



THE MORAL LIMITS OF SABOTAGE – THE WAR IN UKRAINE –

Lieutenant Vlad-Andrei SKOWRONSKI

Ministry of National Defence
DOI: 10.55535/RMT.2025.1.03

The war that began in February 2022 with the invasion of the Russian Federation in Ukraine currently presents all the characteristics specific to total war. This fact reveals Russia's commitment to conduct a war of attrition, atypical for the 21st century, in order to achieve strategic objectives at any cost. In this context, an upward trend has been noted in the frequency of the use of sabotage actions by both states, through which the enemy's defence capacity is attempted to be damaged through kinetic, punctual actions. New technologies have been integrated into old doctrines regarding sabotage, and the results have been remarkable for making military operations more efficient.

Sabotage fits perfectly into the military activities specific to the grey area, where the boundary between morality and immorality is very sensitive, and for this reason, a comparative analysis of the most representative sabotage activities identified in the conflict in Ukraine is required. Following the analysis, different degrees of morality are attributed to sabotage missions, which are positioned hierarchically, depending on the principledness and military necessity.

Keywords: sabotage; morality; ethics; collateral damage; Ukraine;



SABOTAGE – FROM SIMPLE TO COMPLEX: INTRODUCTION

Sabotage is and will continue to be an important tool for military conflicts, the main advantage of its use being efficiency. Ukraine has demonstrated that the asymmetry on the contemporary battlefield can be compensated by the use of sabotage and resistance groups. The increasing frequency of sabotage actions reaffirms the hypothesis that old military doctrines are not abandoned, but only adapted to the current operational environment.

Sabotage is defined as “an act or acts with intent to injure, interfere with, or obstruct the national defense of a country by willfully injuring or destroying, or attempting to injure or destroy, any national defense or war materiel, premises, or utilities, to include human and natural resources.” (ATP 3-05.1, 2021, p. C-19).

Sabotage activities are divided into two broad categories, depending on the complexity of the mission – simple and strategic/general. While simple sabotage does not require advanced specialized training and does not require special materials or equipment, strategic sabotage requires extensive planning and a specific material base to achieve an optimal result.

The main advantage of this type of mission is the impact generated at a strategic level, with minimal use of human and material resources. On the other hand, the disadvantages include the risks of the saboteur being captured as a result of the clandestine way of operating in enemy territory. In addition, the ambiguity of sabotage can be exploited by public opinion, and the saboteurs can be accused of perfidy or immorality.

It is important that both decision-makers and tactical elements comply with the laws of armed conflict and minimize collateral damage. During an armed conflict, sabotage falls within the bounds of morality if the persons involved in the execution of these missions assume responsibility for their actions and realize that involvement

During an armed conflict, sabotage falls within the bounds of morality if the persons involved in the execution of these missions assume responsibility for their actions and realize that involvement in sabotage implies the loss of the rights specific to combatants. Saboteurs are subject to a special regime, do not have the same rights as prisoners of war and may be sanctioned by the state on whose territory they operate, in accordance with its legislation.



in sabotage implies the loss of the rights specific to combatants. Saboteurs are subject to a special regime, do not have the same rights as prisoners of war and may be sanctioned by the state on whose territory they operate, in accordance with its legislation (FM 6-27/MCTP 11-10C, 2019, pp. 1-15 - 1-18). However, saboteurs must be treated with dignity and have the right to a fair trial: “(...) *such persons must nevertheless be treated humanely and in the case of trial must not be deprived of the rights of a fair and regular trial*” (Ib., p. 5-3).

❖ **Simple sabotage** is used to generate a small but constant pressure on state authorities, in order to increase the morale of their own troops, but also to train saboteurs (*confidence targets*) in order to carry out more complex missions. It is important to note that these activities are subtle and small-scale, so as not to trigger coercive reactions from the authorities. Some examples include puncturing car tires, starting fires or short-circuiting electrical systems.

An advantage of using this strategy lies, first of all, in placing sabotage activities in the grey area, when it is difficult or even impossible to make a clear distinction between peace and war. The unified actions of a significant number of civilians can be interpreted as a gesture of protest against the state authorities, a phenomenon that can only be sanctioned *en masse* when the threshold of violence is significantly exceeded.

Secondly, this mode of operation is specific to fifth-generation (5GW) conflicts, in which the aggressor cannot be identified, or moreover, there are no suspicions of a possible attack orchestrated from outside (Neculcea, 2021, p. 316).

An innovative approach to how sabotage has been adapted to the current operational environment is reported by Richterova et al. (2024). The authors propose for analysis how intelligence services have integrated new technologies in order to recruit agents, minimizing both the costs and the risks of attributing acts of sabotage or intelligence gathering to state-type actors. In this sense, the new approaches of intelligence services have conformed to the increasingly popular trend among employers, that of the “*gig-economy*”. The phenomenon specific to the free market is widespread in the online environment and offers the opportunity for both employers and private individuals to benefit from or provide services, for a fee (Ib., pp. 14-15).

