DOI: 10.53477/2971-8813-22-44

# CyberNSOF – A CRUCIAL FORCE MULTIPLIER IN MODERN WARFARE

**Dan-Marian UNGUREANU**
Master's Degree Student, Naval Forces Department, The Command and Staff Faculty,
"Carol I" National Defence University, Bucharest, Romania
*dan.ungureanu@marina-constanta.ro*

**Alexandru-Lucian CUCINSCHI**
Advanced instructor, Ph.D. Student, Naval Forces Department, The Command and Staff Faculty,
"Carol I" National Defence University, Bucharest, Romania
*cucinschi.alexandru@gmail.com*

***Abstract:*** *Cyber security and special operations (CyberSOF) in the 21st century are constantly evolving and changing to meet today's threats. CyberSOF are constantly evolving as allied countries, strategic partners and key players in the Black Sea discover new tactics to achieve strategic objectives. So far, the one that has remained below the threshold of armed conflict by operating in the grey zone is the Russian Federation. The annexation of Crimea by the Russian Federation is the first strong indicator that CyberSOF binomial operations have been executed. The Romanian Naval Special Operations Forces community is still developing specific guidelines or responses to deter or prevent a major cyber attack on Romania and its NATO partners. This research addresses an aspect of special operations and cyber community that has yet to be explained adequately. To achieve this goal, we will describe how the symbiotic relationship between Naval Special Operations Forces and Cyber Defense Command is crucial within the national military instrument of power at the strategic level and the impact of this binomial on the operational and tactical levels of hybrid conflict can be treated as both a force multiplier and force protection generator for Naval Forces and beyond. According to the specified causes to achieve our objectives, we will present the concept of Cyber Operations and Naval Forces for Special Operations (CyberNSOF), a novel concept that can produce strategic-level effects with minimal forces. Although the two entities presented above are services in the Romanian Military, used as a binomial (CyberNSOF) in support of the supported element, will be able to be used both as force multiplier, force protection element and last but not least as forces executing pre-emptive actions to deter the enemy. Taking these recommendations into account will increase the effectiveness of SOF maritime operations with the support of cyber operations while ensuring the transition to a robust/ real joint capability in response to any emerging existing threats.*

***Keywords:*** *Multi-Domain Operations; Naval Forces for Special Operations; Cyber Operations; CyberNSOF.*

## Introduction

Interconnection through information technology networks has supported development and is generating huge benefits for society. At the same time, the vulnerabilities inherent in accelerated development and the opportunity to easily exploit social outcomes, achievements and welfare are turning cyberspace into a battleground. From simple material interests to economic, social, governmental, geopolitical, geostrategic or military interests, each of the listed components can be addressed through data networks and information technology infrastructure.

On the military side, cyberspace was recognized in 2016 as an operational domain by NATO in response to previous actions by military adversaries, so cybersecurity and cyber defense have gained a privileged status within the capabilities with priority for development and deployment. Naval Special Operations Forces (NSOF), with a high degree of operational flexibility, advanced technology, long-tested and proven mission methodologies and elite trained personnel, traditionally represent a component that generates effects corresponding to conventional actions, but with a fraction of the resources associated with conventional military actions.

In view of the continuing degradation of the security situation in the Black Sea Region area generated by the actions of the Russian Federation as well as observations on the combined use of cyberspace actions and Special Operations Forces to achieve objectives, we assessed that scientific research on the CYBER-NSOF operational binomial is relevant to national, European and allied security interests in the Black Sea region. Cyber operations are constantly evolving as allied countries, strategic partners and key players in the Black Sea discover new tactics to achieve strategic objectives.

The Naval Special Operations Forces Community is still developing guidelines or specific responses to deter or prevent a possible major cyber attack on Romania and its NATO and EU partners in the Black Sea region.

