Doctrine-to-Deployment: Role of Advanced Persistent Threats in Russia's Information Confrontation Doctrine

Elia Gelati[1] and Luigi Martino[2]
[1]Center for Cyber Security and International Relations Studies, University of Florence, Italy
[2]University of Bologna, Italy

eliagelati@gmail.com
luigi.martino3@unibo.it

Abstract: In 2022, before the invasion of Ukraine, many analysts feared the possibility of Russian cyberattacks overwhelming Kyiv's command and control systems and critical infrastructures, plunging Ukraine into darkness and facilitating a ground invasion. The leading entities behind these operations are advanced persistent threat groups: experienced, well-funded cyberspace actors often enjoying State sponsorship. Russian-sponsored APTs are already known for impactful cyberattacks such as the 2015 disruption of the Ukrainian energy grid, and are employed under the direction of the Russian intelligence services. Analysed through the lens of offensive realism, cyberspace appears as a domain of persistent competition among great powers. What this school of thought also posits is that while not revolutionary, cyberattacks can be used for tactical advantages. This stands in contrast with the expectations set by the Russian doctrine of "information confrontation" (or IPb), a comprehensive approach that utilises cyberattacks to achieve political, economic, and military objectives during both peacetime and wartime, with significant investments in APT groups and operations. This research analyses this "doctrine-to-deployment" gap in the role of APT groups within IPb through an offensive realist theoretical lens. It does so by analysing three case-studies of Russian APT operations using a "structured, focused" comparison methodology. These include the 2015 attack on the Ukrainian energy grid, the 2020 data breach on the SolarWinds supply chain and the APT campaigns in the war in Ukraine. By providing a doctrine-to-deployment analysis of APT units within IPb, this research clarifies a lesser-known aspect of cyber warfare: the role of State-sponsored APTs under Russian command. The results indicate that these operations, albeit aligned with State strategic objectives and the doctrine of IPb, do fall short of strategic gains, functioning more as tactical instruments of persistent warfare across wartime and peacetime. In this, the article contributes to the literature by clarifying how APTs function within IPb, bridging Russian military doctrine with international relations theory.

Keywords: Advanced persistent threat (APT) groups, Information confrontation, Russian cyber doctrine, Ukraine conflict, Cyber warfare, Offensive realism

1. Introduction

Cyberspace emerged as the fifth domain of conflict in the 2010s, alongside traditional dimensions of land, sea, air, and space. It is a contested domain, where State and non-state actors compete for strategic advantage (Allen and Gilbert, 2009). Three structural characteristics distinguish cyberspace from conventional domains: attribution ambiguity, low-cost offensives, and weak international governance (Martino, 2018), all of which contribute to making cyberspace an arena of continuous, below-threshold competition among States (Kello, 2017).

Among these actors, Russia is one of the most aggressive and sophisticated ones (Lynch III, 2025), being responsible for some of the most impactful cyberattacks in history, such as the one on the Ukrainian power grid in 2015. Over the years, Moscow codified its objectives and principles for cyberspace within the doctrine of "information confrontation" (or IPb, from the Russian "informatsionnoye protivoborstvo"), merging cyberattacks and information operations for the pursuit of its political hegemony in what it considers to be a domain of continuous conflict (Giles, 2016; Grisé *et al.*, 2022). Between the many assets at its disposal within IPb, Moscow invests funds and resources in advanced persistent threats (or APT) groups. From an offensive realist analytical perspective (Mearsheimer, 2001), these serve as tools to maximise power and ultimately ensure the State's survival in an anarchic environment characterised by intense power competition (Katagiri, 2024).

This research asks what the role of APT groups is within information confrontation, under the lens of offensive realism.

Indeed, previous policy and academic literature has only partly addressed this question. More specifically, works such as Grisé *et al.* (2022), addressed the specific topic of contrasting IPb definitions, while authors Lilly and Cheravitch (2020) and Cheravitch (2021) focused only on specific units, with their work predating active deployment of APT groups in an active warfare scenario; finally, more recently, the question was also tackled

by Voo and Singh (2025), with their efforts lacking a specific theoretical lens and a methodology to address the case-studies and derive relevant findings on the specific role, whether strategic or tactic, of APT groups.