In this context, it is necessary to analyse the moral consequences of this approach and try to answer the question: *How is a saboteur who is not aware that he is carrying out sabotage missions treated?* Situations of this kind seem to be increasingly frequent in the current operational environment, the main reason being the accelerated evolution of technology that allows the recruitment of saboteurs from the online environment. Thus, intelligence services can carry out recruitment actions remotely, via the Internet, without exposing their personnel to the risks of infiltration into enemy territory: “*Available evidence suggests that Moscow has expanded its recruitment of agents-saboteurs online to go beyond the usual suspects*”. (Ib., p. 14). At the same time, this mode of operation has significantly reduced the costs of sabotage actions by manipulating appearances and directing individuals to carry out actions specific to sabotage, without them being aware of the seriousness of the actions they are taking.

The manipulation of appearances by intelligence agencies to recruit and involve civilians in high-risk missions, such as espionage or sabotage, constitutes a serious moral violation. However, in recent history, such situations have been identified that were intended to reduce the risks of exposure to military personnel.

In the context of the war in Ukraine, both states accuse each other of perfidy due to the involvement of young people in acts of sabotage. According to information in the public space, young people are manipulated through online games and messaging applications to set fire to and photograph elements of critical infrastructure (electrical substations) and military equipment that contribute to the war effort (Infosecurity Magazine, 2024).

As a result of a process of manipulation by military professionals, young people commit sabotage with or without discernment, and are later sentenced to prison for their actions.

A slightly different form of simple sabotage is represented by the lack of cooperation of citizens with state authorities, the apparently accidental omission of tasks, the erroneous entry of data in the process of drafting documents, or the delay in the delivery of products or services (ATP 3-05.1, 2013, pp. 3-7).

The advanced form of non-cooperation, which also has a strong subversive effect, materializes through a form of active resistance



The manipulation of appearances by intelligence agencies to recruit and involve civilians in high-risk missions, such as espionage or sabotage, constitutes a serious moral violation.



Sabotage can have a powerful subversive effect, with impressive results also on the political environment. However, taking into account that the Wagner rebellion was triggered by logistical needs on the front and not by a clear intention to affect the defence capacity of the Russian Federation, it can be said that this case does not represent a sabotage mission in the true sense of the word unless it was premeditated.

of the population (*rebellion*) (FM 3-24 MCWP 3-33.5, 2014, p. 5-1) which requires a form of coordination and planning at the central level.

The armed rebellion of the employees of the paramilitary company Wagner in June 2023 is the most conclusive example of such a situation. Motivating the lack of ammunition and conditions on the Ukrainian front, the Wagner leader mobilized the members of the formation to participate in a form of spontaneous strike, through which they defied the state authorities and initiated a march to Moscow, with the aim of negotiating from positions of strength with the decision-makers (ABC News, 2023). The protest generated chaos on the Ukrainian front, having a negative impact on the morale of the Russian troops, respectively a positive impact on the morale of the Ukrainian troops.

Such situations can very easily turn into violent clashes between the masses of people and the police, and the political environment is forced to engage in some form of dialogue with the leaders of the rebellion or to seek peaceful methods of resolving the problem, so that tensions do not escalate.

Under these circumstances, the participants in such a large-scale movement (25,000 servicemen)¹ cannot be held individually liable, especially in the context in which the Russian Federation had established a state of war and needed the servicemen to return to the front. The contractors' rebellion constituted an act of desertion with catastrophic effects for the front in Ukraine and for the state's efforts to manage the war.

This example reveals that sabotage can have a powerful subversive effect, with impressive results also on the political environment. However, taking into account that the Wagner rebellion was triggered by logistical needs on the front and not by a clear intention to affect the defence capacity of the Russian Federation, it can be said that this case does not represent a sabotage mission in the true sense of the word unless it was premeditated.

❖ **Complex sabotage** is carried out following an extensive planning process involving specialists from multiple fields, and the person who is to carry out the mission must benefit from specific training. While simple sabotage can be carried out with limited material

¹ More details at: <https://abcnews.go.com/International/wagner-groups-rebellion-putin-unfolded/story?id=100373557>.

resources, complex sabotage requires obtaining special materials, such as ammunition or explosives.

Another critical stage in the execution of complex sabotage missions refers to the process of prioritizing and selecting targets (targeting). Given the risk and scope of such a mission, the targeting process is beneficial for increasing the efficiency of military operations, respectively the qualitative management of material and human resources. The main tool used during this analysis is the CARVER matrix (Criticality, Accessibility, Recuperability, Vulnerability, Effect, Recognizability). Through this tool, potential targets are evaluated and it is established what results can be obtained at the strategic level, by engaging the targets with tactical level elements.

To illustrate the direct proportionality between the quality of the targeting process and the results of strategic sabotage, reference will be made to the explosion on 08.10.2022 that disabled an element of Russia's critical infrastructure – the Kerch bridge (Crimea). The mentioned sabotage activity was claimed by the Ukrainian intelligence service, in response to the invasion of the Russian Federation (Radio Free Europe, 2022). In the context in which, at the time of the explosion, all the efforts of the Russian Federation were directed towards the front in Ukraine, the effect was multiplied exponentially and manifested itself in most areas of the PMESII (Political, Military, Economic, Social, Informational, Infrastructure) spectrum.

As a result of the unavailability of road and rail infrastructure that lasted for about a month, Russia faced difficulties in supplying troops fighting in southern Ukraine (Kherson) and was forced to seek alternative routes to meet logistical needs on the front. At the same time, the freedom of movement of Russian troops was significantly reduced, forcing them to allocate additional resources to the area.

