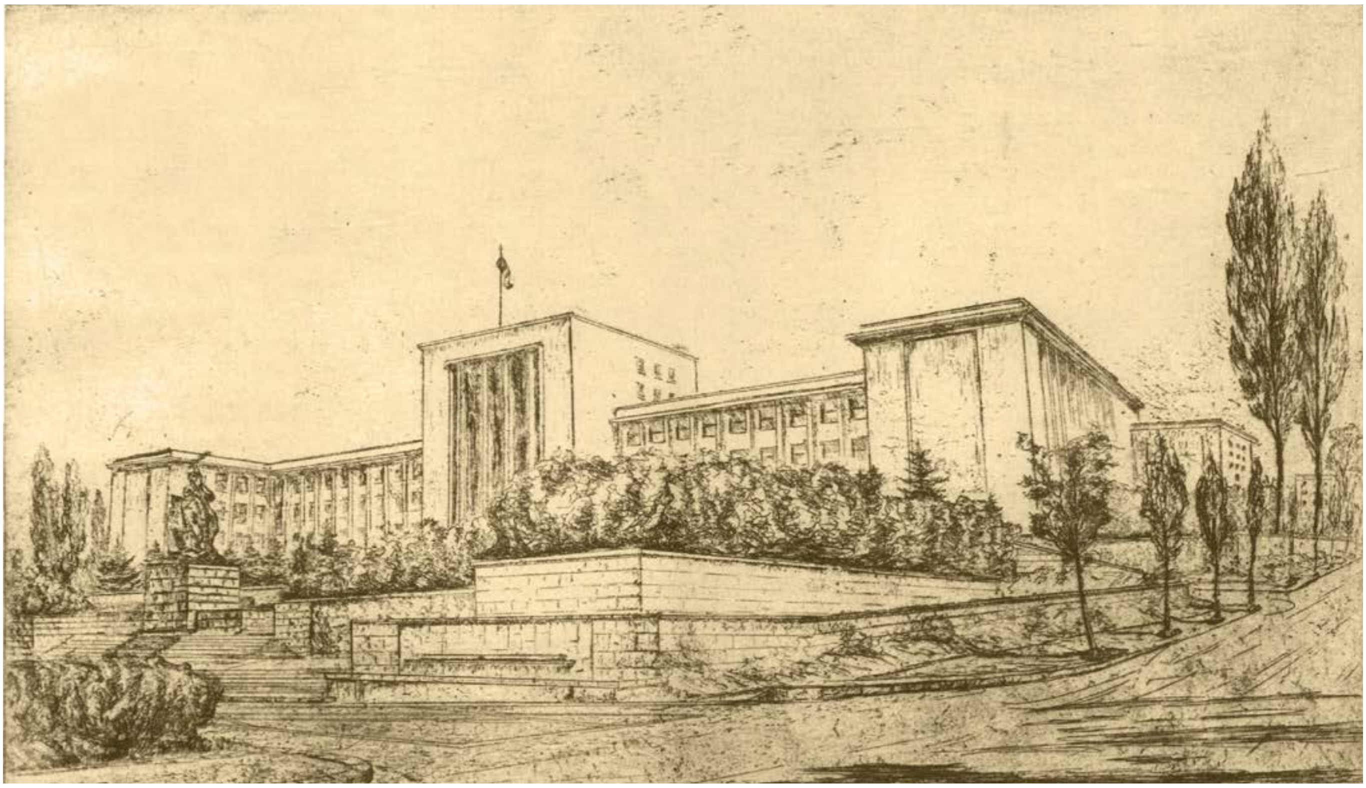
BULLETIN

OF ”CAROL I” NATIONAL DEFENCE UNIVERSITY

4 / 2022



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

PUBLICATION FOUNDED IN 1937

”CAROL I” NATIONAL DEFENCE UNIVERSITY PUBLISHING HOUSE
BUCHAREST, 2022

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.

EDITORIAL BOARD

SCIENTIFIC BOARD

SCIENTIFIC REVIEWERS

CONTENT

INSECURITY AND THE QUEST FOR STATE POLICE IN THE CONTEXT OF THE RESTRUCTURING DEBATE IN NIGERIA’S FOURTH REPUBLIC

Luqman SAKA, Ph.D.*
Sherifdeen Adeoye OLADEJO**

There has been a debate on the modality for the management of the Nigerian Police Force since the return to civil rule in 1999. The debate revolves around the need to devolve constitutional authority on policing to sub-national units. In theory, this will entail moving internal security issues, inclusive of policing, from the exclusive federal list to the concurrent list. Given the heighten insecurity that has plagued the Nigerian state in recent times, this paper examines the restructuring discourse in Nigeria with a specific focus on the call for the establishment of state police within the context of the subsidiarity principle. The study was contextualized within the exploratory research design paradigm and it adopted the qualitative approach in the sourcing and analysis of data. To this end, the paper has drawn information from published media reports that include: opinion, commentaries, editorials and news articles. Data was also sourced from published academic and policy publications that include: articles, chapter in books, books and government documents. Drawing on information from these sources, this paper assesses the positions of protagonists and antagonists of state police in Nigeria. It draws out implications for security governance in Nigeria.

Keywords: Criminality; Constitutionalism; Insecurity; Nigeria; Restructuring; State Police.

Introduction

To argue that Nigeria is facing an existential crisis as it relates to insecurity is practically highlighting the obvious. Currently, there are no geopolitical zones of the country that is not battling one form of insecurity. In Northeast Nigeria, the Boko Haram insurgency has raged for more than a decade. The carnage of the terror group had resulted in losses of lives, destruction of rural communities, population displacement and brought untold hardship to Nigerians that have had to live through the mindless violence of the group. The insurgency had also effectively resulted in the disruption of the economic foundation of the region, wiping off the wealth of millions of people and seriously constraints economic opportunities for Nigerians marginally impacted. In Northwest and part of Northcentral, banditry, cattle rustling and kidnapping has evolved as new forms of criminal enterprises. Highly dynamics, the security crisis in the Northwest and Northcentral Nigeria had morphed from indigene-settlers and farmers-herdsmen conflicts to cattle rustling and banditry. However, the most disturbing of recent has been the incidences of coordinated attacks on schools and the kidnapping of students for ransom with the Kankara, Jengbebe and Greenfield incidences in Katsina, Zamfara and Kaduna states been the most outrageous (ICG 2020) (ICG 2018) (Lar 2018).

In Southwest Nigeria, there are occasional violent clashes between farmers and herdsmen, cults/gangs violence, highway robbery and a rise in the reported incidences of ransom kidnapping. This cocktail of amorphous security challenges had elicited differing policy responses, of which the creation of Western Nigeria Security Network, WNSN code-named ‘the Amotekun Corps’, legislation banning open grazing and illegal occupation of forest reserves are important (Obado-Joel 2020) (Yahaya and Bello 2020). For the South-south, the conflicts between the Nigerian state, communities and oil multinational

***College of Arts and Sciences, University of the Gambia; Department of Political Science, University of Ilorin, Nigeria**
e-mail: *l.saka@utg.edu.gm; sakaluqman@unilorin.edu.ng*
****Federal College of Education (Special), Oyo, Nigeria**
e-mail: *oladejosherifdeen@gmail.com; oladejo.adeoye2288@fcesoyo.edu.ng*

corporations over ownership, access and control of oil wealth and the environmental destruction arising from hydrocarbon exploration had raged for decades. The agitation had morphed into militancy spearheaded by arrays of armed groups in the Niger Delta and piracy in the Gulf of Guinea. Communal clashes mostly over lands, armed robbery and kidnapping are problems in the Southeast. Added on to these is the resurrection of the agitation for secession now spearheaded by the Indigenous People of Biafra, IPOB led by Nnamdi Kanu and the group's increasing violence against state institution notably the Nigeria Police Force. More worrisome is the group deployment of violence as instrument to intimidate citizen in the region and the atmosphere of fear of violence engender by the increasing rascality and criminality of those affiliated with the organization.

Much as the Nigerian Armed Forces, the Nigerian Police Force and other federal security agencies strive to curtail insecurity and rising criminalities they seem to be swimming against the tide. While there are many instances of success, however, their efforts have so far failed to yield the desire positive effects. Indeed, to many watchers of the Nigerian security landscape, the state security architecture seems to be unravelling, as the security institutions struggle to keep up with the evolving security threats poses to Nigeria and Nigerians by criminal elements across the country. The heightened apprehension about rising criminality has pushed to the fore, the call for the restructuring of Nigeria's federal architecture with the objective of devolving more legislative authority/competency to the federating units. Central to the call for restructuring is the debate over the necessity for the devolution of policing power, authority and competency to the state governments. While not calling for the dismantling of the federal police force, proponents of devolution have argued that Nigeria's federating units should be granted the constitutional authority to establish state policing institutions. They argued that legislative authority on policing can be shared with competency effectively demarcated between the national police and policing institutions at the subnational levels.

The study was contextualized within the exploratory research design paradigm and it adopted the qualitative approach in the sourcing and analysis of data. To this end, the paper drawn it information from secondary sources that includes; news articles, opinion pieces, commentaries, editorials and press interviews published in Nigerian newspapers as it relates to the argument for and against decentralization of policing power, authority and services. It also utilized information sourced from official documents and reports published by governmental and non-governmental bodies. Drawing on information from these sources, this paper assesses the positions of protagonists and antagonists of the state police in Nigeria. It draws out implications for security governance in Nigeria in the context of a teething security challenges. The paper is structured into six sections. Following this introduction is the section that discusses the principle of subsidiarity as it relates to the devolution of authority and responsibility especially in federations. Section three and four examine the arguments for and against state police in Nigeria's fourth republic respectively. Section five discusses the incidences of rising criminalities in Nigeria and the necessity for the creation of state police and this was followed by the concluding thought.

Federalism and the principle of subsidiarity

The role of the police in every society is crucial to the maintenance of law and order. According to Odeyemi and Obiyan (Odeyemi and Obiyan 2018), the police as an institution is mostly charged with the responsibility of providing security or at the least a socio-psychological feeling of security for the citizen. To this end, policing entails an attempt at maintaining social order while the police as an institution is established to enforce the law and maintain social order. Discourse on the management of police and the tier of government that should have policing authority is of critical importance in a multi-ethnic, multi-religious and complex federal political system like Nigeria. This becomes even significant, in the context of the nation's evolving security landscape.

To be fair to the proponents of restructuring, what has emerged as the model of federal governance in Nigeria under past military autocracies and since the return to civil rule in 1999 has been a system that reinforces a high degree of centralization of power, legislative authority and competency in service delivery. The flip has been that, often times, Nigeria’s federating units are forced by circumstances of the federal constitutional and institutional processes to relates with the federal government and operates within the federal arrangement from a position of weakness. This runs contrary to the underlying assumptions, and principles that guide the operations of the federal political system, the most essential being the non-subordination of the federating units to the national government and the principle of subsidiarity as it relates to functional authority and competency over service delivery.

Federalism as a principle and form of state organization is an ingenious political device essentially deployed for the accommodation of diversity within a political entity or, alternatively, for ensuring oversight over a large territorial expanse (Ayoade 2020, 9). Thus, federalism as a political instrument for the organization of the state is often deployed to ensure the protection and advancement of diversity (differences) while enhancing the promotion of political stability of the federal state. It then means that while unity of purpose can be achieved, uniformity, as it relates to processes, would be anathema to the ideal of federalism and federal governance (Ayoade 2020, 10). However, it is important to state that the notion of federalism and federal principle stated above often approximate processes in aggregative federations. Whereas for dis-aggregative (holding together) federations like Nigeria the need to advance national unity is often elevated to the position of ‘deity’ to the extent that it sometimes becomes the foundation for political and governance crisis.

Federalism as a state organizing principle denotes an institutional framework that entails at its core the division of legislative authority and competency among national and subnational governments within a distinctly defined political entity (Rozell and Wilcox 2019). Thus, as Jega notes (Jega 2021), irrespective of whether the subnational government were initially independent and came voluntarily to form a federation (aggregative) or they were compelled by political/historical circumstances into such union (dis-aggregative), the subnational government would by legal, constitutional and institutional arrangement and processes have coordinate, or shared responsibilities with the national government. As Jega notes (Jega 2021), an underlying objective of the federal system is the non-conflictual management of diversity, through equitable and just sharing/division of political power, administrative authority and resources in a manner directed at advancing national progress while recognizing and protecting the diversity of federating units.

An important rule that often guides the division of legislative authority (devolution/division/decentralization) in a federal system is the ‘principle of subsidiarity’. In its basic conception, the principle of subsidiarity regulates authority within a political order. The overriding objective has been to ensure that powers, authority, administrative competency or performance of tasks should rest with sub-national units within a political arrangement unless allocating them to national unit/federal government would ensure higher comparative advantage, as it relates to, efficiency or effectiveness in the discharge of administrative responsibilities or exercising of authority (Follesdal 1998). Central to the application of the principle of subsidiarity is the notion that an allocation of legislative authority or competency in the administration of tasks must satisfy a condition of comparative efficiency (Follesdal 1998).

As Follesdal argued (Follesdal 1998), the principle of subsidiarity should be holistically applied to ensure that decisions are taken as closely as possible to the people. The principle of subsidiarity can include a necessity condition, empowering national government to take action only when subnational governments cannot achieve the desired result as it relates to effectiveness and efficiency in the administration of responsibility and service delivery on their own. Follesdal further stressed that the principle of subsidiarity can also regulate how the national government is to act, so as to respect the autonomy of sub-national unit. Taking other things as constant, the federal government should employ directives that stipulate results while leaving the choice of means to federating units rather than adopting detailed regulations which are directly applicable to member states (Follesdal 1998).

Thus, the subsidiarity principle should be essentially taken to be ‘a de-centralizing principle, which favours decentralization over centralization as it relates to decision-making’ (Evans and Zimmermann 2014). It contains clear limits to state intervention or other forms of centralized power arrangements (Mulé and Walzenbach 2019). In a nutshell, at the heart of subsidiarity is the affirmation that with the existence of joint competence, decision-making capacity should be allocated to the lowest political unit possible. Commenting on the utility of the principle, Reho noted (Reho 2019) that taking subsidiarity seriously means that the federal/national/union government should mainly act as the guarantor of its members’ integrity, autonomy, independence and identity and not as an agent of uniformity and centralization.

In essence, devolution is central to the applicability of subsidiarity as a cardinal principle of competency assignment in federal systems. The current call for the restructuring of Nigeria’s federal architecture that has become strident will entails some forms of stepping down of legislative authority and administrative competency over few areas wherein the federal government had long exercise dominance. It might also entail joint sharing of authority and competency in other areas wherein the federal government has long enjoyed sole authority. Central among such few areas wherein sharing of authority and competency might be needed if the clamour for restructuring sails through will be over the establishment, management and control of the Police and the exercising of policing authority.

Proponents of decentralization and restructuring in Nigeria have often cited the over-centralization of control, command and operational system and process that characterized the working of the Nigerian Police Force and ‘the one size fit all’ approach to policing Nigeria as an impediment to the realization of the objective of security provisioning in the country. Thus, when decentralized, policing will then entail collaboration and synergy between agencies of the federal government and those of the federating units (Agboga 2020) (Crook and Manor 1998) (Agrawal and Ribot 1999).

Federalism and the argument for the creation of the state police in Nigeria

The increasing call for the restructuring of Nigeria’s federal architecture should be expected and not treated as a misnomer. From historical accounts, there had been series of attempts at restructuring the framework that underpins the operation of the Nigerian state under colonial rule and in the post-colonial era (Agbaje 2018) (Agbaje 1998) (Saliu 2018). More than this, it is important to note that, constitutional change and adaptation, is normal and not exceptional, as far as the character, nature and working of federal systems are concerned (Kincaid 2012) (Suberu 2015). This is more so, as Suberu noted (Suberu 2015, 3), in ‘post-authoritarian and/or heterogeneous federations with a recent history of non-inclusivity or centrist constitution’ with all the constitutional and political landmines contained therein in such constitutions. all of which aided constitutional mortality in such federal political systems all of which aided constitutional mortality in such federal political systems.

Thus, as Agbaje averred (Agbaje 2018, 104), it will be wrong to argue that the ‘so-called, inscrutable’ Nigerian factor is solely responsible for the rising call for restructuring of the nation’s federal framework. On the contrary, the calls and debate about the need to restructure Nigeria’s federal architecture has been on for much longer, albeit with changing concepts, contents, and intents. The call is necessarily a consequence of a certain set of problems inherent in certain types of federal systems (Agbaje 2018). Given the need to address diversity problems as they arise, what works for a federation might not work for another. Indeed, for the same federation what had worked in decades past might become the source of tension and crisis in the future.

However, it is also important to state that the essence of the adoption of a federal framework is the need to constantly adapt to changing political realities thus, institutional and constitutional frameworks in federations are often not cast in stone. But as Agbaje has highlighted (Agbaje 2018), federal systems whose constitutional and institutional frameworks contained serious inherent problems that seem to contradict and negate the core assumptions underlying federal systems would not but be prone to constitutional and institutional crises, and this seems to be the case for Nigeria since the return to civil rule. The contradictions and inherent problems that predispose the Nigeria federation to crisis at present might have informed Jega’s position (Jega 2021, 2) that while Nigeria is technically and substantively a federation, ‘it is one of the worst models of political accommodation of diversity, as well as power and resource sharing’.

As Agbaje noted (Agbaje 2018), there are number of proposals on the approaches better suited to Nigeria as it relates to restructuring. Saliu also averred (Saliu 2018) that there are as many positions among Nigeria’s power elite and the citizenry alike on what restructuring should entail. One of the important proposals espoused on the Nigerian public space is that which call for constitutional reform. Key in the argument of proponents of this option is the contention that the 1999 federal constitution place too much political power, legislative authority and competency, as well as, resources at the disposal of the federal government, thus stifling the capacity of the thirty-six federating units. For proponents, the best option is to devolve power, authority and resources away from the central and invest such at the federating states. The argument has been that doing this will stimulate competition, raise the potential for innovative ideas and promote sub-national units’ development and by extension overall national development. Key on the agenda of those calling for devolution especially on security and notably policing is the argument for the sharing of policing power between the federal government and the governments of the federating units.

Protagonists of the agenda for the devolution of policing authority and competence as means for addressing Nigeria security crisis cut across the strata of the Nigerian society. Making the case for the creation of state police, former Governor of Lagos State and current Minister of Work and Housing, Babatunde Fashola was quoted to have argued that:

> Every state that has the power and can give judgment through its state high courts and magistrates and make laws through its state assemblies and legislators must have the concomitant powers to enforce its law and police its state (Aleyomi 2013).

In the same vein, Egunjobi quoted lawyer and human rights activist, Femi Falana as stating that “the issue of establishing state police is necessary in a federation”. While the adoption of a unified, single national police institution was informed by political considerations after the Nigerian civil war, current realities especially as it relates to worsening security environment calls for a rethink (Egunjobi 2016). Affirming the need for such rethink, the Chairman of the House of Representatives, Committee on Judiciary, Onofiok Luke was quoted to have stated that:

> The Constitution envisages Nigeria as a federal state. Granting allowance to state governments to establish police force and other security apparatuses will bring Nigeria into the original constitutional contemplation of a federal state (Baiyewu 2021).

Indeed, rather than being an exception, devolution of policing power, authority and competency was an important hallmark of federal practices across many federations. Although, as Hooghe and Marks noted (Hooghe and Marks 2003, 235), large jurisdictions have the opportunity of exploiting economies of scale in the provision of public goods, however, large jurisdictions become problematic when they impose a uniform policy on diverse ecological systems or territorial heterogeneous populations. Indeed, there is an extensive federalism literature that had examined the optimal allocation of authority across multiple tiers of government and how governments at different levels interact, cooperate and coordinate towards achieving synergy in the delivery of public goods and services (Benz 2000) (Kincaid 2001) (Oates, Fiscal federalism 1972) (Simeon and Cameron 2000) (Tullock 1969) (Wright 1987). A substantial part of the argument for multi-tiers governance was captured in Oates decentralization theorem (Oates 1999, 1122).

The argument that large jurisdiction becomes problematic when they impose a ‘one-size fit all’ single policy on a large geographical expanse that is highly heterogeneous capture the crisis of policing in Nigeria. It also underscores the failure of the Nigerian Police Force at addressing the country’s evolving security crisis. Aleyomi (Aleyomi 2013) had alluded to the issue of geography and ecology when he notes that Nigeria’s large territory and heterogeneity is an important issue to consider in making the case for the constitutionality of state policing. There is the argument that local level policing through the establishment of state police will aid the penetration of community and help promote community-friendly policing, a practice that has been problematic given the heightened level of community suspicion and mistrust against the Nigerian Police Force. This mistrust against the Nigerian Police Force was informed by years of policing through harassment, intimidation, and violence by personnel of the Nigerian Police. The bottled-up anger culminated in the public protests against the Nigerian Police Force between 2017 and 2018 and the October 2020 #EndSARS protest in Lagos and across other major cities (Ojedokun, Ogunleye and Aderinto 2021) (Amusan and Saka 2018) (Akinlabi 2017) (Agbibo 2015).

Not granting Nigeria’s federating states power, authority and competency over policing seem to be a disservice. This is because state governments have been committing significant resources to policing through their provisioning of logistics, physical structures, arms and ammunition and other resources needed for effective policing to federally controlled police commands operating in their jurisdictions. Governor Nasir El-Rufai of Kaduna state, alluded to this when he was quoted as stating that:

> The state governments today bear most of the burden of the running costs of the federal police anyway, so why not the state police now. So, I repeat my persistent call for State police as soon as possible (Isenyo 2021).

That the states have been committing significant funds to the operational cost for running the Nigerian Police Force in their domains is an indication that the federal government has been abdicating her funding to the Nigerian Police Force while still retaining management and control (Eboh 2014). This goes against the dictates of fairness and justice aside from the fact that it is against the logic of federal principle, practices and extant thinking about multi-tiers governance as espoused by Oates (Oates 1999). More importantly, it is no longer a sustainable policing model given the mirage of security challenges confronting the Nigerian state which the unified and federally controlled Nigerian Police Force seems to no longer find answers to nor capable of effectively addressing. There is also the argument that while the federating states collect huge funding as ‘*security vote*’ monthly from the federation account, there is a clear lack of accountability in the utilization of the vote. To this end, allowing states to establish local police and turning the opaque ‘*security vote*’ to matching grants solely devoted to maintaining sub-national policing agencies might be financially prudent (Odeh and Umoh 2015).

Given Nigeria’s territorial expanse and the country’s heterogeneity, applying uniformity in policing methods, approaches and processes go against the principle of decentralization and multi-tiers governance practice. Indeed, proponents of state police have argued that different regions of Nigeria had peculiar security challenges. Because of the peculiarity, it is better if personnel recruited to serve as police officers have a better grasp of the geography of crime in the area they are to serve for their effectiveness. This can better be achieved when state governments are allowed by law to establish local police authority and draw recruits from within their localities against the posting of officers and men from disparate geographical and cultural backgrounds all around the country as currently practised by the Nigerian Police Force (Eme and Anyadike 2012). This sentiment was also echoed by the Chairman House of Representative Committee on Judiciary in the course of the House ongoing constitutional review and considerations of the proposed alterations to provisions of the constitution on policing. The Chairman, Honourable Onofiok Luke was quoted as stating that:

> The federal structuring of our security does not encourage community policing or localization of policing. Recruitment and subsequent deployment of police officers in their local area are one of the major ways of curbing crime. Such officers understand the

area, terrain, language, behaviour and attitude of the people he or she is policing (Baiyewu 2021).

In essence, not until people familiar with the geography of crimes in a locality are entrusted with the responsibility of policing their localities, Nigeria cannot begin to talk of effective policing and indeed community policing (Ojong and Bem 2020) (Egunjobi 2016).

Arguments against the devolution of policing power and authority in Nigeria

Given the process of evolution of the Nigerian state and her political history, the debate about the propriety or otherwise of devolution of policing power and authority will continue to elicit divergent positions. As there are proponents, there are also those that passionately argued against the devolution of policing authority and the creation of police at the sub-national level in Nigeria. The most important argument deployed by antagonists of the idea of state police has been that anchored on the ‘fear of abuse’ of such authority and the concern that sub-national police will become an instrument of intimidation and oppression of political opposition. Antagonists of state police are quick to reference the nation’s political history to remind anyone willing to listen of how regional political leaders abused local the power of policing during the first republic.

Antagonists of the proposition are quick to express the fear that the tendency is there for highly ambitious political leaders at the sub-national level to turn state police into an instrument for political vendetta. For antagonists, it is not a matter of whether it will happen, but rather that of when and how quick this tendency will manifest. Espousing this position, Adedeji (O. Adedeji 2012), noted that nothing has changed in the condition that initially led to the dismantling of the native authority police as operated during Nigeria’s first republic. In taking the argument further, Odeyemi and Obiyan (Odeyemi and Obiyan 2018) note that governors may use state police to pursue personal political interests, harassing political opposition and muffling dissenting voices, perpetrate elections fraud and trample on the fundamental rights of citizens.

Not relying on the argument of past abuse of the native authority police as a yardstick to gauge whether state police will become subject of abuse or not, Aleyomi (Aleyomi 2013) notes that antagonists of the idea, have pointed to the emasculation of the local government system as a pointer to what to expect with police institution control and manage by political elite at the sub-national level. While the 1999 constitution of the federal republic of Nigeria legislates for the establishment of a system of democratically elected local government, most state governors and the House of Assemblies under their beck and call have manage the local government more as fiefdoms of the state governors against the dictate of the constitution and without minding the democratic rights of the people to elect those that manage the local government on people’s behalf. Pointing to this, antagonists of state police argued that the state governors will use the instruments of control under their watch to abuse the institution of police if the states are allowed to establish their policing agency.

Eme and Anyadike (Eme and Anyadike 2012) also note that stakeholders have argued that creating state police at this stage in Nigeria given the heightened level of mutual distrust among the constituting segments may amount to an invitation to chaos. Apart from the impunity of state governors and the possibility of abuse of power, state police could lead to the disintegration of the country, especially now with the fragile nature of social relations among ethnic nationalities. Antagonists are pointing to the uproar that the creation of the Western Nigeria Security Network WNSN (Amotekun Corps), the regional security outfit by Southwest Nigeria governors has caused. Antagonists of state police are pointing to arguments coming from Northern Nigeria elite that the WNSN security agency was created with the intent to use the outfit to chase Fulani herdsmen away from Southwest Nigeria. The continued reports of clashes between the outfit and armed herdsmen have not helped in disabusing the minds of Northern Nigeria elite and ordinary northerners. For the Yoruba of Southwest Nigeria and their elite, ‘Amotekun’ has come to stay and the political leaders have argued that the states in the region have the right to police their forests and protect lives and properties given the failure of the federal government control security institutions to effectively secure their people and territory.

Antagonists of state police have argued that there are outfits that are purportedly performing community policing functions now or that have done such in the past without been designated as state police (James, 2014). Opponents argued that these outfits have been used as instruments of intimidation and have been accused of abusing the rights of citizens in their areas of operation. Opponents have highlighted the dispensing of jungle justice by vigilante groups backed by state governments in the past such as the dreaded Bakassi Boys that operated in Abia and Anambra states, the Odua's People's Congress in Southwest Nigeria, and the Hisbah outfit in Kano (Lar 2018) (Odeh and Umoh 2015) (Baker 2002). There is also the argument that sanctioning the establishment of police outfits by the thirty-six states of the federation will berth the creation of multiple police agencies which might result in clash of authority and jurisdictions (Aleyomi 2013) (Odeh and Umoh 2015) (Ojong and Bem 2020).

Rising insecurity and the propriety of state police in Nigeria's fourth republic

Discourse on the restructuring of state architecture especially in federal systems has always remained contentious sometimes rancorous depending on the level of the development of political process and culture of tolerance. To that extent, discourse on restructuring in Nigeria in general and devolution of policing authority and competency, in particular, has remained fractious especially in the absence of elite consensus on the issue. Protagonists and antagonists of restructuring and devolution have neither being able to speak respectively to one another nor agree on what to devolve, when to devolve and how to approach the devolution process. The rancorous nature of the debate notwithstanding, there is a common agreement that there is the need to rejig the constitutional and institutional foundations of the Nigeria federal arrangement (Jega 2021).

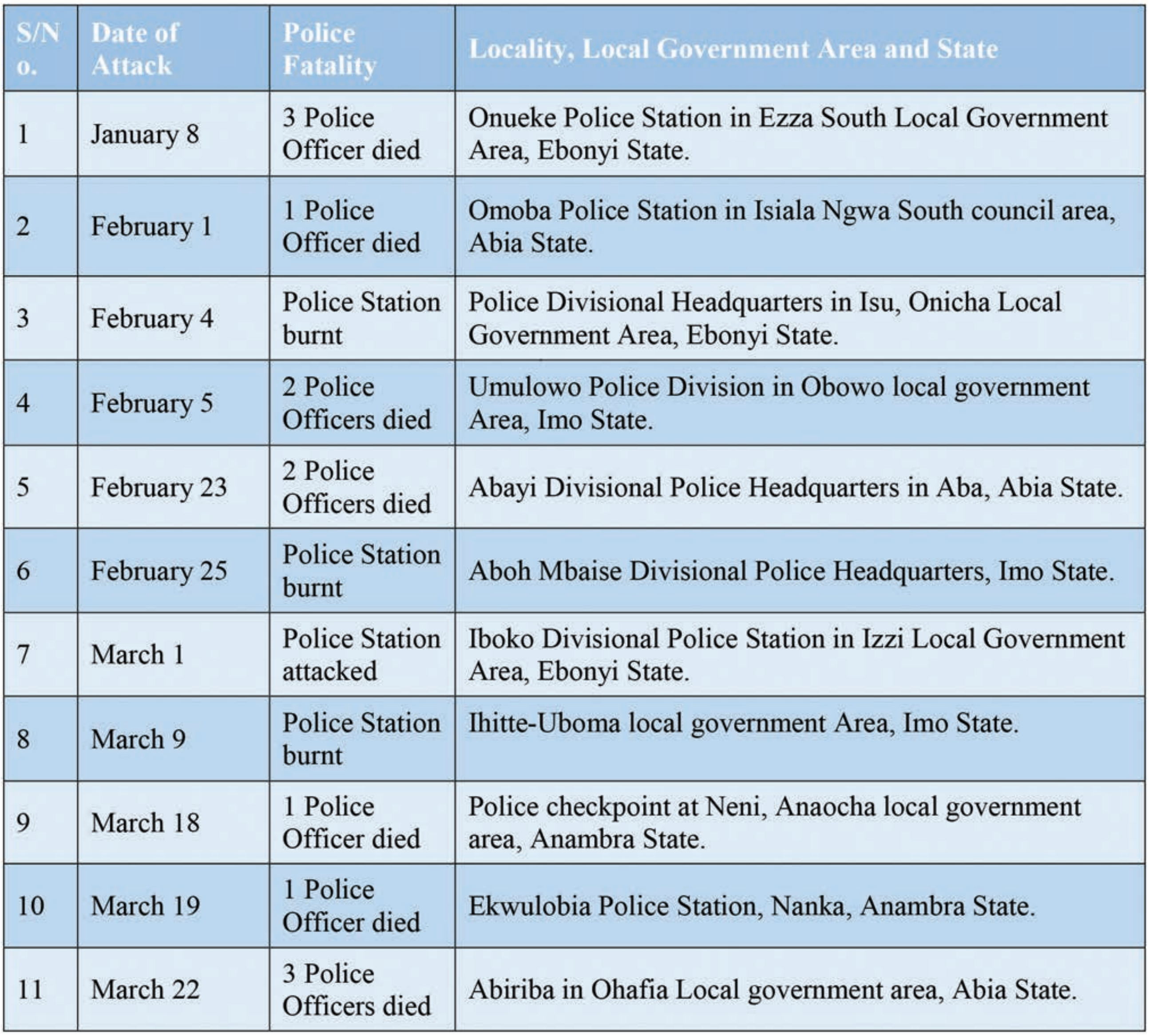
As it relates to giving constitutional authority to Nigeria's federating states to establish police outfits, the debate has largely lack coordination, like the general discourse surrounding the bigger issue of 'restructuring'. Irrespective of the positions of Nigeria's political elite and Nigerians alike on the propriety or otherwise of the devolution of policing power to federating states, both the protagonists and antagonists on the debate are in agreement that the Nigerian police force needs reorganization to properly address Nigeria's current security challenges. There has been cosmetic tinkering with the operational processes, procedures and practices of the police via reforms embarked upon by successive management teams since the return to civil rule. However, the objective of evolving an institution that conducts policing through intelligence gathering, immersion with and cordial community relations, uphold laws of the land and protect citizen's rights and respect human dignity has largely eluded the Nigerian Police Force.

Clearly, Nigeria is going through a trying time as far as the economy, politics and more importantly security issues are concern. While our current economic, political and governance challenges are serious they all pale when compare with the crisis of insecurity that Nigeria and Nigerians are contending with. The reason being the complexity of the crisis especially as it relates to its nature, dimensions and dynamics. While the elephant in the room remains the Boko Haram insurgency in Northeast Nigeria, the mindless mayhem and violence that defines banditry and kidnapping and the fact that no geo-political zone of Nigeria is exempted make these evolving criminalities an existential threat for Nigeria and her people (A. Adedeji 2021) (Duerksen 2021) (ICG 2020) (ICG 2018). The growing public perception that Nigeria's security agencies are losing the wars against crimes, criminalities and criminals is raising public anger, fear and desperation. As Campbell argued (Campbell 2021), Nigerians anxiety over the country's deteriorating security situation is beginning to morph from fear of criminals to public panic about criminalities and criminals. While the security environment is deteriorating in the South, people in some parts of Northwest Nigeria, have had to flee to Niger Republic to seeks safety from marauding bandits, cattle rustlers, kidnappers and everyday criminals (acaps 2020) (Hamrouni 2021).

Compounding the crisis is the rising incidence of lethal attacks on Nigeria's security agencies especially the Army in Northern Nigeria and Police formations in Southeast Nigeria (Al-Jazeera 2020). Although security issue in the Southeast has been on the front burner since the conclusion of the 2019 general elections,

Table 1: Incidence of Armed attacks against Police Formations in Southeast Nigeria, Jan-Mar 2021

Compiled by authors from BBC New Pidgin (29 March 2021)



S/No.	Date of Attack	Police Fatality	Locality, Local Government Area and State
1	January 8	3 Police Officer died	Onueke Police Station in Ezza South Local Government Area, Ebonyi State.
2	February 1	1 Police Officer died	Omoba Police Station in Isiala Ngwa South council area, Abia State.
3	February 4	Police Station burnt	Police Divisional Headquarters in Isu, Onicha Local Government Area, Ebonyi State.
4	February 5	2 Police Officers died	Umulowo Police Division in Obowo local government Area, Imo State.
5	February 23	2 Police Officers died	Abayi Divisional Police Headquarters in Aba, Abia State.
6	February 25	Police Station burnt	Aboh Mbaise Divisional Police Headquarters, Imo State.
7	March 1	Police Station attacked	Iboko Divisional Police Station in Izzi Local Government Area, Ebonyi State.
8	March 9	Police Station burnt	Ihitte-Uboma local government Area, Imo State.
9	March 18	1 Police Officer died	Police checkpoint at Neni, Anaocha local government area, Anambra State.
10	March 19	1 Police Officer died	Ekwulobia Police Station, Nanka, Anambra State.
11	March 22	3 Police Officers died	Abiriba in Ohafia Local government area, Abia State.

however, the rising incidence of attacks on police formations and personnel resulting in deaths across states in the Southeast has become an issue of serious concern (Chibuzo, et al. 2021). In most of the incidences, the attackers razed down police facilities, burned operational vehicles, looted police armoury and inflicted bodily harm on police personnel resulting in the loss of lives. In some parts of the Southeast, Police personnel now manned their posts, scaling down crime patrols and other policing activities (Alexis 2021) (Business Day 2021) (A. Nasir 2021a). In clearer terms, the Nigerian Police Force is being forced to cede the streets to criminals across communities in Southeast Nigeria.

