THE INFLUENCE OF HYBRID ATTACKS ON A STATE IN AN ALLIED CONTEXT

Claudiu-Florin NISTOR

Land Forces Staff, Bucharest, Romania

The interdependence of states on each other is now increasingly visible, mainly from an economic perspective, due to the opening up of markets along with the phenomenon of globalisation. This relationship becomes more pronounced and visible in an allied or union context, where more relaxed trade policies between states also facilitate the negative effects of hybrid attacks on a member state or neighbour. The influence of such attacks, even if their main purpose is closely related to weakening the combat capacity of the adversary state and facilitating its own military advance, is felt over a wide regional area, undergoing a transformation from an attack with a military objective to an attack with an economic effect. A specific example of this is the hybrid attacks that have been enhanced by the Russian Federation's maritime supremacy in the Black Sea area bordering Ukraine, as a result of which maritime grain exports have been halted, with global effects that have required a joint effort by the main world players to avoid a possible crisis. This article analyses the immediate and medium-term effects of such hybrid attacks, especially those on the European continent, contrasting the two international entities, the European Union and the North Atlantic Treaty Organisation.

Key words: *hybrid attack, Euro-Atlantic area, national interdependence, alliance.*

1. INTRODUCTION

In an international community formed of states that are part of unions, alliances or states between which there is no formal form of connection, problems in one of them (caused by hybrid attacks) can have effects on another, often affecting economic relations. This gives substance to the hypothesis that in the 21st century, given the phenomenon of globalization and the dependence of economic markets on the world, the proper functioning of a state is closely related to the situation of the countries with which it has economic relations. Such a relationship generates, on the one hand, substantial and mutually beneficial economic advantages

evidenced in economic growth, but it also has negative effects since if a state suffers from internal problems or hybrid actions, not only it will be affected, but also the countries with which it has economic relations[1].

Hybrid attacks on a state often also have an indirect economic effect, inevitably affecting countries with relations with the target state. In a union context (e.g. the European Union), economic activities between states take place much faster than between two states with conventional borders, as the Schengen area allows goods and citizens to transit across borders much more easily, reducing bureaucracy and the usual controls [2].

In such an easy area for commercial traffic, the effects of hybrid attacks are ultimately felt by most states of the union, possibly also by those with which it borders. One consequence, caused by Russia's supremacy in the Black Sea region, is the embargo on Ukrainian shipping, thus compounding the economic problems created by the ongoing war [3].

2. THE DIMENSION OF A HYBRID WAR IN THE EURO-ATLANTIC AREA

In order to determine the size of a hybrid war in an allied context, it can be analyzed militarily from the perspective of the North Atlantic Alliance and socio-economically from the perspective of the European Union. In terms of the hybrid component, such a war (in the Alliance concept) involves both state and non-state actors, and its objectives are aimed at both political institutions, the collective mindset of the civilian population and the destabilisation of global security. To achieve these objectives, the main avenues of attack are propaganda, cyber attacks, disinformation and other unconventional tactics. Today's technology facilitates the propagation of the effects of these hostile actions, in terms of speed and intensity, due to the increased interconnectedness of the member states of an alliance or union, mainly caused by the phenomenon of globalisation. [4]

In order to build a basis for combating such hybrid actions, a state needs a sufficiently developed resilience capacity. From a national perspective, Romania has recognised this by including resilience capacity in the first chapter of the "National Defence Strategy for 2020-2024". [5]

Until 2015, from the point of view of the allied military context, the North Atlantic Alliance's official positions included a series of strategic objectives aimed at the security of the entire organisation in terms of protection against the effects of hybrid attacks. However, action on updating policies to prevent and combat hybrid threats has been delayed for the following reasons: [6]

1. Internally, the Alliance has developed a decision-making

process that cannot always be translated into concrete military action or any other instruments of action until hybrid action had an effect on the organisation or its member states;

2. Externally, the potential hybrid threats identified over time have tended to come from the same sphere of influence (predominantly from the Russian Federation, China, Pakistan, etc.), especially since the end of the Cold War;

3. Theoretically, the concepts of hybrid threat or attack require a more determined and concrete approach in line with Alliance policies. At the same time, this presents a number of implementation difficulties, given the decision-making process and security culture of member states [6].