Equally important, the cost of restoring the bridge forced Russia to allocate funds and manpower in that direction, putting additional pressure on the budgetary system. Moreover, the morale of the Russian population was affected by the unpredictability of the situation, and the Ukrainians, by executing a large-scale mission deep inside enemy territory, sent a message with strong symbolic significance to the Kremlin political environment, namely that the Crimean Peninsula is Ukrainian territory.



ROMANIAN
MILITARY
THINKING

As a result of the unavailability of road and rail infrastructure that lasted for about a month, Russia faced difficulties in supplying troops fighting in southern Ukraine (Kherson) and was forced to seek alternative routes to meet logistical needs on the front.



An hour before the Russian Federation launched its invasion of Ukraine, the telecommunications company Viasat experienced significant technical difficulties. As a result, for several hours, Viasat Inc's KA-SAT satellite network was unable to provide internet services to users on the territory of Ukraine, including the armed forces.

❖ **Complex Sabotage in the Cyber Domain.** If during *Operation Jedburgh*, from the territory of occupied France during the Second World War (CIA, 2015), Allied forces soldiers were parachuted deep into enemy territory to physically destroy its communications network, currently, similar effects are achieved through IT professionals.

An hour before the Russian Federation launched its invasion of Ukraine, the telecommunications company Viasat experienced significant technical difficulties. As a result, for several hours, Viasat Inc's KA-SAT satellite network was unable to provide internet services to users on the territory of Ukraine, including the armed forces. Three months later, on 10.05.2022, the *United Kingdom (UK) National Cyber Security Centre* released information that the technical problems of the telecommunications system were the result of a cyber attack, carried out by Russia, with the aim of destabilizing the command-and-control process of the Ukrainian armed forces during the “*special military operation*” (UK National Cyber Security Centre, 2022).

There is thus an upward trend in the integration of new technologies into contemporary conflicts, in order to amplify the effects of sabotage.

TERRORIST SABOTAGE – CONCEPTUAL DISTORTION

A separate perspective on the forms of sabotage in the war in Ukraine is provided by the authors Litvinov et al. (2022) in their work *National Political Forces of Ukraine as a source of threats of sabotage and terrorist activities on the territory of Russia*. It is important to note that the information presented should be treated with scepticism, relevant being the delimitation of the editors towards the vision of the authors (Ib., p. 121).

With direct reference to the war in Ukraine², Russian authors contaminate the definition of the concept of sabotage by combining it with a different concept – terrorism. As a result, sabotage, which represents a type of mission that does not exceed the moral limits of armed conflict, receives an illegal and immoral connotation: “*terrorist sabotage*” (Ib.).

² Although the Russian Federation attacked Ukraine on 24 February 2022, the Kremlin representatives initially used the term Special Military Operation until 22 March 2024, <https://www.lowyinstitute.org/the-interpretor/why-russia-has-only-now-declared-war-ukraine>.

In this context, it is fundamental to mention one of the widely accepted definitions of terrorism, which refers to the instillation of fear, through the use of violent means, in order to achieve a political objective (FM 3-24 MCWP 3-33.5, 2014, p. 5-2).

Therefore, the difference between the two concepts is that sabotage aims at the intentional destruction of any material, space, person or facility that contributes to the state's national defence system, and terrorism aims to achieve a political objective by attacking the physical and moral integrity of the civilian population.

In an attempt to analyse this concept as objectively as possible, it is necessary to refer to one of the situations that was classified by the Kremlin as the result of terrorist activity – the assassination of Vladlen Tatarsky in April 2023. The Russian military vlogger was killed by the explosion of a statuette he had received as a gift during a meeting. Ukraine has not claimed responsibility for this attack to date, but Darya Trepova, who was sentenced to 27 years in prison for handing the statuette to the vlogger, stated that she carried out the mission following instructions received from a Ukrainian citizen, but believed that the statuette contained a communications interception device (Aljazeera, 2024).

A similar event occurred in August 2022, when Daria Dughina, the daughter of one of the main supporters of the war ideology in Ukraine, was killed following the explosion of the car she was driving (NPR, 2022).

The lack of clear evidence from the Russian Federation that could prove Ukraine's involvement in the execution of the two assassinations and the lack of claim by Ukraine for the attacks leave room for speculation, but the two assassinations may represent moral lapses by combatants during the war, given that the people targeted by the explosions were civilians and did not directly contribute to the national defence capacity or the war effort of the Russian Federation.

At the same time, the persons targeted by the two assassinations can be classified as supporters and moral authors of the war in Ukraine. Through their effort to ideologically feed the Russian collective mind with information favourable to the continuation of the war, they indirectly contributed to the war effort of the Russian Federation.



ROMANIAN
MILITARY
THINKING

The difference between the two concepts is that sabotage aims at the intentional destruction of any material, space, person or facility that contributes to the state's national defence system, and terrorism aims to achieve a political objective by attacking the physical and moral integrity of the civilian population.



Such attacks have a strong subversive effect on the morale of the troops, therefore, there are arguments that can classify the two assassinations as acts of sabotage and not terrorist attacks. As an aggressor state, the Russian Federation must bear the consequences of the invasion it launched against Ukraine, and the acts of sabotage are part of the Ukrainian counteroffensive, which is morally acceptable.

