorists, and communication experts have studied the narratives used by major social actors to identify their roles, the forms they can take, and the effects they have when they are used. For example, Oliver Schmitt highlighted how the narrative strategies used during political speeches are perceived and what is the connection between them and political people, also considering the typology of political myths (Schmitt 2018). In this sense, he highlighted how important it is that, in their speeches, intellectuals adapt their messages so that they are understandable to the public.

Strategic narratives, on the other hand, refer to the concept of power, the balance of power between states, international relations, and security studies, as is also evident from one of Barry Buzan's works, which also induces the idea that political discourses must be adapted and explained in order to achieve security by introducing the term *securitization* (Buzan 2008). By using narrative strategies, states manage to position themselves against each other, or even against certain values that are shared or not by masses of individuals.

Undoubtedly, we could not discuss the term strategy, put in a military, diplomatic or geopolitical context, without referring to Sun Tzu's *The Art of the War*, which highlights the importance of planning and adaptability, as well as a deep understanding of the environment in which military actions are carried out in order to achieve victory and advantage in battle, not only through force, but especially

through intelligence, understanding the characteristics of the adversaries and anticipating their movements (Tzu 1994).

Equally, Henry Mintzberg presents the strategies in a more complex manner by classifying them into five distinct categories (McCarthy 2000):

- *Strategy as a plan* presupposes a pre-establishment of an action, drawing guidelines to reach the proposed objectives, prior to the situation, with implications developed in the knowledge of the case and with a well-defined purpose;
- *Strategy as a tactic* is mainly applied to counter the intentions of opponents;
- *Strategy as a model* tries to establish a pattern of behavior, because strategy results from the actions that people take;
- *Strategy as a position* identifies the actor's place both internally and externally, becoming a mediating force;
- *Strategy as a perspective* represents a unique way of perceiving the external environment.

Viewed from the five angles, it can be concluded that strategies are essential when the objectives are to be designed, and the narratives used, having behind them a very well-defined strategy, are defining tools for taking strategic advantage during any type of conflict.

Returning to the phrase of *strategic narratives*, it is increasingly used in contemporary confrontations. Trying to correlate this phrase with the classification of strategies presented previously, it can be concluded that strategic-type narratives include a certain plan when they are conceived, have clearly defined objectives in order to apply them effectively, follow a pattern according to the feedbacks resulting in following their use, they are formulated according to the target groups they aim at and anticipate the reactions of those involved.

According to O'Loughlin, narratives are created and projected in the international environment, following three essential ideas (Miskimmon, O'loughlin and Roselle 2014b):

- they appear in human interactions, define the world, and affect human behaviors;
- they have as a central element the political actors who use the narratives in a strategic way;
- the environment of communication fundamentally affects the way narratives are communicated and how they influence the target audience.

According to the same author, narrative strategies are increasingly used in fields such as political science or international relations, and they represent a useful and effective tool for obtaining the results desired by the state and its leaders, with the aim of influencing the behaviors and attitudes of individuals or entire masses of citizens.

Summarizing, we can say that *"a narrative becomes strategic when it prescribes a type of order that serves particular interests. It must be said that any strategic narrative consists of two major ingredients: power and communication. The junction between the two constructs truths, i.e. it imposes on domestic and international events the meanings desired by the establishment, which means that strategic narratives generate perceptions, emotions, behaviors, i.e. social reality"* (Dumitrescu 2020). In other words, if we bring up the fact that through the application of strategic narratives, we aim to position the public in relation to a certain reality that we present, we can also refer to propaganda or persuasion of the target audience, a communication process in which *"the actors with the best arguments are the winners because they are the ones who manage to convince"* (Popescu 2022).

The strategic narrative can be seen as a firmly formulated and communicated story that appeals to the enduring values shared by the members of an organization, their origins as a collective, and what they want to achieve in the future and, very importantly, the steps that must be completed so that intentions become facts and certainties.

Diachronically, strategic narratives appeared and are increasingly used because of the evolution of the information environment and as a need to adapt to the changes occurring in the current international context. They can be seen as tools that are used in the battle that goes on in people's minds, with the attempt to influence and obtain results in the desired directions. Changing the behaviors of the masses according to their own interests and influencing them to respect certain values are only some of the objectives that are considered when using narrative strategies. As these narratives are better structured and framed in certain patterns, they can create effects that can tip the balance towards a certain side of the hybrid confrontation taking place in the current period.

Therefore, the concept of strategic narratives will differ from the concept of narrative strategies as the first of them refers to the act of communication and the elements involved in this whole process. In contrast, narrative strategies follow the communicative behavior, the techniques used by those who initiate the process, with the aim of achieving pre-established objectives.

Strategic narratives – form, structure, and levels of action

Although it is not yet possible to discuss a clear delimitation or a standard structure that can be traced within them, strategic narratives have aroused the interest of several theorists and researchers, who have tried to identify the structure, form, and key elements that can be found when using such narrative constructions.
Starting from the approach of Miskimmon, O'Loughlin, and Roselle, through which they emphasize that *"strategic narratives are tools through which political*

actors try to build a common interpretation of the past, present and future of world politics with the intention of influencing the behavior of the internal and international actors" (Miskimmon, O'loughlin and Roselle 2014b), they also identified a set of characteristics of these strategic type narratives and presented their approach which includes *five key components* (Miskimmon, O'Loughlin and Roselle 2017):

a) *they are oriented towards the future*. Although a strategic narrative may refer to the past and/or present, its applicability is connected to shaping policy in the future;

b) *they are closely related to identity*. They articulate a distinct (national/ regional) position on a specific issue, policy area, or more generally on the state's place in world politics or the international system;

c) *the content is not fixed*, but is a dynamic and always negotiated social product, based on the interactions of states, both with their societies and with other relevant external actors in the sphere of influence;

d) *they can derive from experiences in history*, calling on previous actions, previous experiences and historical reputation acquired over time;

e) *their audience is both internal and external*. They can be used for ensuring the loyalty of the domestic public, on the one hand, and on the other hand for its use in the delimitation and communication of collective perception in the international sphere.

Analyzing all these elements, it can be concluded that strategic narratives do not have a certain pattern, but can undergo changes depending on the initial intentions, the values that are shared by those who issue such narratives, the values that the audience respects, and the pattern of the target audience, be it internal or external.

In another analysis by the same authors, they present strategic narratives in three steps, tracing their formation, projection, and reception (Miskimmon, O'Loughlin și Roselle 2018). They are built, most of the time, by the governing parties and the Ministry of Foreign Affairs, later they are made public through the speeches of political leaders so that in the end they will be received by the intended audience. Throughout this loop, narrative framers respond to audience interpretations and behavior of the messages delivered to them and adjust content to achieve maximum desired effects, ensuring that narratives are not only comprehensible but also compelling. All these steps are carried out consciously to counteract the new types of risks and hybrid threats that appear to security on the one hand, and on the other hand to pursue and promote their own goals related to the balance of power, spheres of influence, misinformation or weakening cohesion at the societal level.

Considering the previously listed aspects, we cannot continue the analysis of narratives or stories without also acceding to Hanna Merejota's idea that storytelling is the aspect of narrative that shapes our cognitive understanding of the world, our affective orientations, and our senses (Meretoja 2018). So, from here we can extract the idea that narratives are used considering not only the rational part of the target

audience but also their emotions and the elements that can be shaped, appealing to the affective and sensory side, aspects with a complexity of much larger and longer-lasting decoding and interpretation. Therefore, the use of narratives and the achievement of effects may undergo changes depending on the reactions provoked, which implies a continuous adaptation of the messages conveyed.

Also, when we discuss their *form*, narratives can be transmitted through various channels or can be found in various forms. In this sense, one can distinguish narratives in the form of texts, audio, images (photos, maps), multimedia, and these can be distributed either through traditional media or with the help of social media, which is increasingly present in the life of each individual, with the aim of winning people's minds and their perceptions towards the intentions of political actors (Bjola, Cassidy și Manor 2019).

All of these can be disseminated to activate *three levels of action* where narratives can be framed: international, national and at issue level. At the international level, narratives are used to describe how the world is structured, what international interests are, and why not, what the world order is. At the national level, they highlight the status of the state actor, what are its goals and values, and how it seeks to be perceived by other state actors. At the issue level, narratives create the framework for the use of certain government policies and explain why certain policies are needed and how they will be implemented effectively. The three levels are, most of the time, interdependent. They interfere so that the originally set goal is achieved within the estimated time frame (Miskimmon, O'Loughlin and Roselle 2014a).

In addition to all the previously highlighted aspects, it should also be stated that strategic narratives are used in the current context not only to position ourselves towards certain aspects and values but also to attract image capital and sympathy from the audience that we educate through each narrative act that we consciously cultivate (Saliu 2023). Precisely for this reason, RL Boyd paid attention in one of his works to the concept of *narrative arch*. In his view, there are similarities and differences between narrative structures depending on their construction processes, the variables involved, and the phases they go through until they end up affecting the intended human behaviors (Boyd, Blackburn and Pennebaker 2020).

Narrative strategies used in allied context

Trying to identify the *context* in which the need to analyze strategic narratives arose, Oliver Schmitt believes that it is based on the interest to examine the importance of persuasion in contemporary conflicts, the way in which current military campaigns are presented to international or national audiences and the way in which a political community debates strategic issues. Therefore, this interest arises as a result of the need to align with the new methods of action used in conflict management, so that

all involved act, as far as possible, in an informed manner in order to achieve the results estimated in the initial planning (Schmitt 2018).

To be fully understood and to identify the factors involved and their actions, any conflict must be studied from political, diplomatic, international relations, economic, or military perspectives. Following any of these branches, we can observe how each of the actors involved in the confrontation uses a series of strategic narratives to position themselves according to the objectives they have and to create situations of strategic advantage in hybrid confrontations, following the influence of society in the targeted directions.

In the last three decades, NATO has been involved in various operations and missions, and for this it has always had to communicate why and how it does this, primarily to achieve its proposed strategic objectives, but also to counterbalance the narratives of its adversaries (Nissen 2014). For this, the Alliance has had to continuously adjust its own narrative strategies, both to create a common understanding among Allies about its actions and to maintain its legitimacy and defensiveness in the face of challenges, while at the same time trying to eliminate the fear to communicate these actions and to rather focus on what the actions themselves communicate (Mullen 2009).

For example, in order to increase the confidence of the young public in the ability of the Alliance structures to protect the population and Allied territory, as well as to explain the involvement in multinational exercises or international missions, in 2017, NATO started, supported and developed one of the largest strategic communication campaigns, entitled #WeAreNATO, through which it facilitated the access of young people to information about NATO over various events. For this, the strategic narratives used took various forms (images, texts, video) and were used in several contexts and on several channels (press conferences, public events, interviews) by NATO leaders who explained the main mission of the Alliance (NATO-ACT 2017).

Moreover, through the Strategic Concept published in 2022 in Madrid, the Alliance aims to make public its common interests, reiterating, once more, its defensive nature and firm intentions to discourage the escalation of any type of conflict. The content of the document includes, in text form, the narratives pursued by NATO and the responsibilities it assigns to the allied states (NATO 2022). The implementation of this document, like all recent actions carried out by the Allies, also calls for strategic communication used to achieve the proposed common objectives, considering concepts that refer to public diplomacy, public affairs, or military public affairs (Johnsson 2011).

Analyzing all these aspects, we can conclude that through strategic narratives, NATO not only communicates or informs, but also aims to educate the audience with the aim of producing emotions that can be translated into support from the masses and sharing of common values.

As a term, at the NATO level, the narrative was regulated by a document in 2014. It focused attention on the term narrative and how to develop it, step by step, with the aim of being used as a tool in the context of a future military information strategy. In its content appeared, for the first time, the concept of a *narrative arch*, in which the trajectory of the arch (action-effect) is made up of participants or actors who undertake actions that can take forms such as text products, video, audio, speeches, all of which led to the favorable results sought or the initiation of a certain desire. When a narrative comes to an end, causing satisfaction or dissatisfaction, then it is considered resolved. Also, in the same document, the phrase narrative landscape includes several variables (myths, stories, histories, religious or fictional stories) that interact, being an integrated part of the informational environment, that lead to the creation of a favorable context for the delivery of strategic narrative constructions (MNIOE 2014).

If we consider the use of narratives in the information environment, we must take into account the fact that they can be used for propaganda, in all its forms, with the aim of influencing the opinions, emotions, attitudes, and behaviors of individuals (Reddi, Kuo and Kreiss 2023). In other words, information intended to achieve effects uses multiple channels of information propagation, to influence, sometimes negatively, individuals' perceptions and affect credibility.

Currently, information is a key tool in relations between states. When used as a weapon in information warfare, strategic narratives rely on the mixing of truth and falsehood and the misrepresentation of facts to induce distorted and biased interpretations in the public, these reactions being the effects of propaganda, influence, and disinformation (Barclay 2018).

In the NATO Strategic Communication Handbook, narrative strategies are presented and how they should be approached for a better understanding of the information environment. According to this document, narratives represent the coherent communication of various actors involved in operations with the aim of generating perceptions of certain shared values. For this to happen, the narrative strategies, themes, messages used in the discourse, as well as the use of the vulnerabilities of certain audience segments are just some of the defining elements of this process. The identification of stories in different narratives allows a comprehensive understanding of the narrative landscape and the information environment, which is why other fields are involved in this whole endeavor, such as information operations (InfoOps), military public relations, psychological operations (PSYOPS), civilian-military cooperation (CIMIC), intelligence (J2), political counseling (POLAD) and cultural counseling (CULAD). These areas can support the communication and understanding approach and contribute to an integrated outcome. This aspect can be achieved through well-synchronized strategic organizational communication, which considers aspects specific to each previously mentioned area (NATO 2017).

According to NATO, strategic communication involves the coordinated and appropriate use of communication activities and capabilities in support of Alliance policies, operations, and activities with the aim of advancing NATO's objectives (NATO n.d.).

In the context of strategic communication, strategic narratives are part of information warfare to cause information disruption on the adversary's home front. When this happens, they can create alternative realities about facts and events, or even alter collective perception to the point of changing support for the leadership. As a result, strategic narratives, disinformation, and information warfare can also become tools of crisis communication during conflict situations and work towards manipulating the information environment.

Conclusions

In a period characterized primarily by uncertainty and continuous change, as well as by the battle for power and information, the role of narrative strategies becomes defining. It is increasingly difficult to separate narrative strategies from interests, risks, or threats. In all this confrontation in which the messages sent or received must be decoded and interpreted, it is necessary to identify methods and means to counteract the unwanted effects generated by all these new challenges.

Strategic narratives help both to formulate strategy and to communicate actions. Informing the strategy and its associated actions, for example, military operations, ensures consistency with the original intentions. In other words, it ensures the correlation between words and deeds, even though the strategic narrative is normally constructed as an integral part of the strategy formulation process. Thus, the basic characteristic of strategic narratives is that they provide a framework through which information activities can be structured to explain the past, present, and future of conflicts, with the aim of achieving the desired results.
The frequency with which information is disseminated recently creates an increasingly interconnected society, which makes the importance of narrative strategies even greater, their influencing role being defining.

Narrative strategies can be studied from the perspective of several dimensions. Approaching them through the prism of political discourse and by analyzing them according to the audiences they target and the values they bring to attention, are just a few aspects that will be detailed in a future article.
This approach is part of the author's doctoral research. Starting from these aspects, we propose that in the future we consider the correlation of how strategic narratives impact the cognitive dimension of conflicts and identify their models used by major state actors, looking for defining aspects that can change the estimated results within an influencing process.

We believe that at the moment no clearly defined and outlined uses of strategic narratives have been identified, and we also cannot precisely delineate the narrative strategies or techniques that lead to the achievement of superiority in current confrontations, which is why future research will focus on an in-depth analysis of the models used by major political actors that aim to steer audiences in the desired directions.

References

Barclay, Donald A. 2018. "Fake news, propaganda, and plain old lies: how to find trustworthy information in the digital age." *Rowman & Littlefield* 227.

Bjola, Corneliu, Jennifer Cassidy and Ilan Manor. 2019. "Public Diplomacy in the Digital Age." *The Hague Journal of Diplomacy* 14 (1-2): 83-101.

Boyd, Ryan, Kate Blackburn and James Pennebaker. 2020. "The narrative arc: Revealing core narrative structures through text analysis." *Science advances* 6.2 (eaba2196).

Buzan, Barry. 2008. *People, states & fear: an agenda for international security studies in the post-cold war era.* ECPR Press.

Claverie, Bernard and François Du Cluzel. 2022. "Cognitive Warfare Concept." *Innovation Hub.* https://innovationhub-act.org/wp-content/uploads/2023/12/CW-article-Claverie-du-Cluzel-final_0.pdf.

Dumitrescu, Lucian. 2020. *Narațiuni strategice: securizare și legitimitate în relațiitle internaționale.* Institutului de științe politice și relații internaționale „Ion I.C. Brătianu".

Johnsson, Magnus. 2011. "NATO and the Challenge of Strategic Communication." *NATO Defense College.*

McCarthy, Daniel J. 2000. "View from the top: Henry Mintzberg on strategy and management." *The Academy of Management Perspective* 14 (3): 31-42. http://www.jstor.org/stable/4165656.

Meretoja, Hanna. 2018. *The Ethics of Storytelling: Narrative Hermeneutics, History, and the Possible.* Oxford: Oxford University Press.

Miskimmon, Alister, Ben O'Loughlin and Laura Roselle. 2014a. "Strategic narrative: A new means to understand soft power." *Media, War & Conflict* (University of Oxford) 7 (1): 70-84.

—. 2014b. *Strategic narratives: Communication power and the new world order.* Routledge.

—.2017. *Forging the World: Strategic Narratives and International Relations.* Royal Holloway.

—. 2018. "Strategic Narrative: 21st Century Diplomatic Statecraft / Narrativa estratégica : el arte de la diplomacia en el siglo XXI." *Revista Mexicana de Política Exterior* 113.

MNIOE [Multinational Information Operations Experiment]. 2014. "White Paper – Narrative Development in Coalition Operations." v 1.0, Mayen.

Mullen, Michael. 2009. "Joint Force Quarterly." *Defense Technical Information Centre.* From The Chairman: Strategic Communication: Getting Back to Basics. Quarter 4. Accessed December 2023. https://apps.dtic.mil/sti/pdfs/ADA535610.pdf.

NATO. n.d. *About Strategic Communication.* Accessed January 2024. https://stratcomcoe.org/about_us/about-strategic-communications/1.

—. 2023. *Allied Command Transformation.* Accessed December 2023. https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/.

—. 2022. *NATO 2022 Strategic Concept.* https://www.nato.int/strategic-concept/.

—. 2017. *NATO Strategic communication Handbook.* Vol. V 1.0.

NATO Strategic Communication Centre of Excellence. n.d. *About Strategic Communication.* Accessed December 2023. https://stratcomcoe.org/about_us/about-strategic-communications/1.

NATO-ACT. 2017. *We Are NATO - Defence and Security Campain Toolkit.* https://www.act.nato.int/wp-content/uploads/2023/06/nato-dsct.pdf.

—. 2023. *Cognitive Warfare: Strengthening and Defending the Mind.* https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/.

Nissen, Tomas Elkajer. 2014. "Strategizing NATO's Narratives." *Strategy in NATO. Palgrave Studies in Governance, Security and Development* (McMilan).

Pop, Ioan Aurel. 2017. "Războiul informațional, sub lupă." *Prompt Media.* https://www.promptmedia.ro/2017/04/razboiul-informational-sub-lupa-conferinta-la-academia-romana/.

Popescu, Maria Magdalena. 2022. *Comunicarea strategică a informațiilor.* București: Top Form.

Reddi, Madhavi, Rachel Kuo and Daniel Kreiss. 2023. "Identity propaganda: Racial narratives and disinformation." *New Media & Society* 25 (8): 2201-2218.

Rovența-Frumușani, Daniela. 1999. *Semiotică, societate, cultură.* Iași: Institutul European.

Saliu, Hasan. 2023. "Narratives of Public Diplomacy." *Truth Era: The decline of Soft Power. Communication & Society* 36 (2): 209-224.

Schmitt, Oliver. 2018. "When are strategic narratives effective? The shaping of political discourse through the interaction between political myths and strategic narratives." *Contemporary Security Policy* 39 (4): 487-511. https://doi.org/10.1080/13523260.2018.1448925.