In this paper we will highlight that the symbiotic relationship between the Naval Special Operations Forces and the Cyber Defense Forces, i.e. the Cyber Defense Command, is crucial within the national military instrument of power at the strategic level, and the impact of this cooperation on the operational and tactical levels of hybrid conflict can be treated both as a force multiplier and force protection generator for the Naval Forces

Thus, we set out to present the concept of CyberNSOF that integrates or creates a fusion between Cyber Operations and Naval Special Operations Forces missions, a novel concept that can produce strategic-level effects with minimal resources.

Although the two types of entities presented above are part of the force structure in the Romanian Army, and their use as a CyberNSOF binomial in support of the Naval Forces can be both as a force multiplier (both to create a decisive condition and to generate effects at low cost) or as a force protection element, and as forces executing pre-emptive actions to deter the enemy.

Lastly, we will analyze and present the CyberNSOF concept as a perspective on new ways of approaching conflicts, as a solution that can contribute to the achievement of Romania's security interests.

*Cyberspace – concepts, notions and organizational entities*

Cyberspace is part of that information environment in which the armed forces conduct their assets and it can be divided into five domains: maritime, land, air, space and cyber. According to Romania's Cyber Security Strategy (Romanian Ministry of Defense, 2022), the cyber domain encompasses all forms of 'digital warfare'. Similar to the other four domains, the cyber domain has specific characteristics that help determine how a means of power might be used.

NATO member states' concerns about the impact of actions in cyberspace on cyber infrastructure were expressed at the 2008 NATO Summit, which adopted the first version of NATO's Policy on Cyber Defense.

In regard to the theme of cyber attack, paragraphs 72 and 73 of the Declaration of Heads of State and Government issued following the September 2014 meeting of the North Atlantic Council in Wales are relevant in terms of recognizing that cyber attacks can generate effects comparable to traditional attacks, in terms of destruction and the North Atlantic Alliance's response, and in terms of taking military action in cyberspace. (NATO, 2018)

In 2015 a series of studies (DeWeese, 2015) approached the necessity of using the cyber domain capabilities in support of the extended concept of self-defense such as preemptive and anticipatory self-defense due to the fact that the imminence of cyber threats should be taken into consideration in the same manner as the conventional threats.

Subsequently, in the Declaration of Heads of States and Governments, corresponding to the July 2016 meeting of the North Atlantic Council, held in Warsaw, in paragraphs 70 and 71, the following issues were expressed, with relevance to the present work, in addition to the previous declaration, on actions in cyberspace, as follows:

- NATO member states recognize cyberspace as an operational domain similar to air, sea or land in which NATO must protect itself appropriately;

● NATO supports the development of international norms, with voluntary compliance, for responsible behaviour by states and further development of confidence-building measures between states in cyberspace;

In 2018, NATO member states agreed to establish a Cyber Operation Centre (CyOC) within Supreme Headquarters Allied Powers Europe (SHAPE) to coordinate operational activity in cyberspace. Accordingly, at the national level, Law 167/2017 amended and supplemented Law 346/2006 on the organization of the Ministry of National Defense (MoND) to include provisions on cyber defense forces. Subsequently, on 01 December 2018, the Cyber Defense Command was established, as a structure dedicated to ensuring the cyber security of military information technology infrastructure as well as to provide with cyber defense.

The term hybrid warfare attempts to capture the complexity of 21st-century warfare, which involves a multiplicity of actors, blurs the traditional distinctions between types of armed conflict, and even between war and peace. Although hybrid warfare is a Western term, not Russian, all sorts of hostile Russian activities – from the covert use of special forces to election manipulation and economic coercion. (Whiter, 2020)

These threats are multi-domain (land, sea, air, space and cyberspace) and often interdisciplinary. They are likely to be with us for the long term, and defeating them will require a comprehensive multi-level approach. While the United States and its allies and partner nations have already taken steps to protect themselves and confront such complex challenges, there is still a great need to more effectively enable responses, increase deterrence and raise awareness, understanding and resilience.