The perspective according to which the state has a moral duty to defend itself *“by all means”* is also illustrated by Erskine (2004), who refers to the activity of intelligence services as follows: *“the defence of the interests of the national state as a moral duty, holding that the state is compelled to use specific aggressive methods – for example, employing spies and maintaining military forces. Such practices (...) are imperative. Hence, the national state <may not do otherwise> because it should be defended by all means.”* (Erskine, 2004, p. 364).

It highlights the diametrically opposed views of the two combatants regarding the morality of sabotage actions on the battlefield. On the one hand, Ukraine is trying to affect the combat capability of the Russian Federation by executing sabotage actions that produce effects at a strategic level with minimal involvement of human and material resources. Ukraine has claimed only the sabotage actions over which it does not suspect a violation of moral norms and has denied involvement in sabotage activities specific to the grey area, in which the boundary between moral and immoral is very sensitive. Ukraine thus assumes the risk of fuelling the Russian Federation’s narratives regarding the Nazi and terrorist tendencies of the Ukrainian state.

On the other hand, the Russian Federation is aware that Ukraine’s sabotage actions have proven to be extremely effective and, for this reason, it is carrying out a broad campaign of disinformation and conceptual distortion of sabotage, with the aim of gaining the support of international public opinion and discouraging Ukraine from carrying out further missions in this spectrum.

The Russian Federation is aware that Ukraine’s sabotage actions have proven to be extremely effective and, for this reason, it is carrying out a broad campaign of disinformation and conceptual distortion of sabotage, with the aim of gaining the support of international public opinion and discouraging Ukraine from carrying out further missions in this spectrum.

SABOTAGE IN THE WAR IN UKRAINE – COMPARATIVE ANALYSIS

The article uses a research methodology based on the comparative analysis of the most significant sabotage missions assigned to Ukraine during the current war in which it is participating. The criteria on which the analysis has been carried out are (1) principledness – strict compliance with the Law of Armed Conflict/LoAC and international humanitarian law (IHL); (2) utility – the compromise according to which the ends justify the means; (3) the risks assumed on the executor of the mission – direct approach, by using one’s own forces, or indirect approach, by recruiting and training a saboteur, and (4) limitation of collateral damage.

The objective of this analysis is to identify and develop a tool that will contribute to assessing the level of morality of sabotage actions, according to the previously mentioned criteria.

Due to the fact that the war in Ukraine is ongoing and the protection of classified information contributes to the security of operations on the battlefield, much of the information regarding the sabotage missions in which the two state actors were involved has not been made public. Consequently, in the development of the comparative analysis, secondary sources, such as press releases, have been mainly used, which also represents the main limitation of the research.

A point of view regarding the morality of sabotage actions is represented by Walzer’s (1977) vision, which mentions that saboteurs fight for a just cause, but because they fight behind the front line, on enemy territory, they cannot benefit from the same rights as ordinary combatants: *“It is widely agreed that such agents possess no war rights, even if their cause is just”*. (Ib., p. 183).

A different perspective on intelligence activities, applicable also to the field of sabotage, is that ethics in sabotage is an oxymoron. Bellaby offers a strong argument against this hypothesis, namely, the right to self-defence: *“the just cause for engaging in intelligence activities may also be understood in terms of self-defence against a specific threat”* (Bellaby, 2012 in Rønne, 2016, p. 775). Therefore, counter-offensive sabotage actions carried out by Ukrainians on Russian territory can be justified from a moral point of view, especially sabotage carried out



ROMANIAN
MILITARY
THINKING

A point of view regarding the morality of sabotage actions is represented by Walzer’s vision, which mentions that saboteurs fight for a just cause, but because they fight behind the front line, on enemy territory, they cannot benefit from the same rights as ordinary combatants.



on the Ukrainian territories that were illegally annexed by the Russian Federation.

Sabotage and intelligence activities share two major characteristics: their purpose is to prevent a greater evil, and both are discrete activities that often use other people to accomplish their missions. For this reason, the work of Frisk and Johansson (2020), who analysed the ethics of intelligence, represents a starting point in the pragmatic approach to assessing the morality of sabotage actions.

Frisk and Johansson draw a parallel between intelligence activity and a theoretical scenario, *the trolley dilemma*, intended to stimulate reflection on the value of human life and to highlight the extreme consequences of making a decision, respectively of inaction. The problem starts from the assumption that the reader controls a trolley heading towards five people tied to the railway. He can operate a lever to redirect the trolley onto a secondary line to which only one person is tied (*Preventing harm*). The lack of a decision on the part of the reader will lead to the death of five people (*Allowing harm*), and his intervention will sacrifice one person to save five (*Doing harm*). The problem of this exercise is called PAD, based on the initials of the three major dilemmas in the scenario – Preventing, Accepting and Doing “harm”.

By analogy, in the case of the war in Ukraine, sabotage is acceptable if it aims to prevent a greater harm (*Preventing Harm*), and in this case, the purpose of sabotage missions is to affect the enemy’s war effort. Sabotage imposes a form of acceptance of risk to one’s own person, if it is executed directly by a member of the armed forces (*Allowing harm*) and can be executed indirectly, by recruiting and training a third person to carry out the mission (*Doing harm*). At the same time, these actions can be executed for (**O**)ffensive purposes – on the territory of the Russian Federation, or (**D**)efensive – on the territories illegally occupied by the Russian Federation (Donetsk, Kherson, Luhansk, Zaporizhzhia, Crimea).