Todorov, Tzvetan. 1966. "Les catégories du récit littéraire." *Communications - Recherches sémiologiques: l'analyse structurale du récit.* (Edwardsville) (8): 125-151. https://doi.org/10.3406/comm.1966.1120.

—. 1971. *The 2 Principles of Narrative.* The Johns Hopkins University Press.

Tzu, Sun. 1994. *The art of war.* Hachette UK.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Integrative and relational approaches to resilience in the NATO concept and action

Colonel Professor (Ret.) Gheorghe MINCULETE, Ph.D.*
Lecturer Veronica PĂSTAE, Ph.D.**
*"Nicolae Bălcescu" Land Forces Academy, Romania
e-mail: minculetegh@yahoo.com
**"Carol I" National Defence University, Romania
e-mail: pastae.veronica@myunap.net

Abstract

The concept of resilience, suitable for specific operations, has been used within NATO since 2010. The particularity of the term resides in the characteristic phases of implementation in the allied operational environment, which generates appropriate conduct of identifying, analyzing, and avoiding risks, resistance to disruptive and impactful factors, recovery, restoration, and reconstruction of the initial force and action potential. The Alliance's combatant forces will maintain integrity and adequate functionality, even under restrictive, difficult conditions, by implementing, at organizational and operational levels, the two components of layered resilience (operational or military and civil). In this way, a high level of protection, stability, and viability of combat structures of tactical and/or joint forces will be achieved, to face the threats and complex actions of unfriendly (enemy) forces. Through the findings, the present research includes a theoretical approach, with possibilities of concretization in applied resilience in NATO civilian and military fields, because it includes important programmatic details, related to the consequences of the Russian-Ukrainian armed confrontation, which started on February 24, 2022. From here, relevant elements resulted in the consolidation of action power of joint and tactical forces, meant to be engaged in national and multinational operations within the North Atlantic Alliance, against any hostile aggressive forces.

Keywords:
instability; competition; resilience; layered resilience; civil resilience; operational (military) resilience; protection; stability; functionality.

Article info
Received: 21 January 2024; Revised: 14 February 2024; Accepted: 11 March 2024; Available online: 5 April 2024

Citation: Minculete, G. and V. Păstae. 2024. "Integrative and relational approaches to resilience in the NATO concept and action". *Bulletin of "Carol I" National Defence University*, 13(1): 179-193. https://doi.org/10.53477/2284-9378-24-12

Pervasive instability, strategic competition, and recurring shocks shape the general security landscape. Threats can come from both state and non-state actors, in various forms, such as terrorist attacks, cyber-attacks or hybrid warfare, which blur the lines between conventional and unconventional conflicts. The importance of civil-military engagement and cooperation is evident in the face of threats posed by climate changes, natural disasters such as floods, wildfires, and earthquakes, pandemics, and Russia's war of aggression against Ukraine. As new technologies become ubiquitous, the societies of NATO states become more interconnected and interdependent in the economic, financial, informational, and cyber domains. This interdependence has brought significant benefits, but it has also created vulnerabilities and dependencies. In today's security environment, effective and sustained resilience requires a comprehensive approach. This involves the use of the full range of military and civilian capabilities, as well as an active collaboration between the government, the private sector, and civil society (NATO 2023c).

Right after the annexation of Crimea, Alliance planners and commanders implemented several crucial measures to implement the updated NATO Concept, including the development of the Organization's Military Strategy in 2019. As a result, in 2020, the allied Defense Ministers approved the *Concept for the Deterrence and Defense of the Euro-Atlantic Area*. Under these conditions, the term *resilience* has become particularly important - originally mentioned in the NATO Strategic Concept from 2010 (NATO 2010). In 2019, NATO leaders agreed, in the London Declaration, to step up efforts to strengthen resilience. Afterward, at the GLOBSEC 2020 Bratislava Forum, Secretary General Jens Stoltenberg emphasized the future directions of resilience within the Alliance: "In fact, resilience is in NATO's DNA. Article Three of the Washington Treaty places a duty on the Allies to become more resilient. When the treaty was written, the concern was an armed attack from the Soviet Union. Today, we face a far broader range of challenges. That is why, boosting resilience is a key task for the future" (van Mill 2023, 84). In 2021, NATO highlighted the need to implement *national and collective resilience* as „*an essential basis for credible deterrence and defense*" (NATO 2021), given the new challenges and global military threats. The NATO 2022 Strategic Concept, approved during the Madrid Summit in 2022 (LSE IDEAS 2023) reinforces the importance of *national and collective resilience* in all essential allied actions, the first being *deterrence and defense*, as a major objective, reaffirmed at the 2023 NATO Summit in Vilnius (NATO 2023d).

"Resilience in a NATO context refers to the capacity, at the national and collective level, to prepare for, resist, respond to, and quickly recover from strategic shocks and disruptions, across the full spectrum of threats. Simply put, it is the ability for the Allies individually, the Alliance collectively and NATO as an organization to face disruptions and shocks and continue their activities. Geostrategic and military power redistribution requires the ongoing transformation of the NATO

Military Instrument of Power, as well as the alignment of military and non-military capabilities throughout NATO member nations. Alliance's resilience stems from a combination of civil preparedness and military capacity. In this context, civil preparedness directly contributes to NATO defense readiness – well maintained, fast healing, adaptive, durable, and ongoing military systems supported and enabled by civilian capabilities are needed to ensure security and stability throughout the Alliance". (NATO-ACT 2023c).

In the USA, the Department of Defense (DOD) has developed an expanded interpretation of *resilience* as a concept, applying it in the context of national defense. This perspective is reflected in the development of various policies, doctrines, and guidelines, and on the official websites of the DOD and armed services. For example, in Directive 4715.21 on Climate Change Adaptation and Resilience, DOD defined *resilience* as the "ability to anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruptions". This definition is associated with all areas managed by DOD, such as facilities, personnel, operations, transportation, supply chains, research, development, testing, and evaluation. Another example illustrates how the US Army defines *resilience* in the Army Recovery Care Program - a program for wounded, ill, and injured soldiers. Here, *resilience* is described as „the mental, physical, emotional and behavioral ability to face and cope with adversity, adapt to change, recover, learn and grow from setbacks" (Herrera 2021, 2). This concept covers multiple aspects of military life and highlights the importance of developing the necessary skills to face and overcome the challenges encountered in their service (Wheeler 2021, 2).

Currently, the Allied Command Transformation (ACT) is leading the Alliance's operational adaptation process by implementing NATO's fundamental warfighting concept (NATO-ACT 2023a). This approach includes the need for the operational development of the Alliance's power, based on the concept of *layered resilience* developed by ACT, by the requirements of military transformation, adaptation and maintaining of security in a complex international environment, characterized by the continuous growth of military risks and threats (NATO-ACT 2023c).

To carry out this novel work in a balanced way, we proceeded, from a scientific point of view, to identify the sources, obtain, analyze, evaluate, and interpret the information and necessary data to create the content of the sequences. The result is an updated study, useful for those interested in understanding the role and importance of resilience in the NATO concept and action, to carry out further scientific work. The holistic construction of this study actually approaches layered resilience whose components are addressed, from a scientific point of view, as follows: civil resilience in sequence two; and operational (military) resilience in sequences three and four.

General aspects of national and collective resilience within NATO

Each NATO member state must have the necessary resilience to face (with very few losses), possible major shocks, generated by natural disasters, critical infrastructure failures, and hybrid or armed attacks. If we consider the core of the concept, *resilience* represents the individual and collective potential for preparation, resistance, response, and fast recovery from the impact of disruptive factors, to ensure the continuity of activities specific to the functioning of each Alliance state. In this sense, based on Article 3 of the North Atlantic Treaty, ensuring national and collective resilience is essential in designing and achieving credible deterrence and defense, vital for the realization of NATO's efforts to protect societies, populations, and common values. Modern societies are highly complex, with integrated and interdependent sectors and vital services. This makes them vulnerable to major disruptions in the case of a terrorist or hybrid attack on critical infrastructure (NATO 2023c). In Figure 1 we present critical infrastructures (totally or partially) present in NATO member states.

Figure 1 The civil critical potential of each NATO state (Roepke and Thankey 2019)

For most of the Cold War period, civil emergency planning, then known as civil preparedness, was effectively organized and resourced by the Allies, most notably reflected in NATO's structure and command. During the 1990s, however, much of the detailed planning, structures, and capabilities of civilian training underwent significant cuts, both at national and NATO levels. Events such as Russia's illegal annexation of Crimea in 2014 and the rise of ISIS/Daesh have marked a change in the strategic environment. These led the Alliance to strengthen its deterrence and defense posture. Meanwhile, terrorist and hybrid threats, especially recent cyber attacks, continue to target the civilian population and critical infrastructures, mostly owned by the private sector. These developments have had a profound impact, highlighting the need to increase resilience through civilian training. Today, the Allies are taking a step-by-step approach to this, in an effort that complements NATO's military modernization and its overall deterrence and defense posture

(Roepke and Thankey 2019). At the 2016 Warsaw Summit, Allied leaders agreed to enhance NATO's resilience to address the full spectrum of risks and threats, and to develop individual civil capabilities of member countries alongside collective capabilities, to withstand any form of armed attack.

They established seven basic requirements for assessing the level of preparedness on behalf of allied countries, as regards national civil resilience (Figures 2 and 3): • ensuring the functional continuity of government and critical government services (this involves the ability to make decisions and communicate with citizens during a crisis); • achieving continuous energy supply and developing back-up plans to manage outages (the focus is on the ability to provide power consistently and manage outages through well-defined plans); • the effective management of uncontrolled movement of people, simultaneously with the deployment of allied military capabilities (with an emphasis on the ability to manage and control the movement of people, including from military areas); • ensuring sufficient and resilient food and water supplies (especially protected from interruptions or sabotage); • designing and ensuring the capacity to deal with mass casualties and disruptive health crises (the emphasis will be on building civil health systems that can manage crisis situations, with adequate stocks of medical supplies); • the operation of telecommunications and cyber networks in crisis, including the use of 5G technology, with robust options for restoring these systems; • ensuring the rapid movement of NATO forces on the territory of the Alliance, considering that civil services can count on transport networks, even during a crisis (van Mill 2023, 85). These requirements reflect the Allies' commitment to strengthening national and collective resilience, thus contributing to the security and stability of the NATO Alliance by ensuring the continuity of government, essential services for the population, and civil support for the military.

To reduce potential vulnerabilities and risks of attack in peacetime, crisis, and conflict, NATO states will consider a full corroboration of military efforts to defend territories and populations with solid civil/civilian training in the areas of continuity of government, continuity of essential services for the population and giving civil/civilian support for joint-level military operations with national and multinational status. In this regard, considering the major destructions done by the Russian army in Ukraine, and the sabotage against the Nord Stream pipelines, at the NATO and EU level, on March 16, 2023, an operative group was established to raise awareness of the situation, sharing the best practices and developing the principles needed to improve resilience within both organizations. On announcing the joint work initiative, in January 2023, the Secretary General of NATO – Jens Stoltenberg stated in the presence of the President of the European Commission – Ursula von der Leyen: "We want to look together at how to make our critical infrastructure, technology and supply chains more resilient to potential threats, and to take action to mitigate potential vulnerabilities. This will be an important step in making our societies stronger and safer". At the same time, NATO and EU leaders signed a new joint declaration to build the partnership between these organizations at a complex

level, including the use of emerging, disruptive technologies and the cosmic space, also taking into account the influences of climate changes on the security dimension. It is obvious that NATO's joint multinational operational forces, especially those deployed during crises and conflicts, will strictly depend on the services related to civil and commercial sectors as regards transport, communications, energy, and even essential supplies, food, water, ammunition, and fuel, to fulfill their missions. Thus results the importance of robust civil/civilian training to enable Allied societies to withstand attacks and/or major disruptions at any time given supporting the Alliance's combat forces to achieve operational objectives and the end state (NATO 2023c).

Peculiarities of operational resilience within the Alliance

The purpose of realizing operational resilience (Resilient MIoP) within NATO is to support deterrence and defense of the Alliance against any adversary by establishing and using capabilities to anticipate, prepare, and adapt to threats and dangers, as well as by implementing resistance, response and rapid recovery options in the face of strategic shocks (van Mill 2023, 85).

The continuous modernization of NATO has given rise to the Layered Resilience Concept, which includes two components that augment each other, *i.e.* operational (military) resilience and civil resilience, considered essential in supporting the Alliance's military instrument of power (Figure 2). Layered resilience reveals NATO's ability to respond and adapt rapidly to various levels of risks and threats, from conventional to cyber and/or hybrid ones. The main focus of the concept is on operational (military) resilience, to enhance its applicability and realize its interdependencies with civil resilience (shown in sequence 2). In this way, NATO's capabilities of resistance, recovery and adaptation to strategic shocks, will be strengthened (van Mill 2023, 85-86).

Figure 2 Images of layered resilience (operational and civil) within NATO (van Mill 2023, 84)

Following the invasion of Ukraine by the Russian army on February 24, 2022, NATO experts have deemed it necessary to develop a resilience planning process similar to the NATO Defense Planning Process (NDPP) to harmonize and integrate national resilience plans, strategies and capacities. This approach was considered essential to coordinate a strong collective response from NATO, concurrently with the establishment of a high-level resilience task force, with the mission to identify and propose: multidimensional lessons regarding resilience, based on Ukraine's experience in the face of conventional, hybrid, and societal threats; both national and collective resilience requirements to help achieve a more effective unit effort; recommendations on future policies and investments, to achieve the objective of strengthening European resilience (Dowd and Cook 2022, 1-4).

Subsequently, the complexity and amplitude specific to the Layered Resilience Concept (elaborated) involved (at the Alliance level) the establishment of an appropriate thematic framework for *seven areas* belonging to *operational resilience* (Figure 3). Individually, the areas (listed below) required the establishment of thematic working groups – led by the designated allied nations –, as follows: • Command and Control-C2 System, France; • Warfighting Capability, Poland; • Situational Understanding, Greece; • Logistics/Deployability of Forces, Germany; • Response Planning, Romania; • Military Infrastructure, United Kingdom; • Perseverance, Hungary. To achieve the specific objectives, the thematic working groups will be supported by interested parties and necessary experts in each field. Through the methods and procedures used, related to the listed fields, several types of analyses will be carried out to obtain all the information for specific determinations of potential risks, vulnerabilities, and critical deficiencies, which will be taken into account in the future development of the military instrument of power (Dowd and Cook 2022, 85-86).

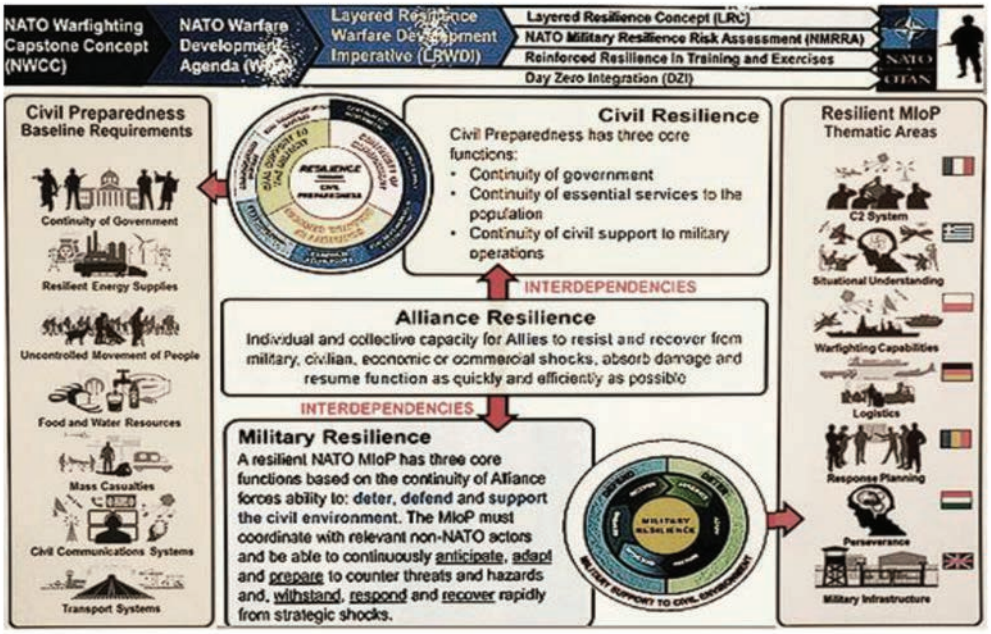


Figure 3 Areas of layered resilience, with focus on operational resilience (Dowd and Cook 2022, 86)

Since Romania is involved in one of the seven areas mentioned, the experts of the Euro-Atlantic Resilience Center (E-ARC) participated in September 2023 in the works of a seminar organized in Poland, for the development of the NATO layered resilience concept. For this purpose, E-ARC specialists coordinated, with the involvement of experts from the Romanian Ministry of National Defense, the process of elaborating the content of the Alliance's doctrine regarding "*response planning*", taking into account several NATO objectives concerning resilience, with an emphasis on: „continuity of government; structured military procedures; rapid mobilization of reserve forces; a harmonious balance between capabilities and capacities" (E-ARC 2023).

The operations of the future involve a continuous confrontation of one's own tactical and/or joint forces with adversary forces, which requires the consideration, design, and manifestation of operational resilience (a component of layered resilience) at tactical and/or joint levels, according to the stages of its development (partly or fully). Therefore, operational resilience highlights a process of preparatory protection, avoidance, evasion, strike-impact, response, restoration and further capability protection of the (national and multinational) combatant force in the action phases integrated with the missions in the theater of multinational joint operations.

Consequently, according to Figure 4, operational resilience involves, in phases, the provision and application of adequate operational risk management at the mentioned action level. It follows, therefore, that the intensive actions of the enemy, with different types of forces and means, can lead to a reduction in operation pace, especially due to the depletion of resources, losses in personnel and equipment, the low and uncertain level of stocks, the physical and mental exhaustion of fighters and their loss of motivation (Herrera 2021, 2-5).

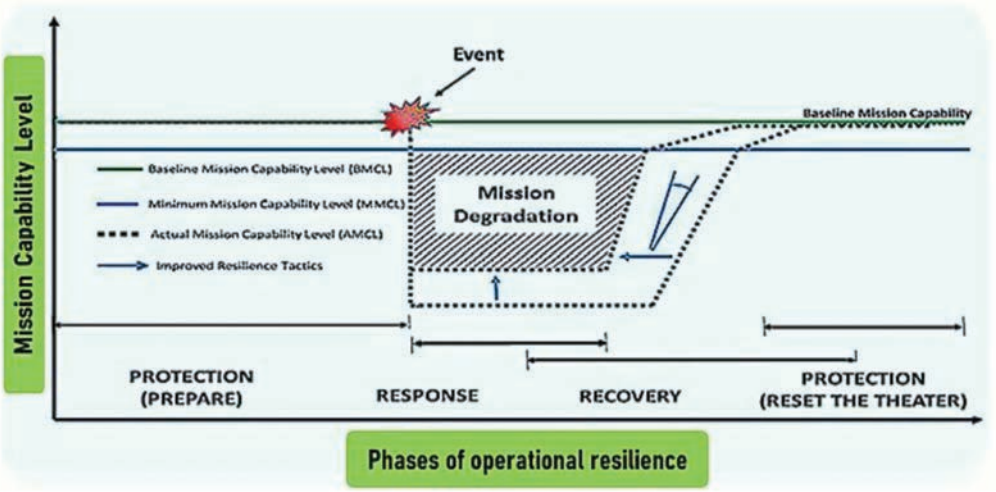


Figure 4 An image of operational resilience configuration at the level of a tactical and/or joint multinational force (Herrera 2021, 3)

In this context, leaders of operational and logistical support structures, at tactical and/or joint levels, are responsible for collaboration both horizontally and vertically in the military organizations to which they belong, including a joint force group. Therefore, the action synergy, created and developed by each combatant leader, together with the available logistic potential, represent the essential pillars of increasing, maintaining or restoring the operational resilience (Figure 5) of each tactical and/or joint level action structure (Minculete 2023, 230-232).

