INFORMATION - A WEAPON OF WAR

Tiberiu TĂNASE[*], **Camelia-Elena GOLEANU**[**]

[*]Romanian Academy (tanasetiberiu2@gmail.com)
[**]Nicolae Titulescu University, Bucharest, Romania (camelia.goleanu2024@gmail.com)

DOI: 10.19062/2247-3173.2025.26.2

Summary: *Beginning with how a top secret agency (SOE) accomplished its dangerous task during World War II of coordinating subversion and sabotage against the enemy by any means necessary - using disguise, deception, bribery, explosives (sometimes disguised as objects such as a dead rat or a bottle of chianti) guerrilla warfare - and even assassination, the research highlights the crucial role of information in national security and how information has been strategically used to influence decisions, manipulate perceptions and gain advantage in a variety of areas, from military warfare to economic and political competition.*

The research also highlights that in the context of globalization and technological advancement, information has become a key strategic resource, as important as material or human resources. The ability to control the flow of information, to disseminate correct information or misinformation and to protect one's own information has become a determining factor in the success or failure of any strategic action.

Thus, the research highlights the various forms of the use of information as a weapon such as information warfare, media warfare, cyber warfare, electronic warfare, influence operations, counterintelligence and emphasizes the importance of developing robust national information security strategies that include measures to protect, detect and respond to information threats. It also emphasizes the need for public education on information literacy and resilience to disinformation.

In conclusion, the research demonstrates that information has been and is a fundamental component of power, and understanding and strategically managing it is essential for the security and prosperity of any entity, be it state, organizational or individual. It also, in this context, emphasizes the need to train specialists capable of understanding the importance, effectively managing and properly using this ”weapon” - information.

Keywords: *information, information warfare, weapon, Vera Atkins, SOE.*

1. INTRODUCTION

With the development of automated data processing systems and, subsequently, computer networks, new forms of warfare have emerged and developed extremely rapidly, such as: sabotage with computer viruses, blocking, filtering or diverting data and information, hacking into computer systems and monitoring the information activities of adversaries and/or other partners who pose some information risk, cyber attacks. Along with manipulation and propaganda, these are part of what specialists call information warfare. The main characteristics of specific information warfare weapons are: invisibility, passivity of action, remote controllability, accessibility (they are easily available and cheaper).

In the new type of warfare, information is not just a necessity, it becomes a major element of the art of war, a formidable weapon for the one who possesses, protects, processes and manages it effectively. It can help win a conflict, military or otherwise, before hostilities visibly break out.

Knowledge has a double valence, firstly theoretical "to have knowledge", and then practical "to know how to do", meaning control over a set of information, which after the processing process gives the beneficiary the ability to act. It can thus be said that knowledge is based on information, on which the satisfaction of the individual's basic and higher needs largely depends.

The need and effort for survival have given information a defensive value, by supporting man in his relationship with his environment, in order to know, anticipate and avert dangers. Its usefulness in discovering and exploiting vital resources gave information economic value. These two values have been accentuated as the various productive activities have emerged and developed, giving information the value of a security resource.

To benefit from the advantages of knowledge, man has had to protect information, i.e. to keep it secret and to use this resource as the basis of any economic, political or military strategy. From this point of view, information has always been a formidable weapon, and today their degrees of use and accessibility have only accentuated this characteristic. The thirst for information that characterizes the modern globalized world has led to fundamental changes in the means of transmitting information, including what we call social media. An eloquent example is the social networking site Twitter, which since 2009 has changed its greeting from the neutral "how are you?" to the more precise "what's going on?".

Information as a weapon can take the form of propaganda, in which information at odds with unfolding events can be both true and false. The forms of propaganda are constantly adapting due to the changes imposed by technology, globalization and social media/virtual media.

This new reality has led Dennis Murphy and James White to assert that "The historical use of information as power was primarily limited to nation-states. Today a blogger can impact an election, an

Internet posting can recruit a terrorist, and an audiotape can incite fear in the strongest of nation-states, all with little capital investment and certainly without the baggage of bureaucratic rules, national values (truthful messaging), or oversight"[2]. Thus, through today's technology, information has become a weapon within the reach of every individual. This weapon can take various forms, from the truth of social movements, to the propaganda of terrorist organizations, all a matter of perception. But what cannot be denied is that easy access to information has opened a window to a new category of risks.

When the possession of information and its use for one's own interests means power, we can speak of an information-power binomial. In this context, information is obtained, possessed and protected by public means, but above all by specialized, secret means and practices as old as history itself, and is used to inform decisions of vital interest.

At the same time, information can only serve the needs of the community if its owners and users base their interests on social needs. Otherwise, vitally important information is diverted from its normal purpose and transformed not only into a tool for maintaining power, but also into a tool for realizing individual or group interests. Moreover, in order to be able to decide and act in accordance with his needs and interests, man needs a wealth of information which gives content and direction to his actions and gives him identity as the subject of social relations. Without this information, human freedom of expression and action is limited or distorted.