This research addresses these issues by delivering a doctrine-to-deployment analysis of the role of APT groups within IPb, deriving hypotheses from an offensive realist theoretical framework, and then testing them through three case-studies of impactful Russian-sponsored cyber operations conducted by APT groups. For this part, the "structured, focused" methodology will be employed (George and Bennett, 2005).

This paper proceeds in six sections. Section 2 establishes the theoretical framework of offensive realism; Section 3 outlines the methodology; Section 4 traces the evolution of the IPb doctrine and maps its APT ecosystem; Section 5 analyses three case-studies that demonstrate APT operations in practice: the 2015 Ukrainian power grid attack, the 2020 SolarWinds hack, and the broader deployment of APT units during the war in Ukraine (2022-). Finally, Section 6 analyses the findings and assesses what these operations reveal about the APT roles within the Russian IPb strategy.

2. Theoretical Framework

Offensive realism is an international relations school of thought that posits that the international world order is one where States are the primary actors, among which distrust of intentions is one of the main drivers of conflict, as State strive for hegemony in order to maximize their chance of survival in what is essentially an anarchical system, without laws or order besides the one States make themselves (Mearsheimer, 2001).

The realist school has often been applied to cyberspace as a result of its similar condition of anarchy and high competition (Eriksson and Newlove-Eriksson, 2021). However, most realist do not think of cyber warfare as a game-changer; rather, it is considered a tool in the arsenal of States to be used in pursuit of its tactical objectives (Gartzke, 2013; Rid, 2013; Smeets, 2018).

Indeed, cyberspace perfectly fits some of the underlying logic of realism through three main characteristics. Firstly, while non-State actors enjoy considerable fortune in the fifth domain on the account of the lower cost of offensives (Nye, 2011), States are still the dominant actors with access to considerably more resources, which allow them to launch more precise and impactful operations against more defended targets (Gartzke, 2013; Lindsay, 2013; Smeets, 2022). Secondly, difficulties in attributing cyberattacks leads to higher uncertainty among States' and their intentions, which in turn fosters continuous competition (Kello, 2017). Thirdly, the lack of a unified and enforceable governance system renders this domain anarchical in nature (Kello, 2022). All of these characteristics transform cyberspace into an arena of persistent competition, where great powers must seek to maximize power for the sake of their survival (Lynch III, 2025).

To do so, and to offset the balance of power, they must use any tool at their disposal, such as advanced persistent threat (APT) groups (Katagiri, 2024). These are mostly State-sponsored cyber units (Steffens, 2020) that are among the most impactful actors within cyberspace, being responsible for cyber operations such as disruption of critical infrastructures or exfiltration of critical information.

As a revisionist power, Russia frequently makes use of these APT groups (Katagiri, 2024), among other cyber forces such as patriotic hackers and institutionalised troll farms (Abrams, 2016). It does so, according to the doctrine of "information confrontation", a "whole-of-government" approach that passes through the information environment and the cyber domain to reach political, military and economic objectives (Grisé *et al.*, 2022). Russia's substantial investment in APT capabilities, their embedding within intelligence structures, and their persistent employment, suggest that Moscow expects strategic returns from these instruments. IPb doctrine also elevates information operations as tools for achieving state objectives across peacetime and wartime, implying that cyber capabilities should deliver value commensurate with their sophistication and integration.

What emerges from this theoretical framework are two testable hypotheses: H1) if APT groups function as instruments of state power maximisation, their operations should systematically align with Russian strategic objectives; this is evidenced through a target selection that reflects state priorities and timing coordinated with geopolitical context; and H2) given Russian investments in APTs, operations should achieve cumulative strategic effects, such as intelligence advantages, policy changes, or capability degradation, contrary to what offensive realism posits for cyberspace. The analysis tests these hypotheses through three case-studies.