This policy on hybrid threats and actions has evolved over time, so that since 2015, the organization has developed new strategies aimed at combating them by:

1. preparing the North Atlantic Alliance and its member states;
2. deterring hybrid threats;
3. countering them from the perspective of supporting any member or ally. [4]

A first direction, as an integrated part of the new strategies, is the preparation of member states by identifying the vulnerabilities of each state, analysing and disseminating each hybrid threat in by specialists of a special section, part of the Joint Security and Intelligence Division, which has been set up within the North Atlantic Alliance in response to future hybrid threats. [4]

This structure responds to issues related to hybrid threats by combining both military and civilian instruments, thereby improving the organisation's ability to deal with such threats.

The Alliance supports Member States in identifying their vulnerabilities, increasing their resilience and provides, upon request, critical situation support in various areas such as: C.B.R.N. incidents; critical infrastructure protection; strategic communications; civil protection; cyber defence; energy security; counter-terrorism. [4]

Another area of preparedness for member states is the exercises conducted by each state to educate themselves and raise awareness of the dangers posed by hybrid threats, involving both military and civilian elements in the process.

Anticipation of hybrid threats is a basic prerequisite for dealing with the hybrid problem. It contributes to increasing the ability of own forces to avoid hybrid action and improves decision-making. [4]

The last line of action, relates to countering hybrid threats in

support of any member state or ally, with reference to the need to ensure continuity of anticipation and preparedness activities to counter their effects. In this respect, if these activities are successfully carried out, in the event of a real situation, specific Alliance forces will be able to intervene at very short notice, anywhere and at any time.

An analysis of an individual state as compared to a member of a military alliance (or union) shows that the potential for responding to hybrid threats or actions must be commensurate, and its effectiveness increases as more experienced actors are involved in the decision-making process, whereas a state isolated in this respect may be unable to react adequately to such an event.

Membership of an international community (union or alliance) offers the possibility for a state to reduce the potential negative influence of the dominant state actor in the area, otherwise its possibilities for action are reduced. Such a situation is represented by the Republic of Moldova, which does not belong to the European Union or the North Atlantic Treaty Organisation.

The negative influence of the Russian Federation on the Republic of Moldova has manifested itself especially in the economic sphere. Due to the almost exclusive dependence on the Russian market, the export of mainly raw materials and unprocessed products and the price of energy, the gross domestic product of the Republic of Moldova was among the lowest of all countries on the entire European continent [7].

3. THE EFFECTS OF HYBRID ACTIONS ON A TARGETED STATE

According to the second point of the Alliance's Strategy for responding to hybrid threats [4], anticipating future hybrid attacks is an important part of addressing this issue, providing an opportunity to take measures that will ultimately lead to deterrence. This deterrence can be achieved both by building an appropriate defence that meets current needs, but also by threatening potential retaliation by responsible actors, whether state or non-state. In this regard, the crippling of a critical infrastructure (physical or virtual) by hybrid means (cyber attacks, sabotage, etc.) should be followed by immediate countermeasures by both the European Union and the North Atlantic Alliance, and doctrines need to be updated or developed in this regard. [8]

In 2022, the effects of hybrid instruments were felt across the Euro-Atlantic area, with sabotage actions on critical infrastructure key elements of certain states, with consequences for large parts of the European continent.

Some sabotage actions even

include the use of drones to achieve their objectives. In this case, on 6 October 2022 in Denmark, authorities reported several unauthorized drone flights in the area of the North Sea gas pipelines. These types of incidents have been repeated within a short period of time in the same area, and given that the possible target for action was a major gas pipeline, part of critical infrastructure, several European countries have proceeded to increase their defence capabilities.

One such example is Norway, which sent military structures to protect offshore oil and gas installations, and France, which increased its capacity to protect sea cables below sea level, prompted by fears of a possible imminent hybrid attack from Russia [9].

At the same time, two days after this event, another incident was reported in Germany, where rail transport in the north of the country was disrupted due to sabotage. According to the authorities the probability of an accidental event is zero, as the cables essential for rail transport were deliberately cut in two separate locations. This attack has caused serious delays to rail transport and the perpetrator of this attack on critical infrastructure has not yet been identified. [10]

Another example of a concrete hybrid action took place on 18 October 2022 in the United Kingdom area of the Shetland Islands archipelago, specifically, their connection to the outside world was disrupted as telephone cables and internet connections were severed in two separate locations. Although government authorities have stated that there is a possibility of an accident, the likelihood of two such events occurring in the same area is minimal, leaving room for hybrid actions. [9]

