Кострікова Анна Юріївна,
здобувачка першого (бакалаврського) рівня вищої освіти факультету комп'ютерних наук Харківського національного університету радіоелектроніки, м. Харків

HYBRID WARFARE IN THE 21ST CENTURY: HISTORICAL CONTINUITY AND CONTEMPORARY THREATS

The concept of hybrid warfare has become a key term in both academic discourse and global political discussions over the past two decades. Although widely associated with recent conflicts, hybrid warfare has clear historical roots that reflect an enduring pattern of combining conventional, irregular, informational, and cyber tactics to achieve military and political goals. In the context of 21st-century global security challenges, hybrid warfare represents not only a method of aggression but a comprehensive strategy aimed at destabilizing societies, manipulating public opinion, and undermining state sovereignty [5, p. 25].

Historically, elements of hybrid warfare can be traced back to ancient and medieval conflicts where psychological operations, espionage, and insurgencies complemented battlefield tactics. However, the modern notion of hybrid warfare gained prominence following the 2006 Israel-Hezbollah conflict, where Hezbollah combined guerrilla warfare, information operations, and conventional tactics [3, p. 44]. This form of conflict was further refined in the Russo-Georgian War (2008) and reached its apex in Russia's annexation of Crimea in 2014, where unmarked troops, information manipulation, and cyberattacks blurred the line between war and peace.

The defining characteristic of hybrid warfare is its multidimensionality. It includes:

- Traditional military force;
- Proxy actors and insurgent groups;
- Disinformation campaigns via mass media and social networks;
- Cyber operations targeting critical infrastructure;
- Economic pressure and lawfare (manipulation of legal systems for strategic gain).

These tools are not used independently but in synchronization, creating a "fog of ambiguity" that complicates the response of target states. For instance, the use of cyberattacks against power grids combined with

disinformation about government failure can rapidly degrade public trust and social cohesion [4, p. 92].

In contemporary global affairs, hybrid warfare is particularly visible in the actions of authoritarian regimes, most notably Russia and China. Russia's interventions in Ukraine and Syria, China's influence operations in Southeast Asia and beyond, as well as Iran's use of proxy militias, exemplify the transnational nature of hybrid threats [5, p. 29]. Unlike traditional wars, hybrid campaigns are often undeclared, prolonged, and deniable, making them difficult to address through conventional military or diplomatic means.

One of the greatest challenges hybrid warfare presents is the erosion of legal and ethical norms. The lack of formal declarations of war, the use of non-state actors, and manipulation of civilian platforms like media or humanitarian aid complicate international responses and accountability under international law. Moreover, hybrid tactics disproportionately affect civil societies by spreading fear, polarization, and mistrust, often turning democratic freedoms (such as open internet and free speech) into vulnerabilities [6, p. 302].

Ukraine’s experience since 2014 is a central case study. The Russian hybrid strategy has encompassed military invasion, cyberattacks on banking and energy sectors, deepfake videos, troll farms, electoral interference, and support for separatist groups in Donbas. This model of warfare not only seeks territorial control but aims to weaken Ukraine’s institutional legitimacy and integration with Western allies [2, p. 75].

In response, Ukraine and its international partners have developed multi-level countermeasures: establishing cyber defense units, launching strategic communications departments, reforming the security sector, and initiating legal mechanisms for sanctioning foreign actors. NATO and the EU have likewise acknowledged hybrid warfare as a core security threat, emphasizing resilience, intelligence sharing, and digital infrastructure protection [1].

The academic community plays a crucial role in developing frameworks to understand and counter hybrid threats. Interdisciplinary research combining political science, international law, cybersecurity, and communication studies is vital for devising comprehensive defense strategies. In particular, education systems should incorporate media literacy and digital hygiene to enhance societal resilience against hybrid aggression [4, p. 59].

In conclusion, hybrid warfare is not a temporary or peripheral phenomenon — it is a structural challenge of our era. It reflects a shift from industrial warfare to postmodern, information-driven conflict. Addressing it requires not only military preparedness but strategic awareness, legal innovation, and democratic unity. Understanding the continuity between historical tactics and their modern reconfigurations allows societies to better anticipate, resist, and respond to complex security threats of the 21st century.

References

1. European Commission. Joint Framework on Countering Hybrid Threats: A European Union Response. Brussels, 2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52016JC0018

2. Hoffman F. G. Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington: Potomac Institute for Policy Studies, 2007. 75 p.

3. Johnson D. E. Military Capabilities for Hybrid War: Insights from the Israel Defense Forces in Lebanon and Gaza. Santa Monica: RAND Corporation, 2010. 160 p.

4. Pomerantsev P. This is Not Propaganda: Adventures in the War Against Reality. London: Faber & Faber, 2019. 255 p.

5. Renz B., Smith H. Russia and Hybrid Warfare: Going Beyond the Label. *Aleksanteri Papers*. 2016. No. 1. P. 25–40.

6. Umland A. The Donbas Conflict in Ukraine: Elites, Protest, and Partition. Stuttgart: ibidem Press, 2020. 302 p.

Левдер Андрій Іванович,
кандидат педагогічних наук, доцент,
доцент кафедри історії, теорії держави і права та філософії ПВНЗ «Міжнародний економіко-гуманітарний університет імені академіка Степана Дем'янчука», м. Рівне

«МУЗЕЙ МИРУ» СТВОРЕНИЙ СТЕПАНОМ ЯКИМОВИЧЕМ ДЕМ'ЯНЧУКОМ: ЙОГО ЗАВДАННЯ У ВИХОВАННІ МОЛОДІ ТА ПРОПАГАНДИ ІДЕЇ МИРУ

Дем'янчук Степан Якимович народився 30 грудня 1925 р. в селі Орепи Новоград-Волинського району Житомирської області у селянській родині. 19-річний юнак у складі 3-го Білоруського фронту