The Impact of Non-State Actors on Security: Insights from the War in Ukraine

Daniela Irrera*

Abstract

The war in Ukraine, which began in 2014 and escalated in 2022, has showcased contemporary warfare strategies that have been observed and adopted by non-state armed groups (NSAGs), including insurgents, paramilitaries, and mercenaries. The relationship between terrorism, organised crime, and non-state armed actors (NSAAs) has been analysed as a strategic means of exploiting illicit markets. This relationship is primarily evident in failed and fragile states, where it is used to profit from war, technology, and the cyber environment. This chapter analyses the impact of NSAAs on the global security agenda, particularly in light of technological advances. It argues that this impact has significantly changed since the war in Ukraine, representing a new threat capable of challenging security dynamics at regional and global levels.

Introduction

The conflict in Ukraine has marked a turning point in international dynamics and in the European defence agenda, by demonstrating modern warfare tactics that could be adopted by various actors, including non-state ones. The latter can be broadly defined as individuals or entities that do not officially represent a government, yet possess significant political, social, and economic influence (Mullins, 2024). Non-state armed actors include terrorists, insurgents, contractors, foreign fighters, mercenaries, and organised crime groups.

This chapter analyses the impact of NSAAs on the global and European security agenda in light of technological advances. In particular, it argues that the impact has changed significantly after the beginning of Russia's aggression war in Ukraine, representing a renewed threat. Non-state

* Daniela Irrera is a Professor of International Relations at the Centre for Higher Defence Studies (CASD) in Rome, Italy.

actors are often employed by states to exert malign influence. However, their autonomous capacity to develop an agenda and pursue a strategy is increasing rapidly. According to the ACLED Conflict Index, political violence has significantly increased and become highly diversified if compared to the period five years ago, mostly due to the new phase of the conflict in Ukraine. The number of civil wars has decreased, and they are replaced by hostilities perpetrated by local militias, rebels, or groups with a national agenda (ACLED, 2024).

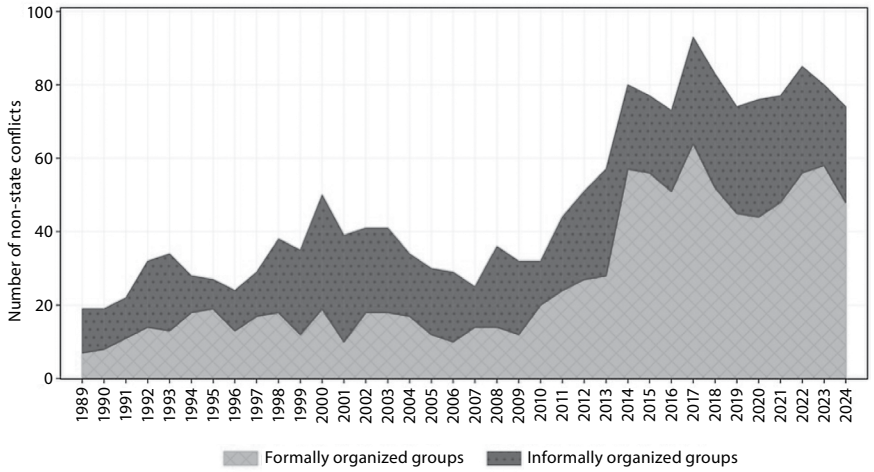

Fig. 1. Non-state conflicts by organizational level of the warring sides (1989–2024). Based on UCDP 25.1 data.

According to the UCDP data, the number of conflicts which are escalated by non-state actors increases and introduces serious concerns in security dynamics. A non-state conflict is defined by UCDP as 'the use of armed force between two organised armed groups, neither of which is the government of a state, which results in at least 25 battle-related deaths in a year', and, as shown in *Fig. 1*, escalation can be initiated by formally or informally organised groups. In that regard, the latter (primarily terrorist groups) are the more active.

This poses a significant threat to global security, prompting states to develop the necessary capabilities and responses. Since Europe has been constantly targeted by terrorists, it has extensively worked on developing

strategies to tackle the root causes of conflicts and political violence, although most efforts have focused on deradicalisation policies and measures against violent extremism.