Information has acquired the quality of being a substitute for other economic resources, of circulating at high speed, conferring advantages to the possessor. Societies that have paid attention to the processing and use of information have moved rapidly towards the information society. This has also been due to the fact that information, unlike other economic resources, is extensible to the limits of human capacity and time, due to its natural power of diffusion, its ability to be reproduced in time of use, its possibility of being transmitted, and its use as exchange value in transactions.

The value, the usefulness of information and the price for obtaining it have historically turned it into a means of aggression or defense (weapon), on which the triad was built to know - i.e. to gather information; to prevent the adversary from knowing you - i.e. to carry out counter-intelligence activity; and to make the adversary wrong or misinformed - i.e. to disinform him. This triad confirms the scale and complexity of the means used to maintain priority, maintain exclusivity over information, and protect it severely by maintaining secrecy over information of vital interest to a community.

State-political practice confirms that, in the context of the explosion of information technology, these weapons cause greater damage than conventional warfare. At the same time, information or, to be more precise, intelligence is an instrument of national power, through which vital national interests are promoted and defended, first and foremost, but also other types of state interests, as is also revealed by the development of information as a weapon (military specialization). The information tool is primarily intended to provide decision-makers with the necessary support for the adoption of the best decisions. This function is attributed to institutions specialized in obtaining and protecting information. It also plays a central role in preventing one of the most serious risks to national, regional or international security - international terrorism.

The relevance of the information tool as an instrument of the state can be highlighted by examples from the history of the last century, when information power was used as a weapon of war.

2. SPECIAL OPERATION EXECUTIVE (SOE)

A brief foray into history reveals that in June 1940 Britain was driven off the continent by Hitler's conquering armies. As the British stared the invasion in the face, a group of unconventional warriors planned a new form of war. With an order from Winston Churchill to set Europe on fire, this top secret agency was given the dangerous task of coordinating subversion and sabotage against the enemy by any means necessary - using disguise, deception, bribery, explosives (sometimes disguised as objects such as a dead rat or a bottle of chianti), guerrilla warfare - and even assassination.

Created in 1940 to carry out espionage, sabotage and reconnaissance operations in the territories occupied by Nazi Germany and to support local resistance movements, SOE aimed to launch combat operations by means other than classic warfare and by relying on the power of information.

SOE was nicknamed Churchill's Secret Army and had around 13.000 members, 3.200 of whom were women. SOE operatives operated in France, Belgium, Greece, Greece, Albania, Yugoslavia, Italy, etc., as well as in East Asia and were infiltrated by parachute or submarine transport, communicating with the command center by radio hidden in suitcases.

The SOE has had a significant impact on modern intelligence agencies, influencing the methods of special operations, espionage and sabotage used today. After its disbanding in 1946, many of SOE's tactics and strategies were taken over by MI6 and other Western intelligence agencies.

Among the most important influences of the SOE on modern intelligence services are infiltration and sabotage techniques, support for resistance movements, clandestine operations (the SOE demonstrated the effectiveness of covert operations, leading to the development of specialized units such as the CIA's Special Activities Center), innovations in espionage technology.

In addition, the SOE was active in Spain during the Second World War, where it conducted economic intelligence operations against German interests.

Today, many of the principles of SOE are applied in intelligence operations, particularly in counter-terrorism and hybrid warfare.

SOE conducted many daring operations during the Second World War, making a significant impact on the Allied war effort. Among the most important missions were:

- Operation Foxley - A British plan to assassinate Adolf Hitler at his residence in Obersalzberg (Operation Foxley was based on intelligence about the German leader's daily habits). Although not implemented, it demonstrated the SOE's ability to devise operations to eliminate enemy leaders. Only a few SOE operations were undertaken in Germany, mainly due to the high dangers and lack of support from the local population. After June 6, 1944 [3], the Austrian and German sections of SOE was reorganized and enlarged. Operation Periwig, a plan to simulate the existence of a large anti-Nazi resistance movement in Germany, was carried out despite the restrictions imposed by SIS (Special Intelligence Service)[4] and SHAEF (Allied Expeditionary Forces)[5]. It was an operation of disinformation and psychological warfare mounted by the Special Operations Executive (SOE) in the last months of World War II, beginning in November 1944. The main aim was to create the illusion of a widespread anti-Nazi resistance movement inside Germany in order to induce confusion, paranoia and divert German security resources.

- Sabotage of the Norsk Hydro plant - An SOE team destroyed heavy water production facilities in Norway, preventing Nazi Germany from developing nuclear weapons. The Norsk Hydro plant in Vemork, Norway, was the target of crucial sabotage operations by Allied forces and Norwegian resistance. The plant was the only one in Europe to produce heavy water in significant quantities, an essential element the Nazis considered vital to their nuclear research program to develop atomic weapons. The Norsk Hydro sabotage is considered one of the most successful and daring sabotage operations of the Second World War.

