THE ARCHITECTURE OF AMBIGUITY. ELEMENTS AND EVOLUTION OF RUSSIAN HYBRID WARFARE IN UKRAINE

Cătălin Bucurel BAIU, Daniel ȘTEFĂNESCU

"Henri Coanda" Air Force Academy, Brașov, Romania (catalin.baiu@afahc.ro, daniel.stefanescu@afahc.ro)

DOI: 10.19062/2247-3173.2026.27.2

Abstract: *This study examines Russian hybrid warfare as operationalized in Ukraine between 2013 and 2024, arguing that it represents the most comprehensive and empirically documented case of integrated grey-zone conflict in the contemporary era. Drawing on open-source intelligence reports, security studies scholarship, and legal analysis, the paper analyzes six core dimensions of Russia's hybrid approach: theoretical doctrine, information and cognitive operations, cyber warfare, electronic warfare, unconventional proxy forces, economic coercion, and lawfare.*

The analysis reveals a deliberate strategy of ambiguity — combining plausible deniability with escalation dominance — designed to undermine target-state cohesion, fracture Western alliances, and achieve strategic objectives below the threshold of conventional warfare. Crucially, however, the Ukrainian case also illuminates the conditions under which hybrid strategies can fail: when the target state exhibits 'whole-of-society' resilience and when adversary coercion inadvertently accelerates the opposing coalition's cohesion and capability development.

The paper concludes with implications for NATO posture, democratic resilience, and the evolving character of 21st-century conflict.

.

Keywords: *hybrid warfare, grey-zone conflict, reflexive control, information operations, cyber warfare, electronic warfare, lawfare, energy blackmail, Wagner Group, Ukraine-Russia conflict*

1. INTRODUCTION: THE GREY ZONE AND THE UKRAINIAN CRUCIBLE

The conflict in Ukraine — spanning from the covert destabilization efforts of 2013 through to the full-scale invasion of 2022 and its protracted aftermath — constitutes the preeminent contemporary laboratory for hybrid warfare. No other geopolitical episode of the modern era provides such a rich, sustained, and multidimensional case study of grey-zone competition in action.

Hybrid warfare, situated within the analytical framework of the 'grey zone,' encompasses a spectrum of hostile activities that deliberately operate below the threshold of conventional war. It integrates traditional military force with irregular tactics, cyber operations, information campaigns, economic coercion, and legal manipulation. At its strategic core, the Russian approach seeks to overcome power asymmetries by undermining the internal cohesion of the target state and its international alliances — achieving objectives without initially triggering a unified conventional response from NATO.

Hybrid warfare is not a monolithic technique but an integrated doctrine of continuous pressure.

Russia's strategy in Ukraine illustrates that the battlefield of the 21st century is cognitive as much as physical — waged in the information environment, the electromagnetic spectrum, and courtrooms as much as on the front line.

This study analyzes six interlocking pillars of Russia's approach: theoretical doctrine, information and cognitive warfare, cyber operations, electronic warfare, proxy forces, economic coercion, and the weaponization of law.

It also examines where and why this strategy has failed — offering lessons for democratic resilience in an era of perpetual grey-zone competition.

2. THEORETICAL FOUNDATIONS: THE RUSSIAN WAY OF WAR

The conceptualization of hybrid warfare within the Russian strategic context is deeply rooted in a synthesis of historical experience and modern adaptation. Understanding this theoretical bedrock is essential before examining its operational manifestations.

2.1 The 'Gerasimov Doctrine' and Its Discontents

Western analysts commonly invoke the 'Gerasimov Doctrine' as a prophetic blueprint for the annexation of Crimea and the Donbas war. However, this framing is contested. The Russian strategic perspective frequently characterizes these methods as a defensive response to Western-led 'colored revolutions' and the perceived encroachment of NATO — a form of asymmetric retaliation rather than offensive innovation.

General Valery Gerasimov, Chief of the Russian General Staff, articulated in 2013 that the rules of war had fundamentally changed, with non-military means often exceeding the effectiveness of weapons in their strategic impact. His article, published in the Russian military journal Voyenno-Promyshlennyy Kuryer, was widely — and arguably incorrectly — interpreted in the West as a strategic doctrine rather than a descriptive analysis of NATO's own methods.

This theoretical debate underscores a significant disconnect: what the West views as an offensive Russian innovation, the Kremlin characterizes as the 'Western way of war' that Russia must emulate and counter. This framing enables Moscow to claim moral equivalence while simultaneously deploying the very techniques it decries.