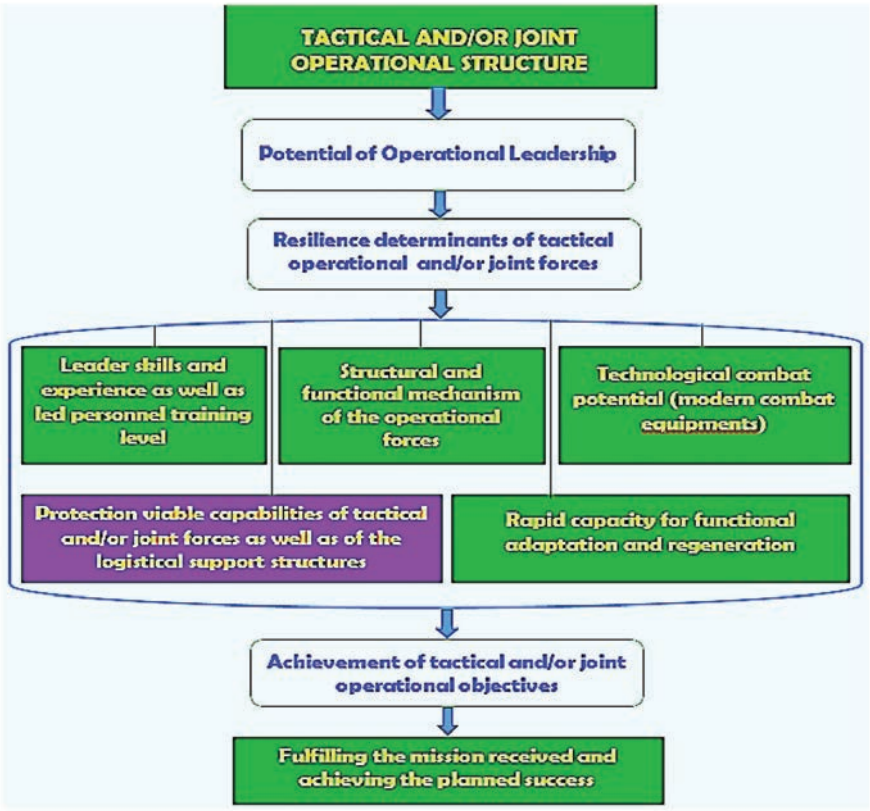


Figure 5 Objective determinations of operational resilience at tactical and/or joint levels (Minculete 2023, 231)

Continuing with the operational resilience of a joint force under NATO command, it follows that its augmentation potential determines the maintenance of the territorial and/or critical infrastructures involved, and the continuous provision of resources (from military and civil sources) necessary to plan and conduct operations during a campaign in the face of the enemy's complex attacks. It follows, therefore, that joint operational forces and the integrated logistics support network must have the ability to operate without significant disruption and to adapt to intensive attempts by adversary forces, meant to distort and diminish one's intentions and resources through multiple force actions (Hagen et al. 2016, 6-11). If the avoidance of disruptive (risk) factors can no longer be prevented, even if visible intervention measures have been taken based on the requirements involved in the action effort, there will be insurmountable discrepancies between the dynamic actions of the combatant forces and the immediate logistic support they need

(Ryczynski and Tubis 2021, 16-22). Thus, with respect to operational logistic resilience, a specific crisis will arise quickly, through a partial or total shortage of logistical resources and services (in the following fields: supply; transport; maintenance; campaign services) and medical support, known in the economic sphere as "logistics culmination", and, at the military operational level – in our view, as "logistics critical point" or "logistics critical deficit". (Minculete 2023, 143-145). The disruption of operational logistic support is highlighted in Figure 6.

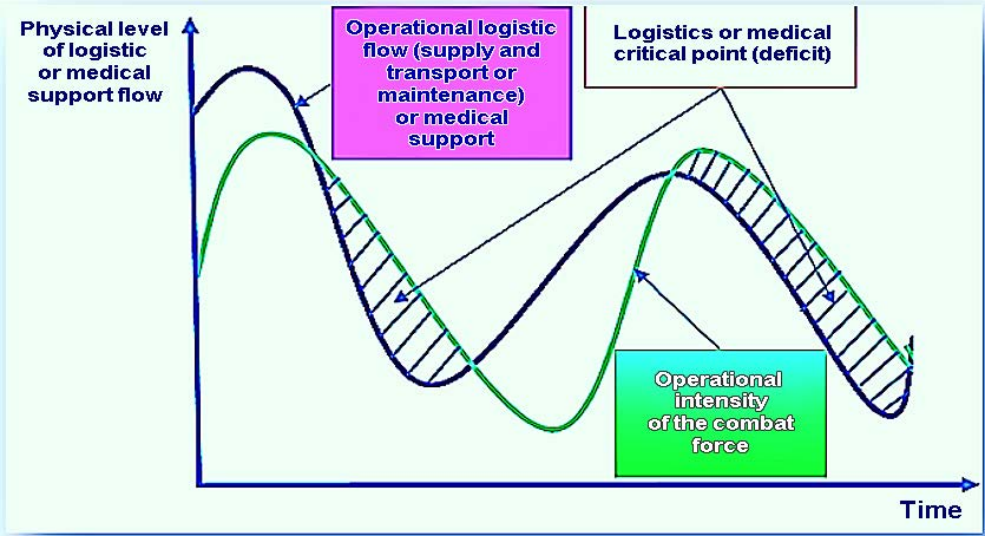


Figure 6 An image of the logistics critical point (deficit) of a tactical and/or joint multinational force (Minculete 2023, 144)

Russia's unjustified and illegal invasion of Ukraine, which generated the largest conflict in Europe since World War II, has now become an armed conflict of attrition and heavy logistic engagement. This complex confrontation highlighted the imperative to address often neglected, but crucial aspects in ensuring the essential operational capabilities required to successfully deploy, execute, and sustain planned operations to accurately accomplish the missions received and achieve the end state (Dowd, Jankowski and Cook 2023, 8-9). Given these conditions, it is necessary to rapidly improve the training capacity and the ability of NATO operational forces, which must be supported by modern, effective, and efficient operational logistics, to ensure an adequate response to counter current and future threats (NATO-ACT 2023b).

As a result, to build high operational resilience, with holistic effects at organizational and inter-organizational levels, it follows the need for intensive planning and performing, by NATO national and multinational operational forces, of training and exercises, modeling and simulation, such as and wargaming for testing leaders, fighters, and for validating processes. According to Alliance experts, training scenarios involving both types of resilience - civil and operational (military) one – will have to include: civil agencies, international and non-governmental organizations, commercial actors and civil defense forces; and current and future

complex environments and threats. At the same time, chaos and failures occurred during training and exercises of NATO operational structures and systems, which will have to be integrated to improve the execution that will be evaluated based on the qualitative and quantifiable resilience indicators (NATO-ACT 2022, 5).

Deterrence and defense, essential factors in achieving operational resilience

The role of deterrence in the military field is equivalent to a state's level of operational potential as compared to that of its adversaries. Through deterrence, adverse threats can be mitigated or diminished, thus, implicitly avoiding the consequences of an extended crisis that could break out. Modern doctrinal approaches highlight deterrence primarily as a psychological process, emphasizing the skillful understanding of the mentality of the opposing forces' elites, who define and propagate the threat through the use of military power of subordinate forces, as well as the ability to influence their immediate conduct. Therefore, message coordination and synchronized transmission on various communication channels, have the role of changing the behavior of the opposing state's leader(s) after understanding the multiple costs and consequences of any reckless military actions at their behest. From here, the doctrinal configuration of operational resilience results, which focuses, apart from the behavioral side, on the theory of games that was and is applied through deterrence with conventional and/or nuclear military potential (Wheeler 2021).
When deterrence is to reach the critical point of failure, NATO operational forces (national and multinational) will have to implement permanent defense and contingency plans (built-in advance based on possible operational scenarios) to face imminent threats, at least in the short term, and prepare the necessary conditions to win the initiative, if it has been diminished or lost (Wheeler 2021).

In the same line, a suggestive historical example of defense and deterrence of the opposing forces is the war of the Finnish state, from the fall and winter of 1939-1940, against the invading Soviet forces, whose potential was given by the force of more than 600,000 soldiers. Finland's defense consisted of only: 300,000 soldiers (including reserves and conscripts); a small number of tanks; a few fighter jets; and a miniscule amount of ammunition for an insignificant artillery force. However, the compensation came from the Finnish civil society prepared to face a far superior enemy. In the course of history, great battles were often won by flexible and much smaller forces than the enemy, and in the case of the Finnish army which was quite inferior to the opposing one, almost all the soldiers were, besides skilled hunters and experienced skiers, capable of combat and survival in the extreme conditions of the Arctic Circle winter. As regards the invading Soviet army, most of the recruits who had to brave the frozen wilderness were not equipped for the combat environment, lacking important items such as snowshoes and skis. Moreover, the Finnish defense

forces gradually drew the invaders inside the national territory, covered by a high layer of snow. Simultaneously the defense organized themselves into small and independent harassing groups, with increased mobility, capable of quick and effective attacks, which enabled them to destroy the less equipped and prepared Soviet units. They were prevented from deploying and forced to move in massive columns along difficult roads, while the Finnish fighters, highly motivated for the liberation of their country, had complete freedom of movement and attack. Later, after 105 days of intense confrontations, the armed conflict that started on November 30, 1939, ended with a peace agreement between the two sides. It resulted, however, in a territorial loss of 11% of Finland, but compensated by the preservation of state sovereignty. The other side, the USSR, lost more than 200,000 people on the territory of the occupied state, compared to only 25,000 Finnish casualties, which portrayed a particularly negative image of the Soviets' international reputation (NATO 2023b).

Today, NATO's military defense power installed in the eastern part of its territory is an important deterrent. This component was built in recent years, when the allied states located in the northern and southern territories of NATO's eastern flank set up, based on the agreements at the level of the Alliance, eight battle groups (BG) with multinational structures (each under a nation-frame). So, as early as 2017, battle groups were established in Estonia, Latvia, Lithuania, and from 2022, in Hungary, Slovakia, Romania and Bulgaria. Moreover, for deterrence and defense, on this eastern flank - from the Baltic Sea in the north to the Black Sea in the south - the Allies have deployed a significant number of ships, aircraft and other troops (NATO 2023b). On January 24, 2024, one of the largest NATO military exercises (after the Cold War), called "Steadfast Defender 2024", designed to be carried out over several months, began in the N-E USA (Felstead 2024). The operational capabilities to carry out the exercise are: „around 90,000 soldiers (from 31 NATO allied states and Sweden); 50 warships (from aircraft carriers to destroyers); over 80 fighter jets (F-35, FA-18, Harriers, F-15), helicopters and countless unmanned aerial vehicles; over 1,100 combat vehicles (namely, more than 150 tanks; 500 infantry fighting vehicles and 400 armored personnel carriers)" (NATO 2024; Reuters 2024). The purpose of this complex exercise is to: test and refine the Alliance's defense plans, to strengthen European defense against the possible actions of "a close adversary" (Felstead 2024); conduct and sustain complex operations "in several fields, for several months, over a geographical area of thousands of kilometers, from the High North to Central and Eastern Europe, in any conditions" (Garamone 2024); demonstration of the Alliance's ability to strengthen the Euro-Atlantic area "through the transatlantic movement of forces from North America" (which involves verifying the Alliance's ability to prepare and rapidly transport North American forces for "strengthening the defense of Europe"). The military maneuvers specific to this exercise will be carried out within "a simulated conflict scenario that would occur with an adversary of almost the same caliber" (Garamone 2024). Following the completion of NATO's New Military Strategy in 2019, and the associated concept for *Euro-Atlantic deterrence and defense* in the following year, the Strategic Plan for the entire area of

responsibility of the Supreme Allied Commander Europe (SACEUR) was approved. This is *a unique military plan* for the use of Alliance forces, both inside and outside the NATO area, considering both major threats: Russia and terrorist groups. The fundamental details on how to address specific threats were then supplemented by detailed regional and subordinate plans.

Thus, during the Summit in Vilnius, the *regional plans* - for the three Joint Force Commands were approved, as well as *the seven strategic plans available to the commanders of functional domains*. The mentioned NATO Commands completely cover the Area of Responsibility of SACEUR (Area of Responsibility - AOR), namely the (joint command) areas: Nordic and Atlantic (at Norfolk-Virginia); Central - with the Baltic states to the Alps, (at Brunssum-Netherlands); South-East (including the Mediterranean and the Black Sea (in Naples-Italy) (LSE IDEAS 2023).

Conclusion

Increased A2/AD (Anti-Access/Area Denial) threats in the emerging strategic environment of Europe, the Middle East, and Asia-Pacific have led the US and NATO joint forces to become sufficiently resilient to any attack, by generating the necessary combat power to achieve operational objectives at tactical, joint and strategic levels. Appropriate options for designing and achieving adequate operational resilience, by a multinational joint Alliance force, require a pertinent analysis of theater interactions between potential adversary attacks and one's own actions, to counter them in a timely, effective, and efficient manner.

From a societal perspective, within the Alliance, resilience represents the ability of a society to resist and recover from shocks such as natural disasters, critical infrastructure failures, and hybrid or armed attacks. From here, two key aspects of resilience result, namely, the capacity to absorb and recover from a crisis. Then, resilient actors must be able to respond to a range of potential shocks, whether anticipated or unexpected, and have the ability to survive.

From an operational point of view, resilience is the ability to absorb shocks at strategic, operational, and tactical levels, by reducing risks, which requires proper management. Any NATO military organization needs to implement operational resilience by adopting an appropriate functional framework that encompasses the critical stages of anticipation, detection, deterrence, resistance, response, and recovery. Each of these elements must be supported by well-grounded procedures, to strengthen, thus, the capacity of any operational structure with national and/or multinational status, to face challenges and/or threats.

At the Alliance level, resilience is not just a modern term, but an essential objective whose implementation generates flexibility, adaptability, and resilience. This requires

procedures for incorporating layered resilience, through the operational (military) and civil components, within the complex actions of deploying and engaging the forces of NATO member states in joint national and multinational operations, to defend the Alliance's territory.

Finally, the role of resilience within NATO is given by its major importance in achieving the security and efficiency objectives of the organization to always counter present-day threats, that are increasingly changing in complexity and diversification. Under these conditions, the Alliance will become progressively prepared, continuously adapted, collaboratively strengthened and able to effectively manage risks, so that it can ensure the conditions of stability and security within a dynamic international security environment, which has become increasingly unpredictable.

References

Dowd, Anna and Cynthia Cook. 2022. "Bolstering Collective Resilience in Europe." *Center for Strategic and International Studies (CSIS).* https://www.csis.org/analysis/bolstering-collective-resilience-europe.

Dowd, Anna, Dominik P. Jankowski and Cynthia Cook. 2023. "European Warfighting Resilience and NATO Race of Logistics: Ensuring That Europe Has the Fuel It Needs to Fight the Next War." *Center for Strategic and International Studies (CSIS).* https://www.csis.org/analysis/european-warfighting-resilience-and-nato-race-logistics-ensuring-europe-has-fuel-it-needs.

E-ARC [Centrul Euro-Atlantic pentru Reziliență]. 2023. *E-ARC participă la seminarul NATO din Polonia privind reziliența stratificată.* https://e-arc.ro/tag/layered-resilience/.

Felstead, Peter. 2024. *Steadfast Defender 24', NATO's largest exercise since the Cold War, kicks off.* https://euro-sd.com/2024/01/major-news/36158/steadfast-defender-kicks-off/.

Garamone, Jim. 2024. "NATO Begins Largest Exercise Since Cold War." *US Department of Defense.* https://www.defense.gov/News/News-Stories/Article/Article/3656703/nato-begins-largest-exercise-since-cold-war/.

Hagen, Jeff, Forrest E. Morgan, Jacob L. Heim and Matthew Carroll. 2016. *The Foundations of Operational Resilience-Assessing the Ability to Operate in an Anti-Access/Area Denial (A2/AD) Environment.* Santa Monica, California: RAND Corporation.

Herrera, G. James. 2021. "Military Installation Resilience: What Does It Mean?" *Congressional Research Service.* https://apps.dtic.mil/sti/pdfs/AD1147490.pdf.

LSE IDEAS. 2023. "NATO's 2022 Strategic Concept: One Year On." *LSE Ideas Global Strategies.* https://www.lse.ac.uk/ideas/Assets/Documents/updates/2023-SU-NATO-OneYearOn.pdf.

Minculete, Gheorghe. 2023. *Determinări relaționale privind modernizarea logisticii operaționale.* Sibiu: Editura Techno Media.

NATO. 2010. "Active Engagement, Modern Defence – Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation adopted by Heads of State and Government in Lisbon." https://www.nato.int/cps/en/natohq/official_texts_68580.htm.

—. 2021. *Strengthened Resilience Commitment.* paragraph 4. https://www.nato.int/cps/en/natohq/official_texts_185340.htm.

—. 2023a. "NATO and European Union launch task force on resilience of critical infrastructure." https://www.nato.int/cps/en/natohq/news_212874.htm.

—. 2023b. *NATO's military presence in the east of the Alliance.* https://www.nato.int/cps/en/natohq/topics_136388.htm.

—. 2023c. "Resilience, civil preparedness and Article 3." https://www.nato.int/cps/en/natohq/topics_132722.htm.

—. 2023d. "Vilnius Summit Communiqué." https://www.nato.int/cps/en/natolive/official_texts_217320.htm?selectedLocale=en.

—. 2024. *NATO Exercise Steadfast Defender 2024.* https://ac.nato.int/archive/2024/nato-exercise-steadfast-defender-2024.

NATO-ACT. 2022. "NATO Resilience Symposium." *Allied Command Transformation-NATO's Strategic Warfare Development Command.* https://www.act.nato.int/wp-content/uploads/2023/05/20221018_resilience_symposium_report-1.pdf.

—. 2023a. "Adaptable Strategy: NATO Warfighting Capstone Concept's 20-Year Vision for NATO and Allied Forces." *Allied Command Transformation-NATO's Strategic Warfare Development Command.* https://www.act.nato.int/article/nwccs-20year-vision-for-nato/.

—. 2023b. "Allied Command Transformation Enhances NATO's Logistics and Sustainment Supply Chains." *Allied Command Transformation-NATO's Strategic Warfare Development Command.* https://www.act.nato.int/article/act-enhances-natos-logistics-sustainment-supply-chains/.

—. 2023c. "Resilience and Civil Preparedness in NATO." *Allied Command Transformation-NATO's Strategic Warfare Development Command.* https://www.act.nato.int/article/resilience-and-civil-preparedness-in-nato/.

—. 2024. "NATO's Steadfast Defender 2024: Unprecedented Military Exercise Signals Alliance Unity and Preparedness." https://www.act.nato.int/article/steadfast-defender-2024-signals-alliance-unity-and-preparedness/.

Reuters. 2024. *NATO to hold biggest drills since Cold War with 90,000 troops.* https://www.reuters.com/world/europe/nato-kick-off-biggest-drills-decades-with-some-90000-troops-2024-01-18/.

Roepke, Wolf-Diether and Hasit Thankey. 2019. "Resilience: the first line of defence." *NATO REVIEW.* https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html.

Ryczynski, J. and A.A. Tubis. 2021. "Tactical Risk Assessment Method for Resilient Fuel Supply Chains for a Military Peacekeeping Operation." Energies 14(15) (15): 4679. https://doi.org/10.3390/en14154679.

van Mill, Jeroen (Lieutenant Colonel). 2023. "The Future of NATO's Resilience. Concepts and Wargaming." *The Three Swords* (39). https://www.jwc.nato.int/application/files/9616/9804/8578/RESILIENCE.pdf.