- Support to the French Resistance - SOE provided arms, equipment and training to resistance groups, contributing to the success of the Normandy landings. SOE operations in France were run by two sections based in London. Section F was under direct British control, while Section RF was under the control of the government-in-exile of Free France led by Charles de Gaulle. Agents of French origin operated mainly in the RF Section. On May 5, 1941, Georges Bégué was the first SOE agent parachuted into Nazi-occupied France to send a radio report and to greet the next agent parachuted into France. Bégué was a qualified radio operator, a vital skill for maintaining liaison between field agents and SOE headquarters in London. Known as Georges One, he was the first SOE radio operator in France. Between May 1941 and August 1944, more than 400 agents were sent to France. Among them were weapons, sabotage instructors, couriers, escape organizers, liaison officers and radio operators.

The SOE included several women (mainly recruited for first aid). Section F sent 39 officers to France, of whom 13 fell in the line of duty. On May 6, 1991, a monument was unveiled in Valençay in the department of Indre, in memory of the 91 agents and 13 female agents of the SOE who gave their lives in the struggle for the liberation of France.

- Operations in the Balkans - SOE worked with Yugoslav and Greek partisans to destabilize Nazi forces in the region.

After the defeat of Yugoslavia by Axis forces in 1941, the country disintegrated. In Croatia there was a strong pro-fascist movement, the Ustaše, but in the rest of the country two resistance movements emerged: the monarchist Chetniks led by Draža Mihailović and the pro-communist Yugoslav partisans led by Josip Broz Tito. The SOE at first supported the Yugoslav government-in-exile and through it the ethnic ethnicists. It soon became clear, however, that the Chetniks were less effective than the communist partisans, and evidence emerged that the Chetniks had collaborated with the Germans in certain regions in the fight against the communist partisans. Although relations between the SOE and the communist partisans had its tense moments during the war, many historians believe that British support was a decisive factor in keeping communist Yugoslavia in the neutral camp during the Cold War. Notable missions include Operation Bullseye (the first SOE mission in Yugoslavia) and missions involving Fitzroy Maclean, who played a crucial role in establishing the link with Tito.

Greece was defeated by the Axis powers after the Greeks had fought fiercely for several months. At the end of 1942, SOE organized the first operation in Greece. The British commando group made contact with the two Greek guerrilla groups operating in the target area - the communist-oriented Greek People's National Liberation Army (ELAS) and the nationalist Greek Republican National League (EDES). With the help of these two organizations, the SOE commandos succeeded in partially destroying the Gorgopotamos railway viaduct on 14 November 1942. Unfortunately, relations between the two resistance groups and the British soon became strained. EDES received most of the SOE's aid, but ELAS managed to capture much military materiel when Italy signed the armistice with the Allies and the Italian army in Greece disbanded. ELAS and EDES became belligerent parties in a civil war in 1943. Several SOE liaison officers were executed during this period by undisciplined ELAS units. SOE's last action was the evacuation of several hundred unarmed EDES fighters to the island of Corfu, lest they become victims of ELAS's revenge.

The main objectives of the SOE in the Balkans were support and unification of local resistance movements, sabotage, intelligence gathering, psychological warfare, diversion of enemy forces.

- In Asia - SOE operated in Burma, Malaya and China, organizing sabotage and supporting resistance movements against Japan. In early 1941, SOE prepared an action plan for Southeast Asia. As in Europe, after the Allies suffered a series of military failures, SOE began to participate in the formation of local resistance groups in territories occupied by the Japanese Empire. Some of these resistance organizations played a major role not only during the war but also in the post-war period.
- An SOE delegation parachuted into Romania in 1943 with several objectives. The first was to penetrate the higher levels of political and military decision-making in Romania. The operation was a masterful combination of propaganda and disinformation, a mixture of truths only partially spoken, in which one can easily fall prey to the myths of espionage[6]. Although it began with the capture of its agents, it had a significant impact on the course of events in Romania during World War II. It facilitated crucial communication between the Allies and Romanian decision-makers, indirectly contributing to the August 1944 coup d'état and Romania's change of sides, an event that shortened the war by several months and had major implications for the fate of Eastern Europe.

These missions demonstrated the effectiveness of SOE in guerrilla warfare and clandestine operations, influencing modern intelligence strategies.

SOE was also tasked with encouraging and facilitating espionage and espionage behind enemy lines and to serve as the central coordinating point for the resistance movement in the British Isles (Auxiliary Units) in the event of the Axis Powers invading the United Kingdom.

The SOE set up a covert branch, the ISRB (Inter Services Research Bureau), which was responsible for creating equipment used in secret warfare and for producing radios, weapons, explosive devices and booby traps used by SOE agents or special troops.