While the Nigerian Armed Forces and the Nigerian Police Force continued to records casualties as they strive to contained rising criminality and insecurity, as table 1 above show, it also needs to be stated that civilian death tolls are also becoming horrendous. Casualty figures continue to mount as insecurity worsen across all the regions of the country especially starting from the beginning of 2021. To highlights the worsening security environment across the country, on Monday 26th April 2021, media accounts reported the death of seventy-seven (77) Nigerians attributed to terrorists, bandits, kidnapping, cultist attacks among others across eleven (11) states cutting across Northern and Southern Nigeria (Ibemere 2021).

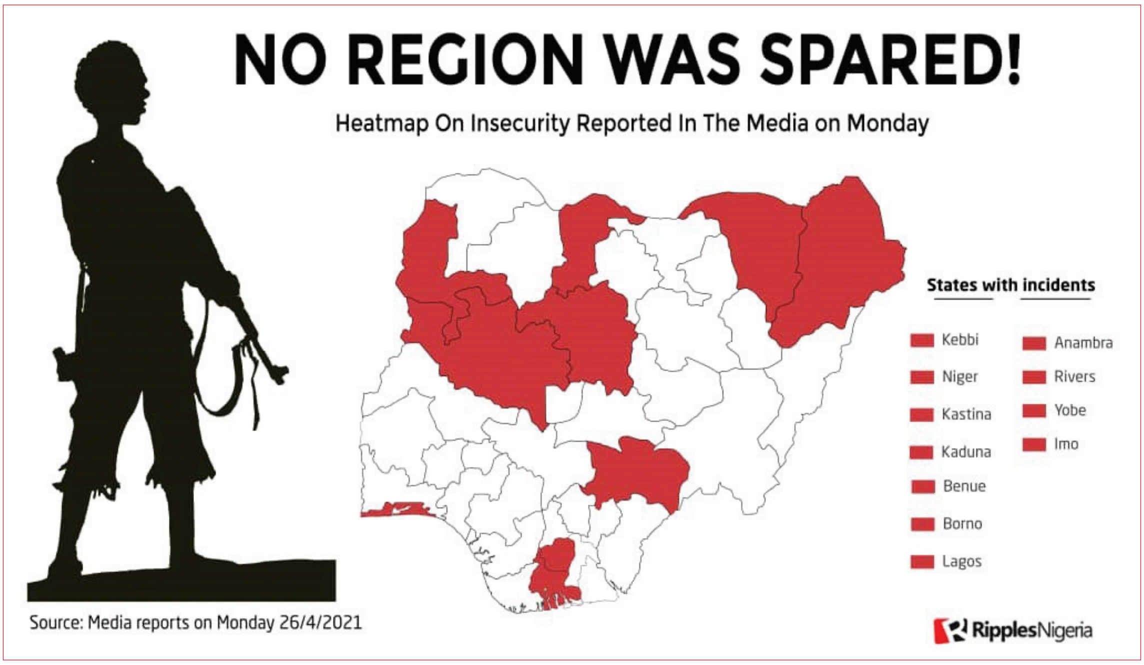
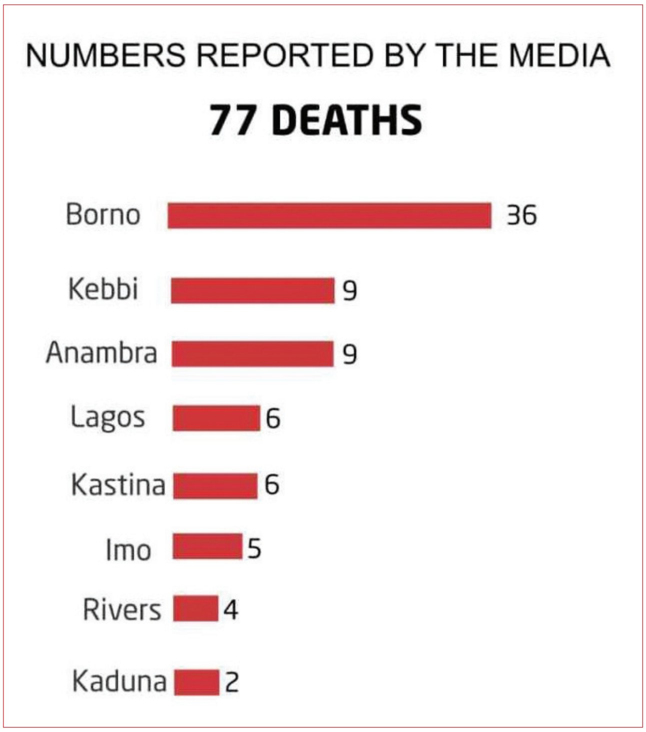


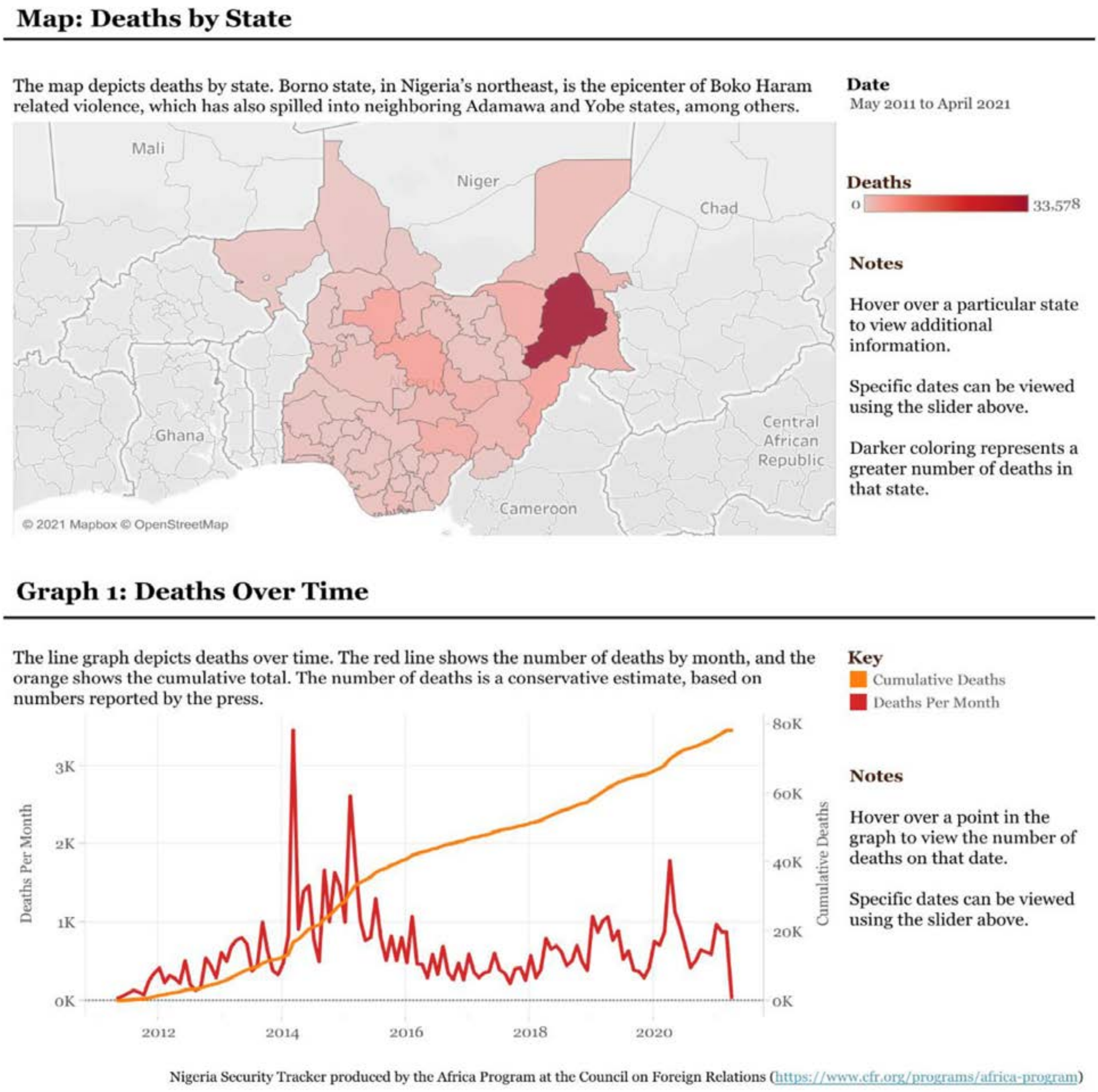
Figure 1 Heat map of reported death in the Nigeria News Media for Monday 26th April 2021. (Ibemere 2021)

Graph 1: Media reports of deaths from armed attacks across Nigeria Monday 26th April 2021 (Ibemere 2021)



Citing the report of a non-governmental organization ‘Nigeria Mourns’, Premium Times newspapers reported that at least 1,603 Nigerians lose their lives to armed attacks across the country between January and March 2021 (A. Nasir 2021b). It was also reported that around 1,774 Nigerians were victims of abduction and kidnapping within the three months covered by the organization’s report (A. Nasir 2021b). As it relates to perpetrators of these crimes, the report noted that 921 people were killed by suspected bandits, 207 people killed by suspected members of Boko Haram or its breakaway faction ISWAP, 205 killed in isolated attacks and 106 were killed in clashes among rival cult groups across the country. It was also reported that 79 people were victims of extra-judicial killings, 53 deaths were attributed to communal clashes and 32 people were killed by suspected herdsmen (A. Nasir 2021b). The first quarter of 2021 was bloody for Nigeria and Nigerians given the incidence of reported attacks against civilian, military units and police formations.

While the year 2021 has been bloody so far in terms of the reported incidence of armed attacks by various armed criminal groups, Nigeria’s security environment has been deteriorating steadily over the decade according to the database from the Nigeria Security Tracker, produced by the Africa Program, Council on Foreign Relations based in New York. As the data in graphs 1, 2 and 3 below show, the incidence of armed attacks against Nigerians resulting in loss of lives has been on a steady increase



Map: Deaths by State

The map depicts deaths by state. Borno state, in Nigeria's northeast, is the epicenter of Boko Haram related violence, which has also spilled into neighboring Adamawa and Yobe states, among others.

Date
May 2011 to April 2021

Deaths
0 33,578

Notes

Hover over a particular state to view additional information.

Specific dates can be viewed using the slider above.

Darker coloring represents a greater number of deaths in that state.

© 2021 Mapbox © OpenStreetMap

Graph 1: Deaths Over Time

The line graph depicts deaths over time. The red line shows the number of deaths by month, and the orange shows the cumulative total. The number of deaths is a conservative estimate, based on numbers reported by the press.

Key
🟧 Cumulative Deaths
🟥 Deaths Per Month

Notes

Hover over a point in the graph to view the number of deaths on that date.

Specific dates can be viewed using the slider above.

Nigeria Security Tracker produced by the Africa Program at the Council on Foreign Relations (https://www.cfr.org/programs/africa-program)

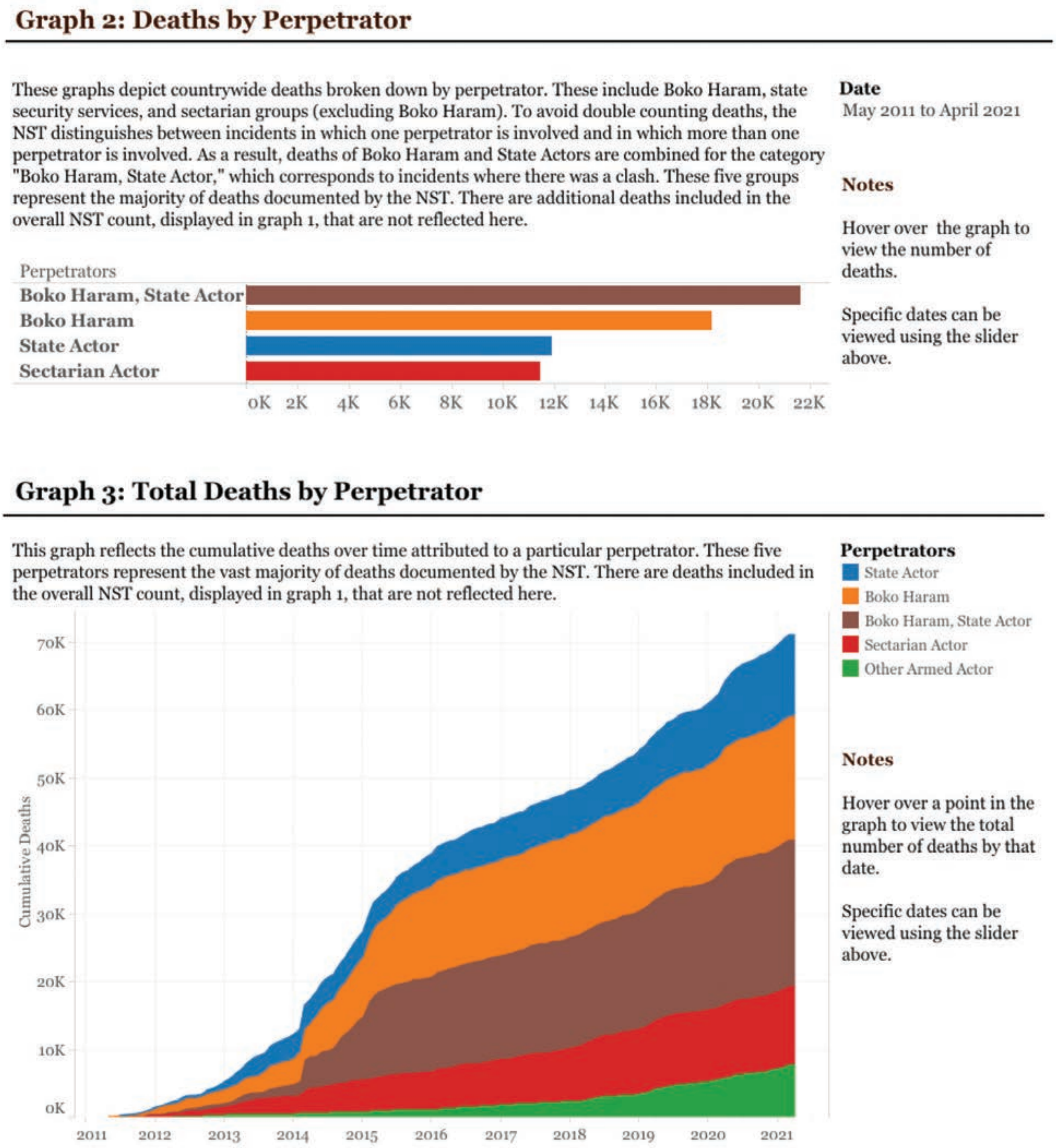
Figure 2 Map showing death by State and graph showing Death Over Time May 2011 to April 2021 (NST 2021)

peaking around 2014-2015 when Nigeria witnessed the worst from Boko Haram attacks. Between 2016 till 2019, reported incidences reduced, however, going by the trend, the incidence of reported armed attacks against Nigerians resulting in deaths is on the rise again starting from 2020.

Graph 2 above shows the death toll over time with the red and orange colour depicting the number of death by months and the cumulative total of death respectively.

In response to the worsening security environment across the country, the Governors of the six Southwest states announced the formation of the Western Nigerian Security Network (Amotekun Corps) in 2020. In the same vein, Governors of the five Southeast states in April 2021 announced their resolve to establish a joint security outfit to be called ‘Ebube Agu’. Related to these two regional outfits was the establishment and operationalization of the Lagos State Neighbourhood Watch, conceived as a community policing outfit. On the constitutional front, there is the increasing possibility that the ongoing constitution review process by the Nigerian National Assembly might give constitutional authorization for the creation of state police. A bill that seeks to amend the 1999 Constitution to allow for the creation of state police and legalize regional security outfits has passed the second reading.

Graph 2: Death by perpetrator and total deaths by perpetrator in Nigeria May 2011 to April 2021 (NST 2021)



Graph 2: Deaths by Perpetrator

These graphs depict countrywide deaths broken down by perpetrator. These include Boko Haram, state security services, and sectarian groups (excluding Boko Haram). To avoid double counting deaths, the NST distinguishes between incidents in which one perpetrator is involved and in which more than one perpetrator is involved. As a result, deaths of Boko Haram and State Actors are combined for the category "Boko Haram, State Actor," which corresponds to incidents where there was a clash. These five groups represent the majority of deaths documented by the NST. There are additional deaths included in the overall NST count, displayed in graph 1, that are not reflected here.

Date
May 2011 to April 2021

Notes

Hover over the graph to view the number of deaths.

Specific dates can be viewed using the slider above.

Graph 3: Total Deaths by Perpetrator

This graph reflects the cumulative deaths over time attributed to a particular perpetrator. These five perpetrators represent the vast majority of deaths documented by the NST. There are deaths included in the overall NST count, displayed in graph 1, that are not reflected here.

Notes

Hover over a point in the graph to view the total number of deaths by that date.

Specific dates can be viewed using the slider above.

Honourable Onofiok Luke, Chairman House Committee on Judiciary that sponsored the bill, in his explanatory note, averred that

> the bill seeks to alter the Constitution, “to provide for state police and other state government security services to enhance security and preservation of lives and properties in Nigeria” (Baiyewu 2021).

This position has been an important rallying cry for protagonists of devolution of police authority.

If the ongoing constitutional review comes to fruition, the bill on devolution of police authority is clear on what it seeks to achieve through the alteration. Specifically, the bill proposes an amendment to Section 197(1) by inserting new Paragraphs ‘e’ and ‘f’ to provide for ‘State Police Council’ and ‘State Police Service

Commission,’ respectively. The Second Schedule to the Constitution will also be altered in Part I by deleting Item 45 (federal control of police) from the Exclusive Legislative List; and in Part II by inserting after Item 30 on the Concurrent Legislative List, new Items 31 and 32. The proposal reads, (Item 31) “The National Assembly may make laws for the establishment of the federal police and other federal government security services” and (Item 32) “A House of Assembly may make laws for the establishment of state police and other state government security services.” The Third Schedule to the Constitution will also be altered by inserting new Paragraphs 9 to 12 (Baiyewu 2021). By these amendments, policing and management of police will effectively come under the Concurrent Lists, thus turning policing to shared authority, competency and responsibility between the Nigerian federal government and governments of the federating states. If the constitution review process is successfully concluded and the alteration on policing at the House of Representatives get the mandated concurrence of the Senate, one can only hope the new arrangement will aid the cause of securing Nigeria and the police power and authority not becomes subject of abuse by political leaders at the sub-national level in Nigeria.

Conclusion

Federalism and restructuring are two sides of the same coin (Agbaje 2018). This is largely because the adaptability of the federal system and the ability of federations to respond swiftly to changing circumstances is one of the most important traits of virile and robust federal systems. The ability to swiftly adapt and innovatively respond to emerging realities even becomes more important for federal systems that are faulty by design and can be said to be non-federalist in process and practice. To this end, a federation that failed to adapt to new circumstances by innovatively restructuring its constitutional, political and institutional practices and processes run the risk of implosion and/or collapse. As important as the federal system it is that a constitutional device should manage diversity since federations collapse largely due to failure to adapt and change.

Even if the Nigerian federal system is going through a trying time, the challenges faced by the country are surmountable. The most important existential threats facing the Nigerian federal arrangement are the heightened insecurity and rising criminalities. While the federal government and the security institutions that it controls strive to address the security crisis, their efforts had not aligned with the Nigerians’ expectations. The worsening security environment has resulted in a call for restructuring with the view to decentralize policing power, authority and competency to Nigeria’s thirty-six federating units. The argument is that the federal and state governments should constitutionally share the exercising of policing power so that the states be allowed to establish, operate, fund, and control police agencies. The belief is that this approach will relieve the federal government of some of the burden of policing Nigeria, encourage community policing, help address the differing security problems of different states and their localities, and ultimately help in addressing Nigeria’s security crisis.

BIBLIOGRAPHY

acaps. 2020. “Nigeria-Banditry violence and displacement in the Northwest.” *Short Note, 24th July.* https://www.acaps.org/special-report/nigeria-banditry-violence-and-displacement-northwest.

Adedeji, Ademola. 2021. “The growing threat of armed banditry in North-West Nigeria.” *Strife Blog.* https://www.strifeblog.org/2021/01/08/the-growing-threat-of-armed-banditry-in-north-west-nigeria/.

Adedeji, O.A. 2012. “State Police in Nigeria: Issues and Challenges.” *University of Pennsylvania Journal of Constitutional Law* Vol. 3. doi:http://dx.doi.org/10.2139/ssrn.2088033.

Agbaje, Adigun. 1998. *”A century of power-sharing”: Nigeria in theoretical and comparative perspective.* Working Paper 99/8, Ibadan: Development Policy Centre.

Agbaje, Adigun. 2018. “An appraisal of the proposals for restructuring in Nigeria.” In *Roundtable discussion on economy and restructuring in Nigeria*, by H.A. Saliu and B.O. Adedamola (Eds.), 104-114. Ilorin: Mandate International Publications Ltd.

Agbibo, D.E. 2015. “Policing is not work, it is stealing by force’: Corrupt policing and related abuses in everyday Nigeria .” *Africa Today* 62: 94-126.

Agboga, Victor. 2020. “Beyond decentralising the Nigerian Police: how Lagos state circumvented debates on police reforms.” *Journal of Contemporary African Studies*, 135-150. doi:https://doi.org /10.1080/02589001.2020.1832972.

Agrawal, Arun, and Jesse Ribot. 1999. “Accountability in Decentralization: A framework with South Asian and West African Environmental Cases.” *The Journal of Developing Areas* 33 (4): 473-502.

Akinlabi, O.M. 2017. “Do the police really protect and serve the public? Police deviance and public cynicism towards the law in Nigeria.” *Criminology & Criminal Justice* 17 (2): 158-174.

Alexis, Akwagyiram. 2021. “Nigerian police launch operation in southeast to quell violence it blames on separatists.” *Reuters News Agency.* May 19. https://www.reuters.com/world/africa/nigerian-police-launch-operation-southeast-quell-violence-it-blames-separatists-2021-05-18/.

Aleyomi, Michael B. 2013. „Is state police a panacea to security threat in Nigeria?” *Afro Asian Journal of Social Science* 4 (2): 1-21.

Al-Jazeera. 2020. “Bandits’ kill 23 Nigerian soldiers in northwest: Report.” July 20. https://www.aljazeera.com/news/2020/07/20/bandits-kill-23-nigerian-soldiers-in-northwest-report/.

Amusan, Lere, and Luqman Saka. 2018. “The Nigerian Police Force and the task of policing democratic Nigeria: Issues and problems.” *Anthropologist* 31 (1-3): 105-116.

Ayoade, John A.A. 2020. *Nigeria: A nation of states or a state of nations?* Ibadan: Senator Abiola Ajimobi Foundation in collaboration with Institute for Peace and Strategic Studies, University of Ibadan.

Baiyewu, Leke. 2021. *Reps approve bill to create state police, security outfits.* The Punch Newspaper 6th July. https://punchng.com/breaking-reps-approve-bill-to-create-state-police-security-outfits/.

Baker, Bruce. 2002. *Taking the law into their own hands: Lawless law enforcers in Africa.* London: Routledge.

BBC News Pidgin. 2021. *Gunmen attack in Nigeria: Abia, Imo, Anambra, Ebonyi see 11 gunmen police attacks in three months.* March 29. https://www.bbc.com/pidgin/tori-56552823.

Benz, Arthur. 2000. “Two types of multi-level governance: Intergovernmental relations in German and European Union regional policy.” *Regional and Federal Studies* 10 (3): 21-44.

Business Day. 2021. “Ominous signs of attacks on police formations in South East.” *The Editorial Board.* April 26. https://businessday.ng/editorial/article/ominous-signs-of-attacks-on-police-formations-in-south-east/.

Campbell, John. 2021. “Nigeria: Anxiety over deteriorating security morphing into panic.” *Council on Foreign Relations.* https://www.cfr.org/blog/nigeria-anxiety-over-deteriorating-security-morphing-panic.

Chibuzo, Ukaibe, David Tarkaa, Ejike Ejike, Obeta Okechukwu, and Eziyi Kalu. 2021. “Nigeria: Rising attacks on police may lead to full-scale insurgency in the South East.” *Leadership (Abuja).* April 20. https://allafrica.com/stories/202104200059.html.

Crook, Richard C., and James Manor. 1998. *Democracy and decentralization in South Asia and West Africa.* Cambridge University Press.

Duerksen, Mark. 2021. “Nigeria’s diverse security threatse .” *Africa Centre for Strategic Studies – Spotlight.* https://africacenter.org/spotlight/nigeria-diverse-security-threats/.

Eboh, N. 2014. “Crime prevention and control in Nigeria: A case for state police.” *Nnamdi Eboh NewsBlog @nnamdiebo.com.* March 2.

Egunjobi, A. A. 2016. “The Nigeria federal practice and the call for state police.” *International Journal of Advanced Academic Research Social & Management Sciences* 2 (7): 1-14.

Eme, O.I., and N.O. Anyadike. 2012. “Security Challenges and the Imperatives of State Police .” *Review of Public Administration and Management* 1 (2): 203-218.

Evans, Michelle, and Augusto Zimmermann. 2014. “The global relevance of subsidiarity: An overview.” In *Global perspectives on subsidiarity*, by M. Evans and A. Zimmermann (Eds.), 1-7. Dordrecht: Springer.

Follesdal, Andreas. 1998. “Subsidiarity.” *The Journal of Political Philosophy* 6 (2): 231-259.

Hamrouni, S.M. 2021. “Fleeing bandit attacks, Nigerian villagers seek safety in Niger.” *UNHCR* . March 02. https://www.unhcr.org/news/stories/2021/3/603dff134/fleeing-bandit-attacks-nigerian-villagers-seek-safety-niger.html.

Hooghe, Liesbet, and Gary Marks. 2003. “Unraveling the Central State, but how? Types of multi-level governance .” *American Political Science Review* 97 (2): 233-243.

Ibemere, David. 2021. “RipplesMetrics… Terrorists, bandits run riot in Nigeria. Over 77 deaths reported in 11 states.” *RipplesNigeria.* April 27. https://www.ripplesnigeria.com/ripplesmetrics-terrorists-bandits-run-riot-in-nigeria-over-77-deaths-reported-in-11-states/.

ICG. 2018. *Stopping Nigeria’s spiraling farmer-herder violence.* Africa Report, No. 262, International Crisis Group.

ICG. 2020. *Violence in Nigeria’s North West: Rolling back the mayhem.* Africa Report, No. 288, International Crisis Group.

Isenyo, Godwin. 2021. “State police, way out of banditry, insurgency, El-Rufai insists.” *Punch Newspaper* . https://punchng.com/state-police-way-out-of-banditry-insurgency-el-rufai-insists/.

Jega, Attahiru M. 2021. *Restructuring in Nigeria: Why? How? When?* Presentation at the 18th Daily Trust Dialogue. Thursday, January 21, 2021. NAF Conference Centre and Suites, Abuja Kado, Kado: Gwarinpa Expressway.

Kincaid, John. 2012. “Constitutional change in federal countries: Comparative considerations .” In *Changing federal constitutions: Lessons for international comparison*, by A. and Knupling, F. (Eds.) Benz. Opladen: Barbara Budrich Publishers.

Kincaid, John. 2001. “Devolution in the United States: Rhetoric and reality.” In *The federal vision: Legitimacy and levels of governance in the United States and the European Union*, by N. and Robert, H. Edited Kalypso, 144-160. Oxford: Oxford University Press.

Lar, Jimam. 2018. “Policing actors, plural processes and hybridization: Histories of everyday policing practice in Central Nigeria.” *Stability: International Journal of Security and Development* 7 (1): 1-15. doi:https://doi.org/10.5334/sta.605.

Mulé, Rosa, and Günter Walzenbach. 2019. “Introduction: two spaces of subsidiarity?” *Commonwealth & Comparative Politics*, 141-152.

Nasir, Ayitago. 2021b. “1,603 killed, 1,774 abducted in violent attacks across Nigeria in three months - Report.” *Premium Times.* May 17. https://www.premiumtimesng.com/news/headlines/461986-1603-killed-1774-abducted-in-violent-attacks-across-nigeria-in-three-months-report.html.

Nasir, Ayitogo. 2021a. “Four policemen killed as gunmen attack police formations across Nigeria.” *Premium Times.* April 24. https://www.premiumtimesng.com/news/top-news/457324-four-policemen-killed-as-gunmen-attack-police-formations-across-nigeria.html.

NST. 2021. “Nigeria Security Tracker.” *Council on Foreign Relations.* https://www.cfr.org/nigeria/nigeria-security-tracker/p29483.

Oates, Wallace E. 1999. “An essay on fiscal federalism.” *Journal of Economic Literature* 37: 1120-1149.

—. 1972. *Fiscal federalism.* New York: Harcourt Brace Jovanovich.

Obado-Joel, Jennifer. 2020. “The challenge of state-backed internal security in Nigeria: Considerations for Amotekun.” *Resolve Network. Policy Note.* https://www.resolvenet.org/system/files/2020-12/RSVE%20Policy%20Note_Obado-Joel_December%202020.pdf .

Odeh, Adiza Mercy, and Nanji Umoh. 2015. “State Policing and National Security in Nigeria.” *Mediterranean Journal of Social Sciences* 6 (1): 412-423.

Odeyemi, Temitayo I., and A. Sat Obiyan. 2018. “Exploring the subsidiarity principle in policing and the operations of the Nigeria Police Force.” *African Security Review* 27 (1): 42-60.

Ojedokun, Usman A., Yetunde O. Ogunleye, and Adeyinka A. Aderinto. 2021. “Mass mobilization for police accountability: The case of Nigeria’s #EndSARS protest.” *Policing: A Journal of Policy and Practice* 15 (3). doi:https://doi.org/10.1093/police/paab001.

Ojong, E.T., and J.A. Bem. 2020. “The controversy over the creation of state police in Nigeria .” *SARJANA* 35 (2): 40-51.

Reho, Federico Ottavio. 2019. “Subsidiarity in the EU: Reflections on a centre–right agenda.” *Wilfred Martens Centre for European Studies.* https://www.martenscentre.eu/wp-content/uploads/2019/04/2.pdf.

Rozell, Mark J., and Clyde Wilcox. 2019. *Federalism: A very short introduction.* Oxford: Oxford University Press.

Saliu, Hassan A. 2018. “The current debate on Nigeria’s restructuring: Its genesis, dynamics and implications for national security.” In *Roundtable discussion on economy and restructuring in Nigeria*, by H.A. Saliu and B.O. Adedamola (Eds.), 76-103. Ilorin: Mandate International Publications Ltd.

Simeon, Richard, and David Cameron. 2000. “Intergovernmental relations and democratic citizenship.” In *Governance in the 21st century*, by B.G. and Savoie, D.V. Edited Peters, 58-118. Montreal: McGill/Queens University Press.

Suberu, Rotimi. 2015. “Managing constitutional change in the Nigerian federation .” *Publius: The Journal of Federalism* 45 (5): 552-579.

Tullock, Gordon. 1969. “Federalism: Problems of scale.” *Public Choice* 6: 19-29.

Wright, Deil. 1987. “A century of intergovernmental administrative state: Wilson’s federalism, New Deal intergovernmental relations, and contemporary intergovernmental management.” In *A centennial history of the American administrative state*, edited by Ralph C. Chandler, 219-260. London: Macmillan.

Yahaya, Jibrin Ubale, and Musa Mohammed Bello. 2020. “An analysis of the constitutional implication of South-West regional security initiative: Amotekun.” *African Scholar Journal of Humanities and Social Sciences* 17 (6): 161-192.

POPULISM AS A POLITICAL STRATEGY: IS IT A THREAT TO DEMOCRACY?

Petar MURGINSKI, Ph.D. Candidate*

Some authors have been highly critical of populism and naturally, this has raised the question of whether populism is dangerous for democracy or not. I wish to provide a critique of this claim and instead suggest that populism is sometimes necessary for established democracies. Developing this argument, this paper proceeds as follows: Firstly, I will outline Urbinati's criticism of populism. Secondly, using Popper's paradox of tolerance, I will show how Urbinati's view is teleological and becomes a defence of the status quo thereby impeding political progress. Thirdly, I will show how populism's relationship with democracy is best conceptualised as a creatively destructive one and how populists, once having accepted the Popperian condition of tolerance, can be a force for good in democracies by illuminating issues which were previously left outside the realm of mainstream politics.

Keywords: Populism; Democracy.

Introduction

The word democracy derives from the combination of the Greek words ***demos*** and ***kratos***. Democracy therefore means that the people (***demos***) hold the power (***kratos***) (Christiano 2018). Similarly, the word populism traces its origins to the Latin word *populus* which literally means people (Friedman 2017). Populists from Chavez to Trump also wish to give power to what they perceive as the true people. Indeed, as Mudde's classic definition puts it, populism should be conceived as a "as a thin-centered ideology" that considers society to be ultimately separated into two homogeneous and antagonistic camps – "the pure people" and "the corrupt elite", and also argues that politics should be an expression of the *volonté générale*[1] of the people" (Mudde 2004, 532). Therefore, both populists and democrats raise one of the most fundamental questions of political theory, namely how to define the people.

While democracy is a system of governance, populism is a "thin centered ideology" which provides a means to take over the democratic government. In turn, this has raised the question of whether populism is dangerous for democracy or not. Some authors have been highly critical of populism. For instance, Taggart (2002) has argued that populism is a "pathology" of democratic politics while Levitsky and Ziblatt (2018) suggest that populism endangers democratic life altogether. In particular, Urbinati has argued that populism is a "disfigurement" of democracy which leads to authoritarianism through the process of monopolizing public opinion for the sake of unity (Urbinati 2014). In this paper, I wish to provide a critique of this argument and instead suggest that populism is sometimes necessary for established democracies[2]. In turn, I will adopt Urbinati's diarchic definition of democracy and focus not on ***procedural*** side of democracy such as the checks and balances on power, but rather on the ***opinion*** side of democracy which is more concerned with.

Democracy Disfigured: Urbinati's Critique of Populism

The core criticism which Urbinati directs towards populism is that it is a "disfigurement of democracy" (Urbinati 2014). She conceptualises democracy as a diarchy because of its dual nature. There is the ***procedural*** side which underpins the democratic process through constitutional checks and balances, but there is also an ***opinion*** side in

[1] A phrase meaning "general will".

[2] In this essay I will focus on established democracies which can experience periods of political stagnations. My theoretical arguments do not extend to newly established democracies which tend to have weaker institutional checks and balances and where the effects of populism would be different.

***Military Academy G. S. Rakovski**
e-mail: *murginski@yahoo.com*

which deliberative procedures and the freedom of expression are a necessary supplement to those institutions. Therefore, a society is democratic not only because of the free, competitive elections but also because of the promise to facilitate “effective political competition and debate among diverse competing views” (Urbinati 2012, 180). Institutions cannot exist without the competition of opinions and visa-versa.

In turn, populists attempt to monopolize the opinion side of democracy for the purpose of the creation of a hegemonic people. For Urbinati, this has negative implications for the relationship between the state and civil society as such a relationship is characterized by the existence of political and social conflicts. Given this tension, the state is an institution which serves to mediate among the varying interests. Populism seeks to infiltrate this tension and reclaim the unifying and subjecting role of representation. As she puts it herself:

“Populism presumes the people (in the singular) is always right – this makes it blur the diarchic structure and prioritize the domain of opinion (unified within one narrative) … both the character and the practice of populism underlines, and more or less consciously derive from a vision of democracy that can become deeply inimical to political liberty insofar as it dissolves the political dialectics among citizens and groups, revokes the mediation of political institutions, and maintains an ***organic notion of the body politic*** *that is averse to minorities and individual rights*”(Urbinati 2012, 130-156).

From this it follows that populism is a call for the concentration of power. By claiming to completely represent the people, “unified within one narrative”, populism shifts away from democratic politics towards authoritarianism (Urbinati 2012, 156).

Urbinati invokes a contrast between a ***Lockean social contract*** and a ***Hobbesian*** one to illustrate this (Urbinati 2014, 200). As populists monopolize the sphere of public opinion under the singular voice of the true people, they are symbolically endowed with a ***Hobbesian sovereignty*** in which there is no right to revolt. By contrast, democratic society requires a ***Lockean social contract*** in which the body politic retains the right to revolt against the opinion of those in government. Urbinati’s concern is that populism impedes the freedom of expression by monopolizing the domain of opinion through the hegemonic discourse of the people (Urbinati 2014, 223). In turn, this opens the door for ***Caesarism***[3] (Urbinati 2014, 224). This essentially equates to authoritarianism which in its extreme form consolidates into a total control of the ***corpus politicum***[4].