Why are Non-State Armed Actors Increasing Their Power?

Studies on terrorism and organised crime, and their interrelations – the so-called "crime-terror nexus" – have been at the forefront of producing theoretical and empirical insights in the scholarly community of International Relations and security studies (Ljujic, van Prooijen, and Weerman, 2017; Felbab-Brown, 2019; Makarenko, 2021; Carrapico, Irrera, and Tupman, 2014; Irrera, 2016). These studies have focused on criminals and terrorists, actors that, despite having different identities, goals, and methods, may share common ground and objectives, converge and establish connections (Makarenko, 2021). Since they are non-state actors, the studies have also covered literature on the nature and modus operandi of non-state actors. Discussions of the environments in which NSAAs operate in, their interactions with other subversive actors, and their impact on conflict zones, can help us understand how they develop and what countermeasures are needed.

Post-Cold War terrorist groups such as al-Qaeda and Islamic State (IS) appear to be sophisticated organisational networks combining largely autonomous cells and structures (Hutchinson and O'Malley, 2007). They are more likely to engage in crimes such as drug smuggling, money laundering, and extortion; however, they do not consider themselves to be common criminals (Hoffman, 2006). Drug trafficking is the largest source of income for organised crime groups and terrorists along with robbery, extortion, kidnapping, arms trafficking, and smuggling. Such activities require extensive organisational capabilities and are therefore more likely to be carried out by structured terrorist groups than by individuals or isolated cells.

Consequently, advances in technology are perceived necessary in this transformation (Hutchinson and O'Malley, 2007). Markets and services offered in the cyber environment have expanded on a transnational scale, producing benefits for subversive actors as well. Although they remain different in their nature and agenda, terrorist groups have adopted new structural forms that are similar to those of organised crime syndicates. Terrorist groups are increasingly using decentralised financial tools, such

as cryptocurrencies, to evade financial control, launder money, and fund their operations. Technology plays a major role in activities carried out by terrorists and has shaped their performance. Terrorist groups use cyber capabilities to launch attacks, steal financial assets, identify targets, recruit individuals more effectively, and plan attacks by gaining the upper hand over their adversaries (Musotto and Wall, 2020). Also, they use technology to build up links with other actors such as insurgents, paramilitary groups, and private military companies (Sullivan and Bunker, 2014; Jones and Johnston, 2013). This can occur in troubled and conflict-ridden environments, because they provide an ideal opportunity for subversive actors to flourish. When terrorists and organised criminal groups are active and well-established, closer cooperation and consolidation between them is more likely to happen (Kalyvas, 2015; do Céu Pinto Arena, 2022; Irrera, 2024).

Unstable conditions can be observed in states affected by political, economic, or social weaknesses. In these states, competitive illicit markets are largely or entirely controlled by organised crime syndicates (Alesina, Piccolo and Pinotti, 2019; Petrich, 2021). This facilitates strategic alliance between criminals and terrorists, but also with other armed groups (e.g., insurgents). The lines between different actors become obscured and they engage in various illegal and violent activities. Contemporary conflicts, such as the war in Ukraine, can offer powerful examples.

The Impact of the War in Ukraine on NSAAs' Performance

The military escalation in Ukraine has had a significant impact on the activities of NSAAs, such as, the increased likelihood of forming alliances and the extent of cooperation in terms of funding sources, recruitment of personnel, and the increased usage of technology.

Regarding the funding, conflict zones provide an ideal context for illicit trafficking. This was observed during the wars in the Balkans or in Africa. In these contexts, alliances among local groups expanded access to more sophisticated weapons and logistical support (Feinstein and Holden, 2014; Tan, 2023). Even in Ukraine, the influx of weapons has been substantial. Initially, these flows of arms have benefitted criminals as well, but this could also be potentially beneficial for terrorist groups further afield. Financial institutions and the ease with which officials can be corrupted or regulatory systems weakened remain a related vulnerability. In the case of a war of

aggression, both Russia and Ukraine have drawn upon decentralised financial instruments to fund their military operations, particularly local volunteer units. The war of aggression has also affected some processes for the recruitment of fighters, mainly foreigners. Both Ukraine and Russia have attracted fighters from different parts of the world who are motivated by ideology, nationalism, or a desire to engage in mercenary work.