The sabotage actions in October 2022 were felt in North-Western Europe, so that in France two days later, on 20 October in Marseille, a similar event as the previous one occurred, with fibre optic cables serving the telephone network and Internet connection being cut, with global effects affecting Asia and Europe. [11]

However, hybrid actions directed against a state are not just about sabotage. In Norway, for example, a Brazilian researcher was arrested on 25 October on suspicion of spying for the Russian Federation by the Norwegian security agency. The latter charges that the false identity of the alleged Brazilian researcher at the University of Tromsø endangers the national security interests of the Nordic state. [12]

Despite the fact that the perpetrators of the hybrid activities described above have not been officially identified, these events cannot remain at the level of random accidents, since the evidence found

proves otherwise, the geographical area is the same, the time of occurrence is very short and the means used in their occurrence are unconventional.

According to the established criteria, these events can be classified as hybrid actions, since they affect the critical infrastructure of a state, their effects are felt on the rest of the continent, affect the civilian population and jeopardise national security interests.

The figure no. 1 shows the evolution of weekly cyber attacks in different industries worldwide. These attacks are an integral part of hybrid attacks and represent only a fraction of the total, so that the total of such attacks is much larger.

In order to produce an overview of hybrid actions, including statistical data and possible forecasting, it is necessary to keep a record of them, by different areas of activity, to meet the main prevention needs of

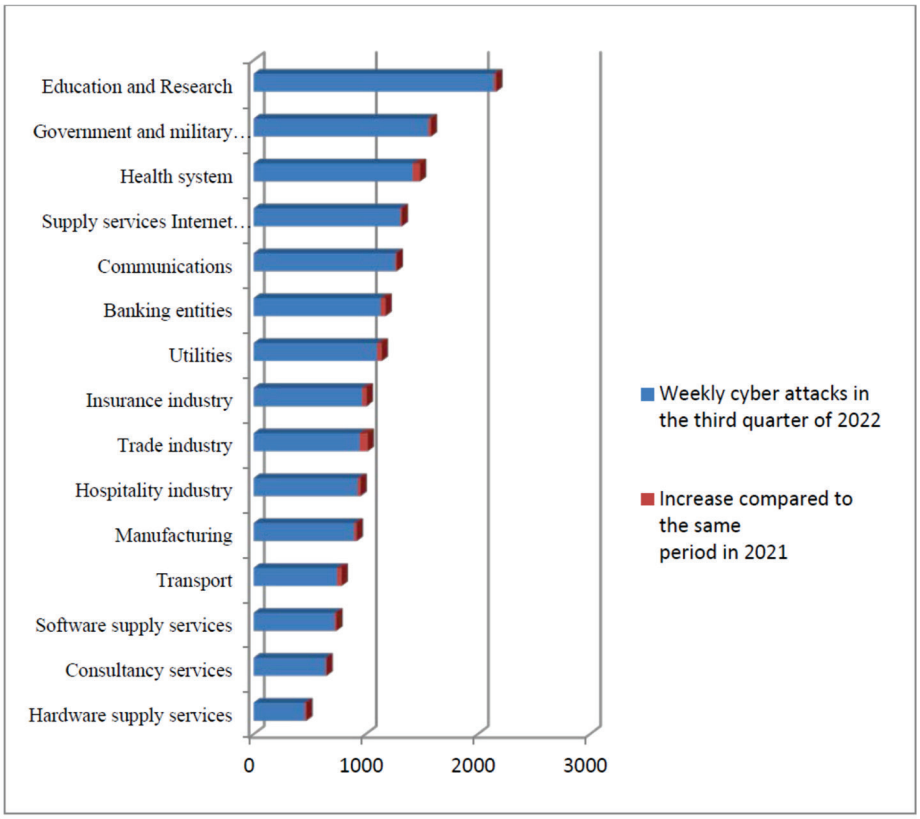

Fig. 1 The evolution of cyber actions, during one week, in the 3rd quarter of 2022, compared to the same period in 2021 [13]

the target countries, thus increasing the chances of anticipating future actions.

4. THE INFLUENCE OF HYBRID ATTACKS IN AN ALLIANCE ENVIRONMENT

In order to base an analysis on the main influences of hybrid actions at the level of an alliance or union, it must be specified that this type of actions targets national vulnerabilities, represented by political actors, military authorities, national economy, social classes, information systems and last but not least, critical infrastructure. In carrying out this type of action, a range of political, economic, civilian and informational instruments is used to achieve the proposed objectives, which go beyond the military border, so that combating this type of attack requires not only a classic military response but also the use of unconventional instruments, while using the measures available in the other sectors of activity affected. [14]

Among the most important effects of a hybrid attack is the economic one (affecting both state and private actors), for which significant funding is needed to remedy and possibly prevent in the future.