Cyberspace, although mentioned in official documents and public statements, has relatively few institutionally assumed definitions.

NATO's Joint Doctrine Allied for Cyberspace Operations AJP -3.20, which was promulgated in January 2020, defines cyberspace as a global domain consisting of electronic systems, information technology equipment and interconnected communications systems, networks and the data processed, stored and transmitted by or through them.

Thus, given the common elements of the definition of cyberspace, it can be identified that the element of territoriality, which contributes to establishing jurisdiction or liability for actions and effects arising from operations in cyberspace, is difficult to clarify or apply in the virtual environment. It is also necessary to note the differences between the concepts of cyber security and cyber defence, and to establish the meaning and scope of the concepts most associated with them, namely cyber incident and cyber attack.

Cybersecurity can be defined as the totality of activities, means and measures to protect networks and information systems and information stored, processed or transmitted in order to ensure confidentiality, integrity, availability, authenticity and non-repudiation, and a cyber incident can be interpreted as any cyber event occurring in cyberspace that is likely to affect cybersecurity. Cyber defense, on the other hand, consists of the totality of activities, means and measures used to counter threats from cyberspace and mitigate their effects on communications and information technology systems, weapons systems and networks and information systems supporting military defense capabilities.

Thus, on the one hand, related to cyber attacks, attention is focused on the violent nature and the level of damage, which can be both in cyberspace and in material terms (destruction, damage, etc.), and on the other hand, for use in the field of cyber security, it is important that the cyber security to be affected, an aspect that can be better included in the concept of cyber incident.

*Naval forces for special operations (NSOF)*

*- contexts involving the use/exploitation of a cyber component -*

We have identified the beginnings of the Romanian NSOF in the first structure of the 39th Diving Centre (similar to a division); a Deep-Sea Diving Group (two diving vessels) and a

Combat Diving Group (with two fast intervention boats and inflatable boats) were foreseen. (39 Diving Center, 2022)

The diversification of the missions and the possibilities of action of the 39th Divers Centre, both in the military and civil (economic) fields, required a resizing of this large unit on a structure appropriate to its status within the Navy, starting on 30 October 1986. Since 2003, the structure of the combat diving groups has been changing, and important changes have taken place at their level, both in view of the commitments undertaken by Romania to join NATO and the need to resize and transform the Romanian Army. Also in 2003, the Special Operations Battalion "Vulturii" is established in Targul Mures, which is operationally subordinated to the Special Operations Component of the General Staff of Defense (ROUSOCOM). Nowadays, the Romanian NSOF also called 164$^{th}$ Squadron is also subordinated to ROUSOCOM.

The intrinsic particularity of NSOF is that they perform missions in and from the maritime area. They can move, usually undercover, hard to detect, underwater, over water, and through the air to and from their targets, to accomplish their objective. In Romania, the Special Operations Forces have three main tasks that define the main missions of the Special Operations Forces: military assistance (MA), special reconnaissance (SR) and direct action (DA) - these mission sets are common to all NATO member states SOF forces. The afore mentioned three main missions, or derivatives thereof, although initially executed in the physical landscape have implications and ramifications in the cyber, maritime, air, land, space environments as well as the development of other types of SOF secondary operations. Thus, we will highlight how cyber operations support each primary mission and its derivatives and highlight the effects produced.

MA is a broad category of measures and activities that support and influence partner entities through training, advice, mentoring or combined operations. According to AJP-3.5 ALLIED JOINT DOCTRINE FOR SPECIAL OPERATIONS: MA is a broad category of measures and activities that support and influence critical friendly assets through organizing training, advising, mentoring, or the conduct of combined operations. The range of MA includes, but is not limited to: capability building of friendly security forces, engagement with local, regional, and national leadership or organizations, and civic actions supporting and influencing the local population (NATO, 2019). The core mission of the Romanian SOF in the Afghanistan theatre of operations was MA.