More generally, terrorist groups have long recruited foreign fighters. New models of cross-border recruitment have been developed, especially for individuals without formal affiliation. Rather than pursuing ethnonationalist or extremist ideologies, separatism, or changes to government structures, groups often have global aspirations, with the goal to influence global governance (Rocha, 2019). These foreign fighters bring combat skills, but also links to international criminal networks, further blurring the lines between terrorism and organised crime. Additionally, some of them have returned home with enhanced combat skills and connections to criminal networks, which could potentially fuel terrorism in other regions (Kaunert, MacKenzie, and Léonard, 2023; de Roy and Bakker, 2023).

The war has also informed and honed the modus operandi of many of these actors. For example, following the collapse of the ISIS caliphate, many organisations have adopted a decentralised model. These autonomous cells carry out attacks with little oversight, making them harder to disrupt. This tactic has been adopted by groups across Europe, the Middle East and Africa, but also by the fighting parties in Ukraine, where numerous groups have started to operate in the same manner, particularly in the early stages (Pearson, Akbulut and Lounsbery, 2017). The absence of centralised command structures has made interactions amongst criminals and other armed groups easier. As much of the fighting in Ukraine has taken place in urban areas, with both sides using civilian infrastructure for cover, terrorist groups increasingly engaged in urban warfare can adopt similar tactics. For example, they have adopted tactics involving embedding fighters among the civilian population to deter direct military strikes or exploit civilian casualties for propaganda purposes. Many of these tactics have been designed and implemented by cyber warfare and the increasing usage of technology (Irrera, 2025). For example, according to some reports, in Kherson City and Antonivka, Russian units used civilians as targets for 'live training exercises' (Stewart, 2025).

Some specific trends have been observed, although it is difficult to measure them empirically. Firstly, the 'improvisation' of techniques and tools

has been a constant feature of terrorist groups operating in conflict zones, due to precarious local conditions and uncertainty surrounding cooperation with other local actors (Bendett et al., 2020). In Ukraine, this practice has evolved, becoming more professional and consolidated. Secondly, the 'weaponisation' of tools, such as surveillance drones and their deliberate use in a hostile or aggressive manner to achieve political or military objectives has increased (Riemer and Sobelman, 2023).

The conflict in Ukraine has popularised the use of commercial drones for surveillance and combat purposes, with the Ukrainian and Russian militaries and irregular forces having used drones to target enemy positions. Terrorist groups, such as IS and others in the Middle East and North Africa, are learning to use drones for reconnaissance and attack purposes, having also adopted them for similar purposes. They are used for surveillance to gather intelligence on enemy positions and thus, weaponised to drop explosives on certain targets. Alongside drones, the 'de-improvisation' process involves guerrilla tactics, such as ambushes and hit-and-run operations to target Russian convoys and positions. Armed groups use more sophisticated remote detonation and placement techniques. They also reinforce civilian vehicles with makeshift armour and weapon mounts to create more mobile and protected platforms of attack. Both features can be seen when cyberspace is transformed into a domain of conflict and warfare, and where information technology is used as a weapon to cause harm by disabling critical infrastructure, stealing sensitive data, and spreading disinformation (Mathur, 2025). Cyber warfare has been used intensively by both Ukrainian and Russian forces (and their proxies) to target each other's important infrastructure, communications, and databases. However, it has also become a crucial tool for both state and non-state actors. Criminal groups, often with links to the Russian government, have launched cyber-attacks with the aim to destabilise Ukraine and its allies. Terrorist groups have moved into the cyber domain, targeting state infrastructure, banks, and other institutions to create chaos and weaken governments. They also use cyber capabilities to spread propaganda or recruit new members. The complex security situation and uncertain economic conditions, along with emerging challenges such as hybrid warfare, cyber threats and terrorism, could prompt NATO and the EU to cooperate more closely (Holt, 2012).