2.2 Non-Linear Warfare and the Blurred Front

This 'new generation' or 'non-linear' warfare emphasizes the promotion of social upheaval and the deliberate creation of a climate of political collapse. Armed force becomes a supplementary tool to finalize a victory already won in the cognitive and political domains. The strategy relies on the blurring of the distinction between war and peace, projecting a 'front' across the entire territory of the adversary rather than a localized physical battlefront.

Historical continuity is vital to understanding this approach. As early as 1584, observers noted that Russian military strength was predicated not merely on force, but on cunning, opportunism, and the intimidation of the adversary. Modern doctrine updates these constants with technology — integrating Soviet-era AGITPROP (agitation and propaganda) with sophisticated cyber capabilities and the theory of reflexive control.

2.3 Reflexive Control: Engineering the Adversary's Decision

The most sophisticated element of the Russian hybrid toolkit is 'reflexive control' — a psychological strategy designed to predetermine an adversary's decision by carefully altering their perception of reality. By feeding the opponent specially prepared information, the initiator induces the target to voluntarily adopt a course of action that serves the initiator's strategic goals.

In the Ukrainian context, reflexive control manifested as a systematic 'softening' of the information environment through narratives portraying the Kyiv government as a threat.

Subsequent military moves could then be framed as defensive or humanitarian necessities, neutralizing potential international coalitions before they could form.

Technique	Mechanism of Action	Intended Strategic Outcome
Distraction	Creating secondary crises or noise to divert attention from the primary objective.	Paralyze adversary decision-making algorithms.
Information Overload	Flooding the information space with contradictory reports to manufacture uncertainty.	Delay international response and sanctions.
Provocation	Inducing a hasty or imprudent response from the target.	Justify escalation as 'self-defense.'
Maskirovka	Concealment of identity and goals through proxies and enforced deniability.	Avoid the legal threshold for an 'armed attack.'

Source: Adapted from multiple security studies analyses of reflexive control theory, including USF Digital Commons and RAND.

3. THE INFORMATION DOMAIN: NARRATIVE AS A WEAPON OF WAR

Information warfare in the Ukraine conflict is treated as a decisive operational domain rather than a mere supporting effort. The Kremlin has systematically integrated psychological pressure, narrative control, and digital disinformation to contest Ukraine's national identity and undermine its sovereignty. This cognitive campaign is directed at four distinct audiences simultaneously: the domestic Russian population, the Ukrainian citizenry, the Western public, and the broader post-Soviet and Global South spheres.

3.1 Core Narratives and the Architecture of Disinformation

Between 2014 and 2024, Russian disinformation was characterized by a relentless offensive designed to sow discord and erode public trust in Ukrainian and Western institutions. The Ukrainian Foreign Intelligence Service's 'White Book 2021' documented how these narratives consistently portray Ukraine as an unstable 'failed state' prone to far-right extremism — messaging intended to suggest that the only solution to Ukraine's instability is a return to the Russian sphere of influence.

The escalation of narrative complexity was especially pronounced in the period immediately preceding the 2022 invasion. Themes such as 'de-Satanization' and accusations of Ukrainian biological and nuclear weapons development were introduced to amplify the sense of existential threat within the Russian domestic information environment.

Narrative Theme	Description	Strategic Intent
De-Nazification	Falsely labeling the Ukrainian government and military as 'Neo-Nazis.'	Justify military intervention as a humanitarian necessity.
Failed State	Highlighting or exaggerating corruption and governance failures.	Discourage Western financial and military assistance.
Genocide	Claiming Ukraine commits genocide against Russian-speaking populations in Donbas.	Provide a legal pretext under international humanitarian law.
Existential Threat	Framing NATO as an aggressor using Ukraine as a proxy against Russia.	Rally domestic support for a 'preventative' war.
Historical Unity	Promoting the thesis that Russians and Ukrainians are 'one nation.'	Erase Ukrainian national identity and justify territorial annexation.

Source: Synthesized from analyses by USF Digital Commons, MDPI, Atlantic Council, and Wikipedia's documentation of disinformation in the Russian invasion of Ukraine.

3.2 The Infrastructure of Disinformation

The dissemination of these narratives relies on a multifaceted, layered infrastructure. State-controlled media outlets such as RT (Russia Today) and Sputnik serve as the formal institutional platforms, while 'web brigades' and troll farms deploy fictitious social media profiles to amplify messages and simulate the appearance of organic public support. The use of a 'Belarusian vector' increased following the contested 2020 Belarusian election, providing an additional conduit for Kremlin propaganda to reach Ukrainian audiences.