If during the execution of mentoring mission of a force that operators have to prepare, train and raise its combat capability we would have a cyber capability that identifies vulnerabilities of the mentored force *(identifying vulnerabilities, checking trusted sources and information technologies infrastructures)*, the training process of these forces would go much easier. Thus, the human resources allocated to these validations and scans could be useful in other actions.

In the matter of special reconnaissance, cyber capabilities have multi-functional uses and can be employed in support of the friendly forces. It is important to highlight the similarities between the world of intelligence, surveillance and SR. Threat assessments should, wherever possible, be based on accurate and timely intelligence. Cyber-centric and traditional intelligence SR domains both involve hacking or breaking into the logic/human logic of a network state and will most likely use the same methods and technology to do so. SR also provides the option to observe a target and interpret the behavior of the population and opposing forces over a long period of time. With regard to DA and the cyber domain, Colonel Duggan, a cyber warfare scholar in general, believes that the basic philosophy underpinning all cyber special operations is the idea of promoting asymmetry of cyber technology to reinforce the rudimentary characteristics of DA mission. (Duggan, 2016) Although the process of killing or wounding an enemy combatant will almost always require the use of kinetic weapons, in the near future, an attacker may be able to use the cyber domain for DA attacks. Using a malware that can cause a computer's battery to explode or, quite possibly, attack a vulnerable system such as a surveillance control or a

navigation system may prove that cyber operators in combination with NSOF operators will become a force multiplier in obtaining the mission success.

## Predicting the Next Fight

In circumstances of the tactical and strategic value of a Cyber attack, what is even more important for Romania is to address the fundamental question: how does Romania develop a tactical-level cyber special operations capability with strategic impact? Have there been any initiatives in Romania to combine the two categories of force to achieve multi-pronged effects? From the research we have done the answer is NO.

In order to integrate an answer to the above questions, I propose to start from the question: how can cyber capabilities enhance NSOF missions to counter the hybrid threats that the Romanian Navy/Army faces today?

To begin with, we identify many similarities between special operations and cyber operations. A one of the first similarities is that the two capabilities operate in the grey zone (Moon, 2018). Madeleine Moon continues to define this grey zone as: Expanding our understanding of security is hampered by the fact that the main threats to NATO today operate in what academics and, increasingly, policymakers, call the Grey Zone. The Grey Zone is where state and non-state actors use threats, coercion, co-optation, espionage, sabotage, political and economic pressure, propaganda, cyber tools, clandestine techniques, denial, the threat of force, and the use of force to advance their political and military agenda. Cyberspace is influencing the future of the military and will especially affect NSOF's unconventional actions, as both force multipliers are similar. The difference between soldiers using real weapons and hackers pulling the trigger online is increasingly diffuse. For example, automated algorithms designed to engage in combat without direct human intervention or oversight would be a perfect tool for a hacker to turn an armed force against itself. Hacking an enemy to attack another enemy without the instigator even entering the physical war zone - all while claiming plausible deniability - is now a potential threat. The physical role that NSOF plays in hybrid warfare will necessarily evolve as future hybrid warfare is largely conducted online.

When it comes to recovering or protecting ships, naval special operations have a very wide variety of missions such as VBSS (Visit Board Search and Seizure), Opposed Boarding (uncooperative boarding) and other specific direct actions. In the execution of the VBSS mission, a very important step is the exploitation of the information provided by the N2 compartment to clearly establish the position of the enemy on board the crew and not least the capabilities they have. Using cyber capabilities, we could easily determine the above and thus streamline the intelligence gathering process. At the same time using cyber capabilities we can access navigation systems and stop the ship thus facilitating the boarding of the ship by NSOF operators.