The Effects on Security Cooperation

The global political system is entering into a new phase of increased cooperation among NSAAs. The fluid and dynamic nature of modern conflicts, exemplified by the ongoing war in Ukraine, provides an arena in which asymmetric warfare strategies can be developed and adopted by non-state actors, including terrorist and criminal groups. This war has introduced innovations in a variety of tactics, such as drone warfare, cyber operations, urban warfare, and decentralised structures. Many of them could be adapted for use in terrorist attacks around the world. Criminal networks facilitate the flow of weapons, illicit goods, and finances that support both state and non-state actors in conflicts. Meanwhile, terrorist organisations are increasingly adopting technological advances in cyber warfare, propaganda and surveillance. Criminals and terrorists have consolidated relations with other violent local non-state actors and identified additional channels for recruiting new fighters. This is not necessarily linked to ideology or extremism, but to the use of contractors, and improved sources of funding. The practices deployed in Ukrainian battlefields have provided an ideal context for the testing and consolidating of new tools and practices. Notably, the war has demonstrated to terrorists, criminals, and other NSAAs how emerging technologies can enhance the use of drones, vehicles and weapons, as well as how the cyber environment can facilitate illicit activities to fund warfare. This will inevitably have implications for regional security, as well as for NATO's counterstrategy and relations with its allies.

Various scenarios could develop in the future regarding these developments, and while the EU has taken steps to strengthen its defence cooperation, it would be difficult to succeed in the face of renewed and multivector security threats. Thus, NATO's role as a substructure within a broader global defence alliance comprising Western states and those that support the West is crucial. The coordination between EU defence policy and expanded NATO structures would depend largely on the specific institutional arrangements and agreements between these entities. The precise nature and extent of this coordination would require detailed negotiations between the relevant parties. To this point, the necessity of containing Russia or protecting against a potential Russian attack cannot be the only basis for shaping European defence. The EU must strengthen its security agenda and capacity in order to address the evolving security landscape and prepare for all other potential threats.

Works Cited

ACLED (2024) Conflict Index. Available at: https://acleddata.com/series/acled-conflict-index.

Alesina, A., Piccolo, S. and Pinotti, P. (2019) "Organized crime, violence, and politics, " *The Review of Economic Studies*, *86*(2), pp. 457–499.

Bendett, S., Blank, S., Cheravitch, J., Petersen, M. B., Turunen, A., and Mankoff, J. (2020) "Improvisation and Adaptability in the Russian Military," Centre for Strategic and International Studies, pp. 38.

Carrapico, H., Irrera D. and Tupman B. (2014) "Transnational Organised Crime and Terrorism: different peas, same pod?," *Double Special Issue of Global Crime*, 15(3–4), pp. 203–218.

de Roy van Zuijdewijn, J. and Bakker, E. (2023) "Twenty years of countering jihadism in Western Europe: from the shock of 9/11 to 'jihadism fatigue'," *Journal of Policing, Intelligence and Counter Terrorism*, 18(4), pp. 421–434.

do Céu Pinto Arena, M. (2022) "The Impact of Ethnic Groups on International Relations," in Charountaki, M. and Irrera, D. (eds.) *Mapping Non-State Actors in International Relations*. Springer International Publishing, pp. 73–94.

Felbab-Brown, V. (2019) "The crime-terror Nexus and its fallacies," in Chenoweth, E. (ed.) *The Oxford handbook of terrorism*. Oxford University Press, pp. 366–383.

Feinstein, A. and Holden, P. (2014) "Arms trafficking," in Paoli, L. (ed.) *The Oxford handbook of organized crime*. Oxford University Press, pp. 444–59.

Hoffman, B. (2006). *Inside terrorism*. Columbia University Press, pp. 1–432.

Holt, T. J. (2013) "Exploring the social organisation and structure of stolen data markets," *Global Crime*, *14*(2–3), 155–174.

Hutchinson, S. and O'Malley, P. (2007) "A Crime–terror Nexus? Thinking on Some of the Links between Terrorism and Criminality," *Studies in Conflict Terrorism*, 30(12), pp. 1095–1107.