3.3 Ukraine's Counter-Narrative Strategy

Ukraine's response has centred on cultivating 'information resilience.' Through institutional reform, strategic communications initiatives, and the mobilization of a volunteer 'IT Army' — comprising cyber specialists, communications professionals, and graphic designers — Ukraine succeeded in debunking viral disinformation and maintaining narrative dominance within its own borders and across much of the Western information space.

4. CYBER WARFARE: PRECISION DISRUPTION AND DATA DESTRUCTION

Cyber operations have been integrated into the Russian hybrid strategy as instruments to destabilize key institutional structures, manipulate information, and degrade national defense capabilities. Ukraine has frequently served as a testing ground — a live-fire laboratory — for sophisticated cyber weapons, with many operations preceding or synchronized with kinetic military movements.

4.1 The Era of Escalating Destruction: 2015–2022

The history of cyberattacks targeting Ukraine reveals a deliberate progression from denial-of-service campaigns to highly destructive wiper malware designed to cause permanent physical and economic damage. This escalatory trajectory should be read as a strategic signal rather than mere opportunism.

- **2015 Power Grid Attack:** The 'Sandworm' group (attributed to GRU Unit 74455) deployed BlackEnergy malware, severing power to approximately 225,000 residents in western Ukraine in December 2015. This constituted one of the first confirmed large-scale cyberattacks against national critical infrastructure, demonstrating the capacity for cyber operations to produce direct, tangible effects on civilian populations.
- **2017 NotPetya Malware:** Originating through a compromised software update to the Ukrainian accounting platform M.E.Doc, NotPetya remains the most destructive cyber operation in recorded history. While disguised as ransomware, it was a 'wiper' engineered to erase data permanently. NotPetya caused an estimated $10 billion in global damages, crippling Ukrainian government systems and spreading to international corporations including Maersk, FedEx, and Merck.
- **2022 Banking and Government DDoS:** On February 15 and 23, 2022, massive distributed denial-of-service attacks targeted PrivatBank, Oschadbank, and the Ministry of Defense — almost certainly designed to generate public panic and institutional disruption in the days immediately preceding the ground invasion.

4.2 Case Study: The Viasat Attack and the Synchronized Opening Salvo

On February 24, 2022 — mere hours before the commencement of the 'special military operation' — a coordinated cyberattack targeted the KA-SAT satellite network operated by Viasat. This operation represents a paradigmatic example of cyber operations synchronized with conventional military action.

Component	Technical Detail / Mechanism
Access Vector	Compromise of a VPN installation in a Turin management center.
Malware Type	'AcidRain' (Wiper) — sharing code with the 2018 VPNFilter campaign, linking it to Sandworm.
Immediate Impact	Disabled thousands of modems in Ukraine, affecting military command and control networks.
Collateral Damage	Disrupted 5,800 wind turbines in Germany and internet access for 30,000 European subscribers.
Strategic Assessment	Intended to interrupt coordination during the initial invasion surge; impact was partially mitigated by landline alternatives.

Source: CyberPeace Institute, Viasat's own KA-SAT incident report, Wikipedia, and ResearchGate analyses.

While Ukrainian officials initially described the Viasat hack as a 'huge loss in communications,' subsequent reporting clarified that landlines remained the primary method for coordinating military operations — averting a total command collapse. Nevertheless, the attack underscored the profound vulnerability of commercial satellite communications in modern warfare, with cascading effects that extended well beyond Ukraine's borders.

4.3 The Wiper Arsenal: A Taxonomy of Destruction

The 2022 invasion witnessed an unprecedented deployment of diverse wiper malware strains, frequently employed in conjunction with 'decoy' ransomware to complicate forensic analysis and obstruct attribution. This taxonomy reveals a systematic, tool-diverse approach to cyber destruction rather than isolated opportunistic attacks.

- **HermeticWiper (FoxBlade):** Detected on February 23, 2022, targeting hundreds of systems across financial, defense, and IT sectors. It abused legitimate drivers to bypass security features and corrupted the Master Boot Record (MBR), rendering systems unbootable.
- **IsaacWiper:** Launched on February 24 against government systems concurrently with the ground invasion — a second simultaneous attack vector designed to overwhelm response capacity.
- **CaddyWiper:** Detected in March 2022 and engineered to damage systems while preserving the attacker's own access to the network — enabling sustained espionage alongside destruction.
- **PathWiper:** A 2024 discovery targeting critical infrastructure by compromising legitimate endpoint administration tools, allowing attackers to mimic administrative commands and evade behavioral detection.