People from a wide variety of social classes and socio-professional backgrounds fought as SOE agents in enemy-occupied territory. The main quality of the agent was a good knowledge of the country in which he was to operate and the language, all the more so in the case of agents whose mother tongue was not the language of the state in which they were to be infiltrated. Agents of mixed parentage, dual nationality or polyglots were highly sought after by the SOE. This was particularly true for France. Many of the agents of Section F were proletarians or sometimes even with a background in the underworld.

Members of the armed forces of occupied countries who had escaped from prison, been exiled or discharged became an important source of agents. In other cases, the agents were mainly loyal to the exiled guvnor, and the SOE was seen more as a means to the end - the liberation of the country from foreign occupation. The inability of the SOE to control such agents often led to dissatisfaction, distrust and even conflict between the British and the governments-in-exile fighting alongside the Allies against the Axis.

SOE hired many Canadians, relying on the direct support of the Canadian government, and adopted an entirely new position in the clandestine struggle against the Axis, ignoring all contemporary social convention. Thus, SOE recruited recognized homosexuals, people with rich criminal records or who had been convicted by military tribunals. Although some of these people might have been considered a security risk, the SOE was prepared to ignore almost any social convention in its struggle against the Axis. Despite such variety, which might suggest security risks to clandestine operations, there is no known case of siding with the enemy.

SOE was forced to develop a wide range of equipment for clandestine combat agents. An SOE agent working clandestinely in enemy territory needed clothes, documents made in such a way as not to arouse suspicion. SOE had a number of workshops for making clothing and for forging identity documents, food cards, or other products such as cigarettes.

In the course of its work, SOE managed a range of important and critical information during the Second World War that had a significant impact on the conduct of the war. It collected data on German troop movements, military installations, equipment and enemy logistics. This information was vital for planning Allied operations and anticipating enemy tactics. SOE agents also investigated and reported on the rail networks, roads, ports, and other transportation routes used by German forces for supply and mobilization. This data helped plan sabotage missions. The SOE worked with various resistance groups throughout Europe, gathering information on their structures, leaders, capabilities and activities. This collaboration facilitated the coordination of sabotage and anti-occupation actions. The SOE also gathered details of factories and industrial plants that produced military resources or equipment for the Nazis. Sabotaging these facilities was a priority to reduce the enemy's ability to sustain the war. Intelligence managed by SOE was essential for the coordination of Allied operations, including the invasion of Normandy. The intelligence SOE provided helped synchronize actions between the various Allied forces involved. By managing this information, SOE was able to achieve its strategic objectives and influence the outcome of the war in favor of the Allies.

3. CASE STUDY - VERA ATKINS

Vera Atkins was born in 1908 in Romania into a family of Jewish origin. Her father, a successful businessman, and her mother, who was of French descent, provided Vera Atkins with a cosmopolitan and cosmopolitan upbringing. The Atkins family moved to France when Vera was young and she spent much of her childhood there. She learned French, a language that would prove crucial to her later career.

However, it was Vera Atkins' academic achievements and exceptional language skills that made her stand out from the start.

After studying in Paris, she moved to London in the 1930s to continue her studies and start a career. But, like millions of others, Vera's life was turned upside down when World War II broke out, and the career she thought destined for her would soon change. Atkins was recruited before the war by Canadian spymaster Sir William Stephenson of British Security Coordination. He sent her on fact-finding missions to Europe to provide Winston Churchill with information on the growing threat from Germany.https://en.wikipedia.org/wiki/Nazi_Germany

In 1941, Vera Atkins was recruited by the Special Operations Executive to help in the world of espionage, covert operations and intelligence gathering. Vera Atkins was initially employed as a secretary, but her outstanding language and organizational skills quickly caught the attention of her superiors. She was soon appointed SOE liaison officer, responsible for managing a network of agents who were parachuted behind enemy lines to carry out sabotage and gather vital intelligence. Her role required not only meticulous diligence, but also an innate understanding of human psychology, as she had to manage agents from all levels of society, ensuring they were well prepared for the dangerous missions they were about to undertake. Atkins served as a civilian until August 1944, when she was commissioned as a flying officer in the Women's Auxiliary Air Force. In February 1944 and she was naturalized as a British citizen. Subsequently, she was appointed as an intelligence officer.

Atkins' main role at SOE was the recruitment and deployment of British agents in occupied France. She was in charge of the SOE agents who worked as couriers and wireless operators for the various circuits set up by SOE. Atkins was in charge of the housekeeping tasks relating to the agents, such as checking their clothing and documents to ensure they were suitable for the mission, liaising with members' families and ensuring their pay was received.

One of the most remarkable aspects of Vera Atkins' role in SOE was her responsibility for the recruitment and training of female agents, a task that was both innovative and challenging. Many of these women were young and inexperienced, but they were involved in some of the most dangerous missions imaginable.