Wheeler, Gerhard. 2021. "Operational Resilience: Applying The Lessons of War." https://nationalpreparednesscommission.uk/wp-content/uploads/2021/05/Operational-Resilience-Applying-the-Lessons-of-War.pdf.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Nigeria's Development Trajectory, Security Conundrum and the State-Citizens Relations

Tajudeen Yusuf ADEYINKA*
Musediq Olufemi LAWAL**
Olawale Olufemi AKINRINDE***
Remi Kasali ALATISE****
*Department of Criminology and Security Studies, National Open University of Nigeria
**Department of Sociology Osun State University, Osogbo, Nigeria
***University of Johannesburg, Johannesburg, South Africa
e-mail: oakinrinde@uj.ac.za
****Department of Sociology and Industrial Relations, Fountain University Osogbo, Nigeria

Abstract

Crime represents a profound threat to societal well-being, generating misery and disorder. Understanding its nature, causes, patterns, and consequences is vital for its effective prevention and control. In Nigeria, the past two decades have witnessed a steady rise in criminal activities, straining resources and impeding national development. Relying on the Social Contract thesis, this study examines how the preponderance of criminality and insecurity has systematically hindered Nigeria's developmental aspirations. In this study, we contend that the state's primary duty is to safeguard citizens and their property, as espoused by the social contract theory. However, the relentless wave of criminality in the last two decades in Nigeria has greatly undermined the social agreement between the Nigerian state and its citizens. This is in addition to the diversion of resources from other state's responsibilities to the security of the citizenry and the defence of the state. The implication of this situation, as revealed in this study, is the general hampering of the comprehensive national progress and prosperity of the Nigerian state. In this regard, we, therefore, recommend the imperativeness of a communal approach towards tackling the spate of security challenges in Nigeria whilst also recognizing that safeguarding the society remains a collective responsibility of both the Nigerian state and its citizenry. By fostering a culture of security amongst all, the Nigerian state and its citizenry can address the pervasive triggers and impact of crime whilst building a safer and prosperous future for all.

Keywords:
crime; insecurity; social disorder; developmental aspirations; social contract; security.

Article info
Received: 31 January 2024; Revised: 18 February 2024; Accepted: 5 March 2024; Available online: 5 April 2024

Citation: Adeyinka, T.Y., M.O. Lawal, O.O. Akinrinde and R.K. Alatise. 2024. "Nigeria's Development Trajectory, Security Conundrum and the State-Citizens Relations". *Bulletin of "Carol I" National Defence University*, 13(1): 194-211. https://doi.org/10.53477/2284-9378-24-13

Crime is a common and regular feature of social life. Its pervasiveness accounts for its recognition as a significant threat to human existence across all known societies (Durkheim, 1938). The fact that much of society's resources are dedicated to crime prevention and management (Carter and Youngs 2016) underscores the relevance of criminality to ordered social life. The widely acknowledged social import of criminality has persuaded scholars to conclude that crime is as old as human society. As anthropological knowledge of primitive social organisation indicates, deviation from societal norms and actual acts of criminality have characterised human societies regardless of size and level of modernisation and complexity (Malinowski 1926, 2; Marshall and Johnson 2005). Crime in the contemporary period is commonly reported in both developed and developing societies (Ahonsi-Yakubu 2001). That crime report permeates the global media scene may be linked to the fact that the prescribed social precepts through which social relations are mediated are routinely compromised across cultures.

Described as an act punishable by law (Odekunle 1992) or the breaking of 'prohibiting' laws to which legitimate punishments are attached (Scott and Marshall 2009), crime varies based on period, place, and society (Henry and Lanier 1998). The prevalence, magnitude, and modes in which criminal activities are perpetrated equally differ spatiotemporally (Cahill 2005). Thus, violations of social rules, whether deliberately or otherwise, are liable to sanctions following the dictates of traditions and conventions of different social settings in which they occurred. In other words, variations in criminal behaviours and the associated punishments are culture-specific. Regarding its effects, criminality could be described as antithetical to development as it generally thwarts genuine efforts and plans toward nurturing human progress. Canter and Young (2016) believe that the nature, techniques and volume of criminality are critical to how society and its culture are constructed and reconstructed. The incidence of crime and its rising profile can be closely linked to poverty, unemployment, inflation, illiteracy, lack of education, greed and over-population (Oguntunde et al. 2018; Kunnuji 2016). An escalation of crime increasingly stimulates insecurity in society and destroys the very basis of trust between the state and its human resources. Underscoring the significance of security to human progress, Oyebode (2011) states that "without security, hardly anything is possible." The nexus between crime and insecurity underscores the need for man to routinely appraise and fine-tune the existing crime management strategies or scout for more effective options to attain a more secure existence.

While crime generally constitutes a significant source of grief to an ordered social life, it is not the only factor of insecurity in human existence (Werthes, Heaven and Vollnhals 2011). Over the years, this fact has necessitated a global effort towards arriving at an expanded conceptualisation of "security" from different perspectives. Apart from the anxieties inflicted by acts of criminality, security has been holistically measured by considering man's social, political, economic, and environmental circumstances, including his access to adequate food, income, good

health and environment, essential social services, and other vital elements that make for a secured existence (Adger et al. 2014; Werthes, Heaven and Vollnhals 2011). Expanding the concept to capture Nigeria's situation vividly, Babangida (2012) identified food sufficiency, water supply, power supply, good roads, good schools, good hospitals, functional infrastructure, decent housing, effective public transportation system, etc., as genuine indices for measuring national security. To guarantee adequate security for members of a social group, however, there is a need to entrench positive cultural values and attitudes. Studying the nature, causes, and patterns of crime has been of tremendous value to social existence given that the social, economic, and cultural consequences on society at large cannot be over-emphasised (Oguntunde et al. 2018). From this standpoint, this paper examines the Nigerian state's capacity to realise its developmental aspirations amidst the rising trend of criminality and insecurity. The rationale for this attempt is to underscore the imperativeness and social values of inculcating a culture of security among the populace.

Nigeria's Security Situation: A Review of Extant Literature

The extant literature has shown that human life is generally becoming more precarious by the day as cases of criminality have become commonplace, while all the state security apparatuses seem lacking in capacity to curtail the trend. There is an increasingly high level of uneasiness and apprehension across all regions of Nigeria as communal and ethno-religious clashes, armed robbery, assassination, murder, and gender-based violence have become daily occurrences. As the number of criminals increases with desperation and ruthlessness, their tactics and strategies become more sophisticated (Otto and Ukpere 2012). In the last decade, however, crime volume has increased, and the pattern has varied as new strategies have been devised to carry out criminal machinations. Apart from the usual categorizations such as stealing, armed robbery, rape, fraud, corrupt practices, assassination, religious violence, and other criminal activities that have gained predominance over the years, additional modern concerns include cybercrime, identity theft, hostage taking, kidnapping, ritual killing, and so forth. The already scary security situation has been unfortunately worsened by violent conflicts, resulting in insurgency and terrorist activities. The political angle to Nigeria's drab security situation has also been aggravated by the secessionist agitations of the Movement for Actualization of the Sovereign State of Biafra (MASSOB) and Indigenous People of Biafra (IPOB) in the South-eastern axis, which ruthlessly impose terror on the social, economic and material existence of the ordinary people daily. Of utmost concern, according to the Civil-Military Fusion Centre (2013), is the height of human misery inflicted by the gruesome activities of the agitators, insurgents, and bandits. In recent years, a seeming atmosphere of siege and social tension has engulfed Nigeria's socio-physical space.

The primary responsibility of any state is to care for and protect its people. This core obligation underscores why security attracts the highest priority among the preconditions for human development (Haider 2011; DFID 2010). In effect, the primary purpose of the Nigerian state as enshrined in Section 14, sub-section (2) (b) of the 1999 Constitution of the Federal Republic of Nigeria (as amended) is to secure the lives, properties, and welfare of the people (The Nigerian Constitution, 1999). In recognition of this, successive administrations in Nigeria have focused on human welfare and promoting the sanctity of human life. Nigeria's annual budgetary allocation to the security sector in the last twelve years (shown in Table 1) underscores the burden placed by the need for security on the Nigerian economy. Although large sums are budgeted to cater for the security needs of Nigerians annually, security challenges continue to mount as large chunks of security funds are being diverted for private use (Abiodun, Asaolu and Ndubuisi 2020).

TABLE 1 Budgetary Allocation to the Security Sector from 2012 to 2022

Year	Budget Allocation in Naira
2012	764.19 billion
2013	953 billion
2014	932 billion
2015	969 billion
2016	1.06 trillion
2017	1.14 trillion
2018	1.35 trillion
2019	1.76 trillion
2020	1.78 trillion
2021	22.7 billion
2022	2.41 trillion
2023	2.98 trillion

Source: www.budgetoffice.gov.ng

Apart from the massive federal allocations for defence and internal security, the 36 states and 774 local government areas make budgetary provisions amounting to billions of naira to secure people within their territorial boundaries (Adebakin and Raimi 2012). These figures exclude the whooping sums paid (albeit secretly) in local and foreign currencies as ransom by families, government agencies, private organisations, etc., to secure the releases of individuals held in one form of captivity or another. Added to these are the large sums annually allocated since the 2009 fiscal year to cater for the amnesty initiative aimed at stemming the tide of militancy in the Niger Delta region. These and many other reasons underscore the socio-economic importance of crime and insecurity to human and national development in Nigeria. While it remains a fact that security is *sine qua non* to socio-economic and political progress, the ever-increasing security expenses and related costs constitute serious setbacks to Nigeria's quiescent economy and have particularly weighed down on the country in the pursuit of her developmental aspirations in recent years.

Recently, efforts by the Nigerian government to deter or disrupt potential attacks and strengthen the nation's security apparatuses via the provision of security facilities and broadcast security tips have been noted in the mass media

(Azazi, 2011). Nonetheless, the penchant for criminality in Nigeria remains very high. This phenomenon can be understood from Obafemi Awolowo's statement in Gbenga and Augoye (2011) that "insecurity is a result of a malignant environment dominated by man's insensitivity to man." Thus, a good number of public officeholders in Nigeria have taken advantage of their privileged positions to introduce and implement policies that impoverish the downtrodden and strip them of their right to security while their interests are protected.

On account of the preceding, Nigeria has consistently ranked low in the Global Peace Index (GPI 2012), thus indicating a worsened state of insecurity in the country. For quite a while now, the government's efforts to secure lives and properties in Nigeria have not yielded enough positive results (Adagba et al. 2012; Uhunmwuangho and Aluforo 2011). In confirmation of the worsening crime situation, a particular pattern appears to have also been formed along the geographical subdivisions of the country (Okechukwu and Onyishi 2011). For instance, armed robbery attacks generally used to dominate Nigeria's criminal scene have recently been surpassed by kidnapping and abduction. In the North, cases of cattle rustling, cross-border banditry, and ethno-religious violence have constituted threats to human security, while the problems of hostage-taking and kidnapping are among the criminal activities commonly reported in the South-South and Southeast. The various sources of security threats to Nigeria and their geographical predominance are shown in Table 2. The changing dimension of criminality has made every Nigerian, irrespective of class, status, sex, age, or geographical location, become a potential victim of this despicable and asocial act.

The country's current insecurity situation has led many to wonder if Nigeria has not returned to the Hobbesian state of nature where life was 'nasty, brutish and short with no just law to checkmate human excesses. To further show the criticality of insecurity in Nigeria, Adahi (2011) observed that public functions and gatherings are now held amidst tight security and that the Nigerian government has done far less to secure itself, not to talk of providing adequate security for the populace as enshrined in the 1999 Constitution of the Federal Republic of Nigeria.

TABLE 2 Patterns and Geographical Prevalence of Insecurity in Nigeria as at 2022

S/N	Security Threat	Zonal Prevalence
1	Militancy, Separatist agitation and vandalism	Southeast, South-South, and Southwest
2	Ethno-religious crisis	North West, North Central, Southwest
3	Banditry, Kidnapping, Ritual Killing	All Zones, but prevalent in the Northwest
4	Terrorism and Insurgency	North-East, Northwest, and North–Central
5	Cattle rustling	North-East, North–Central, Northwest
6	Security Sector violence against civilians	All zones
7	Maritime insecurity (Piracy)	Southwest, South-south
8	Herder-farmer related conflicts	Northwest, Northcentral, Southeast, Southwest
9	Armed robbery, criminal gangs	All zones

Source: Adapted from Duerksen (2021) and Africa Centre for Strategic Studies

The atmosphere of insecurity that pervades the nooks and craning of Nigeria has been worsened by the allegations of compromise and conspiracy levied against security personnel, particularly those at the top stratum, commissioned to give security and safety commands. The impact of the resulting feeling of insecurity on the psychic and overall functioning of Nigerian society cannot be overestimated. Given the presently alarming security challenges and uncertainties, a cross-section of the populace has been canvassing for the creation of state police to complement the present 'unitary' policing structure obtainable within the Nigerian federal structure. The seeming ineptness of the central government has propelled the emergence of some regional security outfits in the last two years. For instance, the five states in Southwestern Nigeria have lately established a security network codenamed *Amotekun* (leopard). Similar agencies like *Ebube Agu* (wonderful tiger) and *Shege–ka–Fasa* (I dare you to attack or surrender) have been established in Southeast and Northern Nigeria, respectively. Given this persistent state failure, one may be tempted to question the appropriateness and applicability of the word "society" in the face of the current social quandary. Thus, exploring the nexus between people and the state may be necessary to understand the significance of the state's role in securing people's lives and properties.

Theoretical Explication

Nigeria remains a country characterized by diverse cultural, ethnic, and religious dimensions, which grapples with an alarming rise in security challenges and criminality. Here, we adopt the Social Contract Theory of Thomas Hobbes, John Locke, and Jean Jacque Rousseau in shedding light on the shortcomings of the Nigerian state in safeguarding the security and welfare of its citizens and the reason why the breach in the social contract between the Nigerian state and the people has constituted a challenge to Nigeria's development aspirations.

Specifically, in the past two decades, Nigeria has witnessed an upsurge in criminal activities, spanning communal clashes, armed robbery, terrorism, and insurgency. The complexity of the security landscape is further intensified by ethno-religious tensions, secessionist movements, and the emergence of regional security outfits, causing significant human suffering and emphasizing the pressing need for effective solutions. Thomas Hobbes argued that individuals, in a state of nature, would relinquish certain freedoms for security under a powerful sovereign. In Nigeria, the escalating insecurity signifies a breakdown of this social contract. The government's inability to establish a monopoly on the use of force allows criminal elements to flourish, challenging the Hobbesian contract (Hobbes 1651).

John Locke, on the other hand, emphasized the protection of life, liberty, and property as the fundamental role of government (Locke 1690). The Nigerian state's failure to curb criminality breaches this contract. Inadequate policing, corruption,

and the misallocation of security funds contribute to a lack of protection, infringing on citizens' rights and properties. The Nigerian police force and other security services continue to face challenges of insufficient personnel, outdated equipment, and low motivation. This failure to provide an effective security apparatus violates the social contract's premise of citizens surrendering certain freedoms for protection. The diversion of substantial security funds for private use exacerbates the challenges. Corruption within the security sector undermines the state's ability to fulfil its end of the social contract, as resources intended for protection are misappropriated.

Similar to Locke's thesis, Rousseau's social contract posits that citizens collectively shape the general will, and the state should ensure the common good. In Nigeria, the fragmentation of society and the emergence of regional security outfits reveal a failure to forge a unified general will. Ethnic and regional tensions undermine Rousseau's theorizing, hindering collective security efforts (Rousseau 1762). Nigeria's diverse ethno-religious landscape has led to regional tensions and the formation of independent security outfits. This fragmentation weakens the state's authority, failing to unite citizens under a common goal of security as envisioned in the social contract.

Unsurprisingly, the evolving nature of security threats, such as cybercrime and terrorism among other thriving criminal enterprises, reveals the failure of the Nigerian state to adapt and respond effectively to the bourgeoning security situations in the state. The state's inability to anticipate and address emerging challenges further breaches the social contract, thereby compromising the citizens' security.
It is however clear that Nigeria's security challenges and criminality demonstrate a significant breach of the Social Contract between the state and its people, as popularised by Hobbes, Locke, and Rousseau. The state's failure in areas of policing, resource management, ethno-religious unity, and adaptation to new threats further highlights the urgent need for comprehensive reforms. Addressing these failures is thus crucial to restoring the social contract between the state and the people whilst ensuring the protection and well-being of Nigerian citizens in a unified and secure nation.

Methodology

This paper adopts a qualitative and descriptive research design to delve into the complex dynamics of security issues in Nigeria's underdevelopment problematics. It scrutinizes existing reports, government documents, and academic publications related to crime, insecurity, and development in Nigeria with emphasis on understanding, through the prism of the social contract thesis, the nature, causes, and consequences of criminality and insecurity, as well as the role of the state in the provisioning of security for the people. Thematic analysis is applied in categorising and interpreting the data obtained from documents, and secondary sources. Thus, the aim is to identify recurring themes, patterns, and nuanced understandings of the security challenges and their impact on development.

Discussion of Findings
The State and Security Needs of Citizens

Social thinkers, both classical and modern, have analysed the nature of human society, particularly concerning the relationship between the state and the people it governs. The social contract theory was propounded through the works of intellectual giants like Thomas Hobbes, John Locke, and Jean-Jacques Rousseau. The central thesis of the theory borders on the notion that in the prehistoric era, man had lived in the state of nature where his life was never secure for reasons of inequality in terms of strength and intelligence. In this natural state, no individual was powerful or smart enough that he could not be outwitted by any other. Each person thinks he is capable of achieving whatever he wants. Hence, there was competition over available limited resources, thus leading to the war of all against all. As the social contract theorists pictured, life in the state of nature was generally chaotic, solitary, poor, nasty, brutish, short, and characterised by fear and apprehensions due to man's greed, selfishness, and lack of just law to checkmate human excesses. The desire to escape this natural arrangement and the need for order, self-preservation, and protection led men to surrender individual powers (excluding their rights) to a sovereign authority capable of utilising the same to achieve collective good. The substance of this theory is that the state results from an agreement entered into by men who initially had no governmental organisation (Laskar 2013). In other words, the powers of the state were derived from the people inhabiting it.

The previous explains why Section 14 (2b) of the 1999 Constitution of the Federal Republic of Nigeria has recognised "security, protection, and welfare of the people of Nigeria as the primary purpose of government" (The Nigerian Constitution 1999). For it to realise its aim in this regard, the Nigerian state has established a wide range of security agencies and institutions, including the Nigeria Army (NA), Nigeria Air Force (NAF), Nigeria Navy (NN), Nigeria Police Force (NPF), Department of State Security Service (DSS), Nigeria Immigration Service (NIS), Nigeria Correctional Services, Nigeria Security Agency (NSA), National Drug Law Enforcement Agency (NDLEA), Nigeria Security and Civil Defence Corps (NSCDC) and several others to curb criminality and provide for the security needs of its people. This arrangement validated the social contract between the citizens and the Nigerian State, more so that individual freedom has been relinquished to enthrone higher-order collective safety and security.

Policing to Secure Nigeria: Issues and Challenges

One of the central government agencies in charge of modern society's internal security and safety is the professional police force, with policing being its primary function. In Nigeria, the Police institution is principally in charge of law enforcement and the lead security agency (Wikipedia n.d.). Policing has always been of great

necessity in all societies for safeguarding safety, order, and social relations. The inevitability of policing becomes more evident in modern societies as social life has become characterised by multiplicities and ambiguities arising from population heterogeneity, urbanisation, industrialisation, and conflicting ideologies (Alemika and Chukwuma 2000). Therefore, the place of the Police in security discourses and management cannot be undervalued. Without the Police, creating and maintaining order, legality, and attaining desired social progress may prove very difficult. As earlier noted, the primary responsibility of the Police is policing. By policing, we refer to acts of securing obedience to extant laws and conforming to the precepts of social order. As Alemika and Chukwuma (2000) have reiterated, the importance of the Police is acknowledged and highly recognised. Still, security responsibilities were not placed solely on her if matters of policing in Nigeria were considered holistically. This points to the fact that policing goes beyond training, kitting, and equipping some specialised officers and men to mount vigilance and ward off criminal acts and tendencies. Everyone, including the ordinary man in the neighbourhood, needs to get involved in the policing process for society to be sufficiently secure.

Being a body of individuals assigned by the state to enforce law and order, the emergence of the Police is a recent development in human history (Reiner 2000). The Nigeria Police, in particular, was established in 1930 (Alemika and Chukwuma 2000). The organisation was saddled with the responsibilities of maintaining law and order and preventing criminal behaviour among the citizens of Nigeria. Its roles are vividly captured in the 1999 Constitution of the Federal Republic of Nigeria, where the Nigeria Police are assigned the statutory powers to:

> Investigate crimes, apprehend offenders, interrogate and prosecute suspects, grant bail to suspects pending completion of investigation or before court arraignment, serve summons, and regulate or disperse processions and assemblies. They are also empowered to search and seize properties suspected to be stolen or associated with crime and to take and record, for purposes of identification, the measurements, photographs, and fingerprint impressions of all persons..., in their custody (The Nigerian Constitution, 1999).