Populism’s rejection of individual rights makes it prioritise unity over equality. In the “one man, one vote” system of democracy this is highly problematic. By simplifying social forces into a singular voice, populism leads to the “verticalization of political consent” (Urbinati 2014, 170). This goes contrary to the democratic mantra of widening consent to all. Therefore, instead of being a force for popular change, populism “inaugurates a deeper unification of the masses under a charismatic leader” (Urbinati 2014, 170).

The distinction between law and opinion is a fundamental feature of democracy which populist attempt to trump. In the *“Origins of Totalitarianism”*, Hannah Arendt has argued that:

“[Totalitarianism] can do without the **consensus iuris**[5] *because it promises to release the fulfilment of law from all action and will of man; and it promises justice on earth because it claims to make mankind itself the embodiment of the law”* (Arendt 1951, 462).

By verticalizing consent and personifying it, populism blurs the distinction between opinion and law. For Urbinati this leads to ***Caesarism*** but we can clearly observe a common theme between her ideas and Arendt’s. The state, for both theorists, becomes a tool of those in power, not a mediator of interests. It does so by monopolizing opinion. Therefore, populism becomes not a “a politics of inclusion but primarily of exclusion” because only one opinion is valid (Urbinati 2012, 150). In Urbinati’s view, populism is not the embodiment, but the disfigurement of democracy.

Qualifying Urbinati’s Critique

To this point, I have established that Urbinati’s critique of populism is about the *opinion* side of the democratic diarchy. Populism verticalizes

[3] A term used to denote an authoritarian or autocratic political philosophy inspired by Julius Caesar.

[4] A phrase meaning “body politic”.

[5] A phrase meaning “law by consent”.

political consent by uniting the will of the people into a singular voice. This creates exclusion, not inclusion. At the heart of this critique lies the concept of tolerance.

Urbinati’s argument is essentially that populists do not accept tolerance of opinion which is a necessary element of democracy. **By prioritizing unity over equality, populism rejects pluralism which in its extreme form can lead to totalitarianism**: a concerned echoed by Hannah Arendt.

However, a closer look at what tolerance consists of reveals that all politics, to various degrees, is about exclusion. ***Karl Popper’s paradox of tolerance*** illustrates this tension (Popper 1957).

Democracies aspire to be tolerant societies. Each tolerant society is faced with a dilemma once exposed to intolerant views. The concept of tolerance demands toleration of all opinions. As Voltaire famously argued: “I disapprove of what you say, but I will defend to the death your right to say it” (Hall 1906). However, this ideal-type vision of tolerance does not work. Only those who accept tolerance as a principle can be tolerated. In *“The Open Society”*, **Karl Popper has argued that the survival of the tolerant society requires an intolerance of those who are themselves intolerant.** If we tolerate intolerant parts of society, there is a risk that once they come to dominate public life, they will end toleration thereby suspending tolerance altogether (Popper 1957, 23-40).

Urbinati’s critique of populism follows a similar logic. Populism is a dysfunctional form of democracy because it distorts representation for the sake of unity instead of seeking tolerance by accepting equality and pluralism. This is done in the name of the true people and by definition it means that those who do not fit within the “organic notion of the body politic” are excluded (Urbinati, 2012, 224). This could be used to justify an authoritarian form of government which makes populism inimical to democracy[6]. Yet, this argument must be qualified. **Urbinati misses a critical caveat which undermines her critique of populism.**

For her, all populists can be measured by reference to a commonly accepted standard of what democratic politics should look like. As such she neglects the nuances that exist between different types of populist movements. In turn, her view becomes ***teleological***. It does not treat the political future as open-ended and contingent, but rather as a moving in a certain direction and populism represents a retrogression from this direction. Through this, populism becomes a symptom of democratic failure rather than the expression of legitimate resentment. Such a view legitimizes the ***status quo*** and instead of being progressive, it actually becomes a conservative defence which impedes political progress.

As a thin-centred ideology which divides the people into two homogenous groups, it is necessary to understand that such a division can lead to Urbinati-style ***Caesarism*** only if these two groups are defined in ethnic or “organic” terms. If this is the case, populism becomes intolerant as the division which it advocates for cannot be overcome by a re-arrangement of the political order. It can only be done through the exclusion of groups which do not fit the organic notion of the ***corpus politicum***. Therefore, in such a scenario, populism is dangerous for democracy as it does not accept the ***Popperian condition of tolerance***.

However, Urbinati’s critique focuses only on the supply-side of populism and it treats the populist leader as an exploiter who is willing to side-line minority rights in the name of unity. From such a perspective, democracy appears to be a self-correcting process in which the populist leader represents a temporary malfunctioning of the system. Crucially, such a view fails to acknowledge that there is a demand-side in which populism can represent a legitimate source of unrest which is ultimately good for democracy. Without it, such an issue may not have come to the forefront of politics at all and this would have made politics less democratic as the people are not truly represented.

In sum, **populism is only dangerous to democracy if it invokes an organic concept of the homogenous people.** If a populist movement

[6] For example, using a similar line of thought, Levitsky and Ziblatt suggest that Trump’s election is an illustrative case-study showing that “democratic backsliding today begins at the ballot box” (Levitsky and Ziblatt 2018, 5). According to them, one of the essential tests for democracies is whether such figures are allowed to participate in political parties, or they are prevented from gaining power in the first place. This way “populism tests the tolerance of representative politics” and it is “most extreme forms” it may be in danger of spilling over into authoritarianism and moving away from democracy altogether” (Ibid., 79).

does that, it means that according to the ***Popperian paradox of tolerance***, it can legitimately be excluded from the political process because it is dangerous for democracy. Once in power, such a populist leader may overthrow the democratic process for the sake of the unity of the homogenous people which are defined in ethnic, blood and soil terms. However, if this attempt to polarize society is triggered by legitimate concerns about socio-economic or moral issues, then populism instead should be viewed as a means to rejuvenate democracy. This is the theme of the final section.

The Populist Creative Destruction

Instead of treating populism as a disfigurement of the democratic process which is dangerous, populism should instead be seen as a means to reinvigorate democracy.

As previously mentioned, the only reason why populism might be treated as a pathology of democracy is if the populist movement in question does not accept tolerance, because as Popper has demonstrated only those political movements which accept that principle can form a legitimate government.

If populists accept Popper’s condition, then they should be perceived as a means to progress democratic politics further rather than to subvert it. Populists do not completely manufacture their consent as Urbinati suggests, but rather they often invoke on issues which are of wide concern to the body politic but have not been addressed by the political elite[7].

In theory, democracy is justified as a political system which is responsive to all citizens. Such ideal can never be achieved in practice because of the principle of ***majoritarianism*** on which democracy is based. Some citizens will be considered political losers in elections, others political winners. Even so, democracy should never be static. Its institutions should always change, and injustices denounced under a process of ongoing monitoring. Accountability is at the core of what democracy is about.

Total agreement on issues is almost impossible to achieve through democratic means due to the complexities of modern societies. Instead, what we often observe are consensuses. For instance, the post-war consensus in Britain on the social-economic order after 1945 or Reagan’s neoliberal consensus in the United States in the late 1970s (Heffernan 2002). Each of these was a consolidation of democratic politics around a set of issues which were broadly supported by the electorate. However, such consensuses are also double-edged swords. On the one hand, they could lead to sustained periods of growth and social equality, but on the other hand they could systematically underrepresent groups in society. Such periods can lead to a crisis of representation in which the body politic becomes disillusioned with politics. In turn, populism can emerge as a counter-weigh to the political establishment by pushing the agenda in the direction of those who are underrepresented.

Indeed, as Ernesto Laclau has argued, populism does two things that are democratic (Laclau 2007, 167). First, it polarizes society by creating two fronts of confrontation. Second, it produces through polarization a new unification of the people around issues that are on the side of the many. From this process, a new political consensus emerges which aligns with the greater needs of a greater number of people. This view is also shared by Margaret Canovan who views populism as a corrective to democracy (Canovan 1999). From this it follows that democratic politics is about conflict which is almost always in flux. The alignment and de-alignment of consensuses around a set of ideas is what makes democracies move. It is at the heart of political progress.

In order for such process to occur, populism must create discontent first. To create a new consensus, the old census must be destroyed. This is the essence of the logic behind the idea of creative destruction (Roberts 2017). Progress can only be achieved through the disruption of established practices.

Polarization should be seen as a vital pre-conditional for a new consensus in politics. As democratic politics is about conflict in which certain groups lose while others win, division is

[7] This is clearly evidenced in structural approaches to the causes of populism which focus on the demand-side. For example, the works on growth regimes of Blyth and Hopkin (2018) and Kaufmann’s Whiteshift (2018) are two examples which trace the causes of populism to larger socio-economic changes and provide evidence that populists are not pure opportunists but actually address some issues which have been side-lined by the political establishment.

inevitable. Populism is, in a sense, politics because it creates division.

Nonetheless a key issue emerges: What if populism only creates destruction? If populists do not offer any solutions, this can lead us to concluding that the creativity of their destruction has a limited utility for democratic politics. From such a perspective, populism is a pathology of democratic politics, not a re-invigorating force, because it does not offer any solutions to the pervasive problems of society but rather uses them for its own political gain.

Crucially, the creative part does not necessarily come from the populist rhetoric but from society as a whole. **Populism serves the purpose of illuminating illnesses which conventional parties had lost in their obsession with managerial politics.**

The key issue is not to create a division based on ethnic lines which cannot be re-arranged but to put forward ideas which divide society along the lines of social, economic and moral issues. **As long as populism creates a division which is centred round a set of issues which the political elite has systematically overlooked, populists have utility for democratic politics.** In other words, once populists accept the ***Popperian condition***, they can propel a realignment of the ***corpus politicum*** in a new consensus. This will always be a collective effort for all those involved in politics, but it is can be the populists that initiate the first step towards this re-alignment of people by breaking political taboos and driving the debate forward.

Democracies work best when they are underpinned by a strong set of norms as to how society should be governed. These norms often stagnate, and people become disillusioned with politics. In such scenarios, populist leaders can enter the scene and cause the realignment of society among a new consensus by illuminating the issues with the current one.

Conclusion

This scientific article has shown how populism is a reinvigorating force for established democracies. The ***Urbinatian criticism of populism*** equates populism with an authoritarian verticalization of consent which was ultimately a pathology of democracy. It only understands populism from the supply side and therefore fails to recognize that populists do not completely manufacture their consent, but rather invoke issues which are often of wide importance in society. As such, her critique of populism becomes ***teleological***. Therefore, it is a defence of the ***status quo*** which does not treat the future as open-ended but views each political development outside an established view as a dangerous retrogression on the path to progress. Instead, we should think of populism as a form of creative destruction. It can destroy political consensuses by shifting the debate towards issues and policies which were left unattended for extended periods of time. Ultimately, this can yield a new reunification of the people conditional on populists accepting the ***Popperian condition of tolerance***.

In Western democracies, political parties which side with populists are often described as making a Faustian pact with the devil. Yet, such critics must remind themselves of Johann Wolfgang von Goethe’s famous quote that “there is strong shadow where there is much light”. Democracies are never the finished product precisely because they are meant to be responsive to the changes in society. When they fail to respond to such changes in society and address issues which are of major concern, populism emerges as a means of shining light where the shadow of progress has settled. In conclusion, the illiberal elements of populism should not be seen solely as a threat to democracy – perhaps they should also be seen as a challenge to democracy.

BIBLIOGRAPHY

Arendt, Hannah. 1951. *The Origins of Totalitarianism*. London: Penguin Modern Classics.

Blyth, Mark, and Jonathan Hopkin. 2018. *The Global Economics of European Populism: Growth Regimes and Party System Change in Europe*. Government and Opposition 54 (2): 193-225.

Canovan, Margaret. 1999. *Trust the People! Populism and the Two Faces of Democracy*. Political Studies 47 (1): 2-16.

Christiano, Tom. 2018. Democracy. The Stanford Encyclopedia of Philosophy. https://plato.stanford.edu/entries/democracy/

Friedman, Uri. 2017. What Is a Populist? The Atlantic. https://theatlantic.com/international/archive/2017/02/what-is-populist-trump/516525/

Hall, Evelyn Beatrice. 1906. *The Friends of Voltaire*. London: G. P. Putnam.

Heffernan, Richard. 2002. *The Possible as the Art of Politics*: *Understanding Consensus Politics.* Political Studies 50 (4): 742-760.

Kaufmann, Eric. 2018. *Whiteshift: Populism, Immigration and the Future of White Majorities*. London: Allen Lane.

Laclau, Ernesto. 2007. *On Populist Reason.* New York: Verso.

Levitsky, Steven, and Daniel Ziblatt. 2018. *How Democracies Die*. New York: Viking.

Mudde, Cas. 2004. *The Populist Zeitgeist.* Government and Opposition 39 (4): 541-563.

Popper, Karl 1957. *The Open Society and Its Enemies*. London: Routledge.

Roberts, Kenneth. 2017. *Populism and Political Parties.* In *The Oxford Hanbook of Populism* by Kaltwasser, Cristobal Rovira and others: 286-302. Oxford: Oxford University Press.

Taggart, Paul. 2002. *Populism and the Pathology of Representative Politics.* In *Democracies and the Populist Challenge* by Meny, Yves, and Yves Surel: 62-80. London: Palgrave MacMillan.

Urbinati, Nadia. 2014. *Democracy Disfigured: Opinion, Truth and the People.* Boston: Harvard University Press.

OPPORTUNITIES FOR DEVELOPMENT OF EU PROFILE IN THE FIELD OF DEFENCE CAPABILITIES. EUROPEAN DEFENCE FUND

Dragoş ILINCA, Ph.D.*

This article brings to attention one of the main developments recorded in the context of European defence cooperation, namely the establishment of the European Defence Fund (EDF). Conceived as an initiative aimed at contributing to the financial support of cooperation projects in the fields of capability development and defence research, the EDF represents an innovation that began to operate starting with 2021, offering additional perspectives for strengthening the Common Security and Defence Policy. Although it is a new initiative, the European Defence Fund was preceded by preparatory measures in which the necessary procedural framework and mechanisms were defined. From this perspective, the analysis developed in this article deepens the thesis regarding the positive impact of EDF for the sustainability of European cooperation in the field of defence. The strategic value of the new tool for integrating capability development and research aspects is another direction explored in the article. Last but not least, the economic role of EDF benefits of special attention in this study, from the perspective of the way in which various entities from the EU territory perceived EDF, being reflected mainly in the increase of their participation in the drafting projects and participating in competition.

Keywords: CSDP; EUGS; EDF; PADR; EU; EDA; EDIDP; disruptive technologies; defence capabilities; NATO.

Introduction

The decision to create the European Defence Fund is placed in the context of the efforts initiated by the European Commission to support the objectives assumed by the member states through the Global Security Strategy of the European Union (EUGS). Adopted in June 2016, at the level of the European Council, EUGS represented a turning point in the evolution of European cooperation in the field of security and defence which will thus acquire a much better-defined profile in the overall EU policies. The perspective advanced through the EUGS focused on how the interaction between member states on defence aspects can strengthen the role of the EU as a global actor in the international security context.

In this sense, the capabilities development was one of the main topics addressed by the Strategy, with an emphasis on the development of a full spectrum of capabilities according to the objectives and the level of ambition assumed by the EU (response to crises, strengthening the capacities of the partners, protection of the Union and its citizens). The priority was placed on optimizing the cooperation between member states in order to overcome the identified shortfalls under the auspices of the European Security and Defence Policy (ESDP) and, since 2016, in the context of the Common Security and Defence Policy (CSDP), the latter created by the Treaty of Lisbon.

****Institute for Defence Political Studies and Military History, Romanian Ministry of National Defence***
e-mail: *murginski@yahoo.com*

Context of European defence cooperation

Within this framework, the main stages in defining the capability priorities were closely linked to political decisions related to objectives of European cooperation in the field of security and defence. Thus, during European Council in Helsinki (December 10-11, 1999), the first Headline Goal of the EU (HLG2003) was adopted. It aimed to create, by 2003, a Rapid Reaction Force, deployable within 60 days, with a force structure of 50-60,000 people and having the potential to be sustained in the theater for up to a year. In this context, a review process was initiated trough annual Commitment Conferences in which the member states made contributions against Headline Goal. Following the first conference, held in November 2000, a series of capability shortfalls were identified in areas such as: strategic air transport; logistics; force survivability, including evacuation capabilities; communications, command, control, computers and information; infrastructure; surveillance and reconnaissance (European Parliament 2006, 10). The review of shortfalls was approached mainly through a new initiative, which was launched in the aftermath of Laeken European Council, in December 2001. Known as the European Capabilities Action Plan, it represented the first defence planning instrument developed in EU context (European Commission 2001).

Since 2003, the consolidation of member states contributions and the launch of first EU military operations (Bosnia Herzegovina and North Macedonia) had determined the revision priorities within fifteen areas of major interest. Afterwards, the planning activities developed under ECAP were taken over by the European Defence Agency (EDA) which was created in July 2004 (Joint Action 2004/551/CFSP). Almost at the same time, the General Affairs and External Relations Council of 17 May 2004 launched the Headline Goal 2010, which was focused on the improvement of rapid reaction capabilities, especially through the creation of Battle Groups structures. The European Council in 17-18 June 2004 endorsed a new objective (European Council 2004). The new requirements and implications generated by the Battle Groups focused on capabilities, especially in terms of interoperability enhancement, speed of deployment, and sustainability. The main parameters forwarded by EU BG Concept were the generic structure of 1.500 troops, able to operate between 30 and 120 days in the theatre and having the capacity to deploy in 5 to 10 days after EU Council’s decision to launch an operation with recourse to Battle Groups (EU Council 2016).

In this context, the defence planning process will be correlated with the Headline Goals. In 8 July 2008, EDA adopted the very first Capabilities Development Plan (CDP) in which the Headline Goals requirements were approached in connection with the security environment evolutions and technological and industrial developments in the field of defence. From this perspective, CDP became the main guidance for the defence capabilities development in European context. Moreover, CDP was a planning instrument meant to provide the baseline for member states, the priorities forwarded by this instrument being regularly assessed (at 4 years). The first CDP advanced 12 actions/priorities focused on the development of defence capabilities such as: counter man portable air defence systems; computer network operations; mine counter-measures in littoral sea areas; comprehensive approach – military implications; military human intelligence and cultural/language training; intelligence, surveillance, target acquisition and reconnaissance architecture; medical support; CBRN; logistic; C-IED; increased availability of helicopters; network enabled capability (European Defence Agency 2008).

A distinct line of action focused on the need for technological and industrial potential development at national level in order to support the capabilities development, while maintaining a conceptual paradigm centred on deepening the cooperation between member states. The advantages of this approach were reflected in extended areas including operational effectiveness, enhanced interoperability, efficiency and mutual trust (European Union 2016, 20). The basic requirement was the investment consolidation and proper use of the available resources for defence. This topic was associated with EU credibility as relevant actor in the international context. The investment in defence capabilities was approached from the perspective of identifying common priorities for member states in order to sustain the EU external commitments. It involves land, air, maritime as well a space and enablers domains. The criteria used by EUGS to describe the European cooperation status were based on the targets agreed in EDA context, namely: equipment procurement (incl. R&D/R&T): 20% of defence spending; European collaborative equipment procurement: 35% of equipment procurement expenditure; defence R&T: 2% of defence spending; European collaborative defence R&T: 20% of defence R&T expenditure (European Council 2017).

The way in which these targets were met was insufficient, according to the EU Global Strategy. The solutions envisaged were focused on two pillars regarding the consolidation of complementarity and practical synergy between national defence policies in particular on „ gradual synchronization, mutual adaptation of national defence planning cycles”. At the same time, the importance of EU funds was underlined for stimulating the research and technologies under Framework Programs that were created in the 80s. Those programs can provide opportunities for financing the research initiatives applicable in the field of security and dual-use technologies. Nevertheless, FPs could not be used for research in the field of defence. At the time of the EUGS adoption it was running the FP8 (2013-2020), known also under the name “Horizon Europe” with an operational budget of 74.8 billion Euros (European Parliament 2017, 22).

Given the complex nature of the capabilities' development process and the rather modest achievements in research on security and defence, the President of European Commission, Jean-Claude Juncker forwarded, in the State of the Union Speech in 14 September 2016, a more ambitious vision on EUGS implementation. The premise of his undertaking was focused on the EU credibility in military field, while underlining the financial and economic major impact of European cooperation in this domain. In his view, this would be beneficial for accelerating the development of key capabilities in European context (Juncker 2016). In this sense, he announced the establishment of a European Defence Fund meant to stimulate this sector and meant to ensure a better correlation between industrial sector and technological advance, with a special view on innovation capacity.

From vision to practice

In the context created by EUGS, the undertakings focused on consolidation of European cooperation intensified mainly in the second half of 2016. Implementation of the new vision of EU role would be sped-up by adopting a dedicated defence initiatives package with specific relevance, which included three components. The first one was related to the EUGS Implementation Plan (adopted by the EU Council in 14 November 2016) which translate in actionable items the strategic orientations of EUGS. This undertaking should be seen in the larger context of division of labour in the development of the EU security and defence profile, especially on the pol-mil aspects of Level of Ambition assumed by EUGS (European Council 2016b). The second component was the implementation of EU-NATO Declaration, signed on 8 July 2016, in Warsaw. The main feature was represented by the new level of interaction between these organisations through the adoption of a new practical cooperation platform[1].

The third component was by far a novelty for the last decades of cooperation in the field of European security and defence cooperation. For the first time, the European Commission got involved in some key aspects of this domain. Thus, Commission's contribution reflected in the European Defence Action Plan (EDAP). This initiative was three-fold, consisting of: creation of European Defence Fund; development of investments for the entire defence supply chain; consolidation of single market in the field of defence. Obviously, this undertaking followed the EUGS patterns and underlined by the President of European Commission two months before. From this perspective, the creation of European Defence Fund provided an answer to the question of how EU profile in the field of security and defence will be sustain financially. On this line, the Commission proposal structured EDF on two components (windows) – capabilities and research, both financed through EU budget. Taking into account the specific character of EU multiannual budget, the EDF was scheduled to enter into force from 1st January 2021 and it will be financed for the entire period of EU Financial Framework 2021-2027.

The main objective of “capability window” was to finance the cooperation projects with the participation of member states in the field of capabilities development. This approach was an answer not only to the relatively insufficient level of coordination between member states in this area, but also to the difficulties to identify additional resources at national level. From this perspective, EDF could be seen as a complementary tool for supporting the member states' efforts in the field of capabilities development. The budget proposed by the European Commission was 5 billion Euros/year for the capability window. This ceiling was considered to allow the fulfilment of EDA target regarding 35% for collaborative projects developed in the European context (European Commission 2016, 9). As regards the “research window”, the Commission proposal was focused on creating another opportunity to finance the collaborative projects in the field of

[1] Through EU-NATO Declaration, a set of cooperation areas was forwarded such as: resilience, hybrid, cyber security, capabilities, defence industry, exercises. Two years later, this inventory will be consolidated by the second Declaration signed on 10 July 2018, in Warsaw.

research, technologies and innovation, which could complement the undertakings developed so far. Definitely, it was not the case for replacing those programs, EDF being designed to stimulate the defence research, which was not approached in the European context. The budget proposed by European Commission for the “research window” was 500 mil. Euro/year starting from 2021.

On 15th December 2016, the European Council endorsed the Commission’s proposal regarding the establishment of European Defence Fund asking to identify the possibilities to involve the European Investment Bank in supporting the research and development in the field of defence. At the same time, the European Commission was tasked to initiate the preparation measures to create the necessary framework for EDF entry into force as it had been scheduled. (European Council 2016a, 4). It is worth mentioning here that EDF launch was an absolute novelty both from the perspective of its own functionality and from the perspective of the use of financial support through EU budget. These were the reasons that determined the idea to take advantage of the period 2017-2020 for preparing the proper conditions for getting a fully operational EDF.

The main steps in this direction took shape in the establishment of ad-hoc instruments meant to test the feasibility of procedural framework for drafting the collaborative project and the parameters of the review process for projects competition and, subsequently, the process of awarding the grants. The European Commission performed the first undertakings in the field of research area by launching the Preparatory Action on Defence Research/PADR (2017-2020) with 90 mil. Euro budget. During this period, under PADR there were launched 10-project calls in various areas such as disruptive technologies, electromagnetic spectre dominance; autonomous systems; force projection etc. In this context, 18 cooperation projects were financed while more than 200 entities from member states (private-owned companies, education-research, and public sector) participated. Typology used for generating the projects was centred on deepening the cooperation under consortia like model with the participation of entities from member states. In this framework, the minim requirements were that consortia must include at least three entities, from the three member states. The main responsibilities for drafting the PADR working programme was retained by the Commission, which could delegate the implementation responsibilities to other EU structures. This procedure would be used in relation with European Defence Agency, which would take the main responsibility for PADR implementation, based on an Agreement with EU Commission (31 May 2017).

The PADR experience would be continued at a higher level in the framework of the new mechanism established in 2018, known as European Defence Industrial Development Program, which would integrate research and development components. It was designed to function for the next two years with a budget of 500 mil. Euro. At large, the procedural typology developed under PADR would be maintained, especially on finance, drafting the projects and forwarding for competition.

As regards the areas approached, EDIDP ensured the required continuity with PADR, mainly on the projects that required more than two years for completion. At the same time, the areas of competence were structured in the spirit of multidisciplinary approach, being also better connected with the CDP priorities and EUGS level of ambition. Thus, an expanded set of areas was taken into account such as remotely piloted systems, satellite communications, positioning, navigation and timing, autonomous access to space and permanent earth observation, energy sustainability, and cyber and maritime security, as well as high-end military capabilities in the air, land, maritime and joint domains, including enhanced situational awareness, protection, mobility, logistics and medical support and strategic enablers (EUR-Lex 2018, 1). The outcome of the two EDIDP years of operation consists in financing 44 projects involving more than 700 entities from EU. It is also worth mentioning that 15 projects (out of 44) were in line with the commitments made by member states under Permanent Structured Cooperation, which was activated[2] at the end of 2017, based on

[2] In 13 November 2017, 25 member states signed a Notification for High Representative for Foreign Affairs and Security Policy in which they informed about the decision to activate the provisions of EU Treaty regarding the Permanent Structured Cooperation (PESCO). Consequently, in 11 December 2017, EU Council adopted the Decision to launch PESCO. This initiative developed in two phases

EU Treaty (Art.28A, E). In accordance with the agreed parameters for EDIDP, the PESCO projects were eligible for a higher rate of financing.

Principles and governance

The EDIDP contribution to paving the way for EDF was extremely important. In fact, EDIDP served as an antechamber in which the entire set of procedures and governance model were tested in order to facilitate the interaction not only between member states, but also between EU structures and relevant implementing actors. At the same time, the EDIDP relevance is visible in the consolidation of cooperation between EU member states in terms of defence. The genuine interests of entities to participate in the competition for EU grants validated the importance of projects in EDF context. Practically, the attraction of those projects was the main factor, which generated a sharp increase in the number of participating entities.

Taking into account these aspects, the main objective of EDF was to contribute to consolidating the capacity for innovation, efficiency and technological competitiveness of European defence industry. In this sense, the pursued priorities meant to reduce the European fragmentation in the field of defence simultaneously with the increasing of output investments in defence for the economic and industrial areas. Special attention was dedicated to the SME involvement in this kind of cooperation as well as to the development of a functional partnership with European defence industry and with other international actors. For those aspects, EDF was intended to act as a stimulus. Extremely relevant in this equation was the added value of EDF in relation with the normative framework of EU in the field of defence. This included both the Directives[3] for internal market as well as the initiatives developed almost in the same period under CSDP.

From this perspective, the EDF role could be seen as being a niche one, focused on creating financial opportunities to support the implementation of EU priorities in research and capability developments through collaborative approaches between member states. Nevertheless, it must be noted that the level of ambition on the financial margin was severely downgraded. Actually, the EDF budget was decreased significantly comparing with the initial proposals made by the Commission. This situation was generated by the overall context of negotiations regarding Financial Framework 2021-2027 and the need to accommodate the implication of the United Kingdom decision of to leave EU. Consequently, the financial envelope agreed for EDF running between 2021-2027 was almost 8 billion out of which 5.3 million for development and 2.7 million for research (European Commission 2020, 2). Nevertheless, we should underline that for the first time in EU history its budget included distinct allocation for defence consisting on two components – EDF and Military Mobility[4]. In this context, EDF is an instrument dedicated to sustaining financially the member states’ efforts thus ensuring co-financing, in different ratios, the actions undertaken in collaborative framework (EUR-Lex 2021, 169-170). At the same time, EDF added value could be seen from the perspective of stimulating innovative character in defence context. Thus, the parameters agreed for EDF included the requirements to allocate between 4% and 8% from the total budget for disruptive and emergent technologies projects (EUR-Lex 2021, 162).

The EDF functional parameters were almost similar to those used in PADR and EDIDP. Thus, the main responsibility for EDF management lies with the European Commission, while the current activities are coordinated through a Program Committee consisting of member states representative and EU structures (European Defence Agency 2007). This committee is responsible for drafting the Annual Working Program, including the main areas for EDF activity in the respective year and for which projects will be delivered. The sources of inspiration for setting up the Annual Program are the priorities agreed in CSDP context as it is the case for CDP, CARD, PESCO as well as other projects and programs coordinated by European Commission in the field of security. The areas agreed through the Annual Program have, in fact, multiannual relevance being implemented in an extended period allowing, thus,

(2018-2021 and 2021-2025) reaching 60 cooperation projects that were developed under PESCO aegis.

[3] Practically, there were Directive 2009/43/EC simplifying terms and conditions of transfers of defence-related products within the Community and the Directive 2009/81/EC.

[4] Military Mobility budget was 1.7 billion for 2021-2027.

a better planning of national resources. From this perspective, the Annual Program includes domains like medical (including CBRN and response capacity), informational superiority, cyber security, space, digital transformation, energy resilience – environment transition, materials, air and ballistic defence, land capabilities, force protection and mobility, maritime capabilities, underwater combat, simulation and training, disruptive technologies, innovative defence technologies (European Commission 2022a, 4).

In this context, the Annual Program provides the general framework for EDF activities. Every area/category is detailed in subjects/topics and, subsequently, in actions. Within this process, the European Commission is responsible for launching calls for projects taking into account the subjects' inventory. The eligibility criteria agreed in EDF context were that consortia consisting no less than three entities from at least three member states must deliver projects. In case of disruptive technologies, consortia membership could be limited at two entities from two member states (EUR-Lex 2021, 165). The review process for the proposed projects is made by European Commission based on several criteria agreed by member states for EDF and corresponding with the objectives of this instrument (EUR-Lex 2021, 166).

Under these auspices, European Commission launched, on 30 June 2021, 23 calls for projects against the above-mentioned areas involving more than 40 subjects. The interest of the entities from EU Member States was maintained on the upward trend similar to the one of the previous EDIDP cycles. Thus, there were forwarded more than 140 projects proposals out of which 61 were selected for co-financing on both windows. The EDF increased attractivity was reflected, also, in the large number of entities involved in projects competition (almost 700) coming from various areas like companies, SMEs, universities, research laboratories. These were coming from 26 member states, participating in various types of consortia established within the scope of supporting collaborative initiatives under EDF. The budget for EDF first year was 1.2 billion (845 million for capability developments and 322 million for research). The objective regarding the development of EU economic profile in the field of defence was reflected in raising at 43% SMEs participation in projects awarded. At the same time, the financial absorption level by SMEs in EDF 2021 was 18%. At the same time, in terms of stimulating innovative character, almost 20% of the funds were allocated to the projects for disruptive technologies, innovative materials and digital transformation. Moreover, the significance of the first year should be seen in the context of interaction between EDF and the other initiatives developed under CSDP. It is notable the connection between EDF and PESCO in which 20% of projects being developed in the context of Permanent Structured Cooperation (European Commission 2022b). For the second year, on 25 May 2022, the European Commission adopted the respective Annual Program having a budget of 926 mill. In the spirit of continuity with the undertakings developed under EDF 202, the project calls were launched in June 2022 being structured on the same categories. The deadline for submission of projects by the consortia established with entities from EU is November 2022.

Conclusions

Obviously, the establishment of the European Defence Fund was one of the major evolutions in developing EU's defence profile. At the same time, the creation of this new instrument corresponds to a new phase in the overall dynamic process of consolidating European shape in defence development and research. From this perspective, EDF's role has to be underlined as an integrated platform of two dimensions which ensure a better connectivity of European cooperation with technological and innovation developments in the field of defence.

At the same time, EDF was coming in a specific context, created by political decision associated with the Headline Goals 2003 and 2010, answering, also, to the EU Global Strategy new level of ambition. In this context, EDF is representing one of the answers constantly searched for in the last two decades for consolidating the baseline of European defence cooperation. Besides being a novelty from the perspective of using EU budget for co-financing the cooperation programs, EDF is an integral part of the ascending approach, which started with the Framework Programs coordinated by European Commission. Equally, EDF is providing additional opportunities for consolidating the collaborative approach in the field of defence. The matrix advanced though annual cooperation programs was welcomed by the economic and industrial sectors. This approach was reflected through the consistent number of participating entities in projects competition. From this perspective, there is no doubt that EDF has the potential to be a catalyst for intra-European cooperation, its credibility being sustained trough financial support for practical projects.

BIBLIOGRAPHY

EU Council. 2016. “European Union Battlegroup Concept.” 11624/14, Brussels. https://data.consilium.europa.eu/doc/document/ST-11624-2014-EXT-1/en/pdf.

EUR-Lex. 2018. “Regulation (EU) 2018/1092 of the European Parliament and of the Council of 18 July 2018 establishing the European Defence Industrial Development Programme aiming at supporting the competitiveness and innovation capacity of the Union’s defence industry.” https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1092.

—. 2021. “Regulation (EU) 2021/697 of the European Parliament and of the Council of 29 April 2021 establishing the European Defence Fund and repealing Regulation (EU) 2018/1092.” https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32021R0697.

European Commission. 2001. *Presidency Conclusions, European Council Meeting in Laeken, 14-15 December 2001*. https://ec.europa.eu/commission/presscorner/detail/en/DOC_01_18.

—. 2016. “Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. European Defence Action Plan.” COM(2016) 950 final, Brussels.

—. 2020. “Multiannual Financial Framework 2021-2027.”

—. 2022a. “Commission Implementing Decision on the financing of the European Defence Fund established by Regulation (EU) No 2021/697 of the European Parliament and the Council and the adoption of the work programme for 2022.” C(2022) 3403 final, Brussels.

—. 2022b. *Results of the 2021 EDF Calls for Proposals.* European Defence Fund.

European Council. 2016a. “European Council meeting (15 December 2016) - Conclusions.” EUCO 34/16, Brussels. https://www.consilium.europa.eu/media/21929/15-euco-conclusions-final.pdf.

European Council. 2016b. “Implementation Plan on Security and Defence.” 14392/16, 14 November. https://www.eeas.europa.eu/sites/default/files/eugs_implementation_plan_st14392.en16_0.pdf.

—. 2017. “Notification on Permanent Structured Cooperation (PESCO) to the Council and to the high representative of the Union for foreign affairs and security policy.” November 13. https://www.consilium.europa.eu/media/31511/171113-pesco-notification.pdf.

—. 2004. “Presidency Conclusions – Brussels, 17 and 18 June 2004.” https://www.europarl.europa.eu/summits/pdf/bru0404_en.pdf.

European Defence Agency. 2008. “Background Note – Capability Development Plan.”

—. 2007. “EU Ministers Adopt Framework for Joint European Strategy in Defence R&T.” November 17.

European Parliament. 2006. “The European Security and Defence Policy: from the Helsinki Headline Goal to the EU Battlegroups.” https://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede030909noteesdp_/sede030909noteesdp_en.pdf.

—. 2017. “EU Framework Programmes for Research and Innovation.”

European Union. 2016. “Strategia Globală de Securitate a Uniunii Europene.”