Jones, S. G. and Johnston, P. B. (2013) "The future of insurgency," *Studies in Conflict and Terrorism*, 36(1), pp. 1–25.

Kalyvas, S. N. (2015) "How Civil Wars Help Explain Organized Crime – and How They Do Not," *Journal of Conflict Resolution*, 59(8), pp. 1517–1540.

Kaunert, C., MacKenzie, A. and Léonard, S. (2023) "Far-right foreign fighters and Ukraine: A blind spot for the European Union?," *New Journal of European Criminal Law*, 14(2), pp. 247–266.

Irrera, D. (2016) "The crime-terror-insurgency 'nexus'. Implications on multilateral cooperation," in Romaniuk, S. (ed.) *Insurgency and Counterinsurgency in Modern War*. CRC Press, pp. 39–52.

Irrera, D. (2025) "How have Terrorists Adopted Tactics from the Russia-Ukraine War? The Crime-Terror-Tech Nexus," in Sadik, G. (ed.) *The Effects Of The Russia-Ukraine War On Countering Terrorism*. Centre of Excellence Defence Against Terrorism, pp. 67–78.

Ljujic, V., van Prooijen, J.W. and Weerman, F. (2017) "Beyond the crime-terror nexus: socio-economic status, violent crimes and terrorism," *Journal of Criminological Research, Policy and Practice*, 3(3), pp. 158–172.

Makarenko, T. (2021) "Foundations and evolution of the crime–terror nexus," in Allum, F., Gilmour, S. (eds.) *The Routledge Handbook of Transnational Organized Crime*. Routledge, pp. 253–269.

Mathur, R. (2025) "Techno-Capitalism and weaponisation of cyberspace," *Global Studies Quarterly*, 5(2). Available at https://doi.org/10.1093/isagsq/ksaf031.

Morcos, P. and Simón, L. (2022) "NATO and the South after Ukraine," *Centre for Strategic and International Studies (CSIS)*, pp. 1–5.

Mullins, S. (2024) "The Role of Non-State Actors as Proxies in Irregular Warfare and Malign State Influence," *Irregular Warfare Centre*, pp. 1–25.

Musotto, R. and Wall, D. S. (2020) "More Amazon than Mafia: analysing a DDoS stresser service as organised cybercrime," *Trends in Organized Crime*, pp. 1–19.

Pearson, F. S., Akbulut, I. and Olson Lounsbery, M. (2017) "Group Structure and Intergroup Relations in Global Terror Networks: Further Explorations," *Terrorism and Political Violence*, 29(3), pp 550–572.

Petrich, K. (2021) "The crime–terror Nexus," in *Oxford Research Encyclopedia of International Studies*.

Riemer, O. and Sobelman, D. (2023) "Coercive disclosure: The weaponisation of public intelligence revelation in international relations," *Contemporary Security Policy*, 44(2), pp. 276–307.

Rocha, I. M. (2019) "Global system dynamics in the relationships between organized crime and terrorist groups," in Ruggiero, V. (ed.) *Organized Crime and Terrorist Networks*. Routledge, pp. 100–116.

Stewart B. (2025) "Ukrainians in Kherson survived Russia's occupation. Now, they're being hunted by drones," *CBC in Ukraine*. Available at https://www.cbc.ca/news/world/ukraine-kherson-attack-drones-1.7443615.

Struwe, L. B. , et al. (2014) "The Ukraine crisis and the end of the Post-Cold War European order: options for NATO and the EU," *Centre for Military Studies*, University of Copenhagen, https://cms.polsci.ku.dk/english/publications/ukrainecrisis/.

Sullivan, J. P. and Bunker, R. J. (2014) "Multilateral counter-insurgency networks," in Bunker, R. J. (ed.) *Networks, terrorism and global insurgency*. Routledge, pp. 183–198.

Tan, A. T. H. (2023) "Global Arms Trade," in Williams, P. D. and McDonald, M. (eds.) Security Studies. Routledge, pp. 535–551.