Figure 1 is a schematic representation of the ethical dilemma faced by military decision-makers when planning a sabotage mission.

Figure 1 distinguishes between the level of morality specific to a number of eight possible types of sabotage missions executed through

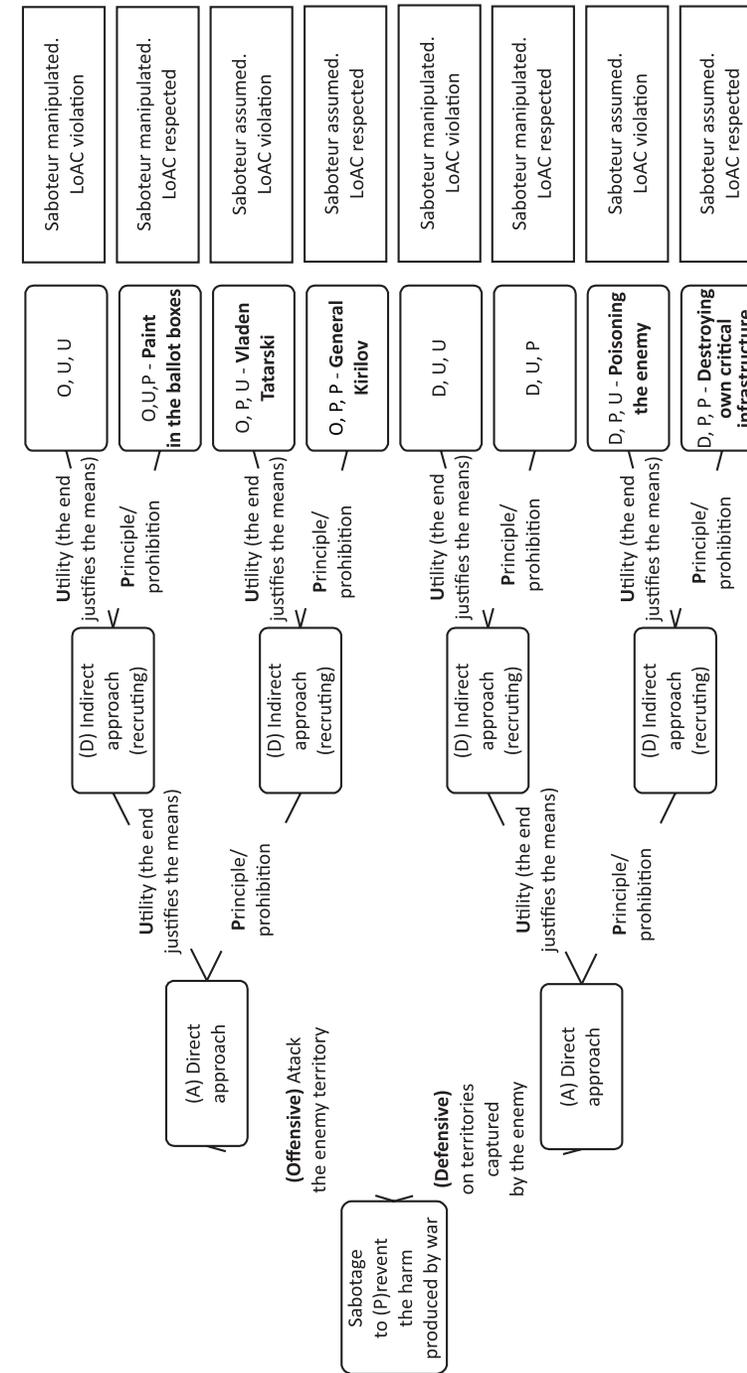


Figure 1: The PAD approach visualised as a decision tree for identifying 12 ethical strategies of sabotage (adapted after Frisk and Johansson)

Sabotage and intelligence activities share two major characteristics: their purpose is to prevent a greater evil, and both are discrete activities that often use other people to accomplish their missions.



an indirect approach (recruited saboteur), respectively four possible variants of a direct approach. The direct approach has not been analysed, because it presents much fewer ethical dilemmas than in the case of the indirect approach. In this regard, a comparative analysis was carried out of concrete cases of sabotage attributed to Ukraine during the war in which it takes part, where the risk of the sabotage mission was transferred by the armed forces to third parties. The eight scenarios were analysed based on the selected criteria, and were subsequently evaluated and hierarchically placed according to the level of morality, as follows:

❖ *D, P, P (Defensive, Principle, Principle)* – represents a defensive action (on territory captured by the enemy), executed by a saboteur who was recruited on the basis of respecting certain principles (without manipulating the saboteur) and trained to act within the resistance group. He agrees to collaborate in order to execute sabotage actions with strict observance of the principles or norms in the field of LoAC&IHL and with the avoidance of collateral damage. His motivation is purely ideological.

The most significant example refers to the destruction of one's own critical infrastructure, in such a way that the enemy cannot use it to carry out military actions: the destruction of bridges (mandatory crossing points), the railway or the electricity supply network.