Juncker, Jean-Claude. 2016. “State of the Union Address 2016: Towards a better Europe - a Europe that protects, empowers and defends.” European Commission - Speech, Strasbourg, 14 September.

JOINT OPERATIONS – THE CONTINUITY OF A FUNCTIONAL INSTRUMENT

Commander Alexandru CUCINSCHI, Ph.D Candidate*
Captain (ret.) Prof. Ion CHIORCEA, PhD**

With the emergence of the notion of multi-domain, all the elements that until now have been associated with the notion of joint, be it battle, operation or formation (in the sense of structure) have become associated with this new fashionable notion, which seems that it tends to replace the older notion of joint. However, we appreciate that the notion of joint should lose neither the importance it has had up to now, in the sense of a concept that has been applied and proved functional, shaping to a large extent the development of the military instrument of power, nor the possible evolutions of this concept, given the solid ground on which are now those who have implemented a joint mode of operation. Thus, in this article we aim at highlighting the main reasoning that have led to the emergence and application of this concept (joint) until now, then describing the current security environment and its implications on the operational level; later we will propose a completion of the joint operations, so that it can be applied under current and future threats.

Keywords: joint; joint operation; threat; security environment.

Compensating the shortcomings/vulnerabilities of one service through the strengths of another service, thus achieving a synergy between at least two services, we appreciate that it can be considered the essence of a joint operation.

Although the same reasoning can be applied within a service by achieving synergy and compensating for gaps between combined arms, the relatively low scale of this type of support generally does not allow the relationship to be classified as *joint*.

However, by widening the palette of types of forces within a service, such as aviation from the composition of the Land Forces and Naval Forces units, we appreciate that the notion of *joint* has begun to include all relevant military actions (in the sense of their scope).

Thus, in addition to strictly planning and conducting a military action, the involvement of other institutions in the National Defense System (inter-institutional level) is also included in the meaning of the word *joint*.

We notice that the notion of *joint* is applied at the tactical, operational, strategic-military and strategic-political level, a fact that indicates to us, on the one hand, the value of the notion itself, being able to describe a wide range of activities, as well as on the other hand, a possible misunderstanding of this concept, in the sense of extending it to activities that do not represent it and are not specific to it (Example: the inter-institutional level – at this level we appreciate that few aspects to achieve synergy can be managed).

As a result, in order to highlight what we consider to be essential to the notion of *joint*, we believe that a return to the origins of the joint operation is necessary and may free it from the elements added later (not all additions have been tested and validated) by those (theoreticians, researchers and teachers in the field of military science) who participated in the improvement, in most cases, of the concept of *joint*.

Thus, in order to highlight the essence of the joint operations, the research methodology will focus on the application of the longitudinal research method, which aims to identify the regularity of the elements that are characteristic to joint operations as well as the deficiencies found during the conduct of such operations. Later, the transversal research method will allow us, by identifying the particularities of the current security environment, to discover the extent to which the

”Carol I” National Defence University, Bucharest
e-mail: *cucinschi.alexandru@gmail.com*
”Mircea cel Bătrân” Naval Academy, Constanța
e-mail: *chiorcea44@yahoo.com*

joint operation can be applied in its current form, and, consequently, we will conclude with some considerations regarding its possible evolutions (predictive method).

We believe that the limits of research should also be mentioned: thus, the options for improving joint operations, which we propose through this article can be implemented under the conditions in which a certain conventional linearity is preserved in the way in which a military action is conducted. Also, in order to obtain relevant data, in the sense of accurately identifying the extent to which the method of improving joint operations by the elements mentioned in this article, it is necessary for these elements to be tested, in the first phase, through war games or simulation (in this article we only propose an improvement of a concept).

Origins of joint operations

According to the generally accepted definition of the current joint operation: operation in which at least two services are involved, under single command; the vast majority of military actions that were located in the vicinity of the sea or involved the projection of force over distant territories can be categorized as joint.

However, we consider that although they tick the elements contained in the definition of the joint operations and fall within its letter, they can hardly be considered in the spirit of the joint operations. Thus, campaigns such as:

- the land-sea campaign in Sicily, 415 BC - 413 BC, in which an Athenian land expeditionary force (5,000 infantry and archers who planned to conduct land operations) used ships (about 100 triremes, numerous transport and cargo ships) to secure the strategic island off the coast of Italy (Sicily) which, it was considered, would have offered a decisive advantage in the war with Sparta (Carafano 2018, 24);

- the Invincible Armada campaign in the Anglo-Spanish War of 1588, which aimed to position the fleet in the English Channel and use land forces in the Netherlands, ultimately proving to be a plan far too ambitious for the Spanish Army (Murray 2002, 30);

- the Gallipoli campaign of 1915, in which although the Allies transported land forces by sea, later trying to support them with artillery strikes in the enemy-held territory and benefited from the uncontested use of the sea, through their inability to move quickly, decisively and using good practice, the joint force yielded all important advantages to the Turks, who used the control of the land environment more effectively (Murray 2002, 32); they focused on executing actions specific to each service and not on achieving a synergy in the campaign as a whole, not being able to compensate for vulnerabilities or enhance strong elements that could have brought success to the joint force.

Thus, the fact that the triremes and transport ships of the Athenians transported the land forces, the Spanish ships established a blockade in the English Channel and the British ships tried to sweep the Dardanelles and bombarded the coastal area, proves that, in this case, the Naval Forces actions carried out actions specific to this service, actions which, although they can be considered to be in support of land forces, by not fitting into the general idea of the joint operation, which is to obtain an effect on the adversary greater than the sum of the effects of the services, we consider that it greatly dilutes the name of the joint campaign, although as we mentioned before, the strictly descriptive elements of the joint operation are fulfilled.

On the other hand, we must admit the fact that, within the mentioned campaigns, the technological level did not allow for a synergy in the true sense of the word, the pace of actions being much slower compared to what was going to happen in the Second World War.

In contrast to these campaigns, in which only the composition of the force can be considered of joint type and the services executed actions specific to the environment in which they operated, the first campaign, which is considered by many experts in military sciences (Hooker and Coglianese 1993) to be truly joint is Operation Weserubung – the code name for Nazi Germany’s assault on Denmark and Norway during World War II on April 9, 1940.

The Weserubung operation can be considered one of the most remarkable applications of the operational art and principles of war, the principle of surprise playing an important role in the German success. The planning made by the German forces, that took into account and exploited the factors of time, space and forces, is another key element in this operation. Also, the fact that the land forces, the navy and the air forces (Heer, Kriegsmarine, Luftwaffe) fought as a team even though they faced the reluctance of the commanders of these services to subordinate themselves to each other and Hitler had to be considered the commander of this operation, it allowed the German Military to defy the Royal Navy by transporting troops directly to their objectives along the Norwegian coast (Hooker and Coglianese 1993).

Analyzing the elements that led to the success of this operation, even in the face of a superior adversary, mainly at sea, led us to a series of lessons that, in our opinion, are still neglected nowadays, most likely due to human considerations, in the sense in which we believe it can be affirmed that the level of training (discipline, intelligence and understanding of the situation in a pragmatic way) achieved by the German military at the beginning of the war was unmatched.

Thus, from the Germans we may learn about the importance of planning and turning apparent disadvantages into opportunities, connecting command and control to operational objectives and commander's intent, and the importance of initiative in military operations (Rice 2007).

In this operation, Germany engaged a joint force in a simultaneous assault, using centralized planning and decentralized execution, utilizing multiple corridors of approach, and having six key objectives. The objectives targeted and exploited the Allies' centers of gravity. Applying force to weaknesses, the Germans crushed Denmark in a single day and destroyed the Norwegian resistance in two months despite the fact that it was supported by strong British and French forces.

This we consider to be the most eloquent example of a joint operation, which in fact represents the implementation of the German military genius of the time, in the letter and spirit of the joint operation.

However, although it is considered the first joint operation in the true sense of the word, one important aspect of what the joint operation truly represents was not possible: commanding and controlling the joint force during the action, which was not possible due to the pride of the commanders of the different the armed forces services; they did not accept the fact that on a certain phase of the operation the service they lead could be less important and thus act in support of another service.

After the Second World War, military thinking continued to be limited to competition among services, each service claiming the possibility of winning the war using only its own means. In addition to these, a new theory emerged, a theory that claimed that strategic dominance could be achieved through nuclear deterrence. During this period, the European countries (many of them NATO members), impoverished after the Second World War, were not willing to consume resources for building classic capabilities (ships, aircraft, tanks) and relied on the nuclear weapon as deterrence.

Despite the lessons learned in World War II, where joint operations proved necessary, little was done to institutionalize joint operations (Carafano 2018, 26).

Thus, until the initiation of the implementation of the air-land battle, which represented a revitalization of the joint operations, this tool patented by the Germans at the beginning of the Second World War and also employed by the other militaries during the war, was not used to its true potential.

Air-land battle – the joint concept that influenced the configuration of the NATO Force Structure

Air-land battle is a concept that falls under joint operations which formed the basis for the modernization of the US Military in the 1970s and 1980s and was subsequently implemented by NATO and NATO members.

The modernization of the US military system was made possible by the establishment of a command (TRADOC[1]) intended for the development of military action (improvement of organization, equipment, weaponry and doctrine) on July 1, 1973 (Del 2017, 37).

The model proposed by TRADOC is the one that led the entire transformation process of the army, being promoted by the publication, in 1981, of TRADOC PAM 525-5, US Army operations concepts, the AirLand Battle and Corps 86, thus introducing the operational concept of air-land battle.

The implementation of the concept began to crystallize with the publication, in 1982, of a

[1] Training and Doctrine Command.

manual that defined the concept of air-land battle, FM 100-5 Operations, and later, even the Naval Forces expressed the intention to implement this concept by publishing a report, in 1988 (Skinner 1988) explaining how it could influence Marine doctrine and maritime strategy.

Next, we will briefly present the main elements that made up this concept-based modernization of the armed forces (Figure No. 1) in order to facilitate the understanding of how the joint operation was revitalized, as well as the complexity of the process as a whole.

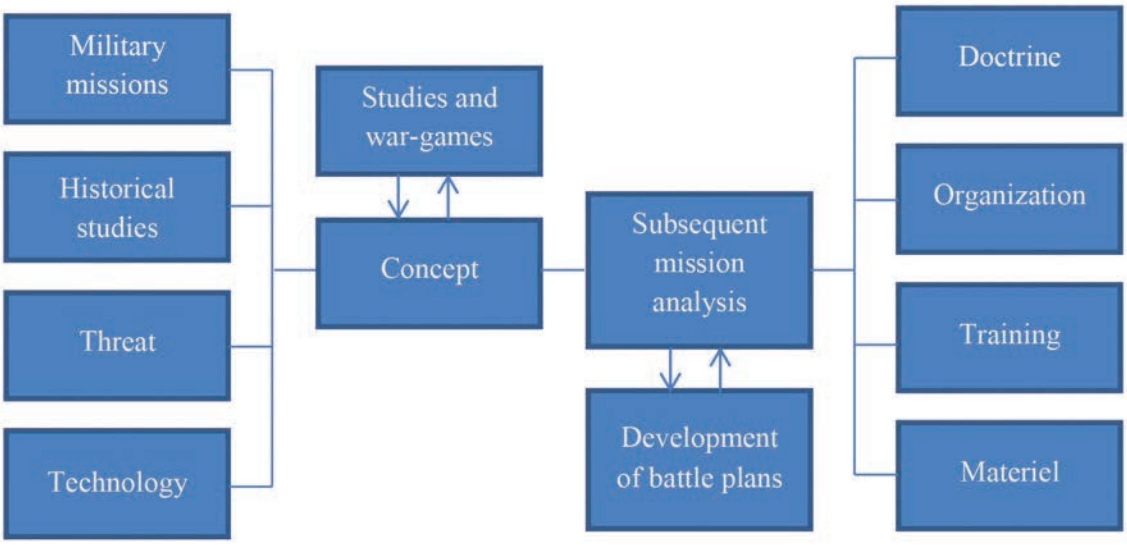


Figure no. 1 Concept based requirement system (Brownlee and Mullen III 1988)

Thus, the main input factors (currently defined as the future operating environment, in the present case – missions, historical studies, threat, technology) on which the concept developed were represented by:

- the identification of a new pattern of conducting the fight by the potential adversaries (in this case, through intermediaries) - The Fourth Arab-Israeli War, October 6 - 25, 1973, between a coalition of Arab states and Israel, in which the Arab Armies, although they were finally repelled by the Israeli Army, being equipped with the latest Soviet technology, they advanced very quickly and in a surprising way into the opponent’s territory (History.com Editors 2018);

- the impossibility of winning a war – the lessons identified from the Vietnam War formed the basis of the air-ground battle concept, motivated by the desire of the US Ground Forces to avoid this type of asymmetric warfare (Malkasian 2014, 115) which, as recent history has shown, was not a strong point of the concept, with the US Army having to deal with various such situations in conflicts following the concept’s implementation;

- increasing combat power (physical, moral and conceptual components) of the USSR – *“the fact that matters is that there is not enough depth of field to fight on and not much space to afford to lose – in the end, as I have described several times, the fact that the reserves of the Soviet Union are much closer than the reserves of the United States, and that the reserves of the Soviet Union are much larger. So when the battle starts we are at a disadvantage and as the war goes on it gets worse”* (Brownlee and MullenIII 1988, 191).

Based on these input factors, the concept proposed by General Starry, commander of TRADOC involved managing the fight with the USSR Military by using army corps as the main combat unit, combining practices that did not represent an element of novelty (maneuver warfare[2], blitzkrieg[3], deep operations[4]), but which were based on superior technology compared to the one of the opponents.

In addition to these elements specific to the Land Forces, the Air Force had the mission of engaging the enemy especially in depth (together

[2] Defeating the adversary by rendering him unable to fight coherently (not by destruction), using a series of tactics to avoid strong points and quickly and aggressively engage vulnerabilities with the aim of morally and physically crippling him.

[3] Fast planning and execution cycle.

[4] Engaging the enemy not only at the contact line but also in the depths of the battle space.

with the artillery), thus preventing them from introducing the second echelon into battle and creating an operational advantage for the Ground Forces – known today as air interdiction as well as close air support.

Testing the validity of the concept was made possible through a series of war games, being the first concept to be tested largely through the use of simulation systems, which reduced the costs to this purpose.

Regarding the capabilities developed having this concept as a basis, it should be noted that not all of them were developed according to the specific requirements, largely due to the fact that sometimes the armament manufacturers were able to influence the procurement decisions.

Full implementation of the concept ended in the late 1980s, coinciding with the breakup of the Soviet Union, which is why this arms race is considered responsible for this collapse.

This rendered nonexistent the threat on which this concept-based modernization process was developed and, as a result, its effective application was no longer possible.

The fact that NATO adopted the air-ground battle, a concept initiated by the US army in 1984, an aspect also proven by its current force structure (consisting of army corps, more recently divisions and brigades also appeared) shows that this concept was implemented and correctly addressed the issue at the time, becoming an operating concept that is still used today.

The implementation of the concept in the Romanian Military was not possible, considering the fact that Romania was a member state of the Warsaw Pact with a different concept of operation, which was based on the number of forces, echeloning, few aspects related to the joint operation and the support among the services being exerted.

Problems encountered by joint operations in the current security context

Currently, actors such as Russia and China have developed new methods of conducting military actions, methods that are largely based on advanced technology, long-range and high-precision weaponry. The complexity of the current environment also comes from the implementation by the two states of different methods of conducting military actions, with the main goal of denying access (A2AD) to increasingly larger areas, Russia specializing in the terrestrial environment and China in the marine one.

Thus, the threat at the operational level is a result of both pragmatic issues, such as studying the traditional US mode of action in recent operations (Desert Storm, Iraqi Freedom and Enduring Freedom) which was based on multinational joint operations, technological dominance, global projection of power, maneuver at tactical, operational and strategic level, effective combined fire system, logistical support and the initiative resulting from the application of the mission command concept (TRADOC Pamphlet 525-3-1 2018, i) as well as some issues related to the application of operational art – tactics, logistics, and advantageous prepositioning are disrupted by the use of A2AD.

The result of the two components led to the denial of strategic depth through specifical military means that aim to separate in time, space, and combat functions the US and its strategic allies located in the area contested by China and Russia.

The fact that Russia and China have invested over the past 25 years in developing an approach to “fracture” the air-ground battle by countering operational phasing over time and support between services, which have become increasingly predictable, means that the joint operations can be conducted only if the environment in which it is carried out is not contested, the sequencing of the operation being possible so that the Naval and Air Forces can engage the enemy by weakening his combat power, after which he is engaged by the joint forces (TRADOC Pamphlet 525-3-1 2018, vii) leads us to the need to approach military operations from a new perspective.

This fact can be achieved by developing a new operating concept, as is the case nowadays, by developing the multi-domain operation or by perfecting/improving existing operating concepts, as we believe may be the case of the joint operations (air-ground battle).

An update option of the joint operation

Currently, the joint operation as it has developed since the Second World War and culminated in the air-ground battle, can still be applied in this form only in spaces that are not contested by the use of specific means of A2AD.

The problem is that these spaces are getting smaller and smaller and are located in areas outside the spheres of influence of the great powers. Most likely, in the future, this type of “classical” joint operation will no longer lend itself to these areas either, considering the fact that the military instrument of power is less and less involved in the fulfillment of the established objectives, these objectives can be fulfilled more easily and discreetly through the other instruments of power.

As a result, we consider that in order for the joint operation, which is in fact the tested and validated method of conducting military actions (as opposed to the new concept of multi-domain operation) to be able to respond to current threats, it must be supplemented with layered defensive systems, on each environment (example: The Iron Dome model) to transform contested space into uncontested space where own forces can maneuver and support each other.

The problem that arises, in this case, is the fact that this space covered by the defensive systems is relatively small, which makes this type of operation lend itself, mainly defensively, on own territory.

However, we consider that, in the future, with the development of systems specifically intended for this purpose, this area can expand and eventually merge with areas developed by allies which develop the same type of concept.

In addition to this defensive area, we believe that, in order to be able to respond to current challenges, joint operation must also meet the following conditions:

- to tend towards the simultaneity of actions and not their separation in time and space, on the model of the supported - supporting commander;
- to include the cyber environment and space – they must be able to represent a real force multiplier, through preventive/offensive actions (as opposed to this type of operation which, as we mentioned, lends itself to the defensive);
- to obtain interconnected services in order to have an appropriate level of readiness, (not coordinated or synchronized).

We should also mention that the joint operations are, in our opinion, part of the multi-domain operation and that the fourth phase (according to TRADOC Pamphlet 525-3-1, 2018) of the multi-domain operation (exploitation) can be carried out under the form of a conventional joint operation

Conclusions

Because the history of armed conflicts has shown that it is preferable to improve an existing concept or the development of a new concept should be done from the perspective of the concept that is tested and validated, and considering the financial effort to implement a new concept, as we have previously mentioned that it was also the case after the Second World War (the implementation of the joint operation was delayed due to lack of funds and political will), we consider a viable option to update the joint operations in the version proposed by us or in another version that responds to threats from a certain region, an update which, although not a major change in military science, can contribute to the short and medium-term management of the identified threat.

Moreover, we believe that adding specific actions from the two new environments – cyber and space (recognized as operating environments in 2016 and 2019) to the conventional joint operations can create many “dilemmas” for a potential adversary so that the joint force will benefit from an operational advantage on the battlefield.

In conclusion, considering the arguments presented in this article, we believe that the “joint” notion and implicitly joint operations, provided that they are fully understood both in letter and in spirit, will continue to represent both a model of good practices and a landmark in the development of new concepts.

BIBLIOGRAPHY

Brownlee, Romie L., and William J. Mullen III. 1988. *Changing an Army. An Oral History of General William E. DePuy, USA Retired.* https://history.army.mil/html/books/070/70-23/CMH_Pub_70-23.pdf.

Carafano, James J. PhD. 2018. “America’s Joint Force and the Domains of Warfare.” *The Heritage Foundation.* https://www.heritage.org/sites/default/files/2017-09/2018_IndexOfUSMilitaryStrength_CARAFANO.pdf.

Del, Stewart. 2017. “Victory Starts Here. A Short 45-Years History of the US Army Training and Doctrine Command.” Combat Studies Institute Press. US Army Combined Arms Center, Fort Leavenworth, Kansas.

History.com Editors. 2018. *Yom Kippur War.* https://www.history.com/topics/middle-east/yom-kippur-war.

Hooker, Richard D. Jr., and Christopher Coglianese. 1993. “Operation Weserubung and the Origins of Joint Warfare.” *National Defence University.* Washington, DC: Institute for National Strategic Studies, Fort Lesley J. McNair. https://apps.dtic.mil/sti/pdfs/ADA528871.pdf.

Malkasian, Carter. 2014. “Air land Battle and Modern Warfare.” *International Forum on War History: Proceedings.*

Murray, Williamson. 2002. *The Evolution of Joint Warfare.* https://apps.dtic.mil/dtic/tr/fulltext/u2/a426537.pdf.

Rice, Mark A. Lieutenant/USN. 2007. *THE PRACTICE OF OPERATIONAL ART IN OPERATION WESERUBUNG: The German invasion of Norway in 1940.* Newport: Naval War College. https://apps.dtic.mil/sti/pdfs/ADA470823.pdf.

Skinner, Douglas. 1988. “Airland Battle Doctrine.” Center for Naval Analysis, Virginia. https://apps.dtic.mil/sti/pdfs/ADA202888.pdf.

TRADOC Pamphlet 525-3-1. 2018. *The US Army in multi-domain operations 2028.* https://adminpubs.tradoc.army.mil/pamphlets/TP525-3-1.pdf.

HOW THE RUSSIA-UKRAINE WAR MAY CHANGE THE CYBERCRIME ECOSYSTEM

Student Claudia–Alecsandra GABRIAN, Ph.D. Candidate*

According to statistics, in recent years there has been an increase in cyber-attacks and their negative impact on individuals, organizations, and governments. Cyber attackers have acquired the resources and expertise to launch massive attacks against other nations to gain strategic advantages, mainly targeting critical infrastructure and public services. Current geopolitical events, through the action launched by the Russian Federation in Ukraine, demonstrate that cyber security threats are ever greater. States' responses to these challenges must be quick and effective, adapted to this context. Over the past year, Russian cybercrime groups have strengthened their position as threats to the global digital ecosystem, demonstrating adaptability, persistence, and a willingness to exploit computer systems. This paper will analyze how cybercrime groups have been more present in the international space due to this war, as well as the importance given to them due to the types of attacks launched and their division into belligerent support camps.

Keywords: Cyber Attacks; Cyber Crime Groups; Ransomware; Cyberspace; Cyber Security; Resilience.

Cyberspace represents an environment of strategic importance, which is made up not only of the Internet and all the technologies, respectively hardware and software interconnected globally, but also of the actions carried out by their users, which make it possible to generate, process, store or transmit data in electronic format. To protect such systems, a better understanding of cybercrime is a necessary condition in order to develop appropriate responses to prevent and combat these types of threats. This phenomenon of cybercrime has global implications, transcends geographical borders, and can be carried out from anywhere, against any person and any technology. There is no single definition of the term cybercrime, but it describes a variety of illegal crimes or what is considered illicit behavior by individuals/groups that launch attacks on critical IT devices, networks, systems, and infrastructure (Donalds and Osei-Bryson 2019).

In response to these ever-growing and ever-present threats, governments around the world have adopted strategies and enforced them through legal frameworks to establish better computer security, a concrete example being Computer Incident Response Teams (CSIRTs, referred to in usual CERT mode), to improve response. They investigate and prevent these types of illicit cyber activities involving the use of information and communication technologies (ICT). According to Ngafeeson, the classification of cybercrime is one of the three important elements to combat it, and Barn argues that a better understanding of cybercrime is a necessary condition for developing appropriate responses and for correct estimates of economic costs, in particular (Donalds and Osei-Bryson 2019). (Donalds, Osei-Bryson, 2022).

The meaning of the term "hacker" has changed over time, and the activities of hackers are usually seen as illegal actions operating in hidden environments, but this is true when they cause intentional damage to society's information systems. Hackers are the primary agents of cybercrime, and their subculture is complex and encompasses multiple motivations, degrees of idealism, and skill sets. Attackers are individuals or groups of individuals who attempt to exploit vulnerabilities, often for personal or financial gain, and they may work for governments conducting espionage for the new battlefield (Sabillon, et al. 2016).

Hacking becomes illegal once it crosses the threshold of gaining unauthorized access to computer systems. Hackers are classified into several categories such as white hats, which work under ethical hacker laws or as security experts; gray hats, who work as security consultants, and black hats, who are motivated by power, anger, or hatred, and have no qualms about stealing or destroying data from networks. Another

****Babeș-Bolyai University, Cluj-Napoca***
e-mail: *claudiaalecsandra@yahoo.com*

important category is cyber terrorists who are part of the category of those who use shorthand and cryptology to exchange information and exchange data online to steal information of important value to society, and hackers as government agents are those individuals or groups who work for specific government purposes that may compromise national cyber security. Cyberterrorism is another element that is part of the construct of what is called cybercrime and refers to that class of cyber terrorists who exploit computer vulnerabilities. Attackers are motivated by political ideology, religion, hacktivist tendencies, or personal motives, and cyber theft refers to those cybercriminals who seek financial gain by stealing and selling information in all possible ways (Sabillon, et al. 2016).

Cyber vulnerabilities are exploited through cyber-attacks, and as technology evolves, new risks and threats emerge that will lead to more advanced hacking Techniques, Tactics, and Procedures (TTPs). In this case, advanced persistent threats (APTs) are known, which refer to when an adversary possesses sophisticated levels of expertise and sufficient resources to achieve their objectives using multiple attack vectors, through target selection, target reconnaissance, command and control, data mining, information dissemination, and information exploitation. Cybercriminals’ targets are critical infrastructure, healthcare, public health, information technology (IT), financial services, and energy sectors (Sabillon, et al. 2016).

From the category of cyber-attacks, the following are mentioned: identity theft, which involves stealing someone’s identity, whereby the attacker claims this role to obtain financial benefits. Phishing represents a category of fraudulent processes that steal confidential information from users using spam email. Distributed Denial-of-Service (DDoS) refers to those attacks that use a network of several or even thousands of zombie computers that attack a specific target to overload it for failure. Malware attacks are malicious software that is installed through various viruses, and worms, and ransomware is a category of malware that locks users’ data to receive payment for unlocking the data (Sabillon, et al. 2016).

Cybercrime is constantly on the rise as these attackers advance through new technologies such as artificial intelligence (AI). From the point of view of obtaining financial goods, the most representative forms of cybercrime are economic espionage, intellectual property theft, financial crime, and ransomware. In terms of state support for cybercriminals, some states are permissive and use the information obtained by them for domestic purposes, for example, in Russia, where there is a close link between the state and organized crime that protects the most advanced cyber criminals. In Russia, cybercrime groups are allowed to pursue their financial motivations, and they are protected by the law, but in exchange for this protection, they must use their skills to support the interests of the government (Smith and Lostri 2022).

Cybercrime groups

Cyberspace has become an important area of warfare, taking place primarily on the Internet, where nations can fight without pooling troops and capabilities. This allows countries with a small military presence to be as powerful as other nations in cyberspace by penetrating other nations’ computer systems and networks. These attackers have the resources and expertise to launch massive Internet attacks against other nations, to cause damage or disrupt services, such as shutting down a power grid, but also to gain strategic advantages. The presence of cybercrime groups is more prominent and they seek to cooperate with cybercriminals who have essential skills that these groups can use or need to carry out certain operations, and these people can be coders and hackers.

Information technology has transformed the way certain groups are structured and organized, and criminals can collaborate on hacking activities using pseudonyms, and the risk of revealing their identities and locations to other group members is relatively low. One of the main challenges is the identification of organized cybercrime groups as the extent to which these groups operate exclusively, predominantly, and/or partially online (UNODC 2021). A nation can constantly attack another nation’s infrastructure, steal its military secrets and collect information on technology to bridge industrial and military gaps, and the implications of disclosing personal data and access to sensitive data can give attackers the ability to blackmail even government personnel (Neethu 2020).

The current geopolitical events, through the action launched by the Russian Federation in

Ukraine, have transformed the world and people have been put in front of the war in Europe. Seizing this opportunity and pursuing political, economic, and military interests, cyber security threats have become bigger and bigger, and cyber security challenges are evolving and will continue to do so. The security of people and cyber networks has acquired a political significance concerning the state, society, nation, and economy, and the targeting in particular of critical infrastructures intersects with financial, transport, energy, and national security infrastructures (Surdu 2018, 365-372).

Ransomware attacks and CONTI grouping

Over the past year, Russian crime groups have solidified their position as threats to the global digital ecosystem, demonstrating adaptability, persistence, and willingness to exploit computer systems. A ransomware attack involves malicious software that deploys malware to encrypt and exfiltrate data, which it then holds for ransom, often demanding payment in cryptocurrency. Moreover, attackers exfiltrate sensitive data before deploying ransomware to prevent victims from backing out of negotiations. According to statistics, ransomware actors have shifted from a high-volume opportunistic approach to a more selective methodology in choosing victims. Attacks on medical systems have increased, due to perceived weaker security controls and the greater propensity of these victims to pay the ransom due to the criticality of their services. Additionally, since late 2019, ransomware groups have adopted new extortion tactics to maximize revenue and create an additional incentive for victims to pay. In one such tactic, known as “double extortion,” ransomware operators exfiltrate massive amounts of a victim’s data by encrypting it and then threatening to publish the stolen data if ransom demands are not met (Financial Crimes Enforcement Network 2021).

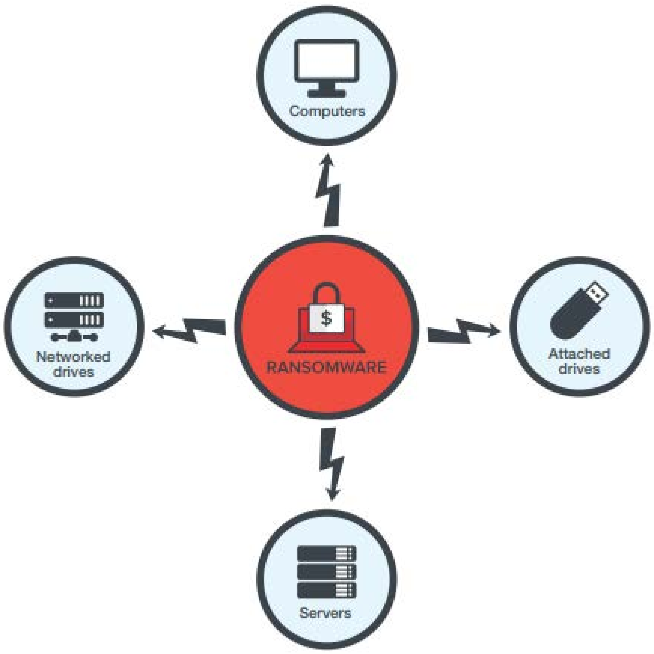


Figure no.1 Ransomware attack mode (TrendMicro 2021)

The second half of 2021 was rich in ransomware attacks, they were not only very active, but also increasingly aggressive. If the number of detections per active customer per country is considered, then we get a slightly different distribution. The following table shows the percentage of customers with at least one malware detection per country in 2021, and here it is noted that the Republic of Moldova has been the target of malware attacks since 2021. This raises several other questions about whether the Republic of Moldova was targeted by several cyber-attacks before the war in Ukraine started, which indicates that most of the time, analyzing the evolution of cyber-attacks, as well as their targets and their change, mainly determines a thorough analysis of the goal pursued by these types of attacks, as well as why the Republic of Moldova represented a target for them.

Ransomware is one of the most profitable cyber-attacks at the moment; it will continue to expand to macOS, and Linux, as well as new environments such as virtual cloud systems and IoT, in general, anything that is connected to an access network is a potential target (Acronis 2021). Most ransomware attacks come from Russia or its allies, and so most ransomware will try to see if a computer is running a common language spoken in Russia or one of its close allies, and if the answer is favorable, the ransomware will abandon the attack. Some attackers recommend enabling Russian as a second language on your computer, if possible, in order to prevent more ransomware from infiltrating. Russia has thus become a cyber-safe country, or as they are also called „havens” for ransomware criminals, and today many ransomware clusters are located in or around Russia (Grimes 2021). During the reporting period, the frequency and complexity of ransomware attacks increased by more than 150% and thus became one of the biggest threats facing organizations today, regardless of the sector they belong to. Cryptocurrency remains the most common payment method for these actors, with Monero being the preferred one due to the increased anonymity and unknown nature of transactions (ENISA 2021).

Conti is a Ransomware-as-a-Service (RaaS) that was first spotted in December 2019, as with other ransomware families, actors using Conti steal files and sensitive information from compromised networks and threaten to publish these data if the ransom is not paid (MITRE ATT&CK 2021). The Cyber Security and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) have observed increased use of Conti ransomware in more than 400 attacks on US and international organizations. In typical Conti ransomware attacks, malicious cyber actors steal files, encrypt servers and demand a ransom payment (CISA 2021).

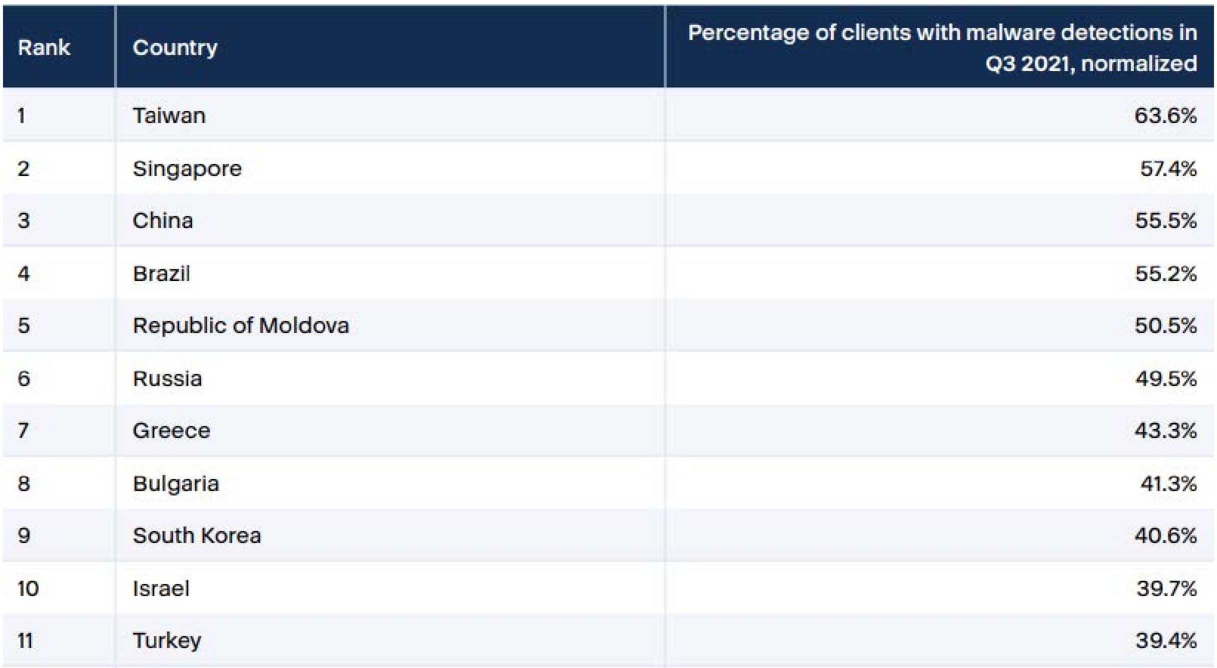
To secure systems against Conti ransomware, CISA, the FBI and the National Security Agency (NSA) recommend implementing mitigation measures that include requiring multi-factor authentication (MFA), implementing network segmentation, and keeping operating systems and software up to date (CISA 2021).

Conti actors often gain initial access to networks through spear phishing campaigns that use personalized emails containing malicious attachments or malicious links. CISA and the FBI observed that the Conti group used Router Scan, a penetration testing tool, to maliciously scan routers, cameras, and network-attached storage devices with web interfaces (CISA 2021).