5. ELECTRONIC WARFARE: CONTESTING THE ELECTROMAGNETIC SPECTRUM

Electronic warfare (EW) occupies a central position in Russian military doctrine, viewed as an asymmetric tool to offset the technological advantages of the West. Russia has consistently invested in EW modernization since 2009, deploying systems across tactical, operational, and strategic levels.

5.1 Strategic Jamming and UAV Neutralizations

The reliance of modern military forces on GPS, cellular networks, and wireless communications has made EW a pivotal — and frequently underreported — element of

the Ukraine conflict. Russian forces deploy sophisticated systems to disrupt command-and-control infrastructure and degrade the effectiveness of Ukrainian drone operations, which have been a decisive asymmetric capability for Kyiv.

EW System	Strategic Function	Primary Targets
Krasukha-4	Wide-range radar jamming up to 300km.	Airborne/space-based radar and intelligence satellites.
Borisoglebsk-2	Core system for detecting and suppressing radio emitters.	Communications channels and GPS-dependent systems.
Leer-3	Mobile phone signal disruption via Orlan-10 drone relay.	Cellular networks; used to geolocate and disrupt troop clusters.
Zhitel	Detection and location of ground/airborne signals.	Ground radio signals and aircraft communications.
Repellent-1	Protection against small drone swarms.	Radio frequency control and UAV data transmission links.

Source: ICDS, CLAWS, Kyiv Post analysis, Army Technology, and Wikipedia.

5.2 Tactical Adaptation: The Rise of 'Trench EW'

After sustaining initial reverses owing to the unwieldiness and poor coordination of large EW formations, Russian forces consolidated their capabilities along demarcated frontlines. This tactical evolution gave rise to the phenomenon of 'trench electronic warfare' — compact, automated devices positioned in field fortifications to create localized 'no-fly' zones for Ukrainian first-person-view (FPV) drones.

In a striking counter-adaptation, Russian forces began experimenting with 'wired' or optical fiber drones to bypass electronic interference entirely — essentially reverting to a pre-electronic command method to defeat electronic countermeasures. This adaptive cycle illustrates the dynamic, iterative character of hybrid warfare technology.

5.3 EW as a Psychological Instrument

EW in the Russian hybrid strategy functions not merely as a technical instrument but also as a psychological one. By exploiting access to soldiers' personal communications, Russian forces disseminate disinformation and propaganda directly to Ukrainian troops — a practice consistent with the Soviet-era tradition of psychological operations directed at enemy combatants. The capacity to contest the electromagnetic spectrum enables Russia to generate effects that transcend the conventional battlefield, extending into societal stability through the disruption of civilian telecommunications.

A hallmark of the 2014–2022 period was the systematic use of unconventional forces to achieve strategic objectives while maintaining plausible deniability. This strategy complicated the international legal and political response, challenging traditional definitions of 'armed attack' under international law and creating a deliberate gap between political will and legal obligation.

6. THE 'LITTLE GREEN MEN' AND THE CAPTURE OF CRIMEA

The term 'little green men' denotes the masked Russian military personnel in unmarked green uniforms who seized strategic points in Crimea in February and March 2014. These troops — identified as members of the Special Operations Forces and Spetsnaz GRU — occupied airports, military bases, and the Crimean parliament building.

President Putin initially claimed these were 'local self-defense units,' a characterization he subsequently retracted following the completion of the annexation.

This tactic was a classic application of maskirovka (concealment/deception) - intended to give the Kremlin time to create a 'fait accompli' on the ground before an international response could coalesce. The speed and precision of the operation, combined with the deliberate absence of insignia, exploited the gap between the speed of military action and the ponderous pace of international legal and diplomatic response.

6.1 The Wagner Group: Privatizing Hybrid Warfare

The Wagner Group represents the commercialization and privatization of Russian hybrid warfare capability. Operating as a private military company (PMC) in a legally ambiguous space under Russian constitutional law, Wagner provided the state with a flexible offensive capability deployable without public accountability or formal acknowledgment of casualties.