Women trained by Vera Atkins were often sent to Nazi-occupied Europe to carry out sabotage, gather intelligence and organize resistance cells. These women spies worked in dangerous conditions, living undercover for months, often with little support.

Vera's ability to recruit and manage these women was extraordinary, and many of her recruits became legendary figures in the espionage world. One of her most famous recruits was Noor Inayat Khan [6], a young Muslim woman of Indian origin who became the first female radio operator in Nazi-occupied France.

Noor's bravery and her capture and execution by the Nazis left a lasting impression on Vera Atkins, who was devastated by the loss of her agent, but continued her work with renewed determination to thwart Nazism.

In conclusion, Vera Atkins used intelligence consistently and effectively in all aspects of her work in the SOE, from selecting and training agents, to monitoring missions and investigating the fate of the missing.

Her attention to detail, exceptional memory, and ability to analyze information were essential to the success of SOE operations and to her post-war efforts to shed light on the fate of the lost agents.

4. FROM CLASSIC WARFARE TO INFORMATION WARFARE

Information warfare is a modern form of conflict that includes information warfare, media warfare, cyber warfare, electronic warfare and, usually, the use of digital technologies to influence, destabilize or control information flows.

Information warfare includes various tactics such as computer virus sabotage (creating and spreading malicious software to affect the functioning of computer systems), blocking, filtering or diverting data (manipulating information flows to prevent access to certain resources or to redirect information to unauthorized sources), hacking (illegally accessing networks to obtain sensitive information or to monitor adversaries' activities), cyber-attacks (cyber-attacks that may have destructive purposes, such as deleting data or disabling critical infrastructure). These methods are often combined with manipulation and propaganda to influence public opinion or destabilize adversaries.

It is a constantly evolving field, and cybersecurity specialists are constantly working to develop solutions to protect against these threats.

In modern warfare the specific form of conflict is waged by fully specialized forces using specific means such as smart computer/information systems capable of operating in a permanent mode by specific means. In this confrontation, information is used both as a weapon and as a shield, without resorting to traditional armed force or limiting its use as far as possible.

The aims of the two types of warfare, classical and informational, differ fundamentally in nature, scale and methods.

The aim of the Second World War was to**:**

- Territorial and geopolitical objectives: The Axis powers aimed to expand territory, create empires and establish regional or global hegemony. The Allies aimed to stop aggression and restore sovereignty to occupied states.
- Ideological: The conflict was marked by the clash between totalitarian ideologies (fascism, Nazism, Japanese militarism) and democracy, as well as expansionist and racist ideologies.
- Resource control: Securing access to strategic natural resources has been an important factor for some powers.
- Changing world order: the war led to a major reconfiguration of global power.

The purpose of the information wars concerns:

- Influencing public opinion and behavior: the main aim is to shape the perceptions, attitudes and decisions of individuals and groups, both internally and externally.
- Undermining trust and polarizing society: The aim is to erode trust in institutions, exacerbate social and political divisions and create chaos and instability.
- Manipulating democratic processes: interference in elections, disinformation campaigns and discrediting democratic systems are frequent targets.

- Strategic and political advantage: Modern wars can be used to gain political, economic or military advantage without resorting to direct armed conflict.
- Erosion of the opponent's ability to respond: Through misinformation and manipulation, the aim is to paralyze the decision-making process and weaken the opponent's ability to respond.

Consequently, the following differences can be identified between the two types of wars:

- World War II was an open military conflict, with physical battles and massive loss of life and resources. Information wars are mainly fought in cyberspace and in the cognitive sphere, targeting people's minds.
- While the Second World War involved armies, airplanes, tanks and bombs, modern wars use fake news, propaganda, social networking, cyber attacks and other techniques to manipulate information.
- The victims of World War II were mainly soldiers and civilians killed or physically injured. In modern wars, the victims are citizens whose opinions are manipulated, whose trust is undermined and whose democratic processes are disrupted.
- World War II was an open and visible conflict. Modern wars are often clandestine and difficult to attribute, making it difficult to identify the aggressor and counter attacks.
- World War II was a global conflict directly involving most of the world's states. Modern wars can have a global scale thanks to the internet, but often target specific targets or population groups.

In conclusion, while the Second World War was a physical conflict for territory, power and ideology, today's modern wars are subtle conflicts for mind and information control, with the aim of influencing public opinion, undermining trust and gaining strategic advantage.

Although both types of warfare are based on information, the forms of modern warfare are fundamentally caused by the components of the information age, namely technical progress in weaponry and military concepts and, on the other hand, the leap forward in communications and its modes of manifestation, namely the internet and satellite communication, which have made the media and social media not only facilitators but also manifestations of modern warfare. What was once clearly structured and defined as global security in relation to national security or public order and the safety of the individual is now in mutual communication. The result is that modern warfare is multidimensional, encompassing internal and external aspects, of peace or conflict, targeting military threats or threats from civilian entities (hakirs, terrorism, organized crime, etc.).