Conti actors are known to exploit legitimate remote and desktop monitoring and management software. CISA and the FBI observed that Conti actors used different Cobalt Strike server IP addresses unique to different victims, and after the actors had stollen and encrypted the victim’s sensitive data, they used a double extortion technique where they asked the victim to pay a ransom to release the encrypted data and threatened the victim with the public release of data if the ransom was not paid (CISA 2021).

As of February 28, 2022, Conti actors remained active and Conti ransomware attacks against US and international organizations were reported to have increased to over 1,000, with notable attack vectors including Cobalt Strike (CISA 2021). In May, this group shut down its operating platform and a decentralized hierarchy took place, and the US Department of Defense offered rewards of up to $10 million for any information that could lead to the identification of important individuals that are part of this grouping.

After they attacked the government of Costa Rica and a national security alert was put in place, this group voluntarily ceased on May 19, 2022, while an reorganization process was taking place in order to ensure the smooth transition of



Rank	Country	Percentage of clients with malware detections in Q3 2021, normalized
1	Taiwan	63.6%
2	Singapore	57.4%
3	China	55.5%
4	Brazil	55.2%
5	Republic of Moldova	50.5%
6	Russia	49.5%
7	Greece	43.3%
8	Bulgaria	41.3%
9	South Korea	40.6%
10	Israel	39.7%
11	Turkey	39.4%

Figure no. 2 Malware detections in countries (TrendMicro 2021) members of the ransomware group. The takedown followed the group’s public allegiance to Russia in its invasion of Ukraine, dealing a huge blow to its operations in Ukraine and causing the leak of thousands of private data. Conti’s affiliation with Russia had other consequences, chief among them being its inability to extract ransom payments from victims due to economic sanctions imposed by the West (The Hacker News 2022a).

After Conti publicly supported Russia’s invasion of Ukraine, a cybersecurity researcher identified the malware’s source code and internal chats between affiliates and made them public. Conti and Hive are currently positioned as two of the biggest players on the ransomware scene. The Conti leaks were about exposing interesting inside information between Conti operatives, such as various jobs, roles within the organization, and their process for hiring new affiliates. Based on the chat logs that were analyzed between Conti and the victims, the following techniques are observed: Conti’s communication style is relatively professional, marked by seemingly scripted introductions and an emotionless tone. Actors stay on message, explaining to the victim that they are infected and emphasizing the consequences for the victim if they fail to pay the ransom and try to convince them to pay as quickly as possible (Mckay 2022).

The latest known data on this grouping suggests that former members of the Conti cybercrime group were involved in five different attack campaigns targeting Ukraine from April to August 2022. According to the Google Threat Analysis Group (TAG), they identified those ongoing cyber activities targeting the Eastern European nation against the background of the Russian-Ukrainian war. UAC-0098 is far from the only Conti-affiliated hacking group to target Ukraine since the start of the war, targeting Ukrainian organizations and European non-governmental organizations (NGOs) (The Hacker News 2022c).

UAC-0098 is an initial access broker known for using the IcedID banking trojan to give ransomware groups access to compromised systems on enterprise networks (Gatlan 2022). A concrete example in this sense is given by Ukraine’s Computer Emergency Response Team which detected a cyber-attack on Ukraine’s critical infrastructure, which it attributed to UAC-0098, but this is not the only example of a massive cyber-attack that targeted Ukraine and the country’s security systems (CyberSecurity Help 2022).

Changing the cybercrime ecosystem

Since this war is still ongoing, its impact on cyberspace and cybercriminal groups is considerable, as members of these cybercriminal groups reorganize their attack strategies and operate more in social media, to attract supporters. The call they make is mostly for both camps, and the Australian University of Adelaide discovered millions of fake tweets from an army of pro-Ukraine bots spreading disinformation and anti-Russian propaganda. The hashtag #IStandWithUkraine was posted by bots at a rate of 38,000 tweets per hour, and after that, the number of tweets increased to 50,000 per hour. The researchers note that the peak of activity of pro-Ukraine bots occurred between 6:00 PM and 9:00 PM in US time zones (Gaskin 2022).

Hackers being divided into two camps, pro-Ukrainian and pro-Russian, try in the virtual environment to obtain or transmit as much information as possible that could influence citizens in a certain way. A relevant piece of information on this topic is mainly related to the hacker group called Anonymous, who since the beginning of the war have shown their support for Ukraine, and thus have massively attacked the central operating systems of various institutions and state systems of Russia, a concrete example being the Central Bank of Russia. Instead, among the targets of pro-Russian hackers, there are also countries besides Ukraine that are targeted, for example, Poland. Most of the time, these attacks target the transportation industry and critical infrastructures.

In recent months, the joint efforts of defense and security institutions in several countries have made it possible to arrest prominent hackers from groups such as LockBit and Killnet, who were prosecuted for attacks against several institutions and organizations. Major cyber-attacks also targeted the intelligence services of countries such as Estonia, Poland, Romania, Bulgaria, and Moldova. For example, the pro-Russian group Killnet has claimed responsibility for several cyber-attacks, including an attack on the website and services of the US federal electronic tax payment system. The Hive cluster also attacked more than 1,300 companies worldwide. It targeted a wide range of enterprises and critical infrastructure sectors, including government facilities, communications, critical manufacturing, information technology, healthcare, and public health (The Hacker News 2022b).

Once the war began, the cybercrime ecosystem shifted to targeting Ukraine in particular, creating a Ukrainian IT army estimated at around 215,000 volunteer affiliates targeting Russian state-sponsored media outlets. The military has executed cyber-attacks on approximately 8,000 Russian assets, successfully targeting the defense industry and countering disinformation campaigns by state-sponsored institutions. Ukrainian President Volodymyr Zelensky noted that Ukraine’s IT army had successfully prevented more than 1,300 Russian cyber-attacks in the last eight months of the Russian invasion. For example, after Russia destroyed a major data center in the country, Ukraine moved to the cloud, allowing it to build public ledgers and make payments to war-affected citizens (Dark Reading 2022).

So far, cybercrime groups change this ecosystem by targeting Ukraine and the countries that support it, changing the way these groups have attacked in the past and the likely targets they would have had before this war. The fact that the mobilization of the population in social media is used to attract hundreds of thousands of people to hacktivism, does nothing but prove that this war is also found in cyberspace, it goes beyond the normal borders of territory and has global valence. Forecasts regarding these types of cyber-attacks take into account their scale and how these groups will act, as well as how the potential countries targeted by them will implement strategies to prevent major cyber-attacks, especially on critical infrastructures.

Conclusions

In the conclusions of the article, the following aspects can be mentioned that are justifiable for the researched subject; thus, it is found that cyber-attacks are increasingly complex, and the war in Ukraine is a source of motivation to support or not the belligerents by the cybercrime groups, hence the division of these groups into camps. Ransomware groups have been active since 2020, and in the Russian Federation, it is recognized that cybercrime groups receive support, which then acts in the interest of the state.

The CONTI group is relevant to analyzing how the current war may alter the cybercrime ecosystem because this relatively new group, which has supported and acted against states that do not support Russia’s action, has been split only after several cyberattacks have been launched, and will then be resumed under a different identity, but essentially pursuing the same goal. In Russia, offensive operations are aided by advanced technology such as Artificial Intelligence (AI) and automation to provide command and control, and thus cyberspace can be seen as a much more advantageous area in hybrid warfare for these groups to exploit.

The fact that Russia is trying to isolate the Russian Internet from the global one is an example to justify arming Russia from within, to practice its cyber activities to target adversary countries. This increased its geopolitical influence and helped amplify its power as a strong player on the international stage. Geopolitics is an essential and indispensable tool for understanding and analyzing new cyber challenges, but the main factor in this equation is politics while geopolitics is the one that interacts and determines the purpose of cyber-attacks.

The international system may remain one in which the desires of member countries are consistent with the defense and integrity of cyberspace and the security of information systems and critical infrastructure, but the area of hybrid threats will be a more exploited and potential one for state or non-state actors, which will likely put pressure on the economy, politics, critical infrastructures, citizens, etc.

BIBLIOGRAPHY

Acronis. 2021. *Acronis Cyberthreats Report 2022 unveils cyberthreat predictions.* https://www.acronis.com/en-us/blog/posts/acronis-cyberthreats-report-2022-unveils-cyberthreat-predictions/.

CISA. 2021. *AA21-265A-Conti Ransomware TLP White*. https://www.scribd.com/document/529330620/AA21-265A-Conti-Ransomware-TLP-WHITE.

CyberSecurity Help. 2022. “Former Conti Hackers Adapt Their Techniques to Use against Ukraine.” https://www.cybersecurity-help.cz/blog/2878.html.

Dark Reading. 2022. “Ukraine’s ‘IT Army’ Stops 1,300 Cyberattacks in 8 Months of War.” https://www.darkreading.com/endpoint/ukraine-it-army-stops-1300-cyberattacks-war.

Donalds, Charlette, and Kweku-Muata Osei-Bryson. 2019. “Toward a Cybercrime Classification Ontology: A Knowledge-Based Approach.” *Computers in Human Behavior* 92: 403-418. doi:https://doi.org/10.1016/j.chb.2018.11.039.

ENISA. 2021. *Enisa Threat Landscape 2021*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.

Financial Crimes Enforcement Network. 2021. “Financial Trend Analysis.” https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomeware%20508%20FINAL.pdf.

Gaskin, Lee. 2022. “Bots Manipulate Public Opinion in Russia-Ukraine Conflict.” *The University of Adelaide*. https://www.adelaide.edu.au/newsroom/news/list/2022/09/08/bots-manipulate-public-opinion-in-russia-ukraine-conflict.

Gatlan, Sergiu. 2022. “Google Says Former Conti Ransomware Members Now Attack Ukraine.” *BleepingComputer*. https://www.bleepingcomputer.com/news/security/google-says-former-conti-ransomware-members-now-attack-ukraine/.

Grimes, Roger A. 2021. *Ransomware Protection Playbook*. John Wiley & Sons Inc.

Mckay, Kendall. 2022. “Conti and Hive ransomware operations: Leveraging victim chats for insights.” https://s3.amazonaws.com/talos-intelligence-site/production/document_files/files/000/095/787/original/ransomware-chats.pdf?1651576098.

MITRE ATT&CK. 2021. *Conti*. https://attack.mitre.org/software/S0575/.

Neethu, N. 2020. “Role of International Organizations in Prevention of Cyber-Crimes: An Analysis.” Nalsar University of Law, Hyderabad, 5-17. https://www.researchgate.net/profile/Neethu-N-2/publication/350525198_Role_of_International_Organisations_in_Prevention_of_Cyber-Cri.

Sabillon, Regner, Victor Cavaller, Jeimy Cano, and Jordi Serra-Ruiz. 2016. “Cybercriminals, Cyberattacks and Cybercrime.” *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*. 1-9. doi: https://doi.org/10.1109/icccf.2016.7740434.

Smith, Zhanna Malekos, and Eugenia Lostri. 2022. *The Hidden Costs of Cybercrime*. McAfee report. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf.

Surdu, Ileana-Cinziana. 2018. “Cybersecurity. Risks, Threats, and Trends of Manifestation in Romania.” *International Conference RCIC’18*. 365-372. https://www.afahc.ro/ro/rcic/2018/rcic’18/volum_2018/365-372%20Surdu.pdf.

The Hacker News. 2022a. *Conti Ransomware Operation Shut down after Splitting into Smaller Groups*. https://thehackernews.com/2022/05/conti-ransomware-gang-shut-down-after.html.

—. 2022b. *Hive Ransomware Attackers Extorted $100 Million from over 1,300 Companies Worldwide*. https://thehackernews.com/2022/11/hive-ransomware-attackers-extorted-100.html.

—. 2022c. *Some Members of Conti Group Targeting Ukraine in Financially Motivated Attacks*. https://thehackernews.com/2022/09/some-members-of-conti-group-targeting.html.

TrendMicro. 2021. “Toward a New Momentum: Trend Micro Security Predictions for 2022.” https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2022.

UNODC. 2021. “Digest of Cyber Organized Crime.” https://www.unodc.org/documents/organized-crime/tools_and_publications/21-05344_eBook.pdf.

NEW THREATS AND VULNERABILITIES REGARDING NATIONAL SECURITY IN THE CONTEXT OF THE CONFLICT IN UKRAINE

Ltc. Cezar-Cristian ALDEA, Ph.D. Candidate*

The events that took place at the end of the twentieth century led to important transformations that determined the need to reconfigure the geopolitical and geostrategic environment in terms of risk diversity, threats and interests of the actors involved. Russia is a key element in establishing the new security architecture as it seems to focus all necessary forces and means on maintaining its influence in Eastern Europe. In this article, I will address not only the main security threats and vulnerabilities deduced from Russia’s military operation in Ukraine, whose purpose is to reconfigure the security environment and restore the new world order, namely the Black Sea region, but I will also refer to the weapons of the mass destruction, cyber-attacks, climate change and, last but not least, the flow of refugees. All these new risks and threats to national security demonstrate once again Romania’s strategic role in shaping global security architecture. Strengthening Romania’s national security is a key element in the coming years in the unpredictable context of the regional security environment.

Keywords: geopolitics; weapons of mass destruction; cyber-attacks; climatic changes; refugee flow.

The security environment has changed dramatically since 2014, while threats and risks continue to be a major challenge for the Alliance, ranging from terrorism to security challenges posed by pandemics, climate change, and migratory flows.

Black sea region

The Black Sea region faces numerous threats either conventional or unconventional. These security issues make the region volatile, insecure, and unstable. The conflict between Russia and Ukraine, as well as the potential conflicts between the zonal states are the basic threats to regional security.

Russia has a strong and robust conventional military armament, which is a threat to NATO, but the issue is particularly acute for the Eastern flank through the operations taking place in Ukraine (NATO 2020, 25). Russia’s actions in the Black Sea area led to the occupation of Snake Island located 50 km off the coast of Romania, proving once again that the area is vulnerable. At present, it is necessary to revise the Montreaux Convention of 1936, which specifies the access to the Black Sea as it favors Russia over NATO.

Although Russia is a declining power through EU economic and social measures, it has proven to be capable of territorial aggression and it is likely to remain a major threat which NATO and implicitly Romania will face in the next decade.

While Russian aggression in Ukraine continued, Russia’s aggressive behavior intensified, according to Mediafax, through large-scale naval exercises with dozens of ships in Black Sea, to demonstrate its attacking power. All these actions have led to severe deterioration of the region, adversely affecting national security.

Russia routinely engages in immediate military intimidation operations in close proximity to Romania, while increasing its scope regarding threats to airspace and, last but not least, to the freedom of navigation in the Atlantic.

Faced with such an actor, NATO will have to be diligent, manifest solidarity and maintain a permanent dialogue if the Russian leaders choose a longer path design (NATO 2020, 48). NATO must maintain adequate conventional and nuclear military capabilities and show greater flexibility so as to deal with aggression within the Alliance, including in spots where Russian forces are directly or indirectly active, especially on the Eastern flank.

Consequently, Romania needs to step up its efforts to ensure that their financial commitments and military contributions are in line with

***1 BDA ”Nicolae Dăscălescu”**
e-mail: *cezar20bv@yahoo.com*

NATO’s strategic needs and are able to ensure effective balance.

Mass destruction weapons proliferation (WDM)

Romania continues to be a pole of interest for states with interests in developing capabilities in the field of weapons of mass destruction and carrier and / or conventional military vectors in high-risk areas, not only as a potential supplier of military equipment, but also from the perspective of using our country mainly as transit space or re-export point to other destinations (Romanian Intelligence Service 2020, 9).

The proliferation of WDM and carrier vectors will show increasing trends, on the one hand, as a result of conflict situations in the neighborhood, and on the other, on the background of the progressive technological growth and the increased interest of the states involved in the development of projects in WDM (China and Russia are constantly investing in their development) for obtaining expertise from abroad, in order to increase the indigenous capacities of production / research-development (Romanian Intelligence Service 2020, 9).

Weapons control, disarmament and non-proliferation play an important role in promoting peace in the Euro-Atlantic Region and maintaining a stable international order.

By 2030, Russia is likely to have completed the modernization cycle of a wide range of its nuclear forces. These forces, together with the conventional ones pose a serious problem as are a threaten to NATO and implicitly to allies’ security. NATO has been actively involved in this issue for many years and is making effective and verifiable efforts regarding the control of nuclear weapons and, last but not least, disarmament efforts.

The threat posed by nuclear weapons is a key element through which Russia seeks to increase the reluctance of Central and Eastern European countries and beyond regarding the implementation of measures that would affect its level of security, as in the case of the NATO anti-missile shield.

In response to Russia’s actions, for instance, Germany plans to buy the interceptor Arrow 3, for long-range threats, while the US and Israel have approved the sale.

Arrow 3 is an extremely maneuverable system designed to provide air defense by intercepting ballistic missiles when they are still outside the atmosphere of Earth. It is considered one of the best interceptors in the world due to it its innovative technological capabilities.

Cyber-attacks

Cyber-attacks are currently evolving; they are launched by state actors and are characterized by incisiveness, having as center of gravity compromising IT&C infrastructures in strategic areas. Cyber actors have diversified tools of action, including innovative malware applications – undetectable by existing cyber security solutions on the market - elements of infrastructure and malware solutions assigned to other entities or open source.

At the national level, the threat has had a growing trend and the main actors are represented by:

- entities associated with some state actors;
- cybercrime groups;
- ideologically motivated hacker groups (Government General Secretariat 2021, 5).

In other cases, the adversaries acted for: conducting cyber-attacks against private businesses; the rental or use of local command and control servers (C2) in Romania for conducting cyber-attacks globally (Romanian Intelligence Service 2020, 8).

The actions of the entities associated with some state actors are of a strategic nature, the purpose being to take over and control the networks and computer systems in order to steal information of interest, disrupt or partially or completely destroy the functionality of some critical infrastructure, and, last but not least, influence socio-political processes.

The threats of cybercrime groups have increased in recent years, the motivation being of financial nature. The main applications used to this end are the following: *ransomware malware* (it is malicious software intentionally designed to prevent a user or organization from accessing files on their own computer, attackers demanding payment as a ransom for unlocking access) and *infostealer* which targets state/private networks and computer systems.

According to the information provided by the EU Cyber Security Agency, the higher redemption demand increased from EUR 13 million in 2019

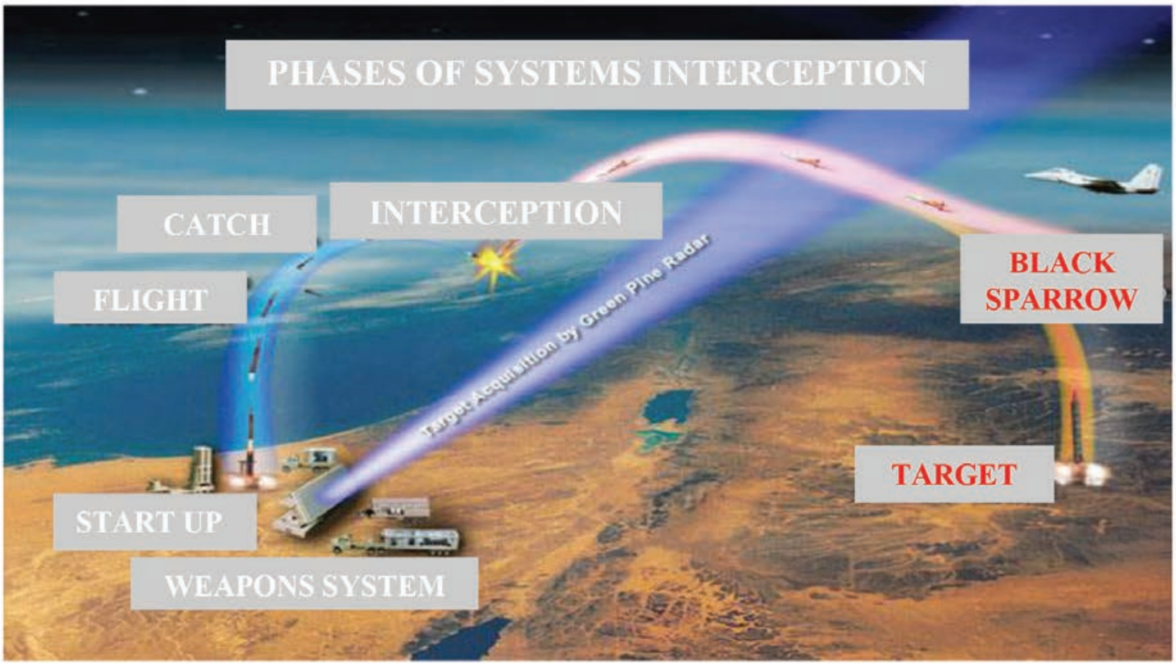

PHASES OF SYSTEMS INTERCEPTION
CATCH
INTERCEPTION
FLIGHT
Target Acquisition by Green Pine Radar
BLACK SPARROW
TARGET
START UP
WEAPONS SYSTEM

Figure no. 1 The phases of missile interception by the Arrow system
Source: https://www.wikiwand.com/en/Arrow_(Israeli_missile)

to EUR 62 million EUR in 2021, and the average redemption paid has doubled: from EUR 71,000 in 2019 to EUR 150,000 in 2020. It is estimated that in 2021 the global damage caused by ransomware reached EUR 18 billion - 57 times more than in 2015.

Threats of ideologically motivated hacker groups are currently insignificant and have as their main target computer systems with a low level of cybersecurity. These following threats: *defacement*, *distributed denial of service* (DDos) and *SQL injection* have been and are currently used against Russia by the group called *Anonymous*. Their management can only be achieved by implementing policies and measures of cyber security, which is constantly adaptable to cyber-attacks (Romanian Intelligence Service 2020, 14). At the same time, it is necessary to develop procedures for testing and auditing the level of cyber security, and last but not least updating software and hardware technologies.

Another measure would be to set up national certification mechanisms, compliance and standardization to identify existing security risks and vulnerabilities (Romanian Intelligence Service 2020, 10). It is imperative to reduce the risks posed by cyber-attacks thus consolidating Romania’s level of cyber security through development and efficiency cooperation formats at strategic, tactical and operational level.

Climate change

Climate change is one of the defining challenges of the times and has serious implications for the security and economic interests of all thirty members of the Alliance. As expected effects: increasing resource deficit, nutrition globalization, and insecurity of water resources (NATO 2020, 41). Climate change has long been known as a threat multiplier and it is increasingly recognized as a „shaping threat” that is dramatically altering the environments in which allied militaries will have to operate in the coming decades. In addition to climate-related risks to military infrastructure and force training, more extreme weather events can also increase the potential for conflict and migration within and beyond NATO’s immediate vicinity.

According to the 2021 global risk report, extreme weather is the number one risk and more dangerous than mass destruction, cyber-attacks and infectious diseases, with implications for air, land and maritime operations (Heise 2021, 3).

Air operations

Climate change will affect air operations, as follows:

● aircraft performance during take-offs and landings directly depends on air temperature, pressure (airfield altitude) and wind; at the same time, the increase in temperatures due to climate change degrades the performance of an aircraft (e.g.: transport planes and helicopters in Afghanistan);

● the frequency and intensity of sand and dust storms will increasingly impede on operations due to flight restrictions;

● cargo planes – should avoid areas of heavy turbulence; mission planning will still be affected;

● overheating of military aircraft and logistics equipment at air bases, which implies increased logistical effort and higher energy consumption;

● changes in the main wind directions at airports must also be taken into account and may require structural changes such as changing the direction of runways;

● in the Arctic Region, they will generate the need to modify supply routes and airfields, consequently search and rescue procedures must be adapted. Future UAV missions will require stable data links and robust GPS systems for control and enforcement procedures.

Land operations

Operating in increasingly extreme climates will pose a major challenge for military personnel (e.g.: reduced drinking water supply due to desertification in certain regions). Extreme weather conditions also cause faster „wear and tear” of military equipment (e.g.: Afghanistan’s arid environment caused weapons to „jam” more often). At the same time, they have significant implications for military logistics (e.g.: floods, snow/ice or storms could block operational supply routes).

Navy operations

NATO’s maritime capabilities in the Arctic will face a number of challenges due to the combination of extremely cold air temperatures, high wind speeds, ice obstacles, large waves, and increased exposure to radiation. Weapons systems and ammunition must be adapted to extreme temperature conditions and such requirements can be anticipated, if necessary, through simulation. On the other hand, in warmer waters the situation is just as dire, with increased salinity in the Gulf of Aden causing the turbines of several UK frigates to fail (Heise 2021, 4). Oceanographic processes (i.e. cooling of the subpolar Atlantic) are associated with changes in precipitation patterns and additional factors of sea level rise; these will have implications for maritime reconnaissance and surveillance.

In 2014, NATO adopted the Green Defence Framework, which aims to reduce the impact on the environment of its military operations and improve NATO’s resilience through investment in green technologies that reduce fuel and energy consumption. Michael Ruehle, director of the hybrid and security challenges department for NATO’s energy policy, highlighted the main problems the alliance had been facing over time such as damage to its equipment and facilities caused by extreme drought or flood. At the same time, he also stated that „being greener means being stronger”, but warned that the green transition would not be free because the improvement of equipment „involves years of development” and implementation (Rühle 2021, 5).

In this sense, Romania must intensify its financial efforts so as to purchase military equipment according to NATO requirements.

Refugee flow

Russia’s aggression against Ukraine has triggered one of the biggest humanitarian aid crises in Europe. Following the research conducted by the International Organization for Migration (IOM) between 09.03 and 16.03.2022, out of the 2,000 internally displaced persons they surveyed:

- almost 30% had come from Kyiv, over 36% had fled Eastern Ukraine and 20% had come from the North;

- almost 40% were now in Western Ukraine, with less than 3% in Kyiv;

- only 5% left their homes in anticipation of the invasion, the vast majority fleeing either at the beginning of the war, or when it came to their area.

IOM estimates that more than half of the displaced persons are women and many are considered particularly vulnerable because they are pregnant, have a disability or are victims of violence.

Refugees also travel to neighboring Western countries, such as Poland, Romania, Slovakia, Hungary and Moldova.

The UN says that as of March 21, 3.5 million people have left Ukraine:

✓ Poland received 2,113,554 refugees;
✓ Romania, 543,308;
✓ Moldova, 367.913;
✓ Hungary, 317.863;
✓ Slovakia, 253.592;
✓ Russia, 252.376.
✓ Belarus, 4.308 (IOM Ukraine 2022, 1-4).

According to Romanian MFA statements, about 80,000 refugees remained on the territory of Romania and so far the situation has been effectively managed by civil society, the state, and NGOs.

With the increase in the flow of refugees (over 1 million), Romania must turn to strategic reserves and, last but not least, to EU support for crisis management, so as to be able to provide assistance to European standards.

Conclusions

Romania is in a strategic context defined by geopolitical instability, highlighting the intensification of strategic competition between actors with global interests.

The Black Sea area is an area of strategic interest for major global players. This situation takes place in the context of the relative decline of power of some actors on the international political scene, amid the reconfiguration of strategic options and the promotion of certain isolationist / coercive policies in international relations. In view of these, as well as the aggression of Ukraine by the neighboring Russia, the emergence of zonal conflicts could be a cause for concern in Romania.

Last but not least, the technological field is in full swing, cyber-attacks are growing, having as major effects misinformation (fake news about military actions, deployments of forces and means, etc.), all within asymmetric and hybrid actions, generating new challenges for Romania and its allies.

The social environment is influenced by an asymmetric population growth, emphasizing the phenomenon of aging, pollution and, last but not least, the phenomenon of migration. Romania is facing an influx of Ukrainian refugees from conflict zones, which has both economic and social implications.

In the context of the vulnerabilities of the security environment, Romania is forced to strengthen cooperation with the United States to ensure national security in the event of aggressive actions in the neighborhood.

Romania must invest sufficiently in financial, technical and human resources, necessary to intensify the Alliance’s response capacity building efforts on the Eastern flank in the face of escalating geopolitical conflicts caused by various social, economic, and cultural interests.

BIBLIOGRAPHY

Çelikpala, Mitat. 2020. “Security in the Black Sea Region.” Policy Report II. https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/GP_Security_in_the_Black_Sea_Region.pdf.

Government General Secretariat. 2021. “Romania s Cyber Security strategy 2021-2026.” http://sgglegis.gov.ro/legislativ/docs/2021/08/sr2dvm1746zwhc0fby5n.pdf.

Hâldan, Romulus. 2018. *Vectors of Russia’s military power - between reality, propaganda, and advertising misinformation.* Bucharest: Top Form Publishing house.

Heise, Rene. 2021. “NATO is responding to new challenges posed by climate change.” *NATO Review.* https://www.nato.int/docu/review/articles/2021/04/01/nato-is-responding-to-new-challenges-posed-by-climate-change/index.html.

IOM Ukraine. 2022. “Ukraine — Internal Displacement Report — General Population Survey Round 2 (24 March - 1 April 2022).” https://displacement.iom.int/sites/g/files/tmzbdl1461/files/reports/IOM%20IDP%20Estimates%20UKR%2016MAR2022_Round%201%20full%20report_v2.pdf.

NATO. 2020. “NATO 2030: United for a New Era, Analysys and recommendations of the reflection group appointed by the Nato Secretary General.” https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf.

NATO Public Diplomacy Division. 2019. “NATO Encyclopedia 2019.” https://www.nato.int/nato_static_fl2014/assets/pdf/2020/1/pdf/2019-nato-encyclopedia-eng.pdf.

Romanian Intelligence Service. 2020. “Inovare în serviciul cetățenilor.” Raportul de activitate al Serviciului Român de informații - 2019. https://www.sri.ro/assets/files/rapoarte/2019/raport_activitate_2019.pdf.

Rühle, Michael. 2021. “NATO and the Climate Change Challenge.” International Politik Quarterly. https://ip-quarterly.com/de/user/239/michael-ruehle.

THE RESPECT FOR FUNDAMENTAL HUMAN RIGHTS DURING AND AFTER THE RUSSIAN-GEORGIAN WAR

Major Mădălina PREDA (DAVIDOIU), Ph.D. Candidate*

The normative and practical value of protecting civilians during armed conflicts and respecting the exercise of human rights and fundamental freedoms even in international armed conflicts is an undeniable one. Changing the forms and means used in armed struggles leads to violations of the provisions of international humanitarian law. The case-law of the European Court of Human Rights in the case of Georgia v. Russia has made a connection between the fundamental rights included in the Convention for the Protection of Human Rights and Fundamental Freedoms and the rights protected by the laws of armed conflicts, a decision of particular importance in the current security context in South-Eastern Europe.

Keywords: armed conflict; humanitarian law; ECHR; rights; civilians.

Developments in the field of arms and armaments technology, increasing both range and lethality, have changed the way armed conflicts are conducted. Global political developments have changed both in terms of the location of the armed fighting and the activity of the belligerents.

Armed actions are carried out around urban centres, which increases the number of collateral victims. The effect of wars on non-combatants comes in two forms. On one hand, civilians are injured or killed as a direct result of warfighting, regardless of whether the attack against them was accidental or intentional. On the other hand, there is another harm to civilians represented by the damage to their dignity as a result of violations of law and order, but also of international norms of humanitarian law such as sexual assaults or actions of violence on ethnic grounds.

Given the importance of protecting civilians during armed conflicts and of defending human rights during stability and peacekeeping operations, this article will outline the legal framework for the protection of human rights in relation to a case study according to which, both during an armed conflict and subsequently, during the occupation phase, there were violations of international conventions, sanctioned by the court responsible with ensuring the compliance with the human rights within Europe. From this perspective, the Russia-Georgia war of 2008 led to human rights violations as decided by the European Court of Human Rights (ECHR).

The main documents in the international humanitarian field are the Hague Conventions on the Laws and Customs of War from 1899 and 1907 and the Geneva Conventions of 1949: Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field; Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea*;* Convention Relative to the Treatment of Prisoners of War*;* Convention Relative to the Protection of Civilian Persons in Times of War. These documents contain prohibitive clauses, unequivocally prohibiting reprisals against the victims of the state of war (civilian population, wounded and sick, prisoners of war or refugees).

Theoretical Considerations on the Protection of Human Rights and Fundamental Freedoms During International Armed Conflicts

International humanitarian law (IHL), as an expression of a balance between military necessity and humanity, provides important rules for the protection of civilians. The IHL states that for the purpose of the armed struggle to win the war against the enemy, the choice of the means and ways of war is not unrestricted. In this respect, “*the civilian population and civilian persons enjoy a general protection against the dangers arising from military operations*” (Legislativ Portal n.d., 25).

***Romanian Navy**
e-mail: *Madalina.Preda@navy.ro*

IHL defines the governing principles for the conduct of belligerents in battle, among them: humanity, distinction, proportionality and caution. Military decision-makers must analyse all the information at their disposal before launching an attack in order to make a tactical decision on the means and methods used. Therefore, armed attacks must be non-discriminatory or proportionate to the intended purpose and all necessary precautions must be considered to minimize the damage that may occur to the civilian population. Furthermore, international rules on the conduct of armed conflicts impose an obligation to grant effective protection to civilians and private property, and, in all circumstances, non-combatants to be treated with dignity and respect for their rights.

Distinction between the civilian population and the combatants as well as between civilian and military objectives must be made at all times during armed conflicts. Consequently, civilians and civilian objectives must be protected against an intentional armed attack. Indiscriminate attacks are prohibited, including three types of attacks: attacks that do not directly target a military objective, attacks using methods or means of war that are not directed against a particular military objective, and attacks using a method or means of war with effects that are unlimited. The regulations of humanitarian law prohibit attacks that could cause accidental loss of life or injury among civilians and damage to private property.

For protecting the civilians during armed conflicts, we can identify several rules from the IHL norms, as follows:

- civil persons may not be the subject of an appeal unless they participate directly in hostilities;
- the person surrendering to the enemy will have his life saved;
- no person shall be subjected to physical or mental torture, corporal punishment or cruel or degrading treatment;
- the legal personality of each individual will be respected; private property is protected and cannot be the target of an armed attack, unless it is used for military action;
- the sick persons will be hospitalized and will be provided with the necessary care according to the medical condition;
- persons will be treated without discrimination on the basis of race, sex, nationality, language, social class, property, public, philosophical or religious opinions or on another basis;
- retaliation is prohibited in camps with prisoners or war refugees.

Factual Aspects Regarding the Conduct of Reprisals in the Russia-Georgia War

The Russia-Georgia war of August 2008, although it lasted only several days, was one that changed the security context in the Black Sea region and created premises for emphasizing the importance of human rights re-enactment in times of military conflict.

The history of this confrontation stems from deep ethnic dissension between Georgians and the separatist population of South Ossetia and Abkhazia. Tensions in the region date back at least to 1920, when South Ossetia wanted to declare its independence, but gained the status of an autonomous region in the Soviet Georgia. Georgia’s declaration of independence from the former Soviet Union and its disagreements with Russian-influenced South Ossetia led to the outbreak of hostilities between Georgia and South Ossetia in January 1991. As a result, a state of relative peace was established, and a ceasefire was agreed between the warring forces, which included the deployment of Russian peacekeepers in the area.

The international precedent on the formation of a state on the territory of another sovereign state through Kosovo’s declaration of independence was used as an example for separatist groups in South Ossetia and Abkhazia. The external context that led to the escalation of hostilities in August 2008 was created by the decisions taken at the NATO Summit in Bucharest in April 2008, according to which Georgia and Ukraine, although not reaching the status of receiving the Membership Action Plan, were officially recognized as countries that could acquire the status of NATO Allies in the future.

Longstanding tensions escalated on the evening of 7 August 2008, when South Ossetia and Georgia accused each other of launching armed attacks and did not respond to calls for a ceasefire, but even intensified the bombing. Russia intervened in the conflict and launched airstrikes on Georgia, and by August 12, Russian troops occupied most of southern Ossetia and several

Georgian cities. Russian forces landed warships in the breakaway region of Abkhazia in Georgia and took up positions off the coast of Georgia from the Black Sea. Meanwhile, the bombing of Georgia’s territory by Russian fighter jets continued, as well as the occupation of villages and the destruction of military bases, residential buildings and other critical infrastructure objectives.