- **Foundational Stage (2014):** Wagner first appeared during the annexation of Crimea and the subsequent war in Donbas, serving as a deniable force for 'special' operations that required separation from official state structures.
- **Expansion and Diversification:** By the 2022 invasion, Wagner's role had evolved from a small covert unit into a major assault force, recruiting up to 50,000 personnel including Russian prison inmates offered pardons in exchange for service.
- **Strategic Utility Beyond Ukraine:** Wagner has been deployed to support pro-Russian regimes in Syria and across Africa, securing mining contracts for Russian state-linked companies in exchange for security services — effectively funding its own operations.
- **The 2023 Rebellion:** The Wagner mutiny highlighted the systemic risks of utilizing powerful non-state proxies. The group's leadership openly challenged the Russian Ministry of Defense, revealing the inherent fragility of hybrid actors that become too powerful to control.

7. ECONOMIC HYBRID WARFARE: ENERGY BLACKMAIL AND TRADE COERCION

Russia has a well-documented history of deploying its vast energy resources as a coercive geopolitical instrument. This strategy — broadly defined as energy blackmail — entails the deliberate manipulation of energy supplies for political or economic leverage. Moscow's 2003 Energy Strategy explicitly identified energy resources as an 'instrument for conducting domestic and foreign policy,' formalizing a practice that had long been implicit in Russian statecraft.

7.1 Mechanisms and Historical Pattern of Energy Coercion

- **Gas Shut-offs (2006, 2009):** Russia cut off gas exports to Ukraine during pricing disputes, forcing rationing in EU countries including Bulgaria. These were widely interpreted as political moves against Ukraine's pro-Western 'Orange Revolution' government — using energy as a political penalty rather than a commercial instrument.
- **Nord Stream Pipeline Strategy:** The construction of Nord Stream 1 and 2 was designed to route Russian gas directly to Western Europe while bypassing Ukrainian territory, eliminating a critical structural deterrent against Russian military action — since any attack on Ukraine would have previously disrupted transit revenues that Western Europe depended upon.

- **Pre-Invasion Supply Reduction (2021):** In the summer and autumn of 2021, Russia limited gas supplies to Europe and blocked coal shipments to Ukraine, citing 'technical problems.' This was a calculated move to lower European gas storage levels before the onset of winter — weakening the economic resilience of potential sanctions coalitions before the invasion.
- **Black Sea Blockades (2022):** The 2022 invasion transformed the Black Sea into a central theater of economic conflict. Russia utilized its naval presence to disrupt Ukrainian agricultural exports, threatening global food security — particularly for food-importing nations in Africa and the Middle East — and internationalizing the conflict's consequences.

7.2 The Strategic Miscalculation: Europe's Green Acceleration

While energy blackmail was intended to fracture European support for Ukraine, it produced a significant unintended consequence: it dramatically accelerated the EU's energy transition and diversification strategy. The 'RePowerEU' plan and the rapid decision to ban most Russian fossil fuels successfully neutralized Moscow's primary economic lever — though not without significant initial price shocks for European households and industries.

8. LAWFARE: THE WEAPONIZATION OF LEGAL NORMS

Lawfare — the strategic instrumentalization of law as a weapon of conflict — constitutes an integral component of the Russian approach. It involves the manipulation of international legal principles to justify aggression while simultaneously using the diplomatic legitimacy of international agreements to prepare conditions for future military conflict.

8.1 The Minsk Agreements as a 'Trojan Horse'

The Minsk I (2014) and Minsk II (2015) agreements were ostensibly designed to end the conflict in eastern Ukraine. In practice, however, they functioned as instruments of 'compliance-leverage disparity lawfare' — a legal mechanism through which Russia extracted Ukrainian concessions while shirking its own obligations.

- **Claiming Non-Party Status:** Although a signatory, Russia argued it was a 'facilitator' and not a party to the conflict, thereby avoiding obligations (such as withdrawal of foreign forces) while pressuring Ukraine to grant autonomy to the Donbas.
- **Manipulating Sequencing:** Russia insisted on holding elections in occupied Donbas before Ukraine reclaimed control of its border — a sequence that would have fractured Ukrainian sovereignty and installed pro-Russian administrations within the Ukrainian constitutional system.
- **Creating a Casus Belli:** In February 2022, Putin recognized the independence of the 'Luhansk and Donetsk People's Republics,' asserting that Ukraine's alleged refusal to implement Minsk necessitated this action — cynically exploiting the legitimacy of Western-brokered agreements to justify an unlawful invasion.

8.2 Strategic Litigation and the Limits of Lawfare

In response to Russian lawfare, Ukraine engaged in its own 'strategic litigation' at the International Court of Justice (ICJ). In Allegations of Genocide (Ukraine v. Russia), Ukraine advanced the innovative legal argument that Russia was abusing the Genocide Convention by deploying false allegations of genocide as a pretext for the use of force.