5. THE NEW DIMENSION OF INFORMATION AS A COMBAT WEAPON

The US intelligence community has conducted a global threat assessment for 2025, highlighting a complex and dangerous security landscape. This assessment identifies various threats to US health, safety, critical infrastructure, industries, wealth, and government, a situation that can be generalized globally. The main conclusions of the assessment include:

- State and non-state adversaries: Seeking to undermine the economic and military power of the US;

- Transnational terrorist and criminal organizations: Directly threatening US citizens;
- Cartels: They are responsible for over 52.000 deaths from synthetic opioids in 2024 and have facilitated the arrival of nearly three million illegal migrants;
- Cyber actors and intelligence services: They target US wealth, critical infrastructure, telecommunications, and media;
- State support for non-state groups: China and India are mentioned as sources of precursors and equipment for drug traffickers;
- Military threats from state adversaries: They possess weapons capable of striking the US mainland or disabling vital systems in space;
- Revisionist powers (Russia, China, Iran, North Korea): They challenge US interests globally through asymmetric and conventional tactics, promoting alternative systems in commerce, finance, and security, while avoiding direct war;
- Cooperation among adversaries: Increases their strength against the US and pressure on other global actors to choose sides.

The 2025 Intelligence Community Report underscores its commitment to monitoring, assessing, and warning about these complex threats, providing critical information to US decision makers [8].

Thus, as the above assessment shows, the challenges facing societies have changed, with national security taking on a new dimension and information, closely linked to national security, being a particularly important value.

National security "refers to the dynamic giant system composed of artificial space, social space, biological space, information space, natural space, cosmic space and all the carriers in the spaces owned by a nation in a state free from danger, harm and serious loss, guided by the coexistence and sustainable development of the nation and the safety of its people with the world in a given period of time".

In the new context of national security, information as a weapon can have two meanings, one positive-defensive (defense, development, progress) and one negative-attack (aggression, destruction).

In a negative sense, information as a weapon can be defined as the strategic and intentional use of information (in all its forms, including news, data, narratives, images, videos and even misinformation or disinformation) by hostile state and non-state actors to undermine national interests, destabilize society, erode trust in institutions, manipulate decision-making processes and achieve objectives that threaten the security, sovereignty and functioning of the state.

This definition emphasizes the following key aspects of information:

- Strategic and deliberate: The use of information is not incidental, but is planned and executed with the specific purpose of adversely affecting national security.
- Multiple forms: information weaponry includes a wide range of tactics, from spreading fake news and propaganda, to data manipulation, cyber-attacks targeting sensitive information, creating divisive narratives and exploiting online platforms to amplify hostile messages.
- Undermining national interests: the ultimate aim is to damage the fundamental interests of the state, such as territorial integrity, political independence, economic stability, social cohesion and the security of citizens.
- Destabilization of society and erosion of trust: cyber attacks often aim to create internal divisions, polarize public opinion, spread fear and distrust of state institutions (government, military, intelligence services, media).

- Manipulating decision-making processes: through disinformation and influence campaigns, attempts are made to alter national political, economic and social decisions in favor of hostile actors.
- Hostile state and non-state actors: Threats can come from rival states, terrorist organizations, extremist groups, sponsored cyber actors, and even domestic actors with subversive agendas.

The characteristics of information as a weapon in the new information and national security context relate to the following:

- Information space vulnerability: Increased reliance on the internet and digital platforms creates a large information space that is vulnerable to cyber attacks.
- Speed and amplification: Social networks and online media allow manipulated information to be disseminated quickly and widely, often beyond the capacity to check and counteract.
- Anonymity and difficulty of attribution: Hostile actors may operate anonymously or through intermediaries, making it difficult to identify and hold the source of the attack accountable.
- Exploiting psychological and social vulnerabilities: cyber attacks are based on exploiting cognitive biases, emotions (fear, anger), social polarization and lack of media literacy.
- Hybridization with other threats: Information warfare is often integrated into hybrid strategies, combining with cyber-attacks, political meddling, economic influence operations and even physical subversion.
- Challenging reality and truth: A central element is undermining trust in facts and credible sources of information, creating an environment of uncertainty and confusion that paralyzes response.

Information has thus acquired "the quality of substituting itself for other economic resources, of circulating at high speed, conferring advantages to the possessor. Societies that have paid attention to the processing and use of information have moved rapidly towards the information society. This has also been due to the fact that information, unlike other economic resources, is extensible to the limits of human capacity and time, thanks to its natural diffusive power, its capacity to be reproduced during use, its ability to be transmitted, and its use as a transaction exchange value"[9].