Under the supervision of international bodies, the participants to the conflict (Georgia, South Ossetia, Abkhazia and the Russian Federation) signed, on 12 August 2008, a peace plan concluded directly under the aegis of the European Union (EU). This agreement included the obligation of the parties to refrain from the use of force, the total and immediate cessation of armed hostilities, and the provision of access for the civilian population to humanitarian aid. The Russian Federation recognized South Ossetia and Abkhazia as independent states in a decree signed by the President Dimitry Medvedev on August 26, 2008, a gesture condemned by the international community.

As a result of the fact that the Russian Federation did not take the committed measures, on 8 September 2008, a new agreement was concluded to implement the ceasefire agreement (the Sarkozy-Medvedev agreement) which provided for the obligation to withdraw Russian troops from the areas bordering Abkhazia and South Ossetia. On September 17, 2008, the Russian Federation signed friendship and cooperation agreements with South Ossetia and Abkhazia.

During the war *“looting, kidnappings, murders and other atrocities by the Russian army on the Georgian civilian population were reported. In these circumstances, Georgia sent a letter to the international community asking for its help and requesting its intervention to stop the atrocities and use of unconventional weapons, a fact also signalled by a human rights observer from the UN”* (Chifu, Oproiu and Bălășoiu 2010, 49). These illegal actions continued even after the end of the armed conflict, the population being affected in terms of the free exercise of their rights, being found degrading acts on prisoners of war and disadvantaged people.

International and regional bodies had an active role in resolving the conflict and the financial, technical and humanitarian aid has supported democracy in Georgia and has ensured the stability of the entire region. On 2 December 2008, the Council of EU took the decision to establish an independent international information mission on the conflict in Georgia, being *“for the first time in history that the European Union has decided to actively intervene in a serious armed conflict”* (Council of the EU 2009). The United Nations (UN) led the negotiations in Abkhazia, while the Organisation for Security and Cooperation in Europe (OSCE) was the main actor in the South Ossetia talks. EU has assumed an important role in its efforts as these organizations adopted a long-term perspective towards Georgia aiming at helping the development of the country.

According to reports by EU and UN observers, on the basis of data collected from the field and witness statements, armed attacks were reported aimed at the mass destruction of Georgian villages in South Ossetia and nearby regions. *“Actions to destroy private property that turned entire areas of Georgian population into ghost cities”* were carried out (OSCE 2008). International organizations as well as international media reported the execution of Georgian ethnics. In this regard, statements of the civilian population were processed, including the people rescued from the famous hostage camp in Tskhinvali. Moreover, it has been reported several cases of elderly people physically unable to flee from the aggressors, captured in large numbers and held hostage (later handed over in exchange for prisoners of war). Houses owned by ethnic Georgians were looted and set on fire, following a policy of ethnic cleansing of Georgians.

Procedural Phase of the War Between Russia and Georgia

Claiming that during the armed conflicts and subsequently violations of the rights of civilians of Georgian ethnicity were carried out by the armed forces of the Russian Federation, the Government of Georgia filed a complaint with ECHR (Application no. 38263/08) in which it claimed that there were flagrant violations of the laws and principles of war that caused serious harm to the population. The government argued that, on the basis of the available evidence, the actions of the Russian army are part of a repetitive pattern of acts and omissions incompatible with international conventions.

According to the application filed by Georgia, the following actions were reported that violate the civil rights during the armed conflicts:

- murder, ill-treatment, robberies and arson of dwellings by the Russian armed forces;

- the non-observance of the treatment of civilian prisoners and the legality of their detention, being detained acts of mistreatment and torture of several prisoners of war by Russian forces;

- violation of the free movement of displaced persons with regard to the return to their regions of origin of forced displaced Georgians;

- violation of the right to education with alleged looting and destruction of schools and public libraries by Russian troops and separatist authorities and intimidation of Georgian students and teachers;

- failure to comply with the obligation to investigate war crimes alleged to be committed by their nationals or armed forces.

Georgian authorities complained of systematic violations of population rights being invoked both the provisions of IHL and European Convention on Human Rights, as follows: art. 2 (right to life), art. 3 (prohibition of torture), art.5 (right to liberty) and art. 8 (right to private life), protocol 1 additional art. 1 (right to private property) and art. 2 (right to education).

In its response, the Russian Federation claimed that the military action was legitimate and in line with the provisions of the IHL and that Georgia's accusations were false and lacking in evidence. Moreover, the competence of the ECHR in relation to the IHL's provisions was challenged and considered that the Court's powers concern only the application of the European Convention for the Protection of Human Rights and Fundamental Freedoms. Russia believes that the injury of civilians and the destruction of property are the result of the actions taken by the perpetrators in the two regions, and the responsibility lies with the governments of South Ossetia and Abkhazia.

Regarding the exception of lack of competence, the ECHR decided to divide the period of the conflict into an active phase of hostilities (8-12 August 2008) and subsequent events. One of the most significant and controversial findings of this judgment is that Russia had no jurisdiction over the territory on which the conflict took place during the war, and the acts committed during this period do not fall under the jurisdiction of the ECHR. The Court has taken into account two reasons for jurisdiction here: effective control over the territory and authority over natural persons. In other words, in its analysis, the ECHR used *“both territorial and personal control as grounds for competence, finding no valid judicial basis for Russia's effective control over the territory of South Ossetia and Abkhazia during the hostilities phase. However, in this case, the European Court of Human Rights failed to establish jurisdiction over persons living in a territory that would otherwise be protected by the Convention”* (Dzehtsiarou 2021, 288).

In its decision from January 21st, 2021, the ECHR ruled that the events that took place during the active phase of hostilities (8-12 August 2008) did not fall within the competence of the Russian Federation and declares this part of the application inadmissible. The ECHR states that the events that took place after the cessation of hostilities (from the date of the ceasefire agreement 12 August 2008) were within the competence of the Russian Federation, so that, in relation to the evidence administered in the case, it is found that there was an administrative practice regarding the killing of civilians, the burning and looting of houses in Georgian villages in South Ossetia and the “buffer zone”, the establishment of poor and unsuitable detention conditions for prisoners who have been exposed to humiliating treatment and who have caused them undeniable suffering and are classified as acts of torture. The ECHR also decides that Georgian citizens have been prevented from returning to South Ossetia or Abkhazia, an incapacity that falls within the competence of the Russian Federation (CEDO 2021).

The subject is of current relevance considering the security situation in the area caused by the attack on Ukraine by the Russian Federation starting with February 24, 2022, an ongoing armed conflict. Despite this decision of CEDO, which undoubtedly states that certain practices of war constitute serious violations of human rights, the monitoring missions of the war in Ukraine (ONU 2022), with duties to monitor the respect for the freedoms of civilians, established by the UN reported *“the serious deterioration of the human rights situation in the country, with thousands of civilians killed and wounded, the massive destruction of civilian infrastructure and housing,* *arbitrary detentions and cases of disappearances, torture and ill-treatment, but also sexual violence”* (OHCHR 2022).

Conclusions

The protection of people’s fundamental rights in times of conflict, crisis and war is done through the activity of regularization through legal instruments (treaties, conventions, resolutions of international organizations) of international humanitarian law as a branch of public international law. The customs of ancient wars have found expression in the texts of international conventions and resolutions of international security organizations forming international humanitarian law.

In full agreement with IHL regulations, the parties to the conflict must take precautions to avoid or minimize the effects of armed actions on civilians, having the obligation to do everything feasible to avoid collateral losses among civilians and damage to private property deemed in excess to the intended real and direct military advantage.

Compliance with rules of international law applicable to armed conflicts is an obligation incumbent to states and to combatants in the theatre of operations. The importance of protecting civilians and other non-combatants in time of war and following it is underlined by the ratification of legal treaties that delimit the rights of civilians in times of armed conflict, by political and media actions condemning acts that cause the suffering of non-combatants and by the active freezing carried out by international institutions on the legality of behaviour in battle. According to the provisions of the IHL, the exercise of the fundamental rights of non-combatants must also persist during armed conflicts.

The ECHR judgment in Georgia v. Russia delivered on January 21st, 2021 has a historical importance regarding the respect of DIU provisions. In the operative part of the ruling, the judges found Russia responsible for several violations of the Convention including illegal killing, torture, arbitrary detentions, looting and destruction of villages during the invasion of Abkhazia and South Ossetia in August 2008, the armed conflict and the occupation that followed. Detailed judgment contributes to the historical record of the conflict and its human cost.

Through the judgment in this case, ECHR has created a new rule in the European public order because until this decision, the court had supervised the application of the European Convention throughout the European area, judging the violations of human rights in the territorial area of the European Convention on Human Rights.

The settlement of the dispute by the European court is a success of recognizing the importance of human rights during and after the unfolding of an armed conflict, being an internationally recognized reparation of the abusive acts of the Russian Federation in carrying out special military operations. Of importance in the light of contemporary security events is the consideration that competence under the ECHR is closely linked to the concept of *control*, whether it is the authority and control of the State agent over natural persons or the effective control of a State over a territory. Therefore, military operations in the active phase of hostilities in an international armed conflict fall outside the jurisdiction of the attacking State and therefore do not fall within the competence of the ECHR, which is not in a position to find human rights violations, which can be protected only by the legal means of IHL.

BIBLIOGRAPHY

CEDO. 2021. *Case of Georgia v. Russia (II).* Aplicația 38263/08, pronunțată la data de 21.01.2021. https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-207757%22]}.

Chifu, Iulian, Monica Oproiu, and Narciz Bălășoiu. 2010. *The Russia-Georgia War. The reactions of decision-makers during the crisis.* Bucharest: Curtea Veche Publishing house.

Council of the EU. 2009. “Independent International Fact-Finding Mission on the Conflict in Georgia.” Report. https://www.mpil.de/en/pub/publications/archive/independent_international_fact.cfm.

Dzehtsiarou, Konstantin. 2021. “Georgia v. Russia (II).” (American Journal of International Law) 115 (2): 288-294. https://livrepository.liverpool.ac.uk/3120615/1/georgia-v-russia-ii.pdf.

Legislativ Portal. n.d. *Additional Protocol No. 1 to the Geneva Conventions of 12 august 1949 on the Protection of Victims of International Armed Conflict 1977.*

OHCHR. 2022. *New report by UN Human Rights shows the shocking toll of the war in Ukraine.* https://reliefweb.int/report/ukraine/new-report-un-human-rights-shows-shocking-toll-war-ukraine-enruuk.

ONU. 2022. *War crimes have been committed in Ukraine conflict, top UN human rights inquiry reveals.* https://news.un.org/en/story/2022/09/1127691.

OSCE. 2008. *Ethnic Cleansing of Georgians Resulted from Russian Invasion and Occupation since August 8, 2008.* Ministry of Justice. https://www.osce.org/files/f/documents/6/b/34091.pdf.

Romanian Association of Humanitarian Law. n.d. *Convention of the Laws and Customs of Land War, Haga, 18 october 1907.*

Romanian Red Cross. n.d. *Convention for the amelioration of the condition of the wounded and sick in Armed Forces in the Field, Geneva, 12 august 1949.*

—. n.d. *Convention for the amelioration of the condition of wounded, sick and shipwrecked members of Armed Forces at Sea, Geneva, 12 august 1949.*

—. n.d. *Convention relative to the protection of civilian persons in times of war, Geneva, 12 august 1949.*

—. n.d. *Convention relative to the treatment of prisoners of war, Geneva, 12 august 1949.*

COMPETITIVE INTELLIGENCE AND OPEN SOURCE INTELLIGENCE – USEFUL TOOLS FOR COMPETITIVE BUSINESS

Raluca LUȚAI, Asst. Prof.*
Adina MIHĂESCU, Ph.D. Candidate**

> *”L’intelligence, ça n’est pas ce que l’on sait mais ce que l’on fait quand on ne sait pas.”*[1]
>
> Jean Piaget

According to principles of economic security, in this era of globalization and interdependencies, we understand that economic agents work competitively in uncertain markets. In the current international economic field, we cannot find either a perfect balance or long-term security conditions. Yet, this insecurity has the ability to stimulate the competitive field, to encourage innovation and adaptive competences. The anticipation of rapid evolutions and transformations which occur within markets or different industries represents a challenge which company managers handle with increasing difficulty. Even though much scholarly attention is paid to conceptual elements of competitive intelligence and its benefits, little is known about the way open-source intelligence can act like an instrument. This paper addresses this gap in the literature and analyze the way open-source intelligence can provide support for competitive intelligence actions.

Keywords: competitive intelligence; open-source intelligence; business-intelligence; methods; instruments; social media.

The ongoing development of the business field entails an intrinsic development, an update with the economic realities of the era of digitization. To meet its objectives, to have a profit and to be competitive, companies are bound to draft previsions and opinions of the future instead of simple and sterile information about their own present activity. From the incipient stage, from the moment of the drafting of a business plan, there is a need to be situated within the competitive field and a very thorough knowledge of it. The directing of resources, the handling of vulnerabilities, the drafting of strategies, all these have information as a starting point. From here, proper management decisions arise. Yet, rough information is, for the most part, useless; it becomes valuable as soon as it creates opportunities and a decisional advantage for the recipient. In the business field, transforming information into intelligence is a work method which pertains to the field of Competitive Intelligence.

In a world of complex interdependencies, a globalized world dominated by technological progress, information and those who hold the information have increasingly more power. An important marker of the globalization process, the Internet has taken over the world and has ensured its role as the main generator of information in all fields, producing veritable metamorphoses in daily life. This revolution has considerably changed the way in which people gather information, express ideas and interact socially and professionally. When we talk about intelligence, we undoubtedly talk about information, and when there is an increasingly wider opening toward information, a change in approach is more than necessary both in public and private fields.

This paper intends to analyze the way in which two new and relevant concepts for intelligence studies, namely competitive intelligence and open-

****Babeș-Bolyai University, Cluj-Napoca***
e-mail: *raluca.lutai@ubbcluj.ro*
*****Babeș-Bolyai University, Cluj-Napoca***
e-mail: *adina.mihaescu@ubbcluj.ro*

[1] Intelligence is not what we know, but what we use when we do not know (Jean Piaget).

source intelligence, intertwine. Starting from the conceptualization of the phrases “competitive intelligence” and “open-source intelligence”, the work analyzes the opportunities that competitive companies have in the technologized and digitalized field in which we live. The final part of the paper inventories, in short, a few instruments from open sources that can be used in competitive intelligence.

Competitive Intelligence and Open-Source Intelligence – recent concepts for contemporary realities

The conceptualization of the economic intelligence field materialized starting with the 1960s, along with American professor Harold Wilensky’s publishing of the work *Organizational Intelligence: Knowledge and Policy in Government and Industry.* The distinguished sociologist emphasizes here a need for the existence of collective strategies and a need for cooperation between governments and companies, toward coordinating a common knowledge and ensuring competitive advantage. Also, it reveals the necessity for knowledge in the economic field, as a strategic engine of societal development and change (Harbulot and Baumard 1997, 1-17).

Starting from the presumption that information is the first and foremost element of decision, we understand its importance and applicability in all fields, from the political and military to the social and economic. The study of intelligence in the economic field asserts itself gradually, as a necessity. The need for such management of knowledge is strengthened by the global competitive field in perpetual change. Competition between companies takes new shapes, and this aspect raises the issue of the systematic integration of these new dimensions in the analysis of competitive fields, both in terms of research and in terms of forming future managers.

In the era of globalization and digitization, it is paramount to understand information as a resource without which progress is rendered impossible. Competition over resources is a self-standing characteristic of economy, and, just as it focused on procuring raw material in the past centuries, it is now found in the procurement of information.

The application of intelligence studies on the economic field is the appanage of *competitive intelligence*. Its complex activities focus toward the objectives of the business field in general and of entrepreneurs in particular. Because economic science is social, within it there are different interpretations and paradigms (Coșea 2006), all of which understand the importance and usefulness of information.

Competitive intelligence (CI) intends to understand the complex economic field of the current time, to gather information and then analyze it, to study and interpret the competitive field, composing a clear and relevant overview of it (Cavallo, et al. 2021, 250-275) Just as the *neoclassical school*[2] establishes value depending on the degree of usefulness (Dixit 2012), so is information relevant only as long as it can be used and it is prone to contribute advantages. In the technological era in which we find ourselves, the multitude of data imposes a rigorous selection of it, a constant classification, organization and adaptation. Thus, CI research is supported by different branches of intelligence structures: HUMINT (intelligence sourced from human sources), cyber intelligence, SOCMINT (intelligence sourced through social media platforms), OSINT (open-source intelligence). The latter, though it does not constitute a rather new INT, has astonishing value within information communities.

Developed along with the informational boom, Open-Source Intelligence (OSINT) is defined in specialty literature as any information that is public, open, available to all, that does not engender implications of a legal nature and that can be collected, validated and analyzed in order to create intelligence products (Clark 2013).

The importance of this new type of intelligence is unquestionable. This aspect is also justified by the North Atlantic Treaty Organization (NATO), for which open sources represent a vital component of its strategic vision. In November of 2011, the Alliance published the NATO Open-Source Intelligence Handbook, a complex handbook which offers, in its first chapter, a most comprehensive definition of this new discipline. OSINT is not seen as a substitute for satellites, spies or other forms of civil and military intelligence. OSINT is considered information which was discovered in

[2] The entirety of all the school of thoughts pertaining to economic liberalism.

the public space, then analyzed and disseminated toward a select audience, mainly the Commanding General and their personnel, with the purpose of catering to a request for intelligence (NATO 2001). In other words, OSINT applies the regular process specific to any type of intelligence, to the wide diversity of open sources, with the purpose of generating intelligence products.

Information gathered by means of open sources is also known, within intelligence communities, as “white information” (Bean 2011). The symbolism of the chosen color is evident: the gathering of information from open sources does not imperil individual rights, does not entail human risks, and it produces a shift in paradigm at the level of information communities. Thus, open sources represent a big opportunity for the intelligence community and others. This intelligence discipline regards the legal exploitation of open sources, the validation and analysis of data and information discovered either through processes of simple observation or through its acquisition. The usefulness of this process is the same as with any other intelligence discipline (HUMINT, SIGINT, etc.), which is to eliminate the unknown from the decisional equation.

The literature divides open sources into two broad categories: (1) traditional sources such as books and broadcast open sources and (2) digital open sources.

1. Traditional open sources

The first generation of open sources is represented by books, magazines, but also by broadcast sources such as radio broadcasts or TV stations. The latter paved the way for this discipline. The history of open sources records the development of this analytical discipline in relation to an academic program developed by Princeton University in which the radio stations of the states beyond the Iron Curtain were analyzed, an activity that brought strategic advantages to the United States. In parallel, books or other types of written publications have always been a useful source of knowledge for government organizations. Their usefulness is also evident in the case of the business environment.

Books are a real open source used in intelligence work. They have always been used not necessarily for their actual content but for the references they contain. Books provide context on a particular issue. Government organizations can use them to gather new information and to understand common or different views towards one or another aspect of society. For the business world, books provide a competitive edge in knowledge. They can increase managers’ knowledge or develop creative visions that make them better understand the market in which they exist and develop. As for the actual understanding of the concept of competitive intelligence, those who run businesses or analysis departments in various companies have at their disposal books such as Kirk Tyson’s The Complete Guide to Competitive Intelligence or Christopher Murphy’s work Competitive Intelligence: Gathering, Analyzing and Putting it to Work. The two papers offer insights into the theory of competitive intelligence: how companies try to outperform their rivals, research methods and sources of information that generate the raw material for creating intelligence or analytical techniques that transform data and information into solid knowledge that can be applied in practice. Successful managers and company directors will apply the theoretical concepts identified in these types of papers to be successful in their field.

Another particularly important category is represented by newspapers and magazines which are useful for their much more specific content dedicated to certain topics. For government institutions, magazines can prove very useful. An eloquent example in this sense is the publication Aviation Weekly, which frequently provided details related to the military capabilities of the former Soviet Union (Williams and Blum 2018). For the business environment, magazines are a useful source for understanding the latest developments in the field or for analyzing the evolution of competitors who will use such supports to launch new products or strategic directions. For those really interested in the competitive intelligence environment publications like Competitive Intelligence Magazine exists. The publication has been offering the public since 1998 articles presenting best practices and innovations that enable companies to make strategic decisions based on information.

To these is added a special category always exploited by open source analysts, namely gray literature or gray information. The term gray literature refers to information obtained from traditional sources for which access is obtained on the basis of a subscription. The U.S. Government's Interagency Gray Literature Working Group, in 1995, defined gray literature as "material of internal or external origin that is normally available through specialized channels and is not found in traditional distribution channels" (Williams and Blum 2018). Gray literature represents a category of open sources particularly important for the business environment. For example, the proceedings of a medical conference related to the Sars-Cov2 virus may represent a starting point for specialists of large pharmaceutical companies. Analysis of reports, technical sheets or other types of gray information can contribute to a deeper understanding of the business environment.

Broadcast sources are a category that includes radio and television broadcasts. Although books, newspapers and magazines have always been a source of data and information, it was only with the development and spread of radio that those involved in the process of gathering information understood how useful radio stations are for their work. After 1980 the whole world was revolutionized by the spread and popularization of television. Through the specific topics they address, through the fact that they cover local events and thanks to the fact that each of us has at least one television, we are all more informed and more connected with the things that are happening near us or far away from us. The intelligence community has understood the ease with which it can gather information and the role that television has in the open source world. The same has been understood by the big businesses who are keenly watching the marketing elements presented by the competitors. The development of digital radio stations and podcasts is an important and useful element for companies that want to know the market, competitors or the latest developments.

2. Digital open sources

> *„Information costs money… intelligence makes money.”*
> (Robert Steel)

The digital world brings radio and television into one place, lowers costs and increases the variety of information that can be exploited. Digital open sources are revolutionizing the sheer amount of information they make available and the availability of that information. The digital open sources that appeared and developed in the last decades bear the name of new media as (a) social media-blogs, websites, virtual worlds (Second Life etc.) or the already famous (b) social networks such as Twitter or Facebook. Social Media is a term used to describe the various technologies concentrated in the virtual world used to interconnect people, businesses in various forms of communication and information exchange. Social Media, through its characteristic elements and the possibilities it offers, has come to reflect every facet of modern man's social life. Different types of social media transform the individual from information consumer to information and content generator, which is vital for OSINT. All the information that surrounds us is our product. We can capture everything, record anything, write or publish anything we want. This produces real metamorphoses at the level of the individual and the business environment that understood the utility that social media offers and chose to be present. The vast majority of large businesses have not only developed websites but have chosen to open accounts on social media platforms. The online environment is used for brand development, customer interaction or marketing.

Intelligence communities have understood the important role of open sources in their activities. Such was also the case with the business field. Both fields have things in common: the need for information and the lack of certainty. Despite these similarities, it is important not to confuse espionage activity with activities specific to competitive intelligence.[3]

Douglas Bernhardt (economic and CI analyst) stated in the work *How to acquire and use corporate intelligence and counter-intelligence* that "a strategy that is not based on intelligence isn't strategy, but guesswork" (Bernhardt 2003, 405-407). Thus, we understand the importance

[3] Competitive activities through information works within legal and ethical principles. In the United States, The Economic Espionage and Protection of Proprietary Information Act has removed the offense of violating the business secret and the offense of private information theft from under the jurisdiction of local and state authorities and has added them under the jurisdiction of federal authorities. There is no such equivalent in the legislation of Romania or the legislation of the European Union; despite this fact, there are several laws which incriminate economic espionage.

of information in business, in the building of the very strategy of a company, the main marker in converging and developing a direction.

CI analysis entails a vast process by which identified information is sorted based on usefulness, then evaluated, analyzed and, finally, assigned to decision makers in the form of complex analyses, dedicated to gaining competitive advantages. The essential purpose of each manager is to gain profit (or as much profit as possible), and this is one of the main economic indicators which signals whether the chosen strategies are favorable.

The activities specific to the field of CI mainly analyze companies in two ways: an analysis method pointing inward (the company’s internal environment) and the second one, pointed outward. While the former regards an in-depth analysis of each and every department, with working structures, processes and organizational charts, the latter aims toward the fundamental knowledge of competition and the field in which the activity is carried out.

The analysis of the company’s external environment, a thorough process of data collection and multiple analyses, is carried out by working with data already on the market, which is to say **open sources**. The challenges raised by this environment to the collection and analysis activities are evident. The saying “looking for the needle in a haystack” is more than relevant, itself being the result of multiplying information and spaces wherein they can exist. The information explosion is a reality which molds many processes that companies launch.

From the vast category of open sources, one of the most important in the business field is represented by digital sources. Websites offer a wide array of information from all areas of activity, but also analyses of economic indicators, statistics, graphs, etc. In the virtual space, there are sites which provide these databases and analyses for a monthly subscription (e.g., marketingdirect.biz, risco.ro, totalfirme.ro). At the same time, there is a possibility to access this data at no costs, by accessing the site of the Ministry of Finance in Romania (Ministry of Finance n.d.). This website provides a wide array of information, both for natural persons and for legal persons. Here can be found data referring to the legislation in force and the latest normative acts (as well as explanations regarding them), templates for applications that can be formulated with regard to the tax administration authorities, but also useful links to other websites of Romanian authorities (Presidency, Senate, the Chamber of Deputies, the People’s Advocate Institution, the Court of Accounts, the Special Telecommunication Service, the National Authority for Consumer Protection, as well as all the Ministries). Also, we can find information regarding the State Budget, Taxation, Public Policies, European Affairs, International Financial Relations, and State Aid.

All these are of particular interest when one aims to outline an analysis of the business field. Any company is obliged to be informed about the legislative acts and their eventual modifications, about the easiest methods of interacting with state authorities, about relating to European institutions and the communal economic field.

From the viewpoint of studying the competitive field, the website of the Ministry of Finance offers an accessible platform for interpellation and gathering of data regarding all economic agents registered in Romania. As for these economic agents and public institutions, information can be sourced regarding identification data, tax information and balance sheets. The latter are exceptionally important, as they constitute official accounting documents in which all of a company’s assets are presented – active and passive. By analyzing them, one can learn company’s profitability ratios, stock variables, the total value of assets, but also total debt value, debt ratio, available resources and their degree of use, the company’s earnings per share, as well as where that specific company is valued and what growth power it possesses.

The website of the Ministry of Public Finance provides information from the central databases regarding the registration of taxpayers, both legal persons and public institutions, tax liability statements (VAT, excise duties, gambling), balance sheets from the past six months from trading companies, stock records regarding outstanding liabilities to the state budget (Ministry of Finance n.d.). Upon accessing the platform, it requires the introduction of the taxpayer identification number, which in fact represents the tax identifier of every trading entity in our country, which is unique and assigned along with the legal person’s authorization to function. Subsequent to its introduction and to pressing the validation button, the platform generates a page with that company's information. Out of these, the most important for an eventual competitive intelligence analysis are: payer name, address, registration number with the Trade Register, authorization, corporate tax, social and medical insurance contributions, etc.

Subsequently, one can check the financial markers in accordance with the balance sheet submitted yearly, beginning with the year 2016 and up to 2021 (the past six years). This information can be accessed for each individual year, such that one can easily gain a statistic over the specific company's evolution and its activity in the past years, and could rather easily generate a forecast of its future developments. The official balance sheet data deals with current and non-current assets, stocks, receivables, debt, capital, total revenue or total expenditures.

All this information is especially useful in conducting an analysis of the competitive field in which a company carries out its activity, but also in relations with suppliers, collaborators and customers. Solvency, as well as profit and loss account and their fluctuations in the past years can provide a clearer overview of the business partners and can influence, for instance, contractual terms. The decision to associate with a certain company can be influenced by the gathered information following a check-up of the company on the Ministry of Finance website.

The website of the Ministry of Finance in Romania represents an eloquent example for the large quantity of information to which companies have access upon analyzing the field in which they function. Aside from these websites, which are the emanation of the governmental element, there are many other websites or platforms created by actants in the private field, available by means of subscriptions or not, which can be accessed by those who wish to gain competitive advantage.

For instance, farmers who wish to be professionals when it comes to handling their own cultures or analyzing their competitors' cultures have at their disposal various commercial satellites that can be easily accessed through different platforms. Satellite images that were exclusively accessed by governmental structures in the past are now at the disposal of the general public. In this respect, platforms like Sentinel Hub[4] or Planet[5] are eloquent. These provide the user with the ability to instantly view data harnessed from different satellites, presenting them with actual agricultural information through which farmers can analyze the evolution and health of their cultures[6]. By using this kind of platforms, they can cultivate more efficiently and more profitably. At the same time, they can also gain an overall perspective over the competitors' cultures.

Technological evolution has also transformed the way in which one can use information gathered from communication systems, radars or other signal-emitting devices. The gathering and analysis of this type of information is specific to the SIGINT field – signal intelligence, but has now become, in certain situations, a source of open information. In this manner arose platforms such as: Flight Radar[7], which monitors air traffic, or Marine Traffic[8], which provides an encompassing picture of marine traffic. The services offered by this kind of platforms can be used by transportation companies and more. Through them, they can optimize certain processes, thus raising their profitability, or know their competition better.

The biggest revolution registered by digital sources deals with the development of social platforms like Facebook, Instagram, LinkedIn or Tik Tok. These platforms build an environment in which the user can play the part of the information consumer or that of the information producer. Within these virtual spaces have also arisen the biggest and smallest of businesses. To maintain a dialogue with customers and to broadcast the most recent and most relevant information about their products or about business evolution, companies are more active than ever on social media. Beyond the marketing element, which offers a clear perspective over the direction in which a company is headed, these companies' customers or their competitors' customers lead online discussions about their experiences, perceptions and wishes.

[4] https://www.sentinel-hub.com/explore/eobrowser/, accessed on 11.11.2022.

[5] https://www.planet.com/markets/monitoring-for-precision-agriculture/, accessed on 11.11.2022.

[6] Different commercial actants have exploited this opportunity and have developed similar platforms in Romania. One example is the ogor.ro platform.

[7] www.flightradar24.com, accessed on 11.11.2022.

[8] https://www.marinetraffic.com, accessed on 11.11.2022.

These conversations offer answers to questions and real-time, unfiltered feedback, which will directly affect the development of future strategies, while simultaneously offering a clear perspective over that particular business field. The analysis tools are various and must be used by all who wish to be one step ahead of the competition.

Although the benefits of the digital environment are obvious, the use of information from open sources also involves a number of challenges. The sheer volume of information available sometimes creates problems. The analyst may face a series of roadblocks that can make the process inefficient, and perhaps even a series of information that has no relevance. Gathering information can thus turn into a never-ending pool of discovery that increases human effort. The large volume of information can cause overload problems and the processing time can be too long.

Conclusions

Acts of information gathering are continually carried out, processes that, once launched, need to be improved, updated and constantly perfected, their finality being represented by strategies, tactics that are, themselves, active processes with a high degree of adaptability.

Information from open sources, and especially information from digital open sources, are a tactical and essential strategic resource that can contribute to the reduction of unpredictability and uncertainty, not only at the governmental level, but also at the level of companies that understand that they need to work in order to be competitive. Open sources provide quick and low-cost access to a vast domain of information that can prove its strategic, operational or tactical usefulness, that offers a framework which enriches already obtained information, contributing to the creation of an overall picture necessary to the field of competitive intelligence.

Even if the advantages take precedence, we cannot disregard the challenges and problems that open-source tools can create for the business field. The problems can mainly deal with overcharging the networks, the predisposition to manipulation or disinformation, and the eventuality of collecting information that is incompletely validated, which can harm the entire process. This is why information provided by the Ministry of Public Finance is more trustworthy, being an official source for enquiry by the economic field (and more) in Romania. Other types of platforms are dynamic (they exist today and may not exist tomorrow) and they sometimes imply additional expenses.

Yet, as mentioned above, using such tools can contribute in a considerable manner to the competitiveness of a business. Even though the benefits are countless, the exclusive use of such platforms does not suffice. They must be placed in a context, analyzed and interpreted. If used only as a source for companies to obtain information, a constant briefing with what is happening all around, especially in a specific field of activity, is achieved. Yet, the final purpose is not this, but aiding the company to compile forecasts and long-term plans, to become a leader, a trailblazer, not a simple follower. Ideally, they will gain a competitive advantage in the long term, a stability, a continual evolution.

Companies that carry out actions specific to competitive intelligence must use tools and methods pertaining to open sources in order to be at the avant-garde of the current globalized economic field.

BIBLIOGRAPHY

Bean, Hamilton. 2011. *No More Secrets: Open Source Information and the Reshaping Od U.S. Intelligence*. Praeger.

Bernhardt, Douglas. 2003. *Competitive Intelligence: How to Acquire and Use Corporate Intelligence and Counter-Intelligence*. Edited by Financial Times Prentice Hall.

Cavallo, Angelo, Silvia Sanasi, Antonio Ghezzi, and Andrea Rangone. 2021. “Competitive intelligence and strategy formulation: connecting the dots.” *Competitineness Review* vol. 31 (no. 2): 250-275. doi:https://doi.org/10.1108/CR-01-2020-0009.

Clark, Robert M. 2013. *Intelligence Collection.* Sage Publications.

Coșea, Mircea. 2006. *Manual de Economie.*

Dixit, Avinash. 2012. “Paul Samuelson’s Legacy.” *Annual Review of Economics* 4 (1): 31. doi:https://doi.org/10.1146/annurev-economics-080511-110957.

Harbulot, Christian, and Philippe Baumard. 1997. *Perspective Historique de L´Intelligence Economique*. Intelligence Économique. https://www.ege.fr/sites/ege.fr/files/downloads/16.perspective_historique.pdf.

Ministry of Finance. n.d. *Agenţi economici şi instituţii publice – date de identificare, informaţii fiscale, bilanţuri.* Accessed noiembrie 11, 2022. https://mfinante.gov.ro/domenii/informatii-contribuabili/persoane-juridice/info-pj-selectie-dupa-cui.

NATO. 2001. *NATO Open Source Intelligence Handbook.* https://www.academia.edu/4037348/NATO_Open_Source_Intelligence_Handbook.

Williams, Heather J., and Ilana Blum. 2018. *Defining Second Generation OSINT for the Defense Enterprise.* RAND Corporation.

THE IMPACT OF ROBOTICS AND ARTIFICIAL INTELLIGENCE ON FUTURE MILITARY CONFLICTS

Col. Silviu-Iulian GIMIGA, Ph.D. Candidate*

Robotics and artificial intelligence are high technologies that are pushing the boundaries of human civilization. Recent decisions made by international military organizations have launched major programs for the development of new technologies that will lead society to modernity while increasing security for the entire world population. The dynamics of technological progress are constantly increasing due to economic and military advantages and, at the same time, the desire of researchers and scientists to go beyond the limits is a result of the challenges we face on a daily basis. The physiognomy of military conflicts is becoming more complex as a result of the unprecedented development of modern military technologies, which, when combined with conventional technologies, change the approaches to planning and the principles of operational use of forces and means.

Keywords: *technology; robotics; artificial intelligence; conflicts; technological progress.*

The use of cutting-edge technology, which is often the key to success in a military conflict, is a challenge for the new generation of soldiers from NATO member countries and from the entire National Defense System in Romania. What exactly does high technology imply? Smart cars, humanoid robots, artificial intelligence devices, quantum computers, and anything else that can be incorporated into existing or new equipment.

Recent scientific research has drawn the attention of the global population to emerging technologies, demonstrating first and foremost the implications they have on specific equipment as well as the approach to specific doctrines, manuals, and operating procedures. Although the war between Ukraine and Russia, which began this year, demonstrates the need to combine classical, conventional technologies with modern ones that make a difference, it is expected that the large-scale introduction of robotics, artificial intelligence, autonomous systems, and quantum technologies on equipment in the endowment of armies will produce profound changes in the conduct of future military conflicts in the not-too-distant future.

Since the communist period, the concept of artificial intelligence has been intensely debated in mass media, scientific communications, and published books, and it continues to be a fascinating topic for the entire modern world. There is currently a series of actions and activities being carried out for the modernization and a rapid, continuous development of military equipment and technique by introducing some initial elements of artificial intelligence, which determines the change in the way military commanders analyze and synthesize information in modern armed conflicts.

Starting with these coordinates, it is interesting to bring to the scientific research plan the need to introduce large-scale artificial intelligence within current and future technologies. The steps that must be taken in approaching future wars are related to the way in which the young generation of soldiers understands to involve actively in the development of equipment and the search for viable solutions to convince the command of the military system to make optimal decisions regarding the acquisition of modern equipment.