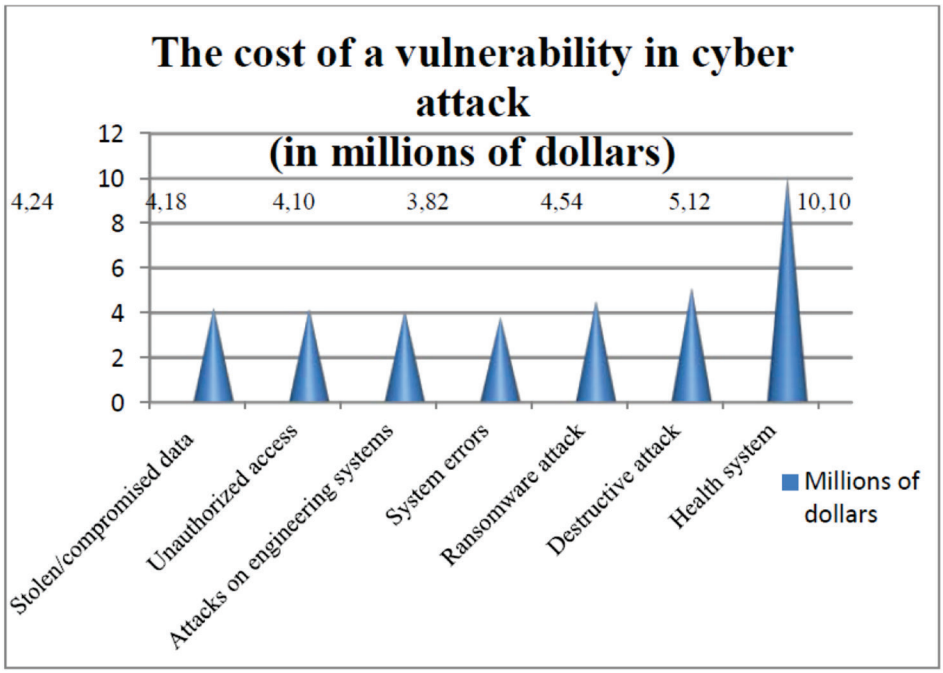

Fig. 2 The average cost of a vulnerability subject to a cyber attack [15]

Figure no. 2 shows the average cost of such a hybrid cyber action affecting either private or state-owned entities that are part of the critical infrastructure. In these cases, the target state may be economically affected, requiring measures to be taken to remedy the damage currently caused and future investments to prevent it.

Such examples, where actions targeted at one member state of an alliance have had effects on other members, are presented in the third chapter of this paper. At the same time, the complexity of actions makes it difficult for states to find a pattern of action and to develop precise methods for their prevention.

As a result of the effects of such attacks, a state's resilience capacity changes in the sense that it has to be able to adapt to possible similar scenarios in the future. In this respect, an example of measures to prevent certain cyber attacks is the increase in the protection capacity of public authorities' IT systems, which must be kept constantly updated in terms of security policies, i.e. anti-virus software must be purchased and staff must be trained to prevent such attacks.

Hybrid threats do not take into account the territorial borders of states and manifest themselves at international level, even if the initial intended target was a victim state, the final effect may be limited to other neighbouring states or even within the international community. This final effect is more visible in the context of the European Union or the North Atlantic Alliance, where due to interdependencies of an economic, social or military nature, the national vulnerability of one state can become a problem for another state actor, member of that alliance. In this respect, given that threats come in an international context, the united effort of action should be synchronised, systemic and combine national and international counter elements. [14]

5. CONCLUSIONS

In the light of the above, it can be concluded that hybrid actions against one member state of the European Union or the North Atlantic Treaty Organisation can have direct effects on other members. In the examples listed above, there is an interdependence of these states in terms of their economic relations and critical infrastructure.

In terms of visibility and reach, the result of damaging a state's critical infrastructure, which is linked to its neighbours, is an obvious topical issue, which has reached a critical stage mainly due to technological

advancement. This type of action is characterised by high efficiency, low cost, affects a large geographical area, generates high costs for restoring the infrastructure involved to operational status and usually affects several sectors of activity, both civilian and military.