Also, taking into account the danger generated by information used improperly or in a negative sense, information security becomes a major problem facing society, which needs to find solutions and take urgent action.

6. CONCLUSIONS

In the new national security context, information has become a formidable weapon, capable of eroding the foundations of the state, destabilizing society and compromising national interests without resorting to traditional armed conflict. Combating this threat requires a comprehensive and coordinated approach, which involves building societal resilience, improving media literacy, actively countering disinformation and strengthening the state's cyber and information security capabilities.

Transnational criminal and terrorist organizations pose a major threat to citizens, national security, and prosperity.

Transnational criminals, terrorists, and other non-state actors endanger the lives of citizens, national security, and internal and external power. Transnational criminal organizations produce and traffic illicit drugs, endangering lives. They are also involved in human trafficking, cyber operations, money laundering, and incitement to violence, all of which threaten national security. Citizens, both at home and abroad, face increasingly diverse, complex, and decentralized terrorist threats. These can come from terrorist organizations or from individuals and small cells that initiate or inspire attacks. Large-scale illegal immigration has strained national and local infrastructure and resources, while facilitating the free movement of known or suspected terrorists.

In this current geopolitical context, information has evolved from a simple communication tool into a sophisticated and ubiquitous weapon, capable of profoundly influencing global power dynamics and posing a significant threat to national and international security. It should be noted that the use of imagological weapons to control the minds of adversaries has always been used as a preliminary and preparatory phase for actual warfare. This structuring of forms of attack was maintained until the middle of the last century in all military conflicts, including the two great world wars.

However, of particular importance was and is the purpose for which information is used so that it is not diverted from its normal purpose and transformed not only into a tool for maintaining power but also into a tool for realizing individual or group interests or as a destructive weapon.

The relevance of the information tool of the state is highlighted both by the current situation we find ourselves in and by the examples that history provides us with when information has been used to organize, start, conduct and win wars.

As a consequence, the development of an information security strategy accompanied by a continuous process of education and training in the field of intelligence analysis can help to avoid many of the dangers associated with the misuse of information, especially information as a weapon.

Also, the development of a national project of education and training in the field of information analysis -Intelligence- can contribute to the organization of a National Intelligence Education and Training System based on educational programs and intelligence analysis, in a modern concept, adapted to the dynamics of the security environment. In addition, it appears that it is more productive to view education, training, coaching and specialization as integrated elements/components of a continuous system and not as separate activities carried out in universities on the one hand and intelligence institutions and structures (agencies/services) on the other hand.

REFERENCES

[1] D.M. Murphy & J. F. White, *Propaganda: Can a Word Decide a War*?, Parameters 37, no. 3 (2007), p.23, doi:10.55540/0031-1723.2383;

[2] D-Day is a term used in military parlance to designate the day on which an offensive operation is launched. D-Day is often regarded as a point of origin against which to measure the timing of various events related to a military operation, both in planning and tracking the progress of the offensive. The best known 'D-Day' is undoubtedly that of June 6, 1944, during which the Normandy landings, the Allied invasion to liberate the European continent from Nazi domination during the Second World War, were launched. Available at https: D-Day (military term) - Wikipedia, accessed on 15 april 2025;

[3] British Special Intelligence Service (Special Intelligence Service/SIS), also known as MI6;

[4] Supreme Headquarters Allied Expeditionary Force Headquarters (SHAEF) was the headquarters of the commander of the Allied forces in northwest Europe from the end of 1943 until the end of World War II. American General Dwight D. Eisenhower was commander of SHAEF throughout its existence. Available at https: Supreme Headquarters Allied Expeditionary Force - Wikipedia, accessed on 5 april 2025;

[5] T.V. Meleşcanu, coordinator, *Istoria și evoluția serviciilor de informații din vremurile biblice până în zilele noastre*, Concordia, Arad, p. 684, 2023;

[6] Wikipedia, the free encyclopedia, *Noor Inayat Khan*. Available at https: Noor Inayat Khan - Wikipedia, accessed on 5 april 2025;

[7] W.Stevenson (2013), *Spymistress : the life of Vera Atkins, the greatest female secret agent of World War II*. Avalaible at https: Spymistress : the life of Vera Atkins, the greatest female secret agent of World War II : Stevenson, William, William, 1924-2013 : Free Download, Borrow, and Streaming : Internet Archive, accessed on 5 April 2025;

[8] Office of the director of National Intelligence, *Annual threat assessment of the U.S. intelligence community,* march 2025, p. 4, 2025. Available at https: Annual Threat Assessment of the U.S. Intelligence Community.pdf, accessed on 12 April 2025;

[9] Chao Wu, *Redefining concepts of nation and national security and establishing their models for the new era*, Journal of Safety and Sustainability 2 (2025) 45-58. Available at https://doi.org/10.1016/j.jsasus.2024.12.002, accesed on 14 April 2025;