Section 4 of the Police Act specifically provides that:

> The (Nigeria) Police shall be employed for the prevention and detection of crime, the apprehension of offenders, the preservation of law and order, the protection of life and property, and the due enforcement of all laws and regulations with which they are charged (FGN 1990).

The above legal provisions place the Nigeria Police at the core of crime prevention and internal security management. In addition, ever since its establishment, the police institution has been contributing its quota towards fulfilling the broad national

security objectives of the Nigerian state. The rising insecurity within Nigerian society has shown that its security management system is grossly inadequate. If the United Nations stipulated standard for an effective policing system is considered, one would understand why the best performance by the Nigerian Police has never been enough, and may never be, to meet the everyday security challenges facing the citizenry unless the requisite attention is accorded to the policing system. Going by the United Nation's (2009) recommendation, a ratio of 1:400 Police per person is required, among other preconditions, for a country to confront security challenges in its jurisdiction amply. By implication, at least one Police should be available to cater to the security needs of 400 persons before any country could reasonably boast of achieving effective crime prevention and management. Personnel deficit, among other essential factors, has contributed significantly to the terrifying security situation in the country today. Nigeria, with an estimated population of over 214.5 million people (World population Review 2022), can boast of having only 371,800 police personnel to manage its internal security (Interpol 2016). Even though it has one of the most considerable police personnel in the world, the current ratio of about one police personnel to six hundred citizens (1:600) is grossly inadequate as it falls below the United Nations' recommendation. Thus, for Nigeria to meet up in her latest efforts to increase the strength of its staff, the country needs to recruit more hands. It is in light of this deficit that one of the erstwhile Inspectors-General of Police has mentioned that the Nigeria Police Force required an additional 155,000 personnel to be able to adequately measure up handling the security issues upsetting the country (Vanguard 2017).

Whether the UN recommended figure is met or not, the capacity of the Police to effectively manage security lies' not entirely on its number but in the spirit of discipline and professionalism that must be built into its daily operations.' Regrettably, everyday encounters of ordinary Nigerians with police personnel or institutions have always generated negative assessments of the Police from significant segments of the Nigerian populace. In several instances, officers and men of the organisation have been accused of complicity in criminal matters. This has been observed to flow from low motivation and professionalism (Alemika and Chukwuma 2000). Additionally, intelligence gathering - a *sine qua none* for efficient and effective policing - is at its lowest ebb. These have created a high distrust between the Police and the masses, regardless of its personnel and equipment sophistication. The ordinary men in the neighbourhoods who may be willing to vouch for information are often suspected and unfairly treated by the Police. All these have discouraged the free flow of information to the Police from willing members of the public. It is also disheartening that the neighbourhood vigilance culture seems non-existent to the extent that people no longer show interest in taking notes of the happenings and wanderings of strange people around them.

Away from the numerical strength of police personnel is the question of the age of the equipment they brandished in most of their engagements. Sources also

indicate that police officers are often low-paid, lacking equipment, and need re-training (Vanguard 2017). Apart from being inadequate, most of their weapons have become outdated. Modern and state-of-the-art equipment needed to facilitate the adequate performance of the Police in combating security challenges facing the Nigerian populace is not available to the Nigeria Police. In the era of internet technology, it is abnormal for basic computer systems to be conspicuously absent in Police stations, let alone officers being computer literate. The gulf between Nigeria's analogue approach and the e-policing system is far apart. Police inefficiency in the maintenance of law and order became glaring as cases of armed robbery involving the use of sophisticated weapons and high casualties, as well as incidences of ethno-religious conflicts, persisted in the country.

State Security Apparatuses and Security Management

Because of the shortfall in public policing, governments in Nigeria have had reasons to engage the Nigerian military deeply, along with other state security apparatuses like the DSS and NSCDC, to complement the efforts of the Nigeria Police in internal security management. While substantiating this claim, Muhammed Abubakar, the GOC of the 2nd Mechanized Division in Ibadan, quoted in Albert (2012), reported that the Nigerian Army was directly supporting the Police to maintain security operations in 33 out of the 36 states of the Nigerian Federation. Hardly is there any state in Nigeria today where the military is not involved in providing internal security. Despite the enormous support offered by the military and large chunks of the nation's resources sunk into the security sector, Nigeria's security situation remains precarious. However, it berates rational judgment to blame the growing insecurity in Nigeria entirely on the Nigerian Police and other supporting security institutions. This is against the backdrop of the facts gathered through studies on the political economy of police operations, which established that no agency or institution could function outside the dictates of its social, economic, political, and cultural environments. In other words, all the state security agencies in the country are just sub-sets of the more extensive Nigerian social system. As a result, the imperfections emanating from Nigeria as a nation having its distinct peculiarities are bound to be reflected in the operations of its security institutions. For instance, despite the shortfall in Nigeria's police per person ratio, services of the Police appear to be for the highest bidders- the elite, as the police officers are quite often assigned to guard the homes of the influential, government buildings, and act as bodyguards for critical public officials (Marenin 1985) and traditional rulers. Such practices teach the rank and file of the Police who needs protection and who does not, who is entitled to police services, and whose demand can be rejected (Alemika and Chukwuma 2000). Ibrahim Coomassie, a former Inspector-General of the Nigeria Police Force, once decried that:

> "… any time a citizen becomes a public figure, his first official correspondence on assuming duty is to write the Inspector-General

> of Police to ask for an orderly and policemen to guard his house… Everybody wants to use the Police as a status symbol. Yet, members of the organisation remain without accommodation, adequate remuneration, tools to work with, transport to patrol, effective communication, and appropriate intelligence outfits to support their operations (Coomassie 1998, 10).

The above underscored that the political, economic, social, and cultural precepts obtained within the Nigerian society are affecting the capacities of its security agencies, particularly the Police, to prevent criminal activities effectively. It is, therefore, self-evident that this pattern of police service delivery persists until now and reflects the economic and political hierarchies in the country.

Since independence, the cumulative experience in Nigeria also demonstrates a linkage between socio-political and economic crises and insecurity. Okechukwu and Onyishi (2011) rightly observed that insecurity has manifested in Nigeria in various forms. While some have emerged via the nation's chaotic political process, others came through ethnic bigotry and religious fanatism. Economic factors have also accounted for the currently biting insecurity situation. Many crises have erupted from struggles among a large army of able-bodied but unemployed Nigerian youths over the distribution or re-distribution of national resources.

Towards a Bottom-top Approach to Security Problems in Nigeria

Culture as an attribute of a social group evolves over time. For any group to develop or imbibe a specific culture, members need to be socialised or re-socialised in the context of the norms and values available in the cultural milieu. To develop a security culture, Nigerians must be appropriately socialised or re-oriented towards achieving the larger objectives of securing lives and property in Nigeria. For instance, with the nature and current level of criminality at the community level in Nigeria, not many people care any longer to seek information about friends and next-door neighbours regarding what they do and where they do it. Also, fewer numbers (if any) have taken time to keep some security alert numbers as made available to the public through various media channels. In addition, many parents do not deem it necessary to instruct or monitor children to be watchful of or monitor all happenings within their immediate environments.

As earlier noted, adult members of society must change their orientations *vis-a-vis* the security of their respective communities. The lingering indifferent attitude must be discarded for a warm embrace of a security-inclined attitude. Keener attention needs to be paid to some taken-for-granted, but security-enhancing dispositions.

For example, people need to be vigilant about movements and events around them and be mindful of the implications of such happenings for personal and community safety. Beyond this, people must be informally trained to avoid revealing personal information to prospective afflicters. Closely related to this is the fact that people need to refrain from discussing personal affairs in public spaces, physical or virtual. Knowledge about police-community relations and the roles of security agents must be deepened. Adult members could be taken through semi-formal classes explicitly focusing on the basic tenets of community security and safety. People of proven integrity should be recruited into committees where security issues would be discussed. Vigilance and alertness on the part of homeowners and other stakeholders regarding the suitability of individuals for membership would help. Even though security matters should be the business of all, attendees at security meetings must, for security reasons, keep security discussions secret.

There is great wisdom in gaining access to the official phone numbers of the security units covering the immediate neighbourhoods or access lines to Police control rooms to alert them when the need arises. Sadly, not many have considered it a necessity to have those important phone numbers on their mobile phones. As a demonstration of sheer lag in security culture, many do not care about these numbers, probably to show their disbelief (or distrust) in the nation's security system.

Perhaps due to negligence, absent-mindedness, pride, or over-westernisation, many find it difficult to recall the details and identities of their valuables and personal effects in cases of burglary or theft. Individuals might need to start paying attention to these details to reduce the chances of losing them totally in cases of attacks. Besides, people must memorise the mobile numbers of close relations or colleagues. These may be useful in cases of distress or emergencies. Driving requires extra vigilance to be secured against the dangers of other reckless road users. This is in addition to being safety and security compliant anytime they are on the wheel.

Parents must be watchful of who their children socialise with. They must always voice out on strange behaviours or items noticed with their children or wards. The benefits offered by the internet and mobile technological revolution are irresistible, while its abuses are also colossal. The positive opportunities must be utilised to reinforce the security network among family members and the community. At home, children could be given helpful security instructions such as some parents instructing their children/wards "not to talk to strangers." This will probably prevent them from being kidnappers, child abusers or paedophiles. As we ride with them in cars, they could be encouraged to take notes of strange events as they drive along.
Security and safety culture can also be entrenched in the school curriculum to traverse the levels of our educational system. Basic tips on pro-security habits could be introduced at the primary and secondary levels. At the same time, courses on safety and security should be developed and incorporated into the general studies

curriculum across Nigeria's higher institutions. The National Youth Service Corps (NYSC) training programmes could also be reviewed and expanded to include more intensive and compulsory military service for a certain minimum number of years. The Turkish Compulsory Basic Military Training (IFOR 2021) and the Israeli Compulsory Military Service (Itsik 2020; Moshe 2004) can be adapted to evolve a more robust and sustainable security policy for Nigeria. It needs to be clarified that it is not until Nigeria is transformed into a police society that it can sufficiently secure its people. There is no gainsaying the fact that Nigeria, going by its population, occupies an important position in Africa and the entire black race. Therefore, it needs a correspondingly strong and formidable security system to remain a rallying point within the continent. The central idea is that the success stories recorded in other climes concerning security management can be shared and adapted to improve Nigeria's security situation.

Conclusion

Environments inundated with crime and insecurity are always permeated with tension and anxiety. That prompted Tagba (2011 cited in Otto and Ukpere 2012) to conclude that an insecure environment impinges directly on development; it disenfranchises communities, contributes to poverty, distorts economies, creates instability, and stunts political development. In Nigeria, apart from the thousands of people who had been killed in the course of one security breach or another, sources of livelihood have been destroyed, families have disintegrated, and social infrastructure has been disrupted (Otto and Ukpere 2012). Efforts to reduce insecurity should not only top the government agenda but should be complemented by actions. However, the discourse on Nigeria's security situation so far has revealed that some factors are limiting the capacity of the Nigerian state to secure its citizens adequately. Given this reality, combating crime should not be left to the Nigerian government alone. However, the fact remains that if the government is collecting taxes, fines, dues, and other financial entitlements and manages all the resources accruable to the state, it owes the citizens the responsibility of securing their lives and property as enshrined in the 1999 Constitution of the Federal Republic of Nigeria.

Nonetheless, it should be noted that even where state resources are effectively managed, citizens still support government security initiatives. Barrett's philosophical axiom quoted in Albert (2012) can guide individuals to their security responsibilities. As Barret suggests, "When it comes to getting things done, we need fewer architects and more bricklayers". As a way out of the current security challenges dazing Nigeria and Nigerians, it is of great essence for people to be conscious of security at individual and collective levels.

References

Abiodun, T.F., A. Asaolu and A.I. Ndubuisi. 2020. "Defence Budget and Military Spending on war against Terror and Insecurity in Nigeria: implications for state politics, economy, and national security." *International Journal of Advanced Academic Research (Social and Management Sciences)* 6 (7): 12-34. doi:10.46654/ij.24889849.s6713.

Abubakar, A. 2004. "The Challenges of Security in Nigeria." A Paper presented at the NIPSS, Kuru.

Adagba, O., Ugwu, S. C. and Eme, O. I. (2012). Activities of Boko Haram and Insecurity Question in Nigeria, Arabian Journal of Business and Management Review, Vol. 1 (No.9): 77-99.

Adahi, R. 2011. "Insecurity in Nigeria: What Hope for the Common Man?" *Leadership* p. 31.

Adebakin, M.A. and Raimi, L. (2012). National Security Challenges and Sustainable Economic Development: Evidence from Nigeria. Journal of Studies in Social Sciences, 1, 10-20.

Adger, W.N., J.M. Pulhin, J. Barnett, G.D. Dabelko, G.K. Hovelsrud, M. Levy, Ú. Oswald Spring and C.H. Vogel. 2014. "Human security. In Climate Change 2014: Impacts, Adaptation, and Vulnerability." In *Global and Sectoral Aspects: Contribution of Working Group II to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change. Part A*, by C.B. Field, V.R. Barros, D.J. Dokken, K.J. Mach, M.D. Mastrandrea, T.E. Bilir, M. Chatterjee, et al., pp. 755-791. Cambridge University Press, Cambridge, United Kingdom and New York, NY, USA.

Ahonsi-Yakubu, A. 2001. "Political Transitions, Crime and Insecurity in Nigeria." *Africa Development* Vol.XXVI (Nos. 1&2): pp.73-98.

Albert, A.O. 2012. *Explaining Security Challenges in Contemporary Nigeria.*

Alemika, E.E.O. and I.C. Chukwuma. 2000. *Analysis of Police and Policing in Nigeria.* A desk study on the role of policing as a barrier to change or driver of change in Nigeria, prepared for the Department for international development (DFID), Lagos: Cleen Foundation.

Azazi, A. (2011). Responding to the Emerging Trends of Terrorism in Nigeria, 5th Policing Executive Forum Conference Proceedings organized by CLEEN Foundation.

Babangida, M.A. 2012. "The search for national security in Nigeria: Challenges and prospects." A paper presentation at ObafemiAwolowo Institute of Government and Public Policy, Agip Recital Hall, Muson-Lagos. http://www.nigerstate.gov.ng/articles/the-search-for-national-security-in-nigeria-challenges-and-prospects.html.

Cahill, M.E. 2005. "Geographies of Urban Crime: An Intra-urban Study of Crime in Nashville, TN; Portland, OR; and Tucson, AZ." An Unpublished research report submitted to the US Department of Justice.

Carter, D. and D. Youngs. 2016. "Crime and Society." *Contemporary Social Science* 11 (4): 283-288. doi:10.1080/21582041.2016.1259495.

Central Bank of Nigeria. 2011. *Annual Report. Functional Classification of Federal Government Expenditure in Nigeria.* Nigeria: CBN Publication.

Coomassie, I.A. 1998. "The Wind of Change in the Nigeria Police Force in ." In *Police, Law and Order in Nigeria*, by Elo Amucheazi and D. O. P. Sanomi (eds.). Abuja: National Orientation Agency.

Copeland, F. 2013. "The Boko Haram Insurgency in Nigeria." *Civil-military Fusion Centre.* www.cimicweb.org.

DFID. 2010. "The Politics of Poverty: Elites, Citizens and States. Findings from ten years of DFID-funded research on Governance and Fragile States 2001–2010. A Synthesis Paper." https://www.oecd.org/derec/unitedkingdom/48688822.pdf.

FGN [Federal Government of Nigeria]. 1999. *1999 Constitution of the Federal Republic of Nigeria and Fundamental Rights Enforcement Procedure Rules.*

—. 1990. *Police Act, CAP 359 of the Laws of the Federation of Nigeria.*

—. 2008. *Police Service Commission Retreat.*

Gbenga, A.G. and J. Augoye. 2011. "'Ibru', Astute Businessman takes a Bow." *The Punch* p.3.

Green, David G., E. Grove and E N.A. Martin. 2005. *Crime and Civil Society: Can We Become A More Law-Abiding People?* London: Institute for the Study of Civil Society.

Haider, H. 2011. "State-Society Relations and Citizenship in Situations of Conflict and Fragility." *Governance and Social Development Resource Centre* (University of Birmingham) 1-23.

Henry, S. and M.M. Lanier. 1998. "The Prism of Crime: The Arguments for an Integrated Definition of Crime." *Justice Quarterly* 15 (4): 609-627.

Hobbes, T. 1651. *Leviathan.*

Ibrahim, J. and O. Igbuzor. 2002. "Memorandum submitted to the Presidential Committee on National Security in Nigeria." *Justice Quarterly* 15 (4): 609-627.

IFOR [International Fellowship of Reconciliation]. 2021. "Conscientious Objection to Military Service and Related Issues." A Submission to the 132nd Session of the Human Rights Committee, Turkey. https://tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/TUR/INT_CCPR_ICS_TUR_44947_E.pdf.

Institute for Economics and Peace. 2012. Global Peace Index 2012: Measuring the State of Global Peace. http://www.economicsandpeace.org/wp-content/uploads/2015/06/2012-Global-Peace-Index-Report.pdf.

Interpol. 2016. *Nigeria/Africa/Member Countries/Internet/Home—INTERPOL.* https://www.interpol.int/.

Itsik, R. 2020. "Compulsory Military Service as a Social Integrator." *Security and Defence Quarterly* 30 (3): 65-80. https://doi.org/10.35467/sdq/124710.

Jegede, S.B. 2011. "Back to State of Nature? ." *The National Scholar* 8 (2): 30.

Kunnuji, M. 2016. "Population density and armed robbery in Nigeria: an analysis of variation across states." *African Journal of Criminology and Justice Studies* 9 (1): art. 5. https://digitalscholarship.tsu.edu/ajcjs/vol9/iss1/5.

Laskar, M.E. (2013). Summary of Social Contract Theory by Hobbes, Locke and Rousseau. https://ssrn.com/abstract=2410525; http://dx.doi.org/10.2139/ssrn.2410525.

Locke, J. 1690. *Second Treatise of Government.*

Malinowski, B. (1926). *Crime and custom in savage society.* Harcourt Brace.

Marenin, O. 1985. "Policing Nigeria: Control and Autonomy in the Exercise of coercion." *African Studies Review* 28 (1): 73-93. https://doi.org/10.2307/524568.

Marshall, B. and S. Johnson. 2005. *Crime in Rural Areas: A Review of the Literature for the Rural Evidence Research Centre.* University College London: Jill Dando Institute of Crime Science, 1-57.

Maslow, A.H. 1943. "Theory of Human Motivation." *Psychological Review* 50 (4): 370-396.

Moshe, S. 2004. "National Service in Israel: Motivations, Volunteer Characteristics, and Levels of Content." *Nonprofit and Voluntary Sector Quarterly* 33 (1): 94-108. doi:10.1177/0899764003260659.

The Nigerian Constitution. 1999. Constitution of the Federal Republic of Nigeria (as Amended). Federal Government Printer, Abuja.

Odekunle, F. 1992. "Security and Development in Africa: Socio-Economic Prerequisites at the Grassroots Level." In *Africa Rise to Challenge*, edited by Olusegun Obasanjo and Felix Mosha. Sango-Ota: Africa Leadership forum.

Oguntunde, P.E., O.O. Ojo, H.I. Okagbue and O.A. Oguntunde. 2018. "Analysis of selected crime data in Nigeria." *Data in Brief* (19): 1242–1249. https://doi.org/10.1016/j.dib.2018.05.143.

Okechukwu, E.I. and A. Onyishi. 2011. "The Challenges of Insecurity in Nigeria: A Thematic Exposition." *Interdisciplinary Journal of Contemporary Research in Business* 3 (8): 172-185.

Otto, G. and W.I. Ukpere. 2012. "National security and development in Nigeria." *African Journal of Business Management* 6 (23): 6765-6770.

Oyebode, A. 2011. "The Imperative of Security." *The National Scholar* 8 (2): 27-29.