3. Methodology

This study employs the "structured, focused" comparison method (George and Bennett, 2005). It is structured in that the researcher formulates standardised general questions derived from the research objective, which are then systematically applied to each case to guide data collection and enable a comparison. The method is focused in that it examines only those aspects of the historical cases that are directly relevant to testing the hypotheses.

The case-studies were selected according to criteria of i) high-confidence attribution and ii) a variation in operational context, to test if coordination and effect expectations hold across different competition phases. The first case-study is that of the 2015 Ukraine power grid attack, which occurred during armed conflict short of open war, representing the first successful cyberattack causing physical disruption of critical infrastructure. The second case-study is the 2020 SolarWinds supply chain compromise, a high-profile espionage operation targeting U.S. sanctions policy apparatus, representing peacetime strategic competition. The third case is the 2022 Ukraine war, examining APT deployment during active conventional warfare, and testing effects in an instance where "Bitskrieg" predictions were prominent (Brantly and Brantly, 2024).

The questions asked for each case are as follows: i) Which APT group conducted the operation, and to which Russian intelligence service are they affiliated? ii) What were Russia's strategic objectives during this period? iii) How did operation timing, targeting, and methods align with those objectives? iv) Which kind of effects were achieved? Questions i-iii) speak to H1. Question iv) tests H2 by distinguishing tactical effects (immediate disruption or intelligence collection) from strategic effects (sustained advantages, policy changes, and capability shifts) and identifying responses that constrain strategic gains.

The literature includes official Russian documents, articles by Russian military theorists, peer-reviewed literature, and technical reports from reputable cybersecurity firms. The research is also supported by reputable cybersecurity and news outlets when necessary.

One of the limitations of this study concerns assessing strategic effects, which require inferring causation from temporal correlation; this is addressed through convergent evidence across multiple sources.

4. Information Confrontation: Doctrine and Operational Ecosystem

The early sponsorship of "patriotic hackers" in cyber warfare in Estonia and Georgia represents the baseline experience of Russian use of cyberspace to achieve political and strategic objectives. Cyber warfare was employed in the first case to react to diminishing Russian influence in the Baltics (Giles, 2011; Haataja, 2017); while in the second, it was to assist in kinetic operations during conventional warfare (Giles, 2011; White, 2018). With the second achieving mixed results, the failures were attributed by Russian officials to the lack of professionalised "information troops", tasked with cyber operations and directed by a military command (Giles, 2011; Lysenko and Brooks, 2018). In 2011, this reasoning was enshrined within an official armed forces document, where a provision was included to position "own" forces and means to ensure Russian information security in the territory of other states (Ministry of Defense of the Russian Federation, 2011), and once more in 2014, within the official military doctrine, where the armed forces are called "to develop forces and means for *information confrontation*" (Security Council of the Russian Federation, 2014).

"Information confrontation" is defined by Grisé *et al.* as "the purposeful use of offensive or defensive informational means to achieve political, economic, military, and other objectives during peacetime, competition, and wartime" (Grisé *et al.*, 2022). "Informational means" are here intended in the Russian sense, merging cyber and information operations (Giles, 2016).

IPb in itself is stratified over a century of different practices, consisting of i) Soviet "active measures" (Abrams, 2016), framing political violence and destabilisation through any means as fundamental in achieving the survival and success of the State; and ii) the theory of "reflexive control" (Thomas, 2019), which entails the manipulation of an opponent to make them behave to the manipulator's advantage.

Among Russian military literature, IPb is reportedly split between "information-psychological warfare", targeting personnel and populations, employed continuously, and "information-technological warfare", targeting technical systems during armed conflicts (Kvachkov, 2004; Chekinov and Bogdanov, 2013). This distinction is reportedly adopted in Russian doctrine (Giles, 2016), though it is often blurred in practice.