Multiple situations have been identified in which Ukrainians in the territories occupied by the Russian Federation initiated sabotage actions against their own critical infrastructure, in order to limit the initiative of the Russian armed forces and to demonstrate their revolt against the invader. In November 2024, members of the resistance group destroyed elements of the railway infrastructure in Zaporizhzhia in order to affect the supply process for troops on the front line (The new voice of Ukraine, 2024). This is the noblest form of sabotage, as a result of the fact that the saboteur is part of the resistance group and consciously decides to contribute to affecting the enemy's war effort, through punctual kinetic actions, behind the front line, with strict adherence to certain principles.

❖ *D, P, U (Defensive, Principle, Utility)* – consists of defensive actions, executed by a saboteur who was recruited based on respecting

certain principles (without manipulating the saboteur) and trained to act within the resistance group, and who considers himself entitled to make concessions from principles or norms in the field of LoAC&IHL to accomplish the mission (the end justifies the means).

In August 2023, the mayor of Kherson, Vladimir Saldo, who was artificially installed in this position by representatives of the Russian Federation, died after consuming food poisoned by a member of the Ukrainian resistance group (Telegraph, 2022). Although the sabotage action was not directed against a military leader, it had a strong impact on the morale of the Russian military occupying the Ukrainian territories.

In December 2023, 24 Russian servicemen died after consuming food and alcoholic beverages received as gifts from members of the resistance group. According to information in the public space, they were intentionally contaminated with toxic substances (arsenic) in order to eliminate the Russian servicemen (Kyivpost, 2023).

❖ *D, U, U (Defensive, Utility, Utility) & D, U, P (Defensive, Utility, Principle)* – represents situations in which the saboteur is manipulated to execute sabotage missions on enemy-occupied territories, in compliance with, respectively in violation of, principles or norms in the field of LoAC&IHL.

During the comparative analysis, no concrete examples of defensive sabotage were identified, executed through saboteurs manipulated by the armed forces of Ukraine to execute missions, and the main reason is that the population on the Ukrainian territories occupied by the Russian Federation does not need to be manipulated to support the resistance group. They are willing to execute defensive sabotage missions for ideological reasons, in order to weaken the war effort of the invaders and recover their territories.

❖ *O, P, P (Offensive, Principle, Principle)* – refers to offensive actions (on enemy territory) carried out by a saboteur who was recruited on the basis of respecting certain principles (without manipulating the saboteur) and trained to act on enemy territory. He agrees to collaborate in order to carry out sabotage actions in strict compliance with the principles or norms of the LoAC&IHL and with the avoidance of collateral damage. His motivation is purely ideological.



In December 2023, 24 Russian servicemen died after consuming food and alcoholic beverages received as gifts from members of the resistance group. According to information in the public space, they were intentionally contaminated with toxic substances (arsenic) in order to eliminate the Russian servicemen.

A saboteur agrees to collaborate in order to execute sabotage actions with strict observance of the principles or norms in the field of LoAC&IHL and with the avoidance of collateral damage. His motivation is purely ideological.



A saboteur agrees to work together to carry out sabotage actions and believes it has the right to deviate from LoAC&IHL for the accomplishment of the mission (use of any means to achieve the goal). Here we can recall the case of the Russian military vlogger Vladlen Tatarsky.

The case of the assassination of Lieutenant General Ivan Kirillov by an Uzbek citizen is representative of this scenario. The saboteur stated that he was recruited through online messaging applications and agreed to carry out the mission for financial reasons. The sabotage mission was publicly assumed by the Ukrainian intelligence services (SBU), which announced that the general was responsible for war crimes against Ukrainians, through the use of chemical weapons prohibited by international conventions. The explosion, triggered by an improvised explosive device (IED), killed both the general and his aide (BBC, 2024). It is important to note that the explosion can be classified as legitimate because it did not cause collateral damage to civilians and did not violate the specific principles of the LoAC&IHL. Furthermore, it targeted a military leader who was directly contributing to the war effort of the Russian Federation.

❖ *O, P, U (Offensive, Principle, Utility)* – it includes offensive-type actions executed by a saboteur who was recruited on the basis of compliance with certain principles (without manipulation of the saboteur) and trained to act on enemy territory. It agrees to work together to carry out sabotage actions and believes it has the right to deviate from LoAC&IHL for the accomplishment of the mission (use of any means to achieve the goal). Here we can recall the case of the Russian military vlogger Vladlen Tatarsky, mentioned in a previous paragraph. At least 50 people were injured in the blast.

The situation gives clues as to the possible agreement of the saboteur in order to assume the risk of collateral damage and, implicitly, of violation of LoAC&IHL by sabotage action (Radio Free Europe, 2024).

❖ *O, U, P (Offensive, Utility, Principle)* – represents an offensive action for the performance of which the saboteur is manipulated (does not agree or is not aware of the result of his actions), but no specific principles or norms of LoAC&IHL are violated and no collateral damage is caused.

During the presidential elections held in the Russian Federation in March 2024, approximately 214 ballot boxes were vandalized by arson or by putting green paint in the ballot boxes. Also in this context, a person threw a Molotov cocktail at a polling station. The authors of these acts are responsible for committing acts of sabotage aimed

at exerting additional pressure on the political environment, in the context of the war in Ukraine. According to the representative of the Central Election Commission of the Russian Federation, some of the individuals who carried out these acts of sabotage stated that they were paid. As a result of the fact that the simple sabotage activities took place in multiple locations and were not isolated cases, the Russian authorities believe that these were not simple gestures of protest by citizens, but a much larger action, coordinated from outside (CNN World, 2024).