Plant, J.B. and M.S. Scott. 2008. *Effective Policing and Crime Prevention: A Problem-Oriented Guide for Mayors, City Managers, and County Executives.* Washington DC: Centre for Problem-Oriented Policing Inc.

Reiner, R. 2000. *The Politics of the Police.* London: Oxford University Press.

Ritzer, G. 2008. *Sociological Theory.* 7th ed. New York: McGraw-Hill.

Rousseau, J.J. 1762. *The Social Contract.*

Scott, J. and G. Marshall. 2009. *A Dictionary of Sociology (3rd ed.).* Oxford University Press. https://www.oxfordreference.com/view/10.1093/acref/9780199533008.001.0001/acref-9780199533008-e-441.

United Nations. 2009. *United Nations Criminal Justice Standards for United Nations Police.* New York. https://www.unodc.org/pdf/criminal_justice/UN_criminal_justice_standards_for_UN_police.pdf.

Uhunmwuangho, S.O. and Aluforo, E. (2011) Challenges and Solutions to Ethno-Religious Conflicts in Nigeria: Case Study of the Jos Crises, Journal of Sustainable Development in Africa, Volume 13, No.5, 109-124.

Vanguard. 2017. *55,000 Additional Personnel Required to adequately police Nigeria – I-G.* https://www.vanguardngr.com/2017/05/155000-additional-personnel-required-adequately-police-nigeria-g/.

Weber, M. 1968. *Economy and Society.* University of California Press.

Werthes, S., C. Heaven and S. Vollnhals. 2011. *Assessing Human Insecurity Worldwide: The Way to A Human (In)Security Index.* University of Duisburg-Essen: Institute for Development and Peace, INEF-Report 102/2011.

Wikipedia. n.d. *The Nigeria Police Force.* https://en.wikipedia.org/wiki/Nigeria_Police_Force.

World population Review. 2022. *The Nigerian Population 2022 (live).* https://worldpopulationreview.com/countries/nigeria-population.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

The theory of the regional security complex — Case study, the riparian states of the Black Sea

Adrian GHENADE, MSc. Candidate*
Elena ONU, Ph.D. Student**
*"Mihai Viteazul" National Intelligence Academy, Bucharest, Romania
e-mail: ghenadeadrian@yahoo.com
**National University of Political Studies and Public Administration, Bucharest, Romania
e-mail: e.tudor37@yahoo.com

Abstract

Known in Antiquity as the Pontus Euxinus, the Black Sea has been the bridge between European and Eastern civilizations since ancient times. Possessing a multi-varied mosaic of cultures, the Black Sea area has facilitated over the centuries, both the development of commercial and political relations and the maintenance and production of conflicts, being like the Sword of Damocles. Located at the intersection of three security zones (Euro-Atlantic, Russian, and Eastern), the Black Sea is currently a vulnerable space in terms of security. Heir to Byzantine culture, most of the riparian states have a complicated internal and external policy, being caught between the idealism of the Western world and the realism of the Eastern European space. At the same time, the revisionism of the Russian Federation and Turkey in terms of foreign policy will also mean a change in the dynamics of the relations between the states bordering the Black Sea, which could result either in its return to the status of a Russian lake or in a division of the spheres of influence between the Russian Federation and Turkey. In this sense, in order to analyze the future security dynamics of the riparian states, we used the theory of the regional security complex, which we consider very appropriate in our study of the Black Sea region.

Keywords:
Black Sea; security complex theory; poststructuralism; Copenhagen School; NATO; security.

Article info
Received: 9 February 2024; Revised: 29 February 2024; Accepted: 18 March 2024; Available online: 5 April 2024

Citation: Ghenade, A. and E. Onu. 2024. "The theory of the regional security complex — Case study, the riparian states of the Black Sea". *Bulletin of "Carol I" National Defence University*, 13(1): 212-222. https://doi.org/10.53477/2284-9378-24-14

The birth of the regional security complex approach

The context of the period of the 80'-90' is marked by a paradigm shift regarding the approach and understanding of the study of international relations and security relations. The new current of thought is not totally antithetical to the traditionalist current, coming more as a complement to this one. Thus, if the traditionalist current of thought associates military problems (hard power) as representing the only real threat to the survival of states, the non-traditionalist current of thought will consider that security problems are of a military, economic, social, societal, and ecological nature. In this sense, non-traditionalists offer a level of analysis that is inclusive at the level of society and even individuals and not just at the level of states. The approach is in full accordance with the new reality characteristic of the end of the Cold War, being marked by the neoliberal and idealist current, in which the emphasis will be placed more on the individual than on the state. Also, the non-traditionalists will analyze security by level, these being national, regional, international/global/systemic. One of the main thinkers of the new non-traditionalist trend and also the pioneer of the new trend is Barry Buzan, a British professor of political science at LSE. In the work People, States and Fear: National Security Problem in International Relations, since 1983, he criticizes the traditional conception of security, coming to formulate the main elements of the future approach of the Copenhagen school, including the idea that the state and society are the two objects security references. In this paper, Barry Buzan will also enunciate a new derivative concept of security, the security complex, which will constitute a new understanding of relations between states in terms of security at the regional level.

The security complex represents the existence of a group of countries with lasting, significant, and intrinsic characteristics of security problems. In this set of states, the major security perceptions are so interrelated that their national security issues cannot be rationally analyzed and solved without reference to the other states. The dynamics of the formation and its structure are determined by the states within it, more precisely by the perspectives of the states towards security and the interactions between the states. The security complex belongs to the postmodernism current, a current that emphasizes primarily the social component in the analysis of security, the approach being one of a multisectoral nature (Buzan 1983, 105-110). The international system is formed by several security complexes, many of them overlapping or intersecting with each other. These can be of several types: geographical, political, strategic, historic, economic, and cultural, and some security complexes can possess several characteristics or even all of them. Based on the postmodernist current, the analysis of security by referring to the security complex is made at the regional level, even if the complex sometimes includes states from outside the region. The logic of security regions is based on the fact that international security is a matter of relationships. International security is about how human communities relate to each other when it comes to threats and vulnerabilities, even as it sometimes refers to how these communities relate to threats from the natural

environment. The emphasis on the relational nature of security is in line with writings on security studies that have emphasized relational dynamics such as security dilemmas, balance of power, arms races, and security regimes. For a group of states to be considered a security complex, it must have a distinctive territorial pattern of interdependence that distinguishes members of a security complex from other neighboring states. Regional security complexes cannot exist under 2 conditions: in some areas, local states have such a low capacity that their power projects little or not at all beyond their own borders. These states have inward-looking security perspectives, and between them, there is no security interaction large enough to generate a local complex. The direct presence of external powers is so great that it suppresses the security dynamics between local states - this state is also called cover (exp. Colonialism, European security dynamics during the Cold War, USA-USSR rivalry). For a group of states to be able to constitute a security complex, it must meet the following structure and all conditions must be met cumulatively: 1) the arrangement of the units in the same geographical space and the existence of some differences between them; 2) the existence of friendship or enmity patterns and 3) the distribution of power between the principals (Buzan 1983, 110-115).

At the conceptual level, there are two types of regional complexes: the homogeneous (classical ones, stated for the first time in the work People, States and Fear: National Security Problem in International Relations, from 1983 by Barry Buzan) and the heterogeneous ones (which preserve the characteristics of the classical complexes, but they are complemented by the economic, financial, social, cultural, societal spectrum, being stated in the work Regions and Powers: The Structure of International Security from 2003, by Barry Buzan in collaboration with Ole Waever).

The classical theory of the security complex

The rationale behind it is that for most actors at the unit level, politico-military security falls into medium-sized bundles, and the most relevant theory is the one that relates to the regional level. Also, the classical theory of security complexes asserts the existence of regional subsystems as objects of security analysis and provides an analytical framework for working with these systems. The theory focuses primarily on the state as the key unit and the political and military sectors. All states in the system are interconnected in a fabric of security interdependence. The pattern of interdependence in a geographically diverse but also anarchic international system is based on regional clusters, which we call security complexes. Security interdependence is obviously more intense between states within such complexes than between states outside them. Security complexes refer to the relative intensity of interstate security relations that form distinct regional patterns, shaped both by the distribution of power and by historic relations of friendship or enmity. As they are formed by local groupings of states, not only do classical security complexes have a central role in the relations between their members; they actually

condition centrally, if at all, how external powers penetrate the region. The external dynamics of security complexes can be located along a spectrum depending on what defines security interdependence: amity or enmity. At the opposite pole is the emergence of conflicts where interdependence is born out of mutual fear, rivalry, and threat perception. In the middle, there are security regimes, in which states treat each other as potential enemies, in which they have entered into assurance agreements with the aim of reducing the security dilemma between them. At the positive end of the spectrum is a pluralistic security community in which states no longer expect or prepare for the use of force in their relations. Regional integration will eliminate a security complex with the same boundaries, transforming it from an anarchic subsystem of states into a single larger actor within the system. The regional integration of the members of a complex will transform the power structure of that complex. The security complex is a product of the anarchic system (Buzan 1983, 93-95). Since the power dynamics are very solid and friendship/enemy relations are constantly changing, there are 4 structural options for evaluating the impact on a regional complex of security: maintaining the status quo, international transformation, external transformation, and coverage. The theory of the regional security complex can be used to generate definitive scenarios and to structure the study and predictions related to the possibilities of change and stability (Buzan 1983, 113-115). After the Cold War, international relations acquired a more regionalized character. As regions are a special type of subsystem, Hans Mourizen argues that states are more fixed than mobile. At the security level, regions have the following characteristics: they consist of two or more states forming a cohesive geographical unit, and the relations between these states are marked by security interdependence, which can be either positive or negative.

Security Complex Theory - Black Sea Case Study After the Annexation of the Crimean Peninsula by the Russian Federation

In terms of security, the Black Sea region is an unsafe area, where three security zones overlap: European, Eurasian, and Islamic, this determines both the existence of hostile relations and the existence of alliances based on friendship between the riparian states (Cojocaru 2014, 23). Being a commercial space since Antiquity, the Black Sea region was primarily a transit space for different peoples, a fact that will fully mark the history of this region through the multicultural and ethnic mosaic created. Taken as a whole, although the diversity of a region often means an increase in creativity and tolerance among the surrounding populations, it seems that in the case of the Black Sea region, the principle of the sword of Damocles applies; this region has been marked by conflicts for almost its entire history between the riparian states. From the Russo-Ottoman wars to the current invasion of Ukraine by Russia, the Black Sea area has almost always been a politically and militarily unstable area, preferring war to trade. Thus, it can be explained that although it holds approximately

between 70 and 200 billion barrels of oil (an amount greater than the reserves of the North Sea and Alaska combined, which turns the region into the second area in the world in terms of energy potential for the West), the Black Sea region, due to unstable security, does not fully enjoy its economic potential (Cojocaru 2014, 25). Thus arises the question "What determines this instability of the region?" An answer to this question is the fact that the states bordering the Black Sea (Russia, Turkey, Ukraine, Romania, Bulgaria, and Georgia) are in a regional complex of security. As I said above, the existence of any regional security complex is determined by the cumulative fulfillment of 3 conditions, which the Black Sea riparian states fulfill. The arrangement of the units in the same geographical space and the existence of some differences between them: the states in the Black Sea region are in the same geographical area, being located in the eastern region of Europe, having direct access to the Black Sea. Also, although they are in the same geographical proximity, at the state level the differences between them are substantial in terms of culture, ethnicity, language, and, in some cases, even religion. Due to these substantial differences found at the level of the states, each country bordering the Black Sea has its own specificity that makes it totally different from the other surrounding countries, making it difficult to achieve uniformity in terms of zonal specificity.

The existence of patterns of friendship or enmity: the Black Sea region was/is the space of clash between Russians and Turks. Since the time of Peter the Great, the Russians have wanted to turn the Black Sea into a Russian lake, the only obstacle to achieving this goal being the Ottoman Empire. Thus, from 1683 until now, Russia and Turkey have constantly disputed their influence over the Black Sea, an extremely important geostrategic area for the achievement of the expansionist foreign policy of both powers. Also, another conflict was between Romania and Bulgaria. As a result of the Berlin Congress of 1878, Romania obtained access to the Black Sea following the ceding of Dobrogea by Bulgaria. Thus, the new border between the two young states represented a reason for a long conflict, both entities until 1945 being in separate camps, both in the two Balkan Wars and both World Wars. At the same time, even when in the Black Sea region there was a pattern of friendship between states, in which 5 of the 6 riparian states were part of a common alliance, the Warsaw Pact (USSR- Russia, Ukraine, and currently Georgia, Romania, and Bulgaria), there were misunderstandings of a territorial nature, Romania ceding Snake Island to Ukraine in 1948, a fact that created tensions among the allies. Although in 2009 the Hague Tribunal recognized 79.34% of the island's territory as Romania's (the rest belonging to Ukraine), both states still have much greater claims to this territory, with disputes continuing even to this day. Also, another pattern of enmity is between Russia and Georgia.

At the beginning of 2000, Russia adopted a new concept at the level of foreign policy and geostrategic framework, declaring itself to be a great power (Smith 2020, 7). Also, by adopting this concept, Russia will show its first signs of revisionism, suggesting that intervention in frozen post-Soviet conflicts (both those in the Black Sea area

and those in neighboring areas) is justified in accordance with its status. This led to the first revisionist tendencies on the part of Russia. In 2004, Georgia, due to its geographical position on the Black Sea, represented a new gateway for Black Sea oil, allowing the installation of pipelines that could bypass the Russian Federation. To the economic reasons we can also add Georgia's desire to be part of the European Union and NATO, organizations that would have allowed it a substantial detachment from its status as a former Soviet socialist republic. Therefore, in 2008, Russia intervened directly in the war in Georgia, and as a result, Abkhazia and South Ossetia declared their independence, an act that is currently recognized internationally only by the Russian Federation. (Cojocaru 2014, 110-112), Nicaragua, and Syria (Curtifan 2018).

Although all past conflicts have had a substantial influence on the Black Sea region, the conflict between Russia and Ukraine has truly had the greatest impact on the region. We will address this conflict later, as I will devote a special section to it in this essay. Distribution of power between the main units: each country bordering the Black Sea has a say in the area's security policies. However, in relation to the distribution of power, at present, the Black Sea has two main actors – Russia and Turkey, which were recently joined by Ukraine. In this sense, we can say that Russia currently has the advantage of the hard power component, through the military capabilities it has in the area, a fact also proven by the constant aggressive policy it practices. Turkey, due to its control over the two straits (Bosphorus and Dardanelles) essential for the connection with the Mediterranean Sea, thus implicitly owns the main economic and commercial area of the Black Sea, a fact that gives it a much more complex advantage over Russia, being stronger in terms of the smart component, Turkey having the opportunity to combine the economic and military components.

On the other hand, Ukraine until the Crimean conflict had the soft advantage of the Black Sea region, with most oil companies with foreign capital located in Ukraine's commercial zone, which is also the most attractive area for foreign investments. A relevant example in this sense is represented by the Skifska company, owned by the British-Dutch corporation Royal Dutch Shell, which in 2012 obtained the right to drill for oil starting in 2015 (unfortunately, the initiative will be abandoned as a result of the Crimean War). Also, until the annexation of Crimea by the Russian Federation, Ukraine had the advantage of having the largest port on the Black Sea, Sevastopol being both the largest port and the most strategically positioned, being a bridgehead connection with the Mediterranean Sea, the Sea of Azov, the Maghreb area and even the Middle East (Cojocaru 2014, 74-75). Thus, we can note that at the level of the Black Sea region, the distribution of power was relatively balanced and no actor could dominate everyone else. We also note that all the necessary conditions for the existence of a regional security complex in the Black Sea area were met simultaneously, which proves the existence of such a complex. Moreover, using the counterexample method, we note that including the 2 limitations that would not have allowed the formation of a security complex (the inability of states to project their power outside their own borders, respectively the

existence of an external power so great that it suppresses the dynamics of security between local states) are not possible for the Black Sea region. First, the region has actors capable of projecting their power beyond its borders. Taking the case of the Russian Federation again, we can see that through the Great Power concept used in its foreign policy, it is able to project its military capabilities outside its own borders, in this sense maintaining a series of frozen conflicts in its former satellite states, but also outside the European continent (the war in Syria, the year 2015). Also, in 2015, Russia adopted a new Naval Doctrine, which offered the Black Sea both a significant defensive and offensive, respectively economic, tactic. On the defensive level, the Naval Doctrine viewed the Black Sea as an essential means of blocking NATO expansion and the deployment of military capabilities near Russia's borders (Davis 2015, 10-11). By annexing Crimea (also called a Black Sea aircraft carrier), on an offensive level, Russia managed to gain control and influence over the communication routes of the entire Black Sea aquarium, from East to West. The extremely good position of Crimea at the geopolitical and geostrategic level allowed the sending of Russian troops within the conflagration in Syria, demonstrating Russia's ability to create pressure on the southern flank of NATO, North Africa, the Middle East, but also an access route secondary to the Planetary Ocean. Another riparian state that can project its power outside its borders is Turkey, which constitutes the second-largest NATO army (Dinu 2020, 7-9). Also, for the Black Sea region, there is no external power so great as to be able to suppress the dynamics of security among local states. Although we would be tempted to state that NATO (and implicitly, the United States), represents a factor that can definitively limit the dynamics of security among the riparian states, this did not happen entirely. Although 3/6 riparian states are NATO members, and 2 states have pro-Western views (Ukraine and Georgia), NATO and implicitly the US have limited military capabilities for acting in this region.

However, on March 16, 2023, the Chairman of the Permanent Select Committee on Intelligence of the House of Representatives, Mike Turner, together with Congressman Bill Keating, the ranking member of the Foreign Affairs Subcommittee of the House of Representatives for Europe introduced the Maritime Security Act for approval with the aim to stop the expansion of conflicts at the level of the Black Sea; being perceived as a matter of security for the United States, this has substantial limitations of a legal nature (The Senate of the United States 2023). According to the Montreux Convention of 1936, warships of states that do not have direct access to the Black Sea must not exceed a tonnage of 15,000 tons and cannot remain for more than 21 days in these waters. Under these conditions, with Russia and Turkey as the dominant actors, it is almost impossible for an external power to radically change the dynamics between riparian states better than a riparian state (Britannica 1936). Thus, regardless of the type of political-military alliance in which the states around the Black Sea find themselves, the main power that will be held in the region will be projected only by the riparian states.

The security complex in the Black Sea as a result of the conflict in the Black Sea

As I have demonstrated through previous arguments, the Black Sea region constitutes and facilitates the existence of a security complex. Currently, Russia is the main actor in the area that constantly maintains hostile relations with the rest of the riparian states, the most recent conflict being the one with Ukraine. Russia and Ukraine share a millennial history, the relationship between the two states being marked by constant conflicts and alliances. At the level of common elements for the two peoples, we can see that they have a common geographical origin (Kiev being the city of "birth" of both kingdoms), they have been part of the same political unit for almost 70 years (USSR) and have had Orthodox Christianity as a common identity element. Despite the similarities, throughout history, the two countries seem to have shared more differences than friendships. In this sense, we can recall the fact that Ukraine was part of the Grand Duchy of Lithuania (Polish-Lithuanian Union), a kingdom that over time had direct conflicts with both Tsarist and Imperial Russia. The fact that Ukraine was part of the Polish-Lithuanian Union will also be found in the national character of the Ukrainians, who consider themselves a different people from the Russians. At the same time, probably the most important constitutive element of a people's identity, language, is very different between the two nations as Ukrainian has a vocabulary consisting of 55% of words of Polish origin, being more similar to this language than to Russian.