The research activities of military engineers and scientists for the development of existing technologies, at the pace imposed by international military organizations, as a response to the interests of the Romanian state to be the first to achieve great goals, as our forefathers did, are a permanent concern and correspond to the national objectives generated by the new existing military conflict in the Black Sea area, in the context of the conflict between Russia and Ukraine.

The new NATO Strategic Concept, which was adopted at the Summit on 29th of June, 2022,

*”Carol I” National Defence University
e-mail: *gimiga.silviu@forter.ro*

defines the Alliance’s new security challenges and outlines NATO’s political military objectives to be addressed. As a result, the impact on Alliance members determines the strengthening of the cyber space, the development of skilled responses to the Russian Federation’s misinformation campaigns, the discovery of solutions to prevent exaggerated population migration, and the reduction of the effects generated by economic constraints, by encouraging private companies to develop cutting-edge technologies capable of responding to such challenges.

The benefits of technological progress are obvious all over the world, but only a few countries can keep up with the unprecedented and rapid development of all technologies. It is international military organizations that initiate policies, research programs, and technological development, and which, thanks to large funds raised as a result of member interest, accelerate technological progress. It remains to be seen how each NATO member state understands and responds to the Alliance’s demands.

This article proposes an examination of the ability to comprehend and promote the need for new military technologies. Are autonomous robots and artificial intelligence required in future military clashes? Is it necessary to revise the logic of military command structures? Could they be the answers to these questions, the key to the development of fields that will be common place in the future, rather than mere fantasies, as we may believe at the moment?!

Emerging technologies and their relevance to NATO

Because all countries around the world are interested in technological advancement in the interest of maintaining peace and prosperity, it is worth considering whether it is time to discuss robotics and artificial intelligence in the military field. Perhaps the world is not ready to face the challenges posed by robotics, artificial intelligence, and bitcoin-based technology because of the low standard of living and ongoing conflicts that have an indirect impact on daily life. Computers are becoming increasingly difficult to use due to the complexity of their software systems, and artificial intelligence may cause significant confusion when it comes to understanding an action or making a decision.

According to scientists and military experts around the world, *“the field of robotics is still in its early stages, but robots will most likely become a very common equipment in future wars”* (Doaré, et al. 2014, 3). The dynamics of technological progress convinces us that we are not far from the use of robots because there already exists equipment for the execution of important activities concerning property rights, free movement, image rights, privacy, the delimitation of virtual areas and borders, and the artificial intelligence tested within systems of any kind, will be developed concurrently with the use of test algorithms.

NATO is celebrating 70 years of scientific and technological research to gain an advantage over potential adversaries this year. Dr. Theodore von Karman was the first scientist to achieve scientific cooperation among NATO members in science and technology. Since 1952, space research has been conducted, and year after year, conditions have been created for the advancement of the human factor, vehicles, medicine, computer systems, simulation and modelling, electronics, maritime research, and so on (NATO Science and Technology Organization n.d.). The new NATO Strategic Concept, adopted at the June 29-30, 2022 summit in Madrid, and the decisions made at the September 14, 2022 North Atlantic Council meeting, *“establish how the Allies will work together to adopt and integrate new technologies, to cooperate with the private sector, to protect innovation ecosystems, shape standards, and commit to principles of responsible use that reflect the Alliance’s democratic values and human rights”* (NATO 2022a).

Starting with these coordinates, all NATO members are to launch research programs and seek collaboration solutions with private companies to introduce new technologies for large-scale production. These NATO decisions are expected to benefit the military system first, by requiring the implementation of cutting-edge information technologies that will allow command and control of troops, as well as obtaining a common operational picture of the battlefield. Furthermore, communication technology, which currently ranks first in the world in terms of technological progress, is critical to the success of military operations. It remains to be seen how artificial intelligence embedded in information and communication systems will anticipate human intentions before scripts and action plans are required. Every day, we seek answers to the question of how technology will develop and what the consequences of rapid progress will be.

When we examine the ability of NATO member armies to collect information, we notice that each one has information structures that, when divided into different sectors of activity, can learn aspects about the enemy, such as strategic objectives, doctrine, strategies, and defense policies, both through human resources in the field and, more importantly, through modern information and communication technologies. The processing and distribution of this information is a critical component to develop, as the speed and accuracy of the data can be critical for combat forces in the field to ensure the success of a military operation. The development of robotics, artificial intelligence, and quantum technologies could be the key to obtaining vital information much faster for a country’s security.

If we had robots with artificial intelligence, we might be able to clear buildings occupied by terrorists or neutralize artificial bombs without having to sacrify people. Of course, the cost of construction and use would be high, but the benefits obtained would be significantly greater. The cutting-edge technology has long been a challenge for the entire global scientific research community, but it is still in its early stages because it is critical that artificial intelligence *“to be implemented in accordance with the ethical code and moral values”* (Ene 2019, 252). Its widespread use, regardless of the benefits and risks involved, can have profoundly changing effects on the daily lives of the entire global population, which is why NATO has established an accelerated start of cooperation with independent companies in the research and production of intelligent military equipment. How does it accomplish this? By establishing agencies at the level of allied commands that specialize in the study, analysis, and centralized procurement of equipment and technologies shared by all Alliance members that are interoperable, necessary, and sufficient for use on national territories or in areas of assumed responsibility.

Artificial intelligence is present in all aspects of social life; it assists us in everything we do through the technologies in which it is embedded, with the assumption that we are aware that we are not acting in a secure environment, and that we are perpetually vulnerable to invasions of our privacy. High-performance computers with artificial intelligence algorithms installed can be turned into self-learning human robots. This aspect contributes to redefining the strategic concepts of security and defense and has an indirect influence on future military operations.

Quantum technologies act as a force multiplier for mass-produced systems, bringing emerging concepts to life. The use of artificial intelligence to improve existing applications results in the development of equipment that, for example, can be extremely useful for nation-state defense and security. The quantum computer has an astounding speed in performing calculations and comparisons, which would be a huge advantage in selecting information needed to avoid conflicts.

As a result, robotics, artificial intelligence, and quantum technologies are fields that can improve humanity’s standard of living by simplifying daily activities as well as having long-term beneficial effects. Physics demonstrates that the principles required to develop these fields are feasible, implying that only time, interest in progress, and financial resources are preventing large-scale equipment production.

Therefore, emerging technologies are constantly on NATO’s agenda because they are changing the way wars are fought and won in an increasingly dangerous and competitive world. Adoption of emerging technologies is difficult to achieve precisely because they must be implemented in accordance with solid principles of responsible use. NATO launched the *“NATO Innovation Fund”* this year to support cutting-edge technologies that can help the world’s increasingly dangerous security challenges. NATO Defence Ministers approved *a “NATO Coherent Implementation Strategy on Emerging and Disruptive Technologies”* (Romanian Government 2022), under which each member country will contribute annually to private companies developing dual-use, emerging, and disruptive technologies.

The United States of America, NATO’s strategic partner, is the one who established the Defence Advanced Research Projects Agency (DARPA) within the United States Department of Defense, a leading institution that has invested billions of dollars in research programs – development of equipment based on algorithms and applications in the field of artificial intelligence. Among the programs developed there are *"real-time analysis of sophisticated cyber attacks, detection of spoof images, construction of dynamic robots that produce casualties in war, human language detection technologies, automatic recognition of enemy targets, analysis of spatial images, and supply chain logistics"* (DARPA n.d.). In 2021, for example, the Agency created a program in which military personnel could have assistants perform complex tasks with minimal error and extend human physical abilities beyond normal limits. Further research, as well as the demand for these benefits by NATO's strategic partners, could be used to carry out tasks such as mechanical repair of malfunctioning equipment, providing first aid on the battlefield, or mentoring aircraft pilots.

The civilian company BAE Systems, which was awarded a series of research and development projects by the US Advanced Projects Research Agency, made software and equipment for *"operational planning and execution of tactical missions, ballistic protection of fighters and bringing them to safety from the fields of combat systems, a wide range of smart munitions and artillery systems, electronic warfare systems that detect and protect against advanced radio frequency attacks, transmit and receive antennas that use artificial intelligence"* (BAE Systems 2022).

The modernization of military equipment is dependent on the R&D sector, which must be allocated at least the value of the procurement sector from all NATO member states' defense budgets. NATO's decision to prioritize cutting-edge technologies as an integration priority is likely to result in significant changes in the approach to bold development projects in the near future.

One of the most complex tasks in the NATO command structure is military operations planning, and automation has become the primary focus of technological attention. Increased speed in information assurance, support for decision-making processes, replication of logic processes that can provide an alternative response, compensating for the lack of specialized personnel in specific fields, and physical security of travelers through facial recognition, voice recognition, and image recognition are all advantages of automation.

The United States of America is now known for its investment in artificial intelligence as a result of the well-known goal of increasing military operability as a major player in NATO. The planning and decision-making process developed and tested by Americans is now implemented as an example for each Alliance member state and represents simplified management and simulation of the operational environment, a useful way to detect and combat threats, treat and select the collected information, and provide rapid delivery of strategic and tactical analyses. Thus, robotics and artificial intelligence enable human performance improvement and evolution.

The experience gained over the last two decades through the participation of all NATO members in operations in the theaters of Iraq and Afghanistan has shown us the real progress achieved by the use of drone systems, and as a result, interest in the field of intelligent machines is increasing year after year. Drones are future weapons that can be used as disruptive factors in both military confrontations and terrorist or crisis situations. They are relatively simple to construct and can take the form of robots, land vehicles, or air vehicles. For the time being, airspace laws are not clearly established, in the sense that there is a need for recommendations regarding their authorized use and clear provisions regarding their improper use.

NATO members' strategies include plans for technological and interoperable advances in the field of emerging and disruptive technologies, for which guidelines on the use of artificial intelligence and its control mechanisms have already been issued. As a result, technology has become a sometimes-unattainable necessity, driving each of us to fulfill obligations. The future is the main character in the game that our minds are constantly playing, and the accelerated transformations of technologies give the impression that humanity is on the verge of extinction, which can cause disorientation.

Analyzing human history, it was found that *"food surpluses fueled politics, wars, art, and philosophy"* (Harari 2017, 95), and technology did not make their lives easier. Furthermore, *"the human brain is not perfectly built like a computer because it has certain limits, determined by its limited capacity and the fact that it dies with the person, the information existing in it cannot be* *preserved for more than a century”* (Harari 2017, 95) and cannot analyze any type of information.

Following the analysis of these considerations in working groups and conferences at the level of NATO experts, the start of endowment programs, tenders, purchase intentions, and the sale of modern military equipment to all Alliance members was initiated. From the standpoint of the long-term war between Ukraine and Russia, it is natural that the modernization of armaments and military technology determines the joint production of equipment such as tanks, fighter and reconnaissance aircraft, surface-to-air missile systems, missile-carrying ships, navigation and communications systems, power generators, and ship handling systems.

Already, great powers such as France have acquired combat helicopters; Israel has signed contracts for the purchase of tanker aircraft; and Serbia has launched programs to modernize its own defense industry, leading us to believe that NATO's signal regarding the development of new technologies was not coincidental.

The conflict in Ukraine, which has been described as a war of attrition, has led us to believe that its outcome is directly related to the ability to stockpile weapons and the efforts of Western countries to supply modern weapons capable of effectively responding to the Russian Federation's challenges, such as HIMARS missiles (High Mobility Artillery Rocket Systems) with a range of up to 80 kilometers, anti-artillery radars, anti-aircraft radars, Javelin missiles, anti-armor missiles, helicopters, tactical vehicles, spare parts, equipment are weapons and techniques that can influence the way of war.

By carefully analyzing recent events, we can see that the conventional war is not over, and it is a challenge for our generation to find solutions that combine established technologies with modern ones based on artificial, robotic, and quantum intelligence in conditions where the human factor is increasingly interested in living a normal life based on peace, prosperity and understanding.

Robotics and artificial intelligence in Romanian military applications

In the modern Romanian society, the military make use of techniques that necessitate care, attention to usage instructions, and physical and emotional intelligence in order to keep them in good working order and achieve the objectives proposed at the level of military structures. The modern equipment and systems with which the Romanian Army is now equipped impose a number of obligations on the entire military force, beginning with their storage, preservation, maintenance, and use, as well as a number of responsibilities for its development and modernization.

“Developments in the technological field determine the diversification and increase in the complexity of security risks and threats, such as cyber-attacks and activities specific to the information field.” (Presidential Administration 2020, 6), therefore attracting the elites of Romanian society is one of the permanent concerns of the military system's command mechanism in order to successfully use the equipment and high-performance technology for the purpose for which they were designed.

“Technological advancement is a never-ending process that affects not only aeronautical organizational systems but the entire society.” (Iordache 2020, 236), which leads us to investigate the rapid evolution of technology as evidenced by the appearance of new systems and equipment in all categories of Romanian Army forces, with the goal of supporting the operational planning process and, implicitly, the decision-making and training processes of the own military structures. The civil domain benefits implicitly from technological progress through the development of the two scientific branches of robotics and artificial intelligence, which are becoming more relevant in our lives, knowing that robots endowed with artificial intelligence will be able to perform a vast array of tasks that exceed human performance.

However, we cannot discuss robotics and artificial intelligence in the Romanian military field at this time because it is only a topic debated within working groups at the level of the international military organizations in which we are members. Modern technologies are required to achieve the following goals: management and simulation of the operational environment, detection and combating of threats, treatment and simplification of collected information, and rapid delivery of strategic and tactical analyses. Autonomous unmanned vehicles, for example, can monitor and recognize targets that are impossible to reach with human resources, enable the use of strike force by eliminating targets, or protect dispersed units or structures in the field.

Romania’s strategy includes an *“exponential development trend of emerging technologies (5G, artificial intelligence, big data, the Internet of Things, cloud and smart computing), which generates, on the one hand, the need for growth and improvement of communications that will support digital services, innovative ones intended to support citizens and the business environment, and, on the other hand, the need to collect and secure data and information circulated in the respective systems.”* (Presidential Administration 2020, 18). To achieve national security objectives, Romania became an active participant in the development and discovery of new technologies through research efforts submitted by military engineers within the Research Agency for Military Technique and Technologies – an elite military unit of the Romanian Army –, the Defense Command Cybernetics, Communications, and Informatics Command, as well as by participating in working groups and forums with specialized personnel, within the working groups and research programs on robotics and artificial intelligence, initiated by NATO and the EU.

The Research Agency for Military Techniques and Technologies has scientific research centers under its umbrella that produce inventions, innovations, and maintenance and modernization elements of techniques and equipment in the categories of land, air, and naval forces.

In order to achieve technological progress, the Romanian Army encouraged *“the use of modeling and simulation in the training of troops as an advantage in the formation of skills and in the development of capabilities.”* (Dogaru 2015, 82). There are currently *Simulation Training Centers* in Romania that control complex programs and applications that bring the reality of the battlefield in front of users and test their technical capabilities, operating procedures, intelligence, and way of action in borderline situations. This is a step forward in the implementation of artificial intelligence and robotics on endowment equipment in the context of future warfare.

We discovered how important new technology was at certain points in the planning of actions and during the conduct of battles based on an analysis of how certain operations were carried out in the theaters of operations as well as military exercises carried out, and how much it meant that the equipment in the endowment was comparable to that of the combatants. As a result, *“the use of technology in the military system inevitably contributes to lowering the risks for the engaged human resource, reducing execution time, and increasing the intensity or complexity of the action”* (Gimiga 2021, 114).

The participation of the Romanian Army with soldiers in the theaters of operations was a huge advantage for the development of knowledge and skill formation in the fields of communications and informatics, logistics, and operations. Veteran militaries were aware of the testing of various combat equipment, military robots, and combat machines equipped with artificial intelligence algorithms, which led to the purchase of similar equipment for the transport, storage, and use of certain categories of armaments, explosives, and means of delivery fire, as well as unmanned aircraft for the execution of reconnaissance and objective destruction.

Numerous meetings and consultations have taken place in recent years at the level of the North Atlantic Alliance, but also at the allied level in the European Union, with an emphasis on artificial intelligence and new technologies, including the need to identify the impact they have on defense concepts and the development of defense capabilities. As a result, the Romanian military is aware that the world’s most powerful armies are developing autonomous weapons or combat robots as part of the joint effort to develop the new armament program, through which NATO armies will be equipped with weapons based on new physical principles, with lasers, drones, tracked vehicles armed with machine guns, and rocket launchers as top priorities. It is obvious that new technologies, increased numbers of qualified soldiers, well-trained teams, and leaders’ ability to quickly adapt to changes will lead to victory in current and future wars.

Future technological integration into Romania’s ability to defeat the enemy’s combat capabilities is heavily reliant on the collaboration of robotic systems and people, both of whom should be present in the first place. By utilizing enhanced autonomy capabilities, fewer soldiers are required to control combat systems, allowing robots to take on boring, unnecessary, and dangerous tasks. Greater autonomy will enable robots and systems to carry out high-risk missions for extended periods of time, extend the ability to penetrate enemy territory, and maintain occupied positions. As a result, the Romanian military, which is already small in size, will be able to focus on the missions that they can best perform.

Romania proposes, through *military ambassadors* sent to various international conferences, the adoption of ethical principles for the use of intelligent military equipment, which acquires the necessary capabilities to carry out the assigned missions on its own, through experience; they must be controllable, so that they cand be deactivated in the event of a malfunction. The autonomy of combat robots and autonomous systems based on artificial intelligence are being studied and debated, with many people believing that humans should be in control and that machines should not be able to eliminate targets based on self-learning algorithms. Because even if the robot is programmed to do something right, it does not know if it is also good, the human factor must decide when the robot soldiers can initiate actions with destructive potential. It is recommended to consider the relationships established between values such as loyalty, duty, respect, honor, integrity, courage, and discipline and the ethics of using the military instrument, respectively. These issues are hotly debated in conferences attended by Romanian military elites, and everyone has an obligation to actively participate in fostering an understanding attitude toward the progressive development of technologies.

Finally, it is not suggested that the presence of robots in the military environment should be viewed solely from the standpoint of lowering the level of risk for the human factor, increasing the degree of certainty of missions, or facilitating the creation of a high-caliber arsenal. Considering that a superior force is determined by combat methods, the selection of objectives, and the employment of advanced military technologies, it is necessary to consider that their constructive and functional particularities confer a qualitative leap in the preparation and conduct of military actions, either in accordance with the ethics of the production of military robots or to promote an education and a new technological mentality circumscribed by the concepts of morality and responsibility, supporting that technological progress beneficial to humanity.

Currently, the majority of Romanians are skeptical about the possibility of expanding robotics and artificial intelligence production on a large scale, but recent studies show that we should be optimistic about the future, thanks to the results of debates organized in these fields through collaboration with research institutions at prestigious scientific institutions around the world. Our intellectual and financial capacity to enter into major development programs, to value more military professional training, and to capitalize on experience and knowledge gained in theaters of operations, allied and transformational operational commands, and global peacekeeping centers provides Romania with the added value required to initiate development programs for existing technologies. It is also necessary to provide the young generation of military engineers with the opportunity to value their knowledge gained at Romania’s prestigious military academies, as well as to establish the necessary framework for motivating and rewarding them when the results obtained demand it.

The preparation of the next generation of military leaders for the robotics era is a constant concern of the Romanian military institution, which has introduced some new disciplines into its annual educational plans that seek to know how to make robots by understanding the principles of making mechanical and intellectual actions, as well as the purposes for which they are created. Military instructors are currently teaching future visions, either by sharing personal intelligence and experience gained on the battlefields of Iraq and Afghanistan, or by presenting unique events experienced in theaters of operations in the Balkans and Africa, or by presenting virtual images developed on the basis of current events analysis.

Financial assistance will never be enough to meet everyone’s expectations, so we should all consider how we can improve our actions and fight for our ideas and the future of the industries in which we work and live.

Analysis of the potential future clashes in terms of artificial intelligence and automation

Deep transformations at the regional and global levels continue to determine the repositioning of actors on the global geopolitical map. It is obvious that the current geopolitical context, both regionally and globally, imposes some instability in the eastern countries, a fact determined by the evolution of military equipment and techniques. Romania is in a security environment marked by complex developments that necessitate, on the one hand, redefining the role of military power and, on the other, adapting response methods to counter risks and threats to national security.

The development of a resilient infrastructure capable of meeting the new operational challenges is required in light of *“the primary role that capabilities for operations in cyberspace play, aggregated in a big data system, including artificial intelligence, Internet of Things (IoT), machine learning, and quantum technology.”* (Presidential Administration 2020, 28). To achieve this goal, the evolution of information and communication means, the gradual implementation of artificial intelligence in existing technologies, and the establishment of premises for the purchase of modern ones that keep up with modernization are all required. The civilian population, which will be an active participant in the war through intelligent communications, is expected to play a decisive role in future military conflicts. The mass media plays an extremely important role in influencing the benefits and drawbacks of technological progress through the information provided to the public.

Because public opinion is becoming more involved in the unfolding of events, political and military leaders must consider their desires when deciding whether to engage their own forces in military confrontations. With the disappearance of international press organizations’ reliance on the leadership of states to obtain access to operational areas by having their own satellites and aerial reconnaissance technologies without a pilot, keeping certain information secret from the mass media and other actors is becoming increasingly difficult.

The distinction between states of peace and war, between a conflict situation and a non-conflict situation, between military and non-military conflicts is becoming increasingly difficult as the area of manifestation of war expands and becomes one of the most complex. Divergence of interests at the political level is the root cause of all conflicts, regardless of category. These factors, along with a multitude of cultural and demographic factors, ethnic and religious differences, and the complexity of urban areas, contribute to an interconnected, dynamic, and extremely volatile operational environment. The operational environment is constantly changing, so commanders must constantly assess it in order to maintain a high level of understanding of the changing nature of threats.

As a result, there is a need to expand the automation of military systems by introducing specific artificial intelligence algorithms to simplify decision-making procedures. Furthermore, *“automation of the systems required for the military field causes a continuous and unpredictable change in the nature of war, implicitly contributing to the need to modify the classic concept of the decision-making process, which is based most of the time on a single option of action.”* (Petrescu 2015, 218).

The modern war is fought with joint military structures – land forces, air forces, naval forces, and special operations forces – distributed in theaters of operations spanning thousands or tens of thousands of square kilometers and interconnected and coordinated in real time by networks of orbital satellites. The automation of existing military technologies has a significant impact on how future wars will be fought. Technological progress, changes in the nature of conflicts, and the emergence of new regional and global military powers are all realities that cause changes in the physiognomy of armed conflict. Because of the rapid evolution of communication and information technologies, which are closely related to space technology, the planning and decision-making process is constantly adapting and changing. This constantly evolving space resource enables the implementation of 5G technologies, which determine the creation of intelligent applications, unlimited databases, and the development of faster and safer actions.

Considering the fact that the interpenetration of the actions specific to the conventional war with those specific to the non-conventional one, represents a reality of the last conflicts carried out or being carried out around the globe, there is a need for a generation of military leaders with well-formed decision-making skills in a comprehensive approach, in conditions of uncertainty, able to adapt faster than the opponent, as well as modern technologies, based on artificial intelligence, adapted to needs. *“Revolutionary technologies such as artificial intelligence, machine learning, quantum physics, three-dimensional (3-D) printing, and DNA research are currently creating more knowledge than has ever existed in all of history.”* (Ullman 2021, 31). Beginning with this reality It goes without saying that the advancement of modern technologies entails the widespread implementation of artificial intelligence on various military and civilian equipment and systems. Future technologies and approaches will continue to shape the outcome of wars and add a new dimension to life on Earth.

Globalization conditions, as well as the availability of technologies in the fields of communications and informatics, bio- and nanotechnology in the industrial sector, force us to research and determine where it is necessary to intervene to maintain the balance of power, in order to limit the use of chemical, biological, radiological, and nuclear weapons, direct and indirect attacks with conventional or non-conventional means, as much as possible.

The inclusion of academia, think tanks, specialist advisors, and a holistic understanding of all the implications that large-scale artificial intelligence would have in support of technology development will assist leaders in developing critical, creative thinking in adapting planning to the strategic context; they will develop the power of armies as well as people’s ability to make decisions and act in complex operational environments.

Conclusions

The article has mainly an informative purpose, with analytical-synthetic elements that are necessary for understanding the current state of knowledge in the field of robotics and artificial intelligence on a global and national scale, especially given that it is still in its early stages. In this sense, continuous research will determine the discovery of solutions to simplify the planning process, reduce the time allotted to each phase, and, implicitly, make the best decision in order to carry out a successful military operation.

Artificial intelligence, in my opinion, cannot replace human consciousness, feelings, and experience among military personnel; thus, technological development and application in armed conflicts must be approached with caution.

Currently, it is expected that the planning, management, execution, and evaluation groups of military operations will be formed by experienced military personnel with advanced knowledge in the fields of operations, human resources and materials, communications, and informatics.

When artificial intelligence algorithms are applied to existing military techniques and equipment, military structures experience personnel and logistical resource reductions. Last but not least, the need for high-quality human resources must be anticipated, and they must be selected, prepared, and trained in conditions that will allow them to use high-end technologies later on.

To have any hope of achieving rapid development, military leaders must be chosen in such a way that they understand the phenomenon of modernization and lead the human force not to exhaust it physically, but to develop it intellectually.

The first direction that should be followed resides in all the commanders’ obligation to study the necessity and importance of artificial intelligence in the decision-making process as well as in modern technology used in the planning process of operations carried out in peace and war.

A second direction to follow is to influence the decision-making power on the need to preserve the balance of forces and means by giving confidence to scientists and military engineers regarding the development of technologies in order to bring the Romanian military structures up to the standards and requirements of international organizations. Each of us is aware that modern technology involves exorbitant costs, but step by step and over time, it can create unexpected benefits for the entire society.

Last but not least, we can find the key to the success of a Romanian industrial revolution by promoting modern ideas and having the ability to influence the direction of funds towards technical-scientific research for the development of military equipment and techniques, by utilizing military and civilian human elites, as well as the existing material resources in Romanian institutions.

BIBLIOGRAPHY

BAE Systems. 2022. *Future technologies.* https://www.baesystems.com/en/what-we-do/future-technologies.

Correia, João. 2019. “Military capabilities and the strategic planning conundrum.” *Security and Defence Quarterly* vol. 24 (nr. 2).

DARPA. n.d. *AI Next Campaign.* Accessed Septembrie 26, 2022. https://www.darpa.mil/work-with-us/ai-next-campaign.

Doaré, Ronan, Didier Danet, Jean-Paul Hanon, and Gérard de Boisboissel. 2014. *Robots on the battlefields.* Fort Leavenworth, Kansas: Combat Studies Institute Press.

Dogaru, Manuel. 2015. “Considerații asupra evoluției modelării și simulărilor militare.” *Buletinul Universității Naționale de Apărare „Carol I”* vol. 2 (nr. 3): 82.

Dughin, Aleksandr G. 2011. *Bazele geopoliticii.* București: Editura Eurasiatica.ro.

Ene, Petru-Viorel. 2019. “Beneficii și riscuri în domeniul inteligenței artificiale.” *Conferința științifică internațională Gândirea Militară Românească.*

Gimiga, Silviu-Iulian. 2021. “Impactul tehnologiei asupra procesului de planificare şi luare a deciziei.” *Buletinul Universității Naționale de Apărare „Carol I“* vol. 10 (nr. 3): 114.

Harari, Yuval Noah. 2017. *Sapiens: Scurtă istorie a omenirii.* Iași: Editura Polirom.

Iordache, Lt. Valentin-Marian. 2020. “Implicaţiile dezvoltării tehnologice asupra siguranţei şi eficienţei în cadrul proceselor organizaţionale din domeniul aeronautic.” *Gândirea militară românească* (nr. 1): 236.

Legislative Portal. 2020. *Hotărârea nr. 22 a ședinței comune a Senatului și Camerei Deputaților pentru aprobarea Strategiei Naționale de Apărare a Țării pentru perioada 2020-2024.* https://legislatie.just.ro/Public/DetaliiDocumentAfis/227499.

NATO. 2022b. *NATO 2022 Strategic Concept.* https://www.nato.int/strategic-concept/.

—. 2022a. *NATO steps up engagement with private sector on emerging technologies.* https://www.nato.int/cps/en/natohq/news_207258.htm?selectedLocale=en.

NATO Science and Technology Organization. n.d. *The von Kármán Medal.* Accessed Octombrie 30, 2022. https://www.sto.nato.int/Pages/theodore-von-karman.aspx.

Petrescu, Dan-Lucian. 2015. “The military scenario, fundamental conceptual framework for the exercises carried out at the combined tactical-operational level.” *Bulletin of ”Carol I” National Defence University* vol. 2 (nr. 1): 218.

Presidential Administration. 2020. “National Defence Strategy of the country 2020-2024.” https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf.

Romanian Government. 2022. *Şedințe de Guvern.* https://gov.ro/ro/stiri/informatie-de-presa-privind-actele-normative-aprobate-in-cadrul-edintei-guvernului-romaniei-din-9-noiembrie-2022&page=1.

Stanciu, Cristian-Octavian. 2015. “Implicaţiile sistemelor şi tehnologiilor moderne în redefinirea unor noi concepte doctrinare.” *Buletinul Universității Naționale de Apărare „Carol I“* vol. 2 (nr. 1): 161.

Ullman, Harlan. 2021. *Al cincilea cavaler al apocalipsei şi noul M.A.D.* Bucureşti: Editura Militară.

THE RUSSIAN ARMY’S DEFICIENCIES IN OPERATION ”Z”

Cadet, Caporal 3rd class Denis-Georgian DINU*

Operation “Z” launched by Russia on 24.02.2022 against Ukraine is facing severe logistical problems on the ground. The railway infrastructure they rely on and cannot fully meet their requirements, outdated logistical equipment, difficulties and limitations in securing fuel requirements have been frequently reported problems in the last weeks of the conflict. The logistics support doctrine of the Russian forces contains some organizational and functional inadequacies. From its analysis it appears that a logistic support battalion with its personnel and equipment is not able to fully meet the support requirements of the forces served. Apparently, this deficiency is encountered both at the tactical and the operational and strategic level, as it becomes evident from the analysis of several articles and scholarly works regarding the current Russian-Ukrainian conflict. The present article aims, based on the analysis of information available from open sources (articles, TV reports and social media posts), to identify the source of the logistical problems faced by the Russian armed forces.

Keywords: *operation ”Z”; military logistics; shortcomings; technique; conventional warfare; doctrine.*

On the 24th of February, 2022, the Russian Federation launched a military operation invading Ukraine, which is widely considered an act of aggression. On the 21st of February, 2022, Russia recognized the independence of the Donetsk and Luhansk People’s Republics, two regions controlled by pro-Russian separatists, and the Council of the Russian Federation authorized the use of military force on the country of Ukraine. Offensives were launched on several fronts, including Ukraine’s borders with Belarus and Russia, and from the occupied territories (Donbas and Crimea). Russian army forces succeeded in besieging or occupying several key cities, such as Kernnihiv, Kharkov, Kherson, Kiev, and Mariupol, but the resistance of Ukrainian forces combined with logistical and operational challenges caused the progress of Russian armed forces to slow down (Wikipedia 2022).

The logistical challenges facing the Russian Federation’s military may stem from poor planning of logistic support to the fighting force. Based on events in Ukraine in recent weeks, we will analyze this planning, demonstrating the causal link between logistical deficiencies and the lack of success of Russian troops, materialized in their stagnation or withdrawal from several fronts.

***”Carol I” National Defence University, Bucharest, Romania**
e-mail: *dinudenis69@yahoo.com*

1. Short comings in logistical support

1.1. The Blitzkrieg doctrine implemented in Operation “Z”

The combat strategy “Blitzkrieg” comes from Germany and can be translated as “Lightning War”. This strategy involves speed and cooperation among forces, especially tank units, motorized infantry and aviation (Dancu 2010). The doctrine we are talking about was used successfully by Germany in World War II against Poland in September 1939, France in May 1940, Greece in April 1941. The Germans would choose a strategic point favorable for conquest, then mobilize their forces to begin military operations. Once a gap was created on the enemy front, forces were given autonomy to advance rapidly into enemy territory. Forces attacked communication centers to disrupt command and control processes and disrupt the enemy (United States Holocaust Memorial Museum n.d.).

We can observe similar points between the implementation of the Blitzkrieg doctrine and Operation “Z” launched on 24 February 2022. Initially, in the first two days of the aggression, Russian troops managed to advance about 200 kilometers into the Ukrainian territory (Vershinin 2022). However, due to major resistance from the Ukrainian army and citizens, the Russian forces advance subsequently stagnated.

1.2 Role of rail infrastructure in supplying troops

The transport of troops and the supply of forces, both within and outside Russia, is planned and executed by the Transport Insurance Department, a department serving the military and authorized by theRussian Ministry of Defense. This department is responsible for: developing systems for military deliveries; planning the cost-effective and efficient movement of troops; calculating the potential risks involved in transport missions (Grau and Bartles 2016, 326-328).

Transport missions are carried out by land (mainly using railways) but also by air and sea, both by using the transport equipment available and by contracting transport services from civilian providers. The national railway system is used to design the logistic support of the Russian army and to form solid supply lines. A large part of the army personnel is transported by trains. Logistics support capabilities in most Russian military operations (including Operation ‘Z’) are also transported by rail. This approach is effective within Russia’s own territory, given Russia’s territorial expansion. However, logistic support and supply capabilities end at the country’s border, from where Russia is forced to use road vehicles. Russia attaches great importance to the use of railways, noting that there are now specialized troops dedicated to their protection, operation and maintenance. These troops total about 10 independent brigades and battalions serving different regions of the country (Grau and Bartles 2016, 326-328).

Russia relies on its railway infrastructure, which is designed to serve direct transport from arms and ammunition factories to the specific depots of large units and establishments. The main reason stems from the vast territory of over 17,100,000 km^2 that the country needs to control (Ambasada României în Federația Rusă 2021), so efficient and effective military rail transport seems to be the optimal solution (Vershinin 2021).

Russia’s railway infrastructure is made up of 1,524 mm gauge tracks, the same gauge being adopted by the other states that were part of the Union of Soviet Socialist Republics, namely Belarus, Estonia, Moldova. (Marian n.d.). We define the railway gauge as the distance between the tracks left on the ground by the wheels of the same axle of a vehicle or the distance between the inner faces of two railway rails, determined horizontally at a 14 mm level below the top of the rail head (Biroul Român de Metrologie Legală – BRML 2005).

A potential attack on Western states would require a logistical effort on Russia’s part far beyond its capabilities, given that most Western states use a rail gauge of 1,435 mm, which is the standard for European rail infrastructure. Ukraine, unlike Western Europe, maintains the 1,524mm standard for rail gauge and so does Russia (Marian n.d.). However, the Ukrainian railway infrastructure cannot be used on a large scale, as the main junctions are in big cities, which are not yet controlled by the Russian army. As of 06.04.2022, Russia had large cities such as Kherson, Melitopol, Berdyansk, Donetsk, Luhansk under its occupation and also had access to the related junctions (Champion 2022).

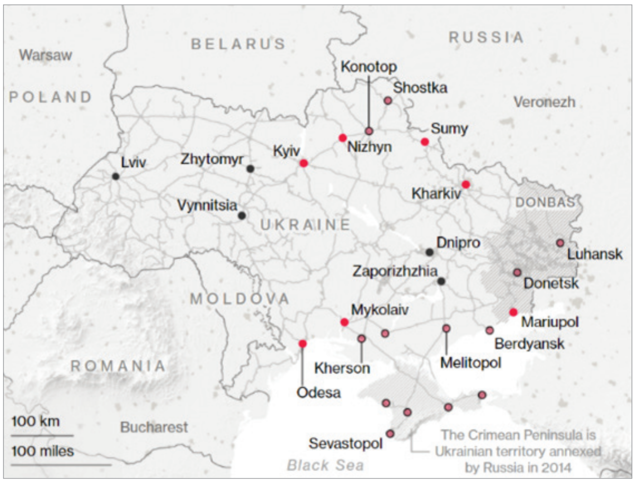
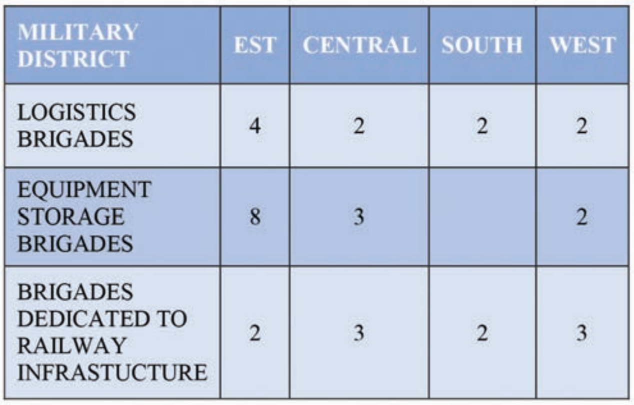


Figure no. 1 Map of Ukraine

An analysis by Gudrun Persson in *Russian Military Capability in a Ten-Year Perspective 2016* provides an overview of MTO forces deployed by districts across Russia. We note that in the western district of the country there are 2 logistics brigades, 2 brigades for equipment storage and 3 brigades dedicated to railway infrastructure, compared to the eastern district of Russia where more forces serving logistics support are concentrated, which creates a possible cause for the deficiency in providing logistics support for Operation “Z” (Persson 2006, 70-71).