One of the most important missions of the naval special operations forces is the defense of critical infrastructure and key objectives along the coast and in Romania's exclusive economic zone. One of the most important major targets of current importance and interest are the maritime oil platforms located approximately 60 miles off the Black Sea coast. The complexity and geographical position make the oil platforms the most difficult targets to defend. For example, in planning a direct action on an oil platform, the type of ammunition must be taken into account *(*in order not to cause irreparable damage, as oil platforms operate with high-pressure pipes for gas extraction*)*, the platform of insertion of the operators *(*air, sea or by diving*)*, the desired effect (hostage release, raid, etc.*)* as well as other variables specific to special operations. Cyber capabilities play a crucial role in the recovery or protection of ships and maritime oil installations. While a wide range of missions can be executed on ships, the options are limited on oil rigs. Therefore, using cyber capabilities we can multiply the effort to gain advantage or relative superiority cited for a given period of time so that operators can gain that decisive advantage for

mission success. For example, in a hostage rescue operation aboard an oil rig cyber capabilities through hacking can access the civilian servers of oil rigs, access civilian phones, radio stations and provide vital information about the presence and location of the enemy, the location of hostages and last but not least triangulate the signal of radio stations used by the attackers to predict or establish a pattern of behavior that the attackers use. This information can be vital to NSOF operators in achieving success.

Romania actively participates in Operation Sea Guardian with a frigate ready to execute counter-piracy operations and maintain maritime security in its area of responsibility every year. (NATO, 2021) On board the frigate there is a naval task force ready to execute the full spectrum of special maritime operations, reporting directly to the ship's commander. If a Cyber team were deployed with the detachment, the effects described above could be achieved with the help of this team and the success of the mission would be exponentially increased.

## Conclusions

The experience that Romanian NSOF gathered in the past decade working with multiple entities provides a strong culture in executing maritime operations unilateral or combined. Using the cyber capabilities in order to support the missions of NFOS and to enhance the outcome of any task that are in their area of expertise is a way of improving the operational perspective.

The real challenge in the endeavor of creating a CyberNSOF capability will be to find the right balance between the competencies and know-how that are to be transferred from cyber operators to FNOS and vice versa in order to achieve the best niche force capability.

On the other hand, an integrated approach of a Cyber and NSOF missions and ways of solving operational task will provide the military decisions makers with some innovative solutions by a fraction of costs and risks of any other kind of military forces assigned on similar missions.

Creating a CyberNSOF capability will be a force multiplier for the future battlefields and the task of building such a force will depend on the fight spirit of SOF and cyber operators, their top of the spear professional knowledges and abilities and the vision of the commanders of those military components as well as their willingness to win the next war.

## Bibliography


39 Diving Center. (2022, May), *Centrul 39 Scafandri*. http://www.centruldescafandri.ro/scurt-istoric/ accessed on 22.05.2022.

Romanian National Ministry of Defense. (2022). *Cyber Security Strategy*. Bucharest.

NATO. (2019). *AJP-3.5 Allied Joint Doctrine for Special Operations.*

Whiter, J. K. (2020, January). Defining cyber warfare. *Journal of European Security Defense Issues 10*, pp. 7-9.

DeWeese, G.S, *Anticipatory and Preemtive Self-Defense in Cyberspace: The Challenge of Imminence,* 7th International Conference on Cyber Conflict: Architectures in Cyberspace, NATO CCD COE, 2015.

NATO, (2018, August). Wales Summit Declaration, paragraphs 72-73.

Duggan, P (2016, April), Man, Computer, and Special Warfare, https://smallwarsjournal.com/jrnl/art/man-computer-and-special-warfare accessed on 22.05.2022.

Moon, M (2018, April), *Rapporteur Sub-Committee on Future Security and Defence Capabilities* – NATO Special Operations Forces in the Modern Security Environment, www.nato-pa.int, accessed on 15.04.2022.

NATO, (2021, September), *NATO OPERATION SEA GUARDIAN FOCUSED PATROLS RETURN TO SEA,* https://mc.nato.int/media-centre/news/2021/nato-operation-sea-guardian-focused-patrols-return-to-sea accessed on 22.04.2022.

# SECTION III

## Defense And Security Studies