At the cultural level, there are also substantial differences between the two peoples, sharing quite different traditions and values. Thus, we can see that both peoples have a sufficiently different national identity, thus theoretically allowing them to evolve in separate directions from the point of view of the political, economic, and social points of view. As a result of the collapse of the USSR in 1991, Russia and Ukraine would once again become two separate entities at the political, economic, and social levels that sought to form their own policy, both internally and externally. In terms of security, in the last decade of the 20th century, the Black Sea region was extremely stable. Except for Transnistria, no conflict took place, and the relations between the states were only economic. The first relevant sign of a desire to change Ukraine and break away from the influence of the CIS states came in 2004, during the Orange Revolution when thousands of Ukrainians marched for better integration into Europe. Another moment when Ukraine's growing distance from the Russian Federation was observed was at the NATO Summit in Bucharest, in 2008, when Ukraine conveyed to the international community its clear desire to join NATO. All these actions culminated in 2014 with the first armed conflict after almost a century between the two countries, with Russia's annexation of the Crimean Peninsula. At the level of the security complex, the annexation of Crimea by Russia marked a renunciation of the status quo within the region which is about 70 years old. Also, by annexing Crimea, Russia considerably increased its tactical and geostrategic advantage in the region, since by annexing Crimea (also called a Black Sea aircraft

carrier), it managed to gain control and influence over the communication routes on the entire Sea Aquarium Black, from East to West. The extremely good position of Crimea at the geopolitical and geostrategic level allowed the sending of Russian troops within the conflagration in Syria, demonstrating Russia's ability to create pressure on the southern flank of NATO, North Africa, the Middle East, but also a secondary access route to the Planetary Ocean. Thus, by annexing Crimea, Russia managed to transform the security complex of the Black Sea externally, by changing its structure (Dinu 2020, 10-11).

Moving on to the present, we can see that the war in Ukraine has once again altered the dynamics of the current Black Sea regional security complex. Although they are traditional adversaries in the region, Russia and Turkey now seem more eager to avoid starting a conflict with each other. Also, the aggression in Ukraine brings Romania and Bulgaria closer to each other, their security region also being the security spectrum of NATO and the European Union. Yet, as I said above, NATO's military capabilities for the Black Sea area are limited by the provisions of the Montreux Convention, a fact that produces a vulnerability in terms of security in the event of the subsequent degeneration of the conflict. Also, another sensitive area in the current context is Georgia, which, after having suffered as a result of the separatism produced in 2008, currently presents multiple vulnerabilities in the face of a possible escalation of the conflict, being a potential direct victim of a possible Russian revisionism (South Ossetia and Abkhazia). In this sense, concern for the national security of Georgia has already been shown by NATO, Romania together with the UK holding the NATO Contact Point Embassy mandate in Georgia for a period of 2 years. The fact that a Black Sea riparian country holds such a mandate in the current conflict in another country shows certain concern about a further generation of this conflict. At the level of the current War in Ukraine, Kyiv tried to consolidate its main strategic arteries from the Black Sea. In this sense, it was sought to defend the port of Odesa, through an extensive process of de-Russification. At the same time, since the beginning of the conflict, Ukraine sank the Moscow ship - one of Russia's main warships, also managing to gain a significant tactical advantage in this conflict.

As I said at the beginning, the security complex theory can also be used to generate scenarios for certain conflicts. In this sense, I believe that in the case of the two main belligerents, Russia and Ukraine, the role of the Black Sea takes on a double meaning, since for Russia it means hegemony, while for Ukraine it means survival. Many experts believe that "whoever controls or dominates the Black Sea can easily project power over the European continent, mainly in the Balkans and Central Europe, but also in the eastern Mediterranean, the South Caucasus and the Northern Middle East. Thus, a possible victory of Russia in the conflict will allow it to have increasing chances to transform the Black Sea into a "Russian lake", a fact that also allows it to return to the ambition from the time of Peter the Great to have access to the Mediterranean Sea, having the real possibility of modifying the Regime of the

Straits, thus imposing its total dominance over the Black Sea. On the other hand, a potential Ukrainian victory would likely mark a return to the status quo specific to the region, by restoring the same pre-conflict spheres of influence. Also, a potential accession of Ukraine to NATO would mark an increase in the influence of the North Atlantic Alliance in the region, a fact that would probably also allow a modification of the provisions of the Montreux Convention.

As I said at the beginning of the paper, in the Black Sea region 3 security areas are intertwined: European, Eurasian, and Islamic. At present, Turkey is the only country that is crossed by all these demarcations, being the smart power actor in this region. The re-election of Recep Erdogan as president will mean a resumption of his neo-Ottoman policies, evidenced by his desire to make Turkey an important player in the Middle East and implicitly in the Islamic world. An important role in this scenario will be played by the current "reacquisition" of Nagorno-Karabakh by Azerbaijan, a traditional partner of Turkey. Thus, the regional security complex would be extended including to the Near East area, a fact that would determine its expansion and the inclusion of new actors. Moreover, Russia's weakening of its support for Armenia will cause Yerevan to look elsewhere for security alliances, including the US, France, India, and Georgia, but also to reconsider its continued participation in the Collective Security Treaty Organization (CSTO), which is under the influence of Moscow. Although Russia has two military bases in Armenia that are designated to deal with the southern or Caucasus external sector and its surroundings and Armenian Prime Minister Nikol Pashinyan has allowed Russia to expand its military influence in his region, despite the role Moscow in Nagorno-Karabakh, a possible reorientation of Armenia to the US would lead to the accession of this country to the Georgia-Ukraine security sub-complex. This fact would increase the security vulnerability of all the riparian states, at the same time increasing the dynamics of relations between them. I believe that this scenario would be possible in the event of the enormous weakening of Russia and Ukraine as a result of this conflict, followed by a possible implosion of Russia and its division into several states, respectively zones of influence, as well as a Ukraine that after the war would not benefit from a reconstruction and would not be welcomed into the European Union or NATO.

Conclusions

We can affirm that the theory of the regional security complex is a useful tool for the geopolitical and geostrategic realities of the 21st century, helping us to observe how it is formed and how conflicts take place in different geographical regions of the world, being one of the theories that allow us to be able to generate certain scenarios about their further evolution. Also, although it was developed in the previous century and improved in 2003, it continues to be a topical subject, given the fact that it emphasizes the social component as well as the financial, economic, and societal sectors, being an extremely complex theory. Based on the above analysis, we

can note that the theory respects the new reality of the post-Cold War international system through the prism of the fact that regions are currently the main dynamics in terms of friendship/conflict, as evidenced by the majority of ongoing conflicts. Thus, based on it, we can identify those areas on the globe that present the necessary characteristics to constitute a regional security complex, thus being able to create certain commercial and economic blocs that help the development of certain regions and implicitly strengthen security. Alternatively, we can identify those regions that present the risk of generating a potential regional conflict with certain likely consequences materialized in the loss of human lives and goods, the aim being to reduce it or perhaps even avoid it.

References

Britannica. 1936. „Montreux Convention." https://www.britannica.com/event/Montreux-Convention.

Buzan, Barry. 1983. *People, States and Fear: National Security Problem in International Relations.* Marea Britanie: Wheatsheaf books Ltd.

Cojocaru, Marius George. 2014. *NATO și Marea Neagră.* Târgoviște: Cetatea de Scaun.

Curtifan, Tudor. 2018. „Abhazia și Osetia de Sud, recunoscute de Siria. Georgia, replică imediată." https://www.defenseromania.ro/abhazia-i-osetia-de-sud-recunoscute-de-siria-georgia-replica-imediata_591759.html#google_vignette.

Davis, Anna. 2015. „The 2015 Maritime Doctrine of the Russian Federation." *U.S. Naval War College Digital Commons*, 10-11.

Dinu, Leonardo. 2020. "The Crimean Aircraft Carrier. RUSSIAN FEDERATION MILITARIZATION OF THE BLACK SEA." *New Strategy Center.* https://www.newstrategycenter.ro/wp-content/uploads/2019/11/FLANKS-Policy-Brief-The-Crimean-Aircraft-Carrier.-Russian-Federation-Militarization-of-the-Black-Sea.pdf.

Smith, Dr.M.A. 2020. *Russian Foreign Policy 2000: The Near Abroad.* Camberley, Anglia: The Conflict Studies Research Centre.

The Senate of the United States. 2023. „S.804 – Black Sea Security Act of 2023." To provide for security in the Black Sea region, and for other purposes. https://www.congress.gov/bill/118th-congress/senate-bill/804/text.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

The service life of military constructions from the heritage of the Romanian Ministry of National Defense: between efficiency and adaptability

Captain Architect Adina SEGAL, Ph.D. Student*

*Domain and Infrastructure Directorate, Romanian Ministry of National Defense;
Ph.D. student in architecture, Ion Mincu University of Architecture
and Urban Planning, Bucharest, Romania
e-mail: segaladina@gmail.com

Abstract

Romania's military infrastructure has undergone significant transformations over time. Periods of expansion and modernization have alternated with phases of reduction and, sometimes, the transfer of barracks into civilian administration. These changes reflect not just technological advancements but also the adaptation to the dynamic requirements of national defense.

The 2008 infrastructure regulations link the employment duration of military facilities directly to military activity, highlighting the need for a flexible and adaptable infrastructure. In this context, the article examines the legislative framework regarding the amortization of investments, the wear and tear of constructions, and the authorization of works, emphasizing the importance of aligning military regulations with civil ones.

In conclusion, the article analyzes the discrepancies between national legislation and military regulations, suggesting revisions and additions to the existing regulations, particularly regarding temporary and semi-permanent facilities, to meet the current and future needs of national defense more effectively.

Keywords:
Defense Infrastructure; Military Constructions; Barracks;
Construction Legislation; Military Regulations.

Article info
Received: 12 February 2024; Revised: 29 February 2024; Accepted: 18 March 2024; Available online: 5 April 2024

Citation: Segal, A. 2024. "The service life of military constructions from the heritage of the Romanian Ministry of National Defense: between efficiency and adaptability". *Bulletin of "Carol I" National Defence University*, 13(1): 223-235. https://doi.org/10.53477/2284-9378-24-15

Romania's military infrastructure has undergone significant transformations over time, evolving alongside the emergence and development of the permanent army. This evolution reflects not only technological and architectural changes but also adaptations to the ever-changing tactical and operational requirements. In this context, the usage duration of military constructions is a critical aspect. This article explores how the life expectancy of military buildings, influenced by technical standards and operational requirements, shapes strategies for developing army infrastructure, emphasizing the importance of balancing investment efficiency and the adaptability of military structures to meet the evolving needs of national defense.

1. The evolution of military infrastructure

The evolution of military infrastructure in Romania has been a process of continuous adaptation to the strategic needs of the army, alternating between periods of expansion and modernization and those of reduction and conversion of facilities for civilian use.

The evolution of the Romanian military infrastructure began with the adaptation of existing structures, such as inns, to meet the immediate operational needs of the army. The limitations of these improvised facilities quickly led to the need for the development of specialized military constructions. The first barracks, built under the influence of experts from the Tsarist army in a multifunctional system, were essential for the initial stage of military infrastructure development. After the Unification of the Romanian Principalities, an increase in the number of military units marked a turning point in the development of military infrastructure. This period was characterized by the transition to a pavilion system in the design of barracks and the introduction of the *"Regulamentul casarmelor (Barracks code)"*, representing an important step in the standardization and modernization of military constructions (Herjeu 1902, 193-308).

This trend of expansion and modernization continued during the periods of the two world wars. During World War I, most barracks were occupied by enemy forces, necessitating their rehabilitation and expansion after the war. In the period of World War II, investments in permanent constructions doubled, reflecting the ongoing need for expansion and modernization of military infrastructure.

At the end of 1952, in the context of deteriorating international relations, the Romanian army began building new barracks and fortification works. However, in 1958, the withdrawal of Soviet troops freed a large part of the military infrastructure, which then passed into civilian administration.

The modernization of existing infrastructure was a continuous process, and a new stage followed in 1968 when, following the occupation of Czechoslovakia by Warsaw Pact troops, Romania intensified investments for the modernization and expansion of barracks to strengthen the army's combat capacity. In contrast, after 1989, political

and economic transformations led to a major restructuring of the army, with significant effects on infrastructure: between 1995 and 2006, many barracks were transferred to civilian administration as a result of the abandonment of compulsory military service (Petrișor 2011, 93).

In conclusion, the history of Romanian military infrastructure illustrates constant adaptation to the army's requirements and a balance between the need for modernization and efficiency. These dynamics underscore the importance of a strategic approach in defining the life expectancy and use of military constructions for the efficient management of military infrastructure.

2. Life expectancy of military constructions

Regarding the life expectancy of military constructions, military regulations, aligned with civilian standards since the 1960s, have established standards that reflect both the purpose of the buildings and the materials used. Regulatory revisions in 2008 introduced a new perspective, linking life expectancy directly to military activity and emphasizing the need for a flexible and adaptable infrastructure.

Regulamentul proprietății imobiliare în Ministerul Apărării Naționale[1] *(The Real Estate Code for the Property of the Ministry of National Defense)* provides a basis for understanding and addressing the life expectancy of constructions in the military context, classifying military facilities into four categories: initial, temporary, semi-permanent, and permanent. Initial facilities, exemplified by tents used by the Romanian army, are temporary and relocatable structures, intended for short-term use, usually no more than six months, in scenarios such as military exercises or emergency situations. They offer austere conditions, being quick and easy to assemble and disassemble. In contrast, temporary facilities, which include improved tents and modular container constructions with temporary foundations, are designed for use over a longer duration, up to 5 years, offering improved living conditions, with access to utilities such as electricity and water. Semi-permanent facilities, made from more durable materials like steel or prefabricated composite walls, are designed to be used between 5 and 25 years, representing an optimal medium-term solution. They are quicker to execute than permanent constructions and, according to the code, must be able to adapt to meet changing requirements over time. On the other hand, permanent facilities represent the most durable solution, being fixed and definitive constructions, designed for special or representative functions and are suitable for long-term use.

[1] Adopted by Order no. M.91 dated September 12, 2008, approving the *Regulamentului proprietății imobiliare în Ministerul Apărării Naționale* (Regulation on Real Estate Property in the Ministry of National Defense) and updated by Order no. DDI-13 issued by the Head of the Directorate of Domains and Infrastructure on June 17, 2022, approving the *Regulamentului proprietății imobiliare în Ministerul Apărării Naționale* (Regulation on Real Estate Property in the Ministry of National Defense).

This classification, first introduced in the *Regulamentului proprietății imobiliare* of 2008, introduces in military regulations the life expectancy of temporary constructions and, a new concept for Romanian construction legislation, semi-permanent constructions. Adopting new notions also used in the regulations of the United States Department of Defense (DoD)[2] represents a step towards modernizing military constructions, however, since these provisions have not been fully correlated with national construction legislation, the application of this new conceptual structure regarding the life expectancy of constructions in a military context remains at the stage of intention.

Military buildings are subject to both specific military regulations and national construction legislation. In the field of construction, life expectancy is determined by 3 parameters: the lifespan established by authorization, the designed life expectancy depending on wear and tear, and the operating duration for the purpose of investment amortization. Therefore, to correlate military regulations with civilian ones, it is necessary to clarify the legal framework and define terms such as operating duration, existence duration, or life expectancy.

2.1. Amortization of the Real Estate Investment

The planned economy of the communist era assumed the existence of norms regarding the life expectancy of each type of building for the calculation of investment amortization and the planning of repair works. These regulations, which also applied to military constructions, classified buildings based on their intended use and the nature of the materials from which they were made, and specified the frequency and cost of maintenance and major repair works. Starting from 1975, *Normele tehnice de cazare (The Technical Standards for Accommodation)* included a nomenclature of buildings and special constructions in which the standard operating duration of each type of building was specified based on its purpose and the nature of the materials used, including norms for maintenance and major repairs (Colban 1998, 30). The standard operating duration began from the date the building was put into operation and represented the depreciation period to which the planning of major repairs in terms of frequency and value was related. This standard operated until its replacement in 2008 with regulations that separately addressed maintenance and current repairs[3] and the domain and infrastructure norms[4].

In the new regulations, the classification and standard operating durations for constructions belonging to the Ministry of Defence are established as the maximum duration specified in the *Catalogul privind clasificarea și duratele normale de funcționare a mijloacelor fixe (The Catalog Regarding the Classification and Standard Operating Durations of Fixed Assets)* approved by Government Decision No. 2.139 of November 30, 2004.

[2] UFC 1-201-01, Non-permanent DOD facilities in support of military operations: Temporary construction level: This level involves buildings and facilities designed and constructed for a life expectancy of up to five years; Semi-permanent construction level: The buildings and facilities at this level are designed for a life expectancy of under 10 years, but with proper maintenance and repairs, this can be extended to up to 25 years.

[3] *Normele tehnice pentru lucrări de întreținere și reparații curente la clădirile și construcțiile speciale din patrimoniul imobiliar al Ministerului Apărării* (The Technical Standards for Maintenance and Current Repairs Works on Buildings and Special Constructions from the Real Estate Heritage of the Ministry of Defense), approved by Order no. M.44 dated May 9, 2008, and updated by Order no. DDI-4 issued by the Head of the Directorate of Domains and Infrastructure on April 14, 2020, approving the *Norme tehnice pentru lucrări de întreținere și reparații curente la clădirile și construcțiile speciale din patrimoniul imobiliar al Ministerului Apărări* (Technical Standards for Maintenance and Current Repairs Works on Buildings and Special Constructions from the Real Estate Heritage)

[4] *Normele tehnice de domenii și infrastructure* (The Technical Standards for Domains and Infrastructure), approved by Order no. M. 45 dated May 9, 2008, and updated by Order no. DDI-12 issued by the Head of the Directorate of Domains and Infrastructure on April 13, 2022, approving the *Normelor tehnice de domenii și infrastructuri* (Technical Standards for Domains and Infrastructure).

This classification approved in 2004 updates the provisions of *Hotărârea nr. 964/1998* for the approval of *Clasificației și a duratelor normale de funcționare a mijloacelor fixe (The Classification and Standard Operating Durations of Assets)* that represented a paradigm shift and aligned Romania with international trends, simplifying the classification of depreciable tangible assets by reducing the number of groups and classes. Starting from 1998, in this classification, the material from which a building is made is no longer considered an essential criterion. Instead, a modern, performance-based approach is adopted, which requires that each asset fulfill a specific function for a predetermined operating period, regardless of the material used in its manufacture. For example, a building for administrative purposes, regardless of the materials it is made of, must operate between 40 and 60 years to amortize the investment. According to *Hotărârea Guvernului nr. 2.139 din 30 noiembrie 2004* for the approval of *Catalogului privind clasificarea și duratele normale de funcționare a mijloacelor fixe*, specific norms for classifying and determining the normal operating durations will be established for constructions that are part of the national defense, public order, and national security system. These norms will be developed by the authorized authorities within the defense system and approved by the Ministry of Public Finance, thus ensuring an approach adapted to this specific sector.

The relevance of this duration of depreciation is reflected in the administration of barracks since, according to the *Regulamentul proprietății imobiliare în Ministerul Apărării*, the demolition of constructions is carried out only after the approval of their decommissioning, and the decommissioning of constructions before the completion of the standard usage duration[5] is administratively investigated[6]. In exceptional situations, fixed assets can be decommissioned before reaching the standard usage duration, based on technical expertise, if they show advanced physical wear and the continuation of their use becomes dangerous or economically inefficient.[7]

In conclusion, the general system for classifying the operating durations of fixed assets does not detail the particular requirements of military infrastructure. To adequately respond to the distinct needs of the national defense system's infrastructure, ensuring the necessary flexibility and adaptability, the development of specific standards that define the normal operating durations for temporary and semi-permanent facilities would be appropriate.

In the context of the regulations of the Ministry of Defence, the standard operating duration of constructions is stipulated both in the *Normele tehnice de domenii și infrastructuri* and in the *Normele tehnice pentru lucrări de întreținere și reparații curente la clădirile și construcțiile speciale din patrimoniul Ministerului Apărării (The Technical Standards for Maintenance*

[5] The normal usage duration is synonymous with the normal operating duration, in *Normele tehnice pentru lucrări de întreținere și reparații curente* (The Technical Standards for Maintenance and Current Repairs) the expression " normal usage duration / operating" is used.
[6] Article 56.
[7] *Instrucțiunile privind scoaterea din funcțiune și casarea activelor fixe, precum și declasarea și casarea bunurilor materiale, altele decât activele fixe, în Ministerul Apărării Naționale* (Instructions regarding the decommissioning and disposal of fixed assets, as well as the declassification and disposal of material goods other than fixed assets, within the Ministry of National Defense), approved by Order No. M.92 of September 16, 2013.

and Current Repairs Works of Buildings and Special Constructions belonging to the Ministry of Defense). To eliminate redundancies *Normele tehnice pentru lucrări de întreținere și reparații curente* could include the normal operating durations for temporary and semi-permanent facilities, while the *Normele tehnice de domenii și infrastructuri* could merely refer to the comprehensive document, thus optimizing the coherence and efficiency of the legislative framework in the field of military infrastructure.