To give the reader an idea of what logistic support in the Russian army means, we will define the term logistic support battalion: a Russian MTO logistic support battalion which usually consists of 1,000 troops and 400 vehicles serving the combat forces, with the capacity to transport about 1,800 tons of material for feeding, armament, TABLE no. 1 Positioning of Russian logistic forces



MILITARY DISTRICT	EST	CENTRAL	SOUTH	WEST
LOGISTICS BRIGADES	4	2	2	2
EQUIPMENT STORAGE BRIGADES	8	3		2
BRIGADES DEDICATED TO RAILWAY INFRASTRUCTURE	2	3	2	3

ammunition, maintenance. The configuration of an MTO battalion comprises a command and an operational part, the operational part being divided into material transport companies, a technical maintenance company and support companies (Grau and Bartles 2016, 332).

2. Poor logistical planning

2.1. Weak supply chain defences

Along a supply chain between the logistics base and the frontline, the structures that provide the necessary supplies to the troops must be protected, especially if the supply chain is formed on a predictable enemy route. Michael Kofman, an analyst at CNA Corporation, stated that Russian troops had poorly planned for the protection of logistical structures, which resulted in massive technical losses (Berkowitz and Galocha 2022). By 10.04.2022, 788 vehicles belonging to MTO logistic forces had been destroyed, 485 damaged and 228 captured by the Ukrainian army (ORYX 2022).

2.2. Outdated logistics technique

Since the supply of fuel, food, arms and ammunition cannot be provided by rail infrastructure alone, these materials must be transported by motor vehicles. These vehicles pose a major problem in advancing troops deep into Ukrainian territory, due to their age, as well as costly and time-consuming maintenance (Vershinin 2021). Russia currently uses 6 different types of trucks to supply troops, of which we list: Kama Automobile Plant (KamAZ), The Urals Automotive Plant (Ural), the Likhacov Plant (Zil), Gorky Automobile Plant (GAZ), Kremenchuk Automobile Plant (KrAZ), and Minsk Automobile Plant (MAZ) (350). These problems were also noted by the Russian army’s technical equipment structures, which led to a halt in the import of two types of military trucks in the mid-1990s (MAZ trucks produced in Belarus and KrAz trucks produced in Ukraine). However, even today these vehicles are still in the hands of Russian operational units on the territory of Ukraine (ORYX 2022). Even though the import of these trucks was stopped more than 25 years ago, the Russian army still faces problems in providing maintenance for them. Russia bought technology from 4 major manufacturers (KamAZ, Ural, Zil, GAZ), each using specific components and sub-components, so interchangeability between them was almost impossible. This led to a considerable effort to maintain the technique. A concrete example can be given by the Zil-131 truck which uses LPG (Liquefied Petroleum Gas) as a fossil fuel, while most of the transport equipment uses diesel fuel. In 1998, The Urals Automotive Plans signed a contract with the Russian army for the purchase of new, more reliable equipment. This led to the development of “Motovoz”, a project involving three new types of trucks (Ural 43206 4x4, Ural 4320-31 6x6 and Ural-5323 8x8). These trucks were designed to be able to split up to 95% of the parts. Due to financial problems, only the Ural 43206 was produced on a large scale and and delivered to the army. The decision was made by Anatoliy Serdyukov, Minister of Defence of the Russian Federation from 2007 to 2012.

Today, the standard truck used by the Russian armed forces is the KamAZ-4350, which is found up to the level of a combat battalion’s logistic support platoon. Russian logisticians believe that a major difference between the “Motovoz” and KamAZ trucks is the level of complexity for providing maintenance. Motovoz trucks were designed so that additional training of personnel in engine and component knowledge is not required, which is not the case with KamAZ trucks which have a higher level of complexity.

The Zil-131 truck (Figure 2) has a 6x6 drive, a vehicle designed for military missions. It was designed in 1966. Production stopped in 1994, with more than 1,000,000 assembled. The Zil-131 chassis has a carrying capacity of 5,000 kilograms for road travel and 3,500 kilograms on rough terrain.

The GAZ-66 (Figure 3) is a vehicle that is also in the Russian Army’s armory. Designed in 1964 and produced in more than 1,000,000 units, the GAZ-66 was for a long time the main material carrier of the infantry structures of the Union of Soviet Socialist Republics.

The Ural-4320 (Figure 4) is a medium-sized truck found on the Ukrainian front. It was designed in 1976 with a 6x6 drive and an engine developing up to 240 horsepower. It has a road carrying capacity of 6 tons, but can also be configured for personnel transport and can hold the equivalent of a platoon (Grau și Bartles 2016, 350-356).

One pattern that can be seen in all these vehicles is the date of manufacture and design, all of which come from the USSR era. More than 40 years on, the demands of the frontline have changed, outdated technology can no longer meet the requirements of a 2022 military operation effectively. Logistic support for the forces must be accelerated and run seamlessly, contrary to what can be seen on the Ukrainian front from the Russian military.

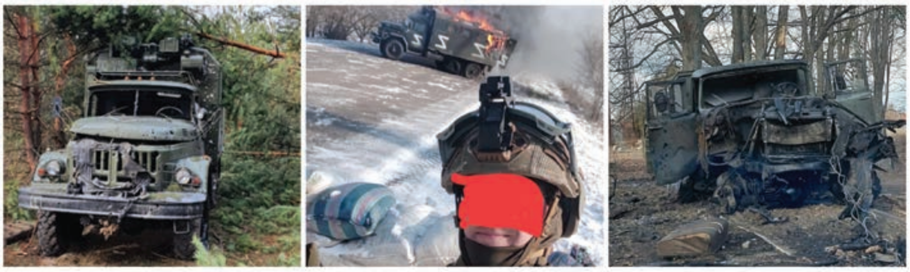


Figure no. 2 Zil-131 trucks destroyed in Russia’s offensive against Ukraine, 2022

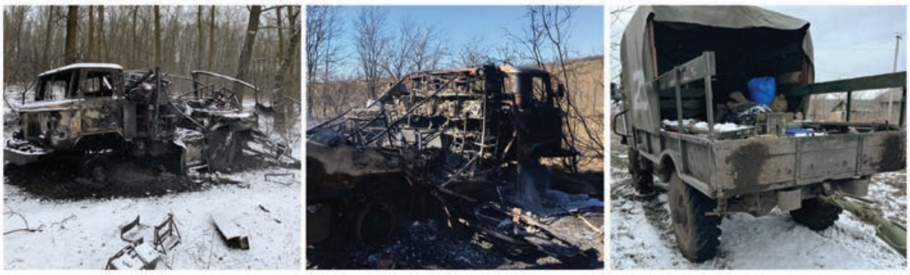


Figure No. 3 Gas-66 trucks destroyed in Russia’s offensive against Ukraine, 2022

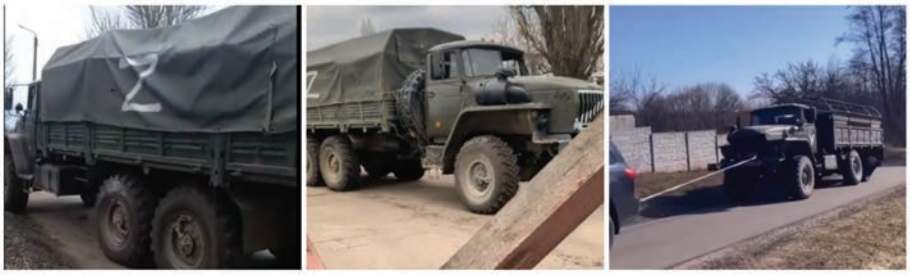


Figure No. 4 Ural-4320 66 trucks destroyed in Russia’s offensive against Ukraine, 2022

2.3. Lack of fuel

Images showing intact technology abandoned on Ukrainian territory also give us a glimpse of poor planning for Operation ”Z” (ORYX 2022). A likely cause of these abandoned trucks and tanks would be fuel shortages. At the organizational level, a Russian Logistic support brigade (MTO) has a battalion under its command with the role of providing fuel and drinking water through pipelines.

Specifically, during the offensive and troop retreat, this battalion creates a pipeline infrastructure, with a lower flow rate than the pipelines supplying fuel to Western Europe, but meeting the needs of the forces on the front (Grau și Bartles 2016, 329-332). The strength of this battalion is the time it takes to install the pipelines, up to 3 or 4 days after occupying the territory.

Once the pipeline system is in place, the army connects to the national fuel and drinking water supply infrastructure, pumping these two facilities to logistics bases in the field, from where they are distributed to sub-units via tanker trucks (Vershinin 2021). Official data show that this type of infrastructure has not been widely implemented in Ukraine, with the Russian army still relying on tanker trucks to supply and fuel frontline equipment, which do not fully meet the needs of the frontline, and linking this deficiency to equipment abandoned by the Russian military for lack of fuel (Vershinin 2021).

Conclusions

By concluding the facts presented above, one can see a deficiency in the planning of the attack launched by Russia against Ukraine, at least from a logistical point of view. These shortcomings

Figure no. 5 Russian military servicing a military structure with the role of fuel supply implementing specific infrastructure

Figure no. 6 Russian servicemen serving a military structure with the role of providing fuel by implementing specific infrastructure

were documented long before a conflict began, with Operation `Z' supporting these assertions with clearly observable facts all along the Ukrainian front. An evocative description of Russia that also applies to the current context was given by German Chancellor Otto von Bismarck (1815-1898), who said that *Russia is never as strong or as vulnerable as it lets on*.

BIBLIOGRAPHY

Ambasada României în Federația Rusă. 2021. iulie 13. Accessed April 19, 2022. https://moscova.mae.ro/node/484.

Berkowitz, Bonnie, and Artur Galocha. 2022. “Why the Russian military is bogged down by logistics in Ukraine.” *The Washington Post.* https://www.washingtonpost.com/world/2022/03/30/russia-military-logistics-supply-chain/.

Biroul Român de Metrologie Legală - BRML. 2005. *Norma de metrologie legală NML 041-05 “Aparate pentru măsurarea elementelor căii ferate sau de metrou” .* https://lege5.ro/Gratuit/g42damzy/norma-de-metrologie-legala-nml-041-05-aparate-pentru-masurarea-elementelor-caii-ferate-sau-de-metrou-din-14062005.

Champion, Marc. 2022. “Railways helped drive Russia off track and into Ukraine’s cities.” *The Economic Times.* https://economictimes.indiatimes.com/news/international/world-news/railways-helped-drive-russia-off-track-and-into-ukraines-cities/articleshow/90026442.cms?from=mdr.

Dancu, Ionel. 2010. *Cum a apărut temuta tactică germană <<Blitzkrieg>>.* https://historia.ro/sectiune/actualitate/cum-a-aparut-temuta-tactica-germana-blitzkrieg-582522.html.

Grau, Dr. Lester W., și Charles K. Bartles. 2016. *The Russian Way of War - Force Structure, Tactics, and Modernization of the Russian Ground Forces.* https://www.armyupress.army.mil/portals/7/hot%20spots/documents/russia/2017-07-the-russian-way-of-war-grau-bartles.pdf.

Marian, Jakub. n.d. *Track gauge by country in Europe.* Accessed April 19, 2022. https://jakubmarian.com/track-gauge-by-country-in-europe/.

ORYX. 2022. *Attack On Europe: Documenting Russian Equipment Losses During The 2022 Russian Invasion Of Ukraine.* https://www.oryxspioenkop.com/2022/02/attack-on-europe-documenting-equipment.html.

Persson, Gudrun. 2006. *Russian Military Capability in a Ten-Year Perspective 2016.*

United States Holocaust Memorial Museum. n.d. *BLITZKRIEG (LIGHTNING WAR).* Washington, DC. Accessed April 19, 2022. https://encyclopedia.ushmm.org/content/en/article/blitzkrieg-lightning-war.

Vershinin, Alex. 2021. *Feeding the bear: a closer look at Russian army logistics and the fait accompli.* https://warontherocks.com/2021/11/feeding-the-bear-a-closer-look-at-russian-army-logistics/.

—. 2022. *Russia`s logistical problems may slow down Russia`s advance - but they are unlikely to stop it.* https://mwi.usma.edu/russias-logistical-problems-may-slow-down-russias-advance-but-they-are-unlikely-to-stop-it/.

Wikipedia. 2022. *Invazia Rusiei în Ucraina (2022).* https://ro.wikipedia.org/wiki/Invazia_Rusiei_%C3%AEn_Ucraina_(2022).

HANNIBAL’S STRATAGEMS

Prof. habil. Mădălina STRECHIE, Ph.D.*

Rome’s fiercest enemy, the one who defeated Rome on its own in the Second Punic War, Hannibalus was one of the most special warriors of all time, so we can call the Second Punic War, his war. It was through all the actions he really took his war with Rome, both after all the outstanding theories about the war, but especially by the fact that the talented Carthaginian general defeated Rome at her home, shattering the myth of her invincibility, as a city of Mars. We are not wrong when we claim that Hannibal would have defeated the god of war in this conflict as well.

From the beginning of military hostilities to their end, the perfect strategist of the Puns fully controlled the theatre of operations, even being its sole director, putting his enemy, Rome, in the most disastrous situation of all time. Basically, Hannibal eliminated the echelon of command of the Roman army, but also the Roman army that is shattered in three successive battles at Trebia, Trasimenus and Cannae, ending up threatening Rome itself through the famous ante portas episode. Even though Hannibal’s war did not result in Hannibal’s peace, the intention of the brilliant general was to eliminate Rome as an armed force and economic strength, an objective fully accomplished during the military operations. The detail that eluded him was the Roman tenacity, the one that stole his peace, but Hannibal has entirely the paternity of the second war between the Puns and the Romans, being to this day a genius of the art of war, unmatched yet.

Keywords: conflict; strategy; disaster; surprise; Pun; ability; special; warrior.

***DEDICATIO*:**
We dedicate this study about one of the most special ancient warriors to all the special warriors of Romania

This study continues our preoccupations about the great military personality of the ancient world, Hannibal, analysing so far other studies dedicated to him about his strategic talent (Strechie 2016, 72-78), or about the Roman-Punic conflict, the real ”clash of civilizations” (Strechie 2015, 370-375) in which he was the main part, or about the emotion produced by him in Rome (Strechie 2020, 99-105), or about the use of terrorism on Rome during his confrontation with the Romans, Punic terror being the most painful for Rome (Strechie 2019, 161-168). This study does not repeat the subject of the other studies, so it does not insist on its italic campaign, on the confrontations or on the psychological effect on the Romans, but wants to frame the second Punic war, Hannibal’s war, in the main theories about the art of war, precisely to prove its paternity on this Puno-Roman clash of the charismatic Carthaginian general, especially since the subject was not treated by the Romanian researchers. So, we propose an original theme and try to prove that the art of war was well known in the ancient world, the generals of the ancient world being still today models worthy of follow, Hannibal being one of the most effective warriors of all time.

We will prove below that after all the military operations, according to the plan and tactics, the second Roman-Punic confrontation is truly Hannibal’s war with the Romans, he is being *pars pro toto Carthaginae* (part for the whole of Carthage - our trans.)

1. The Fatherhood of the Second Punic War

The second Roman-Punic conflict that unfolded between 218-201 B. C. was Hannibal’s because he was the grey eminence, his commander and tactician. The first argument over this paternity is that Hannibal becomes commander of the troops in Spain, a territory under Carthaginian rule, after the assassination of Hasdrubal. At the age of 25, Hannibal is the commander of the joint Punic troops, based in Spain. The first action in the position of commander is the occupation of Sagunt, an ally of Rome, thus unofficially declaring war on Rome who immediately sent envoys to negotiate peace. Peace talks did not even begin, and the Roman expedition was a failure. Hannibal had already made a war plan and began to put it into

***University of Craiova**
e-mail: *madalina.strechie@edu.ucv.ro*

practice by ”marching on Italy” by crossing two mountain ranges (the Pyrenees and the Alps) and not at sea as the Romans expected (Bagnall 2018, 70-72).

In this Second Punic War, Hannibal is *a pater*, as all his tactical plans have been fulfilled, and his goal, annihilating his opponent and blocking him from opposing him appropriately, was successful. The only detail that escaped the brilliant strategist was the perseverance and regenerative capacity of Rome, which not by chance had the following creed of life: TU NE CAEDE MALIS, SED CONTRA AUDENTIOR ITO! (You do not kneel in the face of evil but move forward with more boldness! – our trans.). Hannibal had no way of suspecting that Rome would be reborn as a Phoenix from his own mud in which he plunged it, especially at Trasimenus and Cannae, it was the hazard of war, which cannot be predicted even by the gods. It was precisely this hazard that brought peace to Rome, although Hannibal’s war was lost in the most emphatic way by the Eternal City.

Thus, Hannibal signs with his name the Second Punic War for the main reasons:

1. the effect of surprise: crossing the mountains and attacking Rome where it least expected it;

2. the division of Rome from its allies, which Hannibal draws into a genuine coalition against it;

3. The establishment of a veritable Punic terror within Roman society, not only within the Roman army, which weakened their morale and fighting capacity, establishing a genuine chaos;

4. the use of new weapons, the fighting elephants, with a devastating effect, precisely because of what is called the shock of technology, which disturbed the Romans and blocked them because they did not know how to fight back to this platform of struggle;

5. speed of action and successive victories;

6. The choice of the battlefield was always imposed by Hannibal, the Romans were forced to fight only where the great general wanted, although they were at home;

7. the division of the forces of the Roman army and the establishment of disorder within them;

8. the financial strength of Hannibal’s army, compared to the army of the Roman state, Hannibal taking care to properly finance his war;

9. Hannibal’s masterpieces of strategy: Trasimenus, Cannae, posting at the gates of Rome, with catastrophic effects on the Eternal City;

10. the destruction of the Roman army and its myth of great power in front of its neighbours and allies.

2. The purpose of Hannibal’s war

Hannibal’s war had only one purpose, namely the elimination of Rome, an emerging power at the time, which was looming as a serious competitor of Carthage in the Mediterranean Sea. That is why he made one of the ”boldest military plans” (Mills 2008, 14), and at the same time so surprising. His tactical plan was so simple, but so perfect, being conceived in two stages: marching over the mountains and attacking Rome on land (Mills 2008, 16), not at sea as expected by everyone, especially since Punic superiority was undeniable, and Rome had no chance in a naval battle. The attack was planned from Spain, the European territory of Carthage, which here secured an especially important basis of power, precisely because here in Spain the Carthaginians believed that Rome could attack them, being close in region (Mills 2008, 16). On the principle that the best defence is the attack, Hannibal attacked him first. Therefore, he thoroughly prepared the attack and began with the attraction to his side of the Allies of the Romans, especially from Italy. The best ”allies” of the conjuncture for Hannibal in Italy were the Gauls, old rivals of the Romans, who allied themselves with her for objective reasons, not out of conviction. Attracting the Gauls to the Punic side, thus breaking their alliance with the Romans and at the same time providing Hannibal with the best connoisseurs of the mountains he had to cross (Mills 2008, 17-18), thus providing him with guidance through the unknown mountains.

The composition of Hannibal’s army was based on the hard core of the veterans, who had previously fought under his father’s command, in the First Punic War most of them, and besides this nucleus he also attracted what were called the ”silver spears”, in fact well-trained mercenaries grouped in this distinct corps of army. (Mills, 2008, 18).

In addition to the Gauls, Hannibal also made other allies of his conjuncture, from Spain, namely the Iberians, slightly armed with slingshots, an unbelievably cheap weapon because it did not require ammunition supplies, this being replenished on the ground, stones being found everywhere, especially in the mountains that were to be passed (Mills 2008, 18).

The cavalry was provided by the most qualified for this weapon, namely the Numidians, who later made a career in the Roman army, after the integration of Numidia into roman power. (Mills, 2008, 19). The elephants, his weapon of devastating novelty for the Romans, were from Syria and Egypt, which were the most effective platforms of battle (Mills 2008, 19).

This was Hannibal’s army, made up mostly of Africans, of course from multiple nations, with multiple weapons, a combined force, lethal for those times, which had at its head the most well-trained general, who knew how to form a coalition based on hatred against the Romans. Rome did not confront a single man, Hannibal, faced a coalition, led by one man, which had numerical superiority, weapons, and technologies (elephants) and the fastest cavalry. Rome had only his infantry and a lower cavalry in many respects, the command of his troops was not a unitary one, which also led to the successive disasters of his army. We can say that Hannibal’s war was which, although he was operationally successful, politically, Hannibal lost a peace, which he never wanted.

3. Hannibal’s War Stratagems, a model in the patterns of the art of Mars

3.1. Hannibal and his War Stratagems in the pattern of Sun Tzu’s Art of War

In his war, Hannibal fully respected the laws of war described by the Chinese sage Sun Tzu, laws that are still current today. Thus Hannibal, although from another era and another civilization, fits perfectly together with his war into the philosophy of the brilliant Sun Tzu. Hannibal evaluated the war with Rome according to the five factors of the art of Mars described by the Chinese theorist of the war, namely: 1. moral influence; 2. atmospheric conditions; 3. the land; 4. the commander; 5. Doctrine (Tzu 2004, 7). Moreover, it was Hannibal who forged the fifth factor of the war, namely the doctrine. In the Chinese thinker’s explanation, the ”doctrine” was ”organization, authority, promotion of officers to the proper rank, security of supply routes, and care to meet the essential needs of the military” (Tzu 2004, 9).

Hannibal excelled at all five factors in his war with Rome, but especially at the fifth. The attraction of the allies of the Romans in his coalition ensured, on the one hand, the security of the supply routes and the back, on the other hand he made sure the expedition of the march from the mountains by co-opting the connoisseurs of those mountains, he offered everyone what he wanted, but especially he made himself respected by all and followed by all, through the ”moral influence” that was the hatred towards the Romans, a common feeling not only for the Puns, but also for the Iberians, Gauls, even for some Latin nations other than the Romans.

The Carthaginian general also took into account the atmospheric conditions always, because both when crossing the mountains, he did not travel this distance during the winter, and during his great victories at Trasimenus and Cannae he took into account the weather, the position of the sun, the wind, he did not attack with the sun in front, so as not to be blinded or with his back to the wind, lest he be disturbed by the dust.

The Carthaginian general always chose the land, with great care, both at Trasimenus and at Cannae forced the Roman army to sink into a marshy terrain that not only made it difficult for it to react, but also led it to perish.

Hannibal was the commander par excellence, possessing all the qualities described by the Chinese theorist of war, the unparalleled Sun Tzu: ”By command – authority I mean the qualities of justice, humanity, courage and severity of the general” (Tzu 2004, 9). To the qualities described by Sun Tzu, we allow ourselves to add two more: the capacity for foresight and genius, innate qualities rather than acquired. How could we equate these two native qualities of Hannibal on the battlefield? We find the answer also to the brilliant Chinese thinker, who describes how to devise a war plan, which Hannibal also did masterfully, namely he conceived all his war on ”deception”, simulated ”disorder and hit” the enemy where he wanted, avoided him on land, where the Romans were superior in training, forcing them to fight in the swamps, but mostly he attacked the Romans ”where they were not prepared” and ”acted when they did not expect it” (Tzu 2004, 10-13).

The fiercest enemy of Rome fought his war with only one objective, the victory, he never sought peace with Rome, for a remarkably simple reason, he wanted the destruction of Rome, therefore he cannot be reproached for losing the peace of his war. He was a man of war, not a man of peace. Through the objective of war pursued by the redoubtable opponent of the Romans, he fits perfectly into Sun Tzu’s theories regarding the objectives pursued by a war: ”Victory is the main objective of the war. If she is late, the weapons are chopped and morale grinds down” (Tzu 2004, 17). What Hannibal did not sense was the time of grinding the morale of the Romans, which did not go according to the theories of war. If he could be blamed for an error in his war plan and in military operations it was the lack of an additional objective, in addition to victory. He did not want the submission of Rome, he wanted the elimination of Rome, whose morale was granite, exceedingly difficult to grind.

Although he fulfilled his main objective in his war, almost personally, he obtained not a single victory, but victories in every confrontation with the Romans, thus being an ”expert”, defined by the same always current Sun Tzu: ”Impalpable and immaterial, the expert leaves no traces, mysterious as a deity, he cannot be heard. Thus, the enemy is at his will” (Tzu 2004, 41). The Romans were as a nation, not just as the military force, at the will of Hannibal, who even knocks them at the gates of the city.

War, in the ancient world, was a matter of utmost importance, therefore there were social categories that had as their duty this phenomenon. Hannibal has long prepared this Punic war, which is why he turns it into a personal war. Since childhood little Hannibal (whose name is composed with the name of the god Bal, the Phoenician god of Heaven, it seems that the general’s name translates as ”grace to Bal”) planned to fight the Romans, especially since the first Punic war was underway, then followed a period of peace, in fact a truce desired on both sides. It was during this time that Hannibal mentally prepared his war by acting exactly according to the theory of the Chinese sage: ”When there is peace in the world, a man of good keeps his sword by his side” (Tzu 2004, 58). Hannibal not only held the sword by his side, sharpened this sword and gathered other swords with him, he trained day by day, until the war for him became an automatism, a reflex, which ensured his rapidity, and Sun Tzu described that ”rapidity is the very essence of war” (Tzu 2004, 78).

So, according to Sun Tzu’s war theory, the second Punic war is truly Hannibal’s war. We can say that in this Chinese “art of war”, Hannibal, the grace of the Carthaginian Sky, fits best, almost fully respecting the art of Sun Tzu, as after a textbook.

3.2. Hannibal and his War Stratagems in the pattern of the Art of War of Niccolo Machiavelli

The brilliant strategist of the Puns also successfully fits into the theories of the art of war by one of the most famous ideologues of the Renaissance, Niccolo Machiavelli. Like any Renaissance scholar, in addition to theories about the state, state leadership, politics in particular, Machiavelli also theorized *The Art* of War, in which he makes observations, analyses, and provides models for how to wage war. Hannibal also fits into this philosophy, being very versatile, which proves once again his talent in the art of Mars, always current, both in antiquity and in the Renaissance, then also in the period of Modernity, as we will see.

Thus, Hannibal wages his war, on his own with the Romans, he represents the power of Carthage, the state, and his government, falling within the main idea of the talented Renaissance scholar: ”War must be only the business of governments.” (Machiavelli 1999, 9). Fair, because Hannibal was able to wage his war with the Romans in the name of Carthage, as he was the representative of the government. Also, as a political and military leader, Hannibal demonstrated his extraordinary worth through war, if he had not been the Carthaginian commander in military confrontations, he would have been mentioned marginally in some commercial acts, as a representative of the Carthaginian power, which ruled the Mediterranean Sea and trade there. The war brought him world notoriety and immortality, he remains today through his strategies an example. Machiavelli described in his *Art* about war on this issue: ”War makes values, and peace makes them disappear” (Machiavelli 1999, 11). Basically, if it wasn’t for the war, Hannibal wouldn’t have gone down in history.

The weapon skill highlighted his native talent in the art of Mars, a skill that he acquired as a child, animated by a fierce hatred of the Romans, thus coming to make art from this skill: ”... the appropriation of the art of war, as an exercise, an object of study in the time of peace...” (Machiavelli 1999, 13).

Hannibal was worthy of his name, being a true god on the battlefield, having an extraordinary ability in the field of war because he proved that he can ”fight the enemy that he sees, or that he implies” (Machiavelli 1999, 51). He always acted in this way in confrontations with the Romans, which is why he did not even force the gates of Rome, because he assumed that the despair of the Romans could turn the result. He took all the necessary precautions, not knowing what awaited him on italic land, so that he ”would not rely on luck” (Machiavelli 1999, 99).

In the theatre of operations Hannibal took into account all the elements, even those related to the sun and wind, which may seem insignificant details on the battlefield, but they can disturb a belligerent army, just as Machiavelli advised: ”... when you have your army,... think about it… that the sun or the wind will not blow in your face, for they will disturb your visibility by rays and by the dust that will lift it up in front of you. In fact, the wind reduces the effect of weapons acting at a distance” (Machiavelli 1999, 101). The weapons that struck at a distance were in Hannibal’s time the bows, extremely necessary for him to force them through the rain of arrows to force them to sink into the Lakes Trasimenus and Cannae.

Hannibal, as we have stated in the studies of the undersigned quoted above, caused what is called terror within Roman society, not just among the Roman weapon, thus respecting Machiavelli’s indication in his art of war: ”If during the fight you want to cause disturbances in the enemy’s army, you must suggest an event that will terrify him” (Machiavelli 1999, 105). Hannibal not only suggested the terror, but applied it, because he ”terrified” Rome through the successive massacres of Trasimenus and Cannae, but also with the march on Rome, reaching the gates of the city without encountering any resistance. It is not wrong when it is considered that Hannibal applied to the Romans what is now called psychological operations.

The Roman army was a very well-established one, especially in terms of organization, so Hannibal attacked it ”indefensible”, as the Italian Renaissance scholar suggested that it should be done with an orderly army. By using elephants in combat, Hannibal perfectly calculated that it would also have the effect of surprise and would cause a shock to the Roman army, which had never before faced such combat platforms. And in this respect the brilliant Carthaginian man of arms fits into Machiavelli’s theories: ”New and unforeseen things terrify an army” (Machiavelli 1999, 182).

Incidentally, Hannibal was not only a general who knew the psychology of the military, but he was also a good manager in finding the means, using goods, and financing his army, made up in the largest proportion of mercenaries, thus respecting what Machiavelli considered to be the energy of war: ”Soldiers, weapons, money, bread: here is the vigour of war” (Machiavelli 1999, 183). Hannibal had it all in his confrontation with the Romans.

We see once again how universally valid Hannibal’s methods were in his ”war” with Rome because they are pretty much in any war textbook, whether they are from antiquity, the Renaissance, or the modern era.

3.3. Hannibal and his War Stratagems in the pattern of the war theory of Carl von Clausewitz

The talented Pun general also fits into the famous military art written by Carl von Clausewitz. Hannibal through his war continued the political rivalry between Carthage and Rome, just as the well-known modern theorist described in the art of Mars: ”War is but a continuation of politics by other means” (Clausewitz 2014, 18). Basically, Hannibal continued the Punic policy, which he also coordinated, with violent means. His war has always had a ”political purpose, as the original reason for the war” (Clausewitz 2014, 13). This goal was the elimination of Rome as a competing power with that represented by him. His war had no personal purpose, but was the purpose of his state, which did not want any threat in the Mediterranean Sea, and Rome was a threat that was growing, slowly but surely.

Hannibal’s tactical plan had its purpose, theorized by Carl von Clausewitz as: ”The armed force (of the enemy – our words) it must be destroyed”, but also ”the country and the will of the enemy” (Clausewitz 2014, 19). His war was a total one, that’s why he had ”methodism,” (Clausewitz 2014, 55) along with passion or ”hostile feeling” (Clausewitz 2014, 77).

The main engine of the second Roman-Punic war was its commander, namely Hannibal he is being the ”talent of the high commander” (Clausewitz 2014, 77), we allow ourselves to complete Clausewitz in terms of the adjective, Hannibal was the titanic commander not only of the conflict he led, but of the whole history, being among the first in the gallery of illustrious generals of all time.

The model strategist had everything in his war, however everything Clausewitz thought he should have: ”boldness” (Clausewitz 2014, 80), for two mountain ranges passed, an action considered impossible up to him; he held the ”means of superiority” (Clausewitz 2014, 85), because from beginning to end he was at an advantage, never in retreat; he also practiced the ”economy of forces” (Clausewitz 2014, 93), because both at Trasimenus, as well as at Cannae, he had minimal casualties in his troops compared to the Roman army which was crushed and left without the echelon of officer ship.

Conclusions

These are the theories of war in which I framed Hannibal with his war and stratagems because I wanted to prove that *bellum Punicum secundum* has the fatherhood of the titanic commander of armies, but also that it fits into the most famous textbooks on the art of Mars. It took a selection of the war arts by the undersigned precisely for the economics of our study. I selected war arts from different civilizations and different periods to demonstrate Hannibal’s genius.

Hannibal was more than a general, more than a ruler of Carthage, he was for the entire world a veritable ”jewel”, because as masterfully defines Sun Tzu: ”The general ... it does not pursue his personal glory... but it has only one goal, to protect... it is a precious jewel to the state” (Tzu 2004, 72). He was for Rome, not only the most fierce and capable opponent, but he was also the best teacher, perhaps the most brilliant in *ars belli*. From the confrontations with him, the Roman army and all Roman society hardened its morale, tenacity, and willpower. The Roman army learned its lessons through the supreme sacrifice from the disasters in which Hannibal plunged it, taking over many of its tactics, but especially the attack on the flanks and the use of psychological operations on the opponent.

Not only by chance, but Hannibal is also always up to date, being described by many arts of war, the teacher of all the military, of all times, proves each time that he is a totally special warrior, the one who honour’s his name, being like the god, especially that of war.

BIBLIOGRAPHY

Bagnall, Nigel. 2018. *The Punic Wars. 264-146 BC.* Translated by Teodora Nicolau. Bucharest: Litera Publishing House.

Clausewitz, Carl von. 2014. *About the war.* Notes and scientific text checking by general major dr. Corneliu Soare. Bucharest: Antet XX Press Publishing House.

Machiavelli, Niccolo. 1999. *The art of war.* Translated by Alexandru I. Constantin. Oradea: Antet Publishing House.

Mills, Clifford W. 2008. *Ancient World Leaders. Hannibal.* New York: Chelsea House Publishers.

Strechie, Mădălina. 2015. “The Punic Wars: a “clash of civilizations” in Antiquity”.” *The 21st International Conference The Knowledge-Based Organization, Conference Proceedings 2, Economic, Social and Administrative approaches to The Knowledge-Based Organization.* Sibiu: “Nicolae Bălcescu” Land Forces Academy Publishing House. ISSN 1843-6722.

—. 2016. “Hannibal, model strategist.” *Acta Centri Lucusiensis* (Lucus DacoRomanistic Studies Center in Timisoara) ISSN: 2343-8266, ISSN-L: 2343-8266 (Nr. 4 B). www.laurlucus.ro/acta-centri-lucusiensis/acl-nr-4b2016.

—. 2019. “Forms of Terrorism in Ancient Rome.” *The 25th International Conference THE KNOWLEDGE - BASED ORGANIZATION, Conference Proceedings 2, Economic, Social and Administrative Approaches to the Knowledge – Based Organization.* Sibiu: “Nicolae Bălcescu” Land Forces Academy Publishing House. ISBN 978-973-153-355-1, ISSN 1843-682X.

—. 2020. “The emotion at Rome in front of Hannibal described by Livy.” *The Dialogue of Multicultural Discourse. History, Political Sciences, International Relations.* Târgu-Mureș: Arhipelag XXI Press Publishing House. ISBN 978-606-93590-3-7.

—. Tzu, Sun. 2004. *The art of war.* Translated by Raluca Pârvu. Samizdat Publishing House.

ISSN (online) 2284-9378
ISSN (print) 2284-936X
L 2284-936X

The publication consists of 92 pages.

”CAROL I” NATIONAL DEFENCE UNIVERSITY PUBLISHING HOUSE
Panduri Street, no. 68-72, Bucharest, 5th District
e-mail: *buletinul@unap.ro*
Phone: +4021 319.48.80/0365; 0453

26/16.01.2023 C.4/2023