❖ *O, U, U (Offensive, Utility, Utility)* – consists of offensive actions for the performance of which the saboteur is manipulated, and he violates principles or norms in the field of LoAC&IHL, against his will or without being aware of the result of his actions. This represents the lower limit of morality within sabotage actions, because in order to fulfil the mission, all three criteria that are the basis of the assessment are simultaneously neglected.

The only relevant situation for this type of sabotage missions that was identified during the conflict in Ukraine is not based on a mission coordinated and executed by Ukraine, but by the Russian Federation. Nevertheless, the example is representative of the situation under analysis and is worth mentioning.

At the end of 2024, Infosecurity Magazine published information according to which the Russian Federation developed attractive games for young people and children in Ukraine (including some under the age of 15³), in which they were manipulated to perform sabotage-specific tasks, such as causing fires and directing enemy fire by photographing critical infrastructure elements (Infosecurity Magazine, ib.).

The scenarios presented above highlight that the morality of sabotage actions can be assessed through a comparative analysis based on four relevant parameters (1) principle; (2) utility; (3) risks assumed on the executor of the mission; and (4) limitation of collateral damage. These parameters allowed the evaluation and ranking

³ According to Article 38 of the Convention on the Rights of the Child, states are prohibited from conscripting young people under the age of 15. It is especially true in this situation, when the young people used by the Russian Federation were not conscripted into the armed forces, but manipulated to carry out sabotage and intelligence activities in enemy-occupied territory.



ROMANIAN
MILITARY
THINKING

At the end of 2024, Infosecurity Magazine published information according to which the Russian Federation developed attractive games for young people and children in Ukraine (including some under the age of 15), in which they were manipulated to perform sabotage-specific tasks, such as causing fires and directing enemy fire by photographing critical infrastructure elements.



of specific sabotage actions attributed to Ukraine during the war in which it took part, where the risk of the sabotage mission was transferred by the armed forces to third parties.

CONCLUSIONS

Ukraine has carried out a wide range of sabotage missions against the Russian Federation, but they cannot be classified in an absolute manner as moral or immoral, due to the particularities of each case. However, Ukraine's sabotage actions can be assessed by comparison and can be classified into one of the eight levels of morality described above.

Technological evolution has significantly contributed to minimizing the collateral damage caused by sabotage missions, but at the same time, it has increased the freedom of movement of intelligence services, which can carry out recruitment and manipulation activities of saboteurs from a distance. Although technology is integrated into sabotage actions, the human factor is still relevant in the recruitment, planning, targeting and decision-making process.

These aspects reveal the importance and current relevance of the ethics of sabotage both during the mission planning process and in the execution phase, with the conviction that values such as honour and dignity are two of the main characteristics of decision-makers in the military environment.

The ambiguity of the battlefield confirms that the approach to establishing the ethical level of sabotage actions must start from the hypothesis that such a mission falls into the grey area, where the boundary between treacherous and honourable is very sensitive. However, several clear characteristics have been identified that contribute to the inclusion of sabotage in the sphere of morality: (1) Execution of sabotage against an aggressor. (2) Prevention of a greater evil. (3) Compliance with LoAC&IHL and (4) Lack of manipulation in the recruitment process of a saboteur.

In order for a sabotage action to approach a maximum ethical quotient, it is necessary that the mission respects all four characteristics mentioned above. Otherwise, sabotage involves a moral regression and can be classified as treacherous, immoral or dishonourable for the saboteur.

We consider that this work has achieved its main objectives, those of clarifying the relevance of ethics in sabotage missions in relation to the current war in Ukraine and, moreover, of providing some clear directions for evaluating the morality of these missions.

BIBLIOGRAPHY:

1. ABC News (2023). *Russian rebellion timeline: How the Wagner uprising against Putin unfolded and where Prigozhin is now*, <https://abcnews.go.com/International/wagner-groups-rebellion-putin-unfolded/story?id=100373557>, retrieved on 8 January 2025.
2. Aljazeera (2024). *Russian court jails woman for 27 years over killing of pro-Kremlin blogger*, <https://www.aljazeera.com/news/2024/1/25/russian-court-jails-woman-for-27-years-over-killing-of-pro-kremlin-blogger>, retrieved on 15 January 2025.
3. BBC (2024). *General killed in Moscow a legitimate target, says Ukraine*, <https://www.bbc.com/news/articles/cm2ek388yxzo>, retrieved on 15 January 2025.
4. CIA (2015), <https://www.cia.gov/stories/story/surprise-kill-vanish-the-legend-of-the-jedburghs/>, retrieved on 22 January 2025.
5. CNN World (2024). *Russia opens criminal cases after protesters pour dye in ballot boxes and start fires with voting underway*, <https://edition.cnn.com/2024/03/15/europe/russia-elections-protests-dye-intl/index.html>, retrieved on 15 January 2025.
6. Erskine, T. (2004). *As Rays of Light to the Human Soul – Moral Agents and Intelligence Gathering*. *Intelligence and National Security*, vol. 19, no. 2. pp. 359-381, https://www.academia.edu/8388903/As_Rays_of_Light_to_the_Human_Soul_Moral_Agents_and_Intelligence_Gathering, retrieved on 10 January 2025.
7. Frisk, R., Johansson, L. (2020). *From Samurais to Borgs: Reflections on the Importance of Intelligence Ethics*. *International Journal of Intelligence and Counter Intelligence*, DOI: 10.1080/08850607.2020.1734768, https://www.researchgate.net/publication/340611380_From_Samurais_to_Borgs_Reflections_on_the_Importance_of_Intelligence_Ethics, retrieved on 10 January 2025.
8. Infosecurity magazine (2024). *Russia Recruits Ukrainian Kids for Sabotage and Reconnaissance*, <https://www.infosecurity-magazine.com/news/russia-recruits-ukrainian-children/>, retrieved on 15 January 2025.
9. Kyivpost (2023). *Partisans Kill 24 Russian Soldiers with Poisoned Treats*, <https://www.kyivpost.com/post/25019>, retrieved on 15 January 2025.