2.2. Construction Degradation Over Time

The Government decision *Hotărârea nr. 1.276 din 22 decembrie 2021 privind modificarea anexei la Hotărârea Guvernului nr. 2.139/2004 for the approval of the Catalogului privind clasificarea și duratele normale de funcționare a mijloacelor fixe* specifies that for establishing the classification and normal operating periods of the fixed assets specific to the national defense system, the technical-economic parameters established by designers and manufacturers through the manuals or technical documentations of the respective fixed assets will be taken into account, as well as the effects of moral depreciation. Viewed in terms of wear over time, the standardized service life of buildings or construction elements and related installations is defined within the context of several civil and military regulations.

The usage duration is shorter than the physical life span of the construction. The standard *GE 032-97 privind executarea lucrărilor de întreținere și reparații la clădiri și construcții speciale (Execution of Maintenance and Repair Works on Buildings and Special Constructions)* defines the life expectancy of a construction, also adopted in the *Normele tehnice pentru lucrări de întreținere și reparații curente la clădirile și construcțiile speciale*, as "*the period after which the construction or construction element ceases definitively to fulfill the function for which it was created*". This standard presents in Annex 1 the life expectancy of buildings and special constructions in normal environmental conditions as well as the life expectancy for construction elements and installations that make up the buildings in Annex 2. Life expectancy underlines a final point in the life cycle of the structure or its component elements, a moment when they are no longer efficiently used for the initially established purpose. The life expectancy of the construction is ensured through maintenance and repair works and even extended through rehabilitation and modernization works. Thus, over the life cycle of the building, a designed life expectancy as well as a standard operating duration are defined.

The designed life expectancy *is the duration estimated by the designer*[8] for which a structure or part of it is used for the intended purpose without the need for major repairs, provided that maintenance works are ensured[9].

The standard operating duration[10] is determined taking into account the techno-economic duration established by the designer and manufacturer

[8] SR EN 15978:2012 Sustainability of construction works – Assessment of environmental performance of buildings – Calculation method.

[9] Design code. Foundations of construction design CR 0-2012, 1.3.1 Design terminology.

[10] *Normele tehnice pentru lucrări de întreținere și reparații curente la clădirile și construcțiile speciale din patrimoniul imobiliar al Ministerului Apărării* (Technical norms for maintenance and repair works on buildings and special constructions from the real estate assets of the Ministry of National Defense), approved by Order No. M44 of May 9, 2008, Annex 1 Glossary, point 6.

through technical documentation, as well as the effects of wear over time. This duration coincides with the amortization period[11].

[11] GE 032-97 Standard regarding the execution of maintenance and repair works on buildings and special constructions.

In conclusion, the life expectancy of a construction extends beyond the amortization period, i.e., the standard operating duration, but over the life cycle of the building, repair, and rehabilitation works will be carried out with a frequency given by the projected life expectancy, which relates to the wear of the component materials.
Analyzing the characteristics of temporary and semi-permanent military facilities considering this conclusion, the need arises to adapt the technical solutions of building to the operating duration, namely choosing materials whose cost relative to wear over time justifies their use for a limited operating duration of 5-10 years and respectively 10 to 25 years.

2.3. Authorization of the Construction Works

Another aspect of the proposed classification based on the duration of use is the utilization of temporary constructions for providing initial and temporary facilities, while definitive constructions are executed for semi-permanent and permanent facilities.
Regardless of the materials they are made of, temporary constructions have a limited life duration, as established in the building permit. Following the conclusion of the period specified in the permit, these constructions are dismantled and the land returned to its initial state, according to the obligations imposed by the permit.

Temporary constructions are characterized by their greater flexibility compared to permanent ones, as they are not subject to the same rigorous technical standards. This particularity allows for greater adaptability in terms of material selection and equipment, such as thermal insulation or utility connections, depending on specific requirements and costs. Serving temporary purposes or meeting fluctuating needs, these constructions provide a quick and efficient solution for infrastructure without requiring long-term investments in costly materials or technologies. Additionally, according to the legislation regarding construction works authorization, temporary constructions are subject to the same authorization conditions as permanent ones, but with a simplified procedure based on reduced technical documentation presented in Annex 2 of the *Normele Metodologice de aplicare a Legii nr. 50/1991 privind autorizarea executării lucrărilor de construcții*.

However, neither national legislation nor military regulations specifically address temporary military facilities, which leaves room for ambiguities regarding the minimum standards that must be ensured and the documentation necessary for the authorization of construction works. One document that could be used as a model is the American army's standard for

non-permanent facilities, UFC 1-201-01, which specifies, in addition to a definition for the typologies of non-permanent facilities, the situations in which they are used, what standards must be ensured and what documentation must be presented for their authorization.

2.4. Changing a building's intended use

Buildings are consistently affected by changes over time in the organization of military units' activities. Altering the purpose of a building may entail significant modifications to its conditions of use, and depending on the degree of adaptation required and the resources available for implementing these changes, they can directly impact the duration of the building's use. (Parker 2016, 134). While in some cases, repurposing a building may extend its lifespan to better serve the operational and strategic needs of the military, in others, it might lead to decommissioning if the necessary adjustments are not economically feasible.

The four categories of facilities outlined in the *Regulamentul proprietății imobiliare în Ministerul Apărării Naționale* (Regulation on Real Estate Property in the Ministry of National Defense) — initial, temporary, semi-permanent, and permanent — are classified based on their construction complexity (moral wear and projected lifespan) and duration of use (authorized existence duration, depreciation period, operational lifespan). Moreover, underscoring the flexible and adaptable nature of military infrastructure, the Regulation specifies that the architecture of the semi-permanent facilities' must ensure "the possibility of compartmentalization /redistribution / remodeling of spaces within these constructions or their partial reconstruction, with minimal expenses, for easy adaptation to new requirements in the future."

A proactive approach from the planning stage can ensure a flexible solution aimed at maximizing the efficiency and durability of military infrastructure in line with evolving operational requirements. Strategies adopted for adapting constructions to different purposes include the use of modular architecture or buildings with open plans (Schmidt 2016, 84). Modular constructions are characterized by flexibility and adaptability to changing needs, as they can be reconfigured or expanded based on operational requirements. Made from containers, they are mobile solutions that can be easily transported, deployed, dismantled, and reused elsewhere. This is the most commonly used technical solution for providing temporary facilities. Another strategy for maximizing efficiency and durability is the use of pavilions with open plans. These buildings can be adapted for various functions, from offices and conference rooms to maintenance workshops or physical training spaces, allowing for the reconfiguration of interior space as needed.

The ability of these constructions to adapt over time by changing their purpose raises issues regarding their classification for depreciation purposes, as the *Catalogul privind clasificarea și duratele normale de funcționare a mijloacelor fixe* (Catalog of Classification and Normal Operating Durations of Fixed Assets) considers the

buildings' intended use. The lifespan of these constructions is influenced by their projected duration and material wear, which considers the established military perspective of 5-10 years for temporary ones and 10-25 years for semi-permanent ones. In conclusion, specific norms from the Ministry of National Defense are necessary to establish the depreciation period of these constructions.

2.4. Adaptable military constructions

The Romanian military infrastructure has undergone significant evolution in the past 20 years, adapting to the requirements and challenges of the current security environment. A notable change is the adoption of new construction typologies characterized by adaptability. Among these are modular container constructions and buildings with structural elements made of corrugated sheet metal. These construction solutions represent a rapid response that allows the army to adjust its infrastructure according to the specific dynamics of the military domain.

Figure 1 Cincu urban training facility modules (SMFT 2022)

Figure 2 Container type (Cabine and Containere, n.d.)

Mobile modular container constructions represent prefabricated structures the size of a transport container, adapted as functional spaces for various purposes, such as offices, warehouses, or medical units. These constructions are characterized by their ability to be easily transported, assembled, and disassembled, offering flexibility and adaptability in diverse contexts and needs. The flexibility of modular container constructions lies in their capacity to rapidly and efficiently adapt to various functions and requirements, through the modular reconfiguration and extension of structures, in a cost-effective and environmentally friendly manner, ensuring the ability to quickly respond to fluctuating operational demands.

According to the *Regulamentul proprietății imobiliare* (MApN Real Estate Property Regulation), the use of relocatable constructions does not entail the approval stages required for real estate investments, with simplified approval representing an additional advantage as the construction process is expedited. However, the use of these constructions also presents several disadvantages, including limited comfort, poor thermal and sound insulation, and spatial limitations. In most cases, without significant technical efforts, these constructions do not meet the energy efficiency criterion imposed on permanent constructions or semi-permanent facilities, limiting

their use generally to the duration specified in the regulation of 5-10 years, which is correlated with the technical solution for these types of structures, with a projected lifespan of around 10 years.
Considering that the use of these container modules covers a wide range of functions, for establishing the depreciation period, we propose defining a new class of constructions dedicated to these types of structures, whose period of use is related to the projected lifespan and material wear and tear, respectively operational military constructions with a duration of use of 10 years.

Figure 3 Corrugated Sheet Structural Elements
(Agenția media a armatei 2019)

Figure 4 Corrugated Sheet Pavilions
(Agenția media a armatei 2022)

Buildings with corrugated sheet structural elements are constructed modularly, allowing for expansion and reconfiguration according to requirements through project design. Their production involves manufacturing the sheet structural elements, which are then assembled on-site to form the final structure of the building. These constructions are internally insulated, ensuring along with interior installations (electrical, thermal, sanitary) the specific thermal efficiency and comfort of permanent constructions.
Implemented through the army's own structures, the deployment of these buildings is based on technical execution projects prepared by field specialists and verified by certified project validators according to current regulations.

In Romanian military bases, buildings with corrugated sheet structural elements are used for sheltering and maintenance of aircraft, storage, or as dispensaries, sports fields, to meet the food, rest, or hygiene needs of military personnel. Moreover, the adaptability and flexibility in use due to the open plan ensure the possibility of reconfiguration and reuse for different purposes and successive functions.

As a result, the lifespan of constructions is not defined by their initial purpose but rather by the projected duration, determined by material wear and maintenance level. To clarify this issue, we propose defining a new class of constructions dedicated to these types of structures, whose service life should be based on the projected duration and material wear, namely adaptable military constructions with a service life of 25 years.

Conclusions

Modular container constructions and those made with corrugated sheet structural elements offer a high degree of adaptability and flexibility in use, allowing for reconfiguration and use for various purposes and functions, such as office spaces, storage, or maintenance workshops. However, their ability to adapt to multiple destinations leaves room for interpretation in establishing the amortization period, as they do not fit into the existing categories in the *Catalogului privind clasificarea și duratele normale de funcționare a mijloacelor fixe* (Catalog regarding the classification and normal operating durations of fixed assets) or are not correlated with the operating durations specified in military regulations.

The introduction of modern construction typologies has brought opportunities for the modernization of existing infrastructure but also challenges in coordinating national construction legislation with new military infrastructure regulations. Regarding the duration of use of constructions within the Ministry of Defence regulations, the general system of classification of operating durations of fixed assets does not fully meet the specific requirements of military infrastructure. Therefore, specific standards need to be developed to define appropriate operating durations for temporary and semi-permanent facilities, taking into account the specific needs of national defense and the necessity of infrastructure flexibility and adaptability. For these facilities, from the perspective of construction wear over time, standardizing already tested technical solutions that justify their cost in relation to operating duration of 5-10 years for temporary ones and 10-25 years for semi-permanent ones is opportune. Also, national legislation and military regulations do not specifically address the authorization of temporary military construction works, leaving room for ambiguities regarding the necessary standards and documentation. The US Army Regulation UFC 1-201-01 provides a useful model for addressing these issues, thus establishing standards and documentation required for non-permanent facilities.

In conclusion, addressing the differences between national legislation and military regulations is necessary to ensure the efficiency of the Romanian military infrastructure in its current and future context. For the development of norms that complement existing regulations and provide a clear basis for establishing the duration of use in the military context of modular container constructions and those made with corrugated sheet structural elements, as well as other construction typologies to ensure semi-temporary facilities, the elaboration of regulations specifying the following is opportune:

- Construction typologies and technical solutions;
- Minimum technical standard regarding insulation level, fire protection, and operational safety;
- The technical documentation required for the building permit and who is responsible for its elaboration (especially clarifying the content of the technical documentation accompanying the container module set);

- Type of fixed asset (military equipment or construction) and duration of use for establishing the amortization duration.

Additionally, to ensure an efficient response in terms of duration and costs, this regulation should be accompanied by a catalog of standard projects, already tested and optimized solutions, for providing various facilities in the military bases through the use of modular, prefabricated constructions, or generic plan constructions such as buildings with corrugated sheet structural elements.

References

Agenția media a armatei. 2019. „Ziduri reci, cu suflet la temelie." http://presamil.ro/ziduri-reci-cu-suflet-la-temelie/.

—. 2022. „Cine mai are grijă de patrimoniul armatei?" http://presamil.ro/cine-mai-grija-de-patrimoniul-armatei/.

Cabine and Containere. n.d. „Cabina sector militar." Accessed 20 february 2024. https://www.cabine-containere.ro/cabina-sector-militar/.

Colban, Gh. C. 1998. *Elemente de Legislație În Construcții Și Asigurare Tehnico-Materială de Cazare.* București: Editura Academiei Tehnice Militare.

Departamentul Apărării al Statelor Unite ale Americii. 2022. „Facilități nepermanente ale DOD în sprijinul operațiilor militare." UFC 1-201-01. https://www.wbdg.org/FFC/DOD/UFC/ufc_1_201_01_2022_c4.pdf.

Direcția domenii și infrastructuri. 2020. „Dispoziția șefului Direcției domenii și infrastructuri nr. DDI-4, din 14 aprilie 2020 pentru aprobarea Normelor tehnice pentru lucrări de întreținere și reparații curente la clădirile și construcțiile speciale din patrimoniul imobiliar al Ministerului." Accesat prin aplicația Lexmil din rețeaua INTRAMAN la 17 martie 2023.

—. 2022a. „Dispoziția nr. DDI-13, din 17 iunie 2022 pentru aprobarea Regulamentului proprietății imobiliare în Ministerul Apărării Naționale." Accesat prin aplicația Lexmil din rețeaua INTRAMAN la 17 martie 2023.

—. 2022b. „Dispoziția șefului Direcției domenii și infrastructuri nr. DDI-12, din 13 aprilie 2022 pentru aprobarea Normelor tehnice de domenii și infrastructuri." Accesat prin aplicația Lexmil din rețeaua INTRAMAN la 17 martie 2023.

Guvernul României. 1994. „Ordin nr. 746, din 9 iunie 1994 pentru aprobarea Normelor metodologice de aplicare a Legii nr. 15/1994 privind amortizarea capitalului imobilizat în active corporale și necorporale." *Monitorul Oficial*, nr. 180. 15 iulie 1994. https://legislatie.just.ro/Public/DetaliiDocumentAfis/5317.

—. 1998. „Hotărârea nr. 964, din 23 decembrie 1998 pentru aprobarea clasificației și a duratelor normale de funcționare a mijloacelor fixe." *Monitorul Oficial*, nr. 520. 30 decembrie 1998. https://legislatie.just.ro/Public/DetaliiDocumentAfis/16651.

—. 2004. „Hotărârea nr. 2139, din 30 noiembrie 2004 pentru aprobarea Catalogului privind clasificarea și duratele normale de funcționare a mijloacelor fixe." *Monitorul Oficial*, nr. 46. 13 ianuarie 2005. https://legislatie.just.ro/Public/DetaliiDocumentAfis/58613.

Herjeu, C. 1902. *Istoria Armei Geniului.* București: I.V. Socecu.

Ministerul Apărării Naționale. 2008a. „Ordinul nr. M. 45, din 9 mai 2008 pentru aprobarea Normelor tehnice de domenii și infrastructuri." *Monitorul Oficial*, nr. 405. 29 mai 2008. https://legislatie.just.ro/Public/DetaliiDocumentAfis/93541.

—. 2008b. „Ordinul nr. M.44, din 9 mai 2008 privind aprobarea Normelor tehnice pentru lucrări de întreținere și reparații curente la clădirile și construcțiile speciale din patrimoniul imobiliar al Ministerului Apărării." *Monitorul Oficial*, nr. 402. 28 mai 2008. https://legislatie.just.ro/public/DetaliiDocument/93499.

—. 2008c. „Ordinul nr. M.91, din 12 septembrie 2008 privind aprobarea Regulamentului proprietății imobiliare în Ministerul Apărării." *Monitorul Oficial*, nr. 668. 26 septembrie 2008. https://legislatie.just.ro/Public/DetaliiDocument/97630.

—. 2013. „Ordinul nr. M 92, din 16 septembrie 2013 privind aprobarea Instrucțiunilor pentru scoaterea din funcțiune și casarea activelor fixe, precum și declasarea și casarea bunurilor materiale, altele decât activele fixe, în cadrul Ministerului Apărării Naționale." https://legislatie.just.ro/Public/DetaliiDocument/151635.

—. 2018. „Ordinul nr. M.40, din 8 martie 2018 privind aprobarea Procedurii comune de autorizare a executării lucrărilor de construcții cu caracter special." *Monitorul Oficial,* nr. 738. 27 august 2018.

Ministerul Dezvoltării, Lucrărilor Publice și Administrației. 2012. „Cod de proiectare. Bazele proiectării construcțiilor CR 0-2012". https://www.mdlpa.ro/userfiles/reglementari/Domeniul_I/I_19_1_CR_0_2012.pdf.

—. n.d.. „Normativ privind executarea lucrărilor de întreținere și reparații la clădiri și construcții speciale GE 032-97." Accesat 15 ianuarie 2004. https://www.mdlpa.ro/pages/reglementare22.

Parker, Daniel M. 2016. *Obsolescence: An Architectural History.* Chicago: Everand.

Parlamentul României. 1991. „Legea nr. 50, din 29 iulie 1991 (**republicată**) privind autorizarea executării lucrărilor de construcții." *Monitorul Oficial*, nr. 933. 13 octombrie 2004. https://legislatie.just.ro/Public/DetaliiDocument/55794.

—. 2015. „Legea nr. 227, din 8 septembrie 2015 privind Codul fiscal." Monitorul Oficial, nr. 688. 10 septembrie 2015. https://static.anaf.ro/static/10/Anaf/legislatie/L_227_2015.pdf.

Petrișor, A.I. 2011. *FATE - Conversia fostelor baze militare în centre antreprenoriale. O perspectivă românească.* București: Editura Ars Docendi.

Schmidt, R. and S. Austin. 2016. *Adaptable Architecture – Theory and Practice.* New York: Routledge.

SMFT [Statul Major al Forțelor Terestre]. 2022. „*Exercițiu în poligonul «Operații militare în teren urban» din Cincu.*" https://www.defense.ro/exercitiu-in-poligonul-operatii-militare-in-teren-urban-din-cincu.

Stârzioru, M. and S. Pădureanu. 1995. *Istoria construcțiilor și domeniilor militare.* București: Editura Militară.


AGENȚIA ROMÂNĂ DE ASIGURARE A CALITĂȚII ÎN ÎNVĂȚĂMÂNTUL SUPERIOR
ROMANIAN AGENCY FOR QUALITY ASSURANCE IN HIGHER EDUCATION
Membră ENQA – Full member of ENQA
Înregistrată în EQAR – Registered in EQAR

CERTIFICAT
CERTIFICATE

Universitatea Națională de Apărare „Carol I" din București

a obținut, în urma evaluării instituționale, calificativul
GRAD DE ÎNCREDERE RIDICAT
pentru perioada 2021-2026
following institutional evaluation, attained the HIGH DEGREE OF CONFIDENCE rating for the period 2021-2026

BIROUL EXECUTIV AL CONSILIULUI ARACIS

EDITOR
„Carol I" National Defence University Publishing House
(Publishing house with recognized prestige validated
by the National Council for Attestation of University
Degrees, Diplomas and Certificates)
Adress: Panduri Street, no. 68-72, Bucharest, 5th District
e-mail: buletinul@unap.ro
Phone: +4021.319.48.80 / 0365; 0453

Signature for the press: 09.04.2024
The publication consists of 236 pages.

233/08.04.2024

C.80/2024