Legal Battleground	Russian Argument	International / Ukrainian Response
UN Charter Article 51	Claimed 'collective self-defense' of the Donbas republics.	Rejected: Ukraine had not attacked Russia, and the republics are not UN members.
Genocide Convention	Asserted an 'obligation' to prevent genocide in eastern Ukraine.	The ICJ found no evidence of genocide by Ukraine and ordered Russia to suspend operations.
Responsibility to Protect	Mirrored Western justifications used in Kosovo.	Dismissed as politicization; Russia has historically denied R2P in other contexts.

Source: Leiden Journal of International Law (Cambridge), Brookings Institution, Duke Lawfire, Vanderbilt Law Review, Michigan Journal of International Law.

The ICJ ultimately determined in 2024 that it lacked jurisdiction to rule on Russia's core legal basis for the war — illuminating the 'peril of lawfare': while the misuse of law may be morally indefensible, it does not always constitute a violation under existing international legal frameworks. This gap between legal and moral accountability represents a fundamental vulnerability in the international rules-based order.

CONCLUSION: THE FUTURE OF INTEGRATED WARFARE

The conflict in Ukraine demonstrates that hybrid warfare is not a static concept but an evolving 'doctrine of integrated action.' It dismantles the traditional binary distinction between war and peace, replacing it with a continuum of conflict in which the state and society are subject to sustained, multidimensional assault. Non-military instruments — information operations, cyber capabilities, and economic coercion — can exceed kinetic weapons in their effectiveness within specific operational contexts, but they remain most potent when integrated into a comprehensive strategy of coordinated state mobilization.

As Russia's conventional forces have sustained significant attrition, the Kremlin's strategic posture toward the West may generate increased reliance on hybrid methods: targeted assassinations, subversion of critical infrastructure, and state sponsorship of terrorism through proxies. The transformation of Wagner's successor structures and Russia's deepening partnerships with Iran and North Korea suggest an expanding toolkit rather than a shrinking one.

For scholars of security studies, the Ukrainian case is a gift of analytical richness and a sobering reminder that the most dangerous conflicts of the 21st century may never be formally declared. They are fought in server rooms, satellite uplinks, energy contracts, courtrooms, and the cognitive architectures of publics who must ultimately decide what is real — and what is worth defending.

REFERENCES

[1] RUSI Commentary. 'A Frog in a Pot – Turning Around Russia's Hybrid War.' Royal United Services Institute;
[2] J.K.Wither, Defining Hybrid Warfare, Marshall Center Security Insights, Vol. 10, No. 1. George C. Marshall European Center for Security Studies;
[3] CSIS Analysis, NATO and Countering Hybrid Warfare, Center for Strategic and International Studies;
[4] U.S. Army War College, The War in Russia's Hybrid Warfare, Parameters, U.S. Army War College Press;

[5] RAND Corporation, Understanding Russian Hybrid Warfare: And What Can Be Done About It (CT468);
[6] USF Digital Commons, Surveying New Battlegrounds: Ukraine and the Future of Cognitive Warfare, Journal of Strategic Security;
[7] Cambridge University Press / Leiden Journal of International Law, The 2022 Russian Intervention in Ukraine: What is its Impact on the Interpretation of Jus Contra Bellum?;
[8] CIGI Policy Brief No. 209, Hybrid Warfare: Ukraine, Russia and Western Lessons, Centre for International Governance Innovation;
[9] MDPI, Beyond Information Warfare: Exploring Fact-Checking Research About the Russia-Ukraine War, Journalism and Media, Vol. 6, No. 2.;
[10] Atlantic Council, Ukraine Embraces Openness with New Report on Russian Hybrid Warfare Challenges;
[11] Brookings Institution, Ukraine and the Promise and Peril of Lawfare and Watch Out for Little Green Men;
[12] D. Lawfire, E. Chang on the Minsk II Agreement as Compliance-Leverage Disparity Lawfare;
[13] CFR, *Tracking Cyber Operations and Actors in the Russia-Ukraine War* and *How Russia's Invasion of Ukraine Violates International Law*, Council on Foreign Relations;
[14] ICDS, *Russia's Electronic Warfare Capabilities to 2025*, International Centre for Defence and Security;
[15] Vanderbilt Journal of Transnational Law, Strategic Litigation in Wartime: Judging the Russian Invasion of Ukraine through the Genocide Convention;
[16] FPRI, Putin the Green? The Unintended Consequences of Russia's Energy War on Europe, Foreign Policy Research Institute;
[17] CyberPeace Institute, Case Study: Viasat Attack.