Technological evolution has significantly contributed to minimizing the collateral damage caused by sabotage missions, but at the same time, it has increased the freedom of movement of intelligence services, which can carry out recruitment and manipulation activities of saboteurs from a distance.



10. Litvinov, N.D., Sal'Nikov, M.V., Lavrov, O.L., Mironov, I.K., Nagirnyak, Yu.I., Ovchinnikov, V.V. (2022). *National Political Forces of Ukraine as a source of threats of sabotage and terrorist activities on the territory of Russia*. Saint-Petersburg: Legal science: history and the presence.
11. Neculcea, C. (2020). *Generațiile războaielor – Convențional și neconvențional în evoluția războaielor*. In *Gândirea militară românească*, no. 2. București: Statul Major al Apărării.
12. NPR (2022). *The daughter of 'Putin's brain' ideologist was killed in a car explosion*, <https://www.npr.org/2022/08/21/1118666607/daria-dugina-car-blast-daughter-putin-ally>, retrieved on 15 January 2025.
13. Radio Free Europe (2022). *Ukraine's SBU Claims Responsibility for October Crimea Bridge Blast*, <https://www.rferl.org/a/ukraine-sbu-crimea-bridge-blast/32521472.html>, retrieved on 15 January 2025.
14. Radio Free Europe (2024). *Appeal by Woman Imprisoned for Killing Pro-Kremlin Blogger Rejected*, <https://www.rferl.org/a/trepova-appeal-murder-pro-kremlin-blogger-rejected/32955007.html>, retrieved on 15 January 2025.
15. Richterova, D., Grossfeld, E., Long, M., Bury, P. (2024). *Russian Sabotage in the Gig-Economy Era*. In *The RUSI Journal*, vol. 169, no. 5. pp. 10-21, <https://www.tandfonline.com/doi/epdf/10.1080/03071847.2024.2401232?needAccess=true>, retrieved on 25 December 2024.
16. Rønn, V.K. (2016). *Intelligence Ethics: A Critical Review and Future Perspectives*. *International Journal of Intelligence and Counter Intelligence*, 29:4, pp. 760-784, https://www.researchgate.net/publication/303948883/Intelligence_Ethics_A_Critical_Review_and_Future_Perspectives, retrieved on 22 January 2025.
17. The Interpreter (2024). *Why Russia has only now declared war on Ukraine*, <https://www.lowyinstitute.org/the-interpreter/why-russia-has-only-now-declared-war-ukraine>, retrieved on 7 January 2025.
18. The new voice of Ukraine (2024). *Partisan sabotage cripples Russian rail supply*, <https://english.nv.ua/russian-war/partisan-sabotage-in-zaporizhzhya-disrupts-russian-supply-lines-to-the-front-50467140.html>, retrieved on 15 January 2025.
19. The Telegraph (2022). *Russian-appointed Kherson mayor 'was poisoned by chef'*, <https://www.telegraph.co.uk/world-news/2022/08/07/russian-appointed-kherson-mayor-poisoned-chef/>, retrieved on 15 January 2025.
20. UNICEF (1989). *Convention on the Rights of the Child*. General Assembly resolution 44/25 of 20 November 1989, <https://www.unicef.org/child-rights-convention/convention-text>, retrieved on 15 January 2025.

21. United Kingdom National Cyber Security Centre (2022). *Russia behind cyber attack with Europe-wide impact an hour before Ukraine invasion*, <https://www.ncsc.gov.uk/news/russia-behind-cyber-attack-with-europe-wide-impact-hour-before-ukraine-invasion>, retrieved on 4 January 2025.
22. US Department of the Army (2013). ATP 3-05.1. *Unconventional Warfare*. Washington D.C.
23. US Department of the Army (2014). FM 3-24 MCWP 3-33.5. *Insurgencies and countering insurgencies*. Washington D.C.
24. US Department of the Army (2019). FM 6-27/MCTP 11-10C. *The commander's handbook on the law of land warfare*. Washington D.C.
25. US Department of the Army (2021). ATP 3-05.1. *Unconventional Warfare*. Washington D.C.
26. Walzer, M. (1977). *Just war and unjust wars*. Basic Books: New York.
27. <https://abcnews.go.com/International/wagner-groups-rebellion-putin-unfolded/story?id=100373557>, retrieved on 22 January 2025.
28. <https://www.lowyinstitute.org/the-interpreter/why-russia-has-only-now-declared-war-ukraine>, retrieved on 22 January 2025.