At the same time, the use of cyber-attacks causes mainly material damage and the inability of certain systems to function for a certain period of time, while exfiltrating confidential data. In order to give a broader picture of the average costs of such hostile actions, Figure 2 provides some concrete data in this respect, but it should be noted that these types of actions in the information environment can be directed not only against a state, but also against private operators or even ordinary citizens, with financial benefits being the main objective.

In order to respond to these means of destabilising states, the members of the alliance or union must first of all make national efforts to resolve their own vulnerabilities, and then the main line of effort must be unity of action at international level.

At the same time, because of the complexity of the instruments used in hybrid actions and the distinct planes on which they manifest themselves, there is a need for a clear conceptual definition and measures to prevent and counter such actions, both nationally and in the allied context. The latter must not be carried out at military level alone, as it is not the only one targeted in such an attack, but requires the cohesion of several sectors of activity, from both civilian and military points of view.

ACKNOWLEDGEMENT

This article is original research and has not been published elsewhere.

REFERENCES

[1] Business Terms, *Economic Interdependence*, https://businessterms.org/economic-interdependence/;

[2] Ministry of Internal Affairs, Romania, *Spațiul Schengen,* http://www.schengen.mai.gov.ro/index04.htm;

[3] Council of European Union, *Infographic - Ukrainian grain exports explained*, https://www.consilium.europa.eu/en/infographics/ukrainian-grain-exports-explained/;

[4] North Atlantic Treaty Organization, *NATO's response to hybrid threats,* 2022, https://www.nato.int/cps/en/natohq/topics_156338.htm#:~:text=Hybrid%20threats%20combine%20military%20and,and%20use%20of%20regular%20forces.;

[5] National Defence Strategy for 2020-2024 ;

[6] Galkins, Kaspars, *NATO and Hybrid Conflict Unresolved Issues from the*

Past or Unresolvable Threats of the Present, Monterey, California. Naval Postgraduate School, 2012, https://calhoun.nps.edu/handle/10945/17369;

[7] International Monetary Fund, World Economic and Financial Surveys, *World Economic Outlook database: October 2022,* https://www.imf.org/en/Publications/WEO/weo-database/2022/October/weo-report?.

[8] Prof. Dr. Sven Biscop, *Military Offensives, Hybrid Attacks – And No Peace in Sight,* Egmont Royal Institute for International Relations, 30 september 2022, https://www.egmontinstitute.be/military-offensives-hybrid-attacks-and-no-peace-in-sight/;

[9] James Billot, *Hybrid attacks on the rise across Europe,* The Post, 26 October 2022, https://unherd.com/thepost/hybrid-attacks-on-the-rise-across-europe/;

[10] Sarah Marsh and Andreas Rinke, *"Malicious and targeted" sabotage halts rail traffic in northern Germany,* Reuters, 8 october 2022, https://www.reuters.com/world/europe/rail-northern-germany-standstill-due-technical-issue-2022-10-08/;

[11] John Leicester, *French police probe multiple cuts of major internet cables,* AP News, 21 october 2022, https://apnews.com/article/technology-europe-france-marseille-business-8b33a5634232031f#:~:text=LE%20PECQ%2C%20France%20(AP),phone%20services%20were%20severely%20disrupted.;

[12] Jon Henley and Pjotr Sauer, *Norway arrests 'Brazilian researcher' accused of spying for Russia,* The Guardian, https://www.theguardian.com/world/2022/oct/25/norway-arrests-brazilian-researcher-accused-of-spying-for-russia#:~:text=Norway%20arrests%20'Brazilian%20researcher'%20accused%20of%20spying%20for%20Russia,-This%20article%20is&text=Jos%C3%A9%20Assis%20Giammaria%2C%20the%20suspected,Giammaria%2C%20the%20suspected%20Russian%20agent.&text=Norway's%20domestic%20security%20agency%20has,of%20being%20a%20Russian%20spy.;

[13] Check Point Research: *Third quarter of 2022 reveals increase in cyberattacks and unexpected developments in global trends*, Check Point Software Technologies Ltd, https://blog.checkpoint.com/2022/10/26/third-quarter-of-2022-reveals-increase-in-cyberattacks/;

[14] Patrick J. Cullen, Erik Reichborn-Kjennerud, *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare A Multinational Capability Development Campaign project*, Norwegian Institute of International Affairs, 2017, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf;

[15] International Business Machines Corporation, *Cost of a data breach 2022 - A million-dollar race to detect and respond,* https://www.ibm.com/reports/data-breach;