[10] T. Tănase coordinator, *Inteligența artificială în informații,* Concordia, Arad, 2024, p. 238;

[11] Army University Press, *Military Review January-February 2025*. Available at https: Military Review January-February 2025, accessed on 19 April 2025;

[12] D. M. Murphy & J. F. White, "*Propaganda: Can a Word Decide a War*?", Parameters 37, no. 3 (2007), doi:10.55540/0031-1723.2383;

[13] United States Army War College Press, Parameters Spring 2025 Review, vol. 55, no. 1, DOI: 10.55540/0031-1723.3326. Avalilable at https://press.armywarcollege.edu/parameters, accessed on 2 April 2025;

[14] J.Junguzza, K.Lelito, *What National Culture Teaches Us About Mission Command,* Smart Wars Journal, 2024. Available at https: What National Culture Teaches Us About Mission Command | Small Wars Journal by Arizona State University, accessed on 7 April 2025;

[15] Joint Chiefs of Staff, UNCLASSIFIED CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION, 2021. Available at https: Joint Chiefs of Staff > Doctrine > Joint Lessons Learned intell_ops_fp.pdf, accessed on 14 April 2025;

[16] Wikipedia, the free encyclopedia, *Air tasking order*. Available at https: Air tasking order - Wikipedia, accessed on 10 April 2025;

[17] Wikipedia, the free encyclopedia, *Noor Inayat Khan*. Available at https: Noor Inayat Khan | Biography, World War II, SOE, French Resistance, & Facts | Britannica, accessed on 17 April 2025

[18] United States Marine Corps the Basic School Marine Corps Training Command Camp Barrett, Virginia 22134-5019, *Combat orders foundations B2B0287 student handout*. Available at https: B2B2377 Combat Orders Foundations.pdf, accessed on 10 April 2025;

[19] Wikipedia, the free encyclopedia, *Air Operations Center*. Available at https: Air Operations Center - Wikipedia, accessed on 12 April 2025;

[20] Sky History, *History of America: Vietnam War*. Available at https: History of America: Vietnam War | Sky HISTORY TV Channel, accessed on 17 April 2025;

[21] Wikipedia, the free encyclopedia, *Hugh Brogan*. Available at https: Hugh Brogan - Wikipedia, accessed on 20 April 2025;

[22] Wikipedia, the free encyclopedia, *Vera Atkins*. Available at https: Vera Atkins - Wikipedia, accessed on 16 April 2025;

[23] Wikipedia, the free encyclopedia, *Special Operations Executive*. Available at https: Special Operations Executive - Wikipedia, accessed on 9 April 2025;

[24] F.H.Hinsley, E.E.Thomas, C.F.G.Ransom, R.C.Knight, *British intelligence in the Second World War,* University Press Cambridge, London, 1979. Available at https: British intelligence in the Second World War : Hinsley, F. H. (Francis Harry), 1918-1998 : Free Download, Borrow, and Streaming : Internet Archive, accessed on 18 April 2025;

[25] National Security Agency/Central Security, *NSA Historical figures*. Available at https: Service Marian Rejewski > National Security Agency/Central Security Service > Historical Figures View, accessed on 14 April 2025;

[26] M.Felton Production, Capturing Hitler's Eagle's Nest, 2018. Available at https: SOE Target Hitler - The Eagle's Nest Sniper : Mark Felton Productions : Free Download, Borrow, and Streaming : Internet Archive, accessed on 11 April 2025;

[27] D.Stafford, *Secret agent : the true story of the Special Operations Executive*, BBC Worldwide Limited, London, 2000. Available at https: Secret Agent: The True Story of the Special Operations Executive - David Stafford, accessed on 10 April 2025;

[28] D.Stafford, *Secret agent : Britain's wartime secret service,* BBC Worldwide Limited, London, 2000. Available at https: Secret agent : Britain's wartime secret service : Stafford, David, 1942- : Free Download, Borrow, and Streaming : Internet Archive, accessed on 5 April 2025;

[29] D.Stafford, *Roosevelt and Churchill: men of secrets,* Abacus, London, 2000. Available at https: Roosevelt and Churchill: men of secrets: Stafford, David, 1942- : Free Download, Borrow, and Streaming: Internet Archive, accessed on 23 April 2025;

[30] D.Hamilton-Hill, *SOE assignment*, New English Library. Available at https: SOE assignment: Hamilton-Hill, Donald : Free Download, Borrow, and Streaming : Internet Archive, accessed on 19 April 2025;

[31] Dosare Secrete, Vera Atkins, românca de la vârful spionajului britanic. Available at https://dosaresecrete.ro/vera-atkins-romanca-de-la-varful-spionajului-britanic/, accessed on 16 April 2025;

[32] Wikipedia, the free encyclopedia, *Gustave Bertrand*. Available at https: Gustave Bertrand - Wikipedia, accessed on 14 April 2025.