IPb is implemented through a diverse range of actors, including loosely organised patriotic hackers, State-funded disinformation operations, and APT groups institutionalised within intelligence services. This reflects

the earlier argument from both Russian military theorists and official documentation for the creation and establishment of "forces and means" allocated for IPb. Given the scope of the research, the focus here is on mapping relevant APT groups.

These are primarily embedded within military and intelligence structures, as seen in Figure 1, a distinction hinting at a more specialised area of operations that directly reflects the role of the intelligence agency they belong to, with military intelligence units favouring cyberattacks involving system disruption, SVR-aligned units targeting foreign and diplomatic targets, and FSB-related groups focusing on espionage. However, it is worth noting that this is not always the case. For example, in the 2016 DNC hack, GRU-aligned FancyBear and SVR-aligned CozyBear were both found responsible for what was essentially a foreign espionage operation, typically under SVR purview, while unaware of one another. This form of overlap reduces the effectiveness of operations and increases the likelihood of detection (Melella, Ferazza and Mersinas, 2024).

At the same time, information warfare is enabled by APT groups only insofar as it is about targeted attacks, rather than massive disinformation efforts. A notable example is once again the 2016 DNC hack, where the intention was to destabilise the U.S. Presidential election by strategically releasing information acquired through a cyber operation (Bowen, 2021).

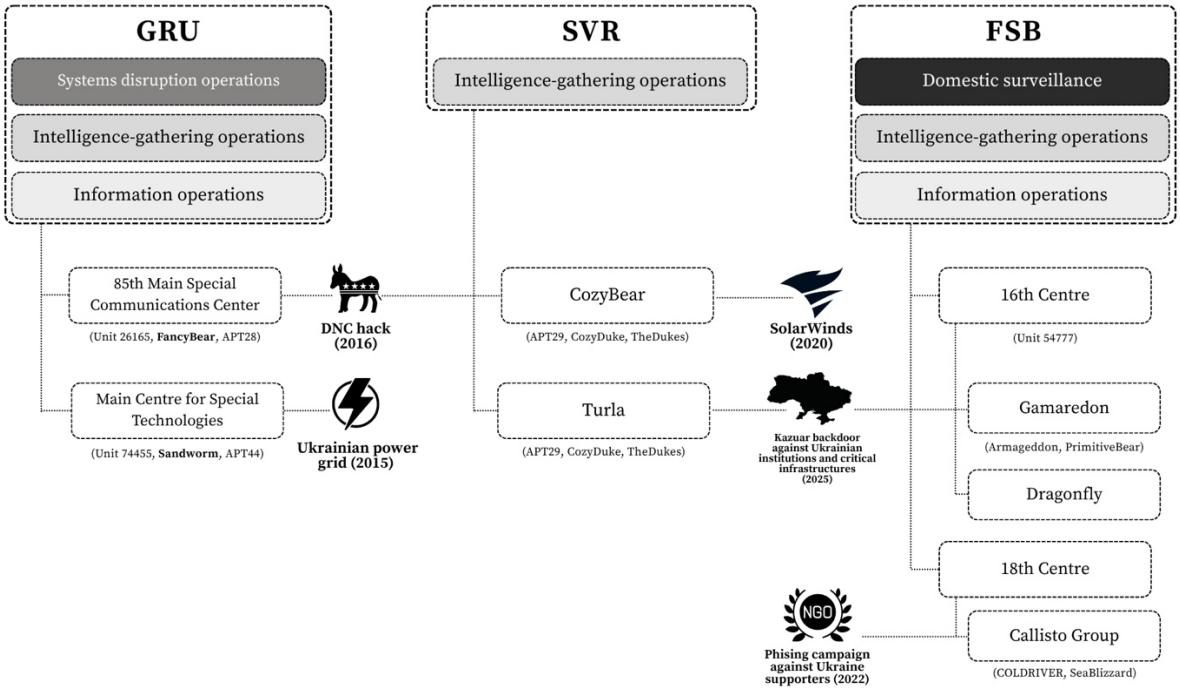

Figure 1: Authors mapping of the APT groups ecosystem under the Russian intelligence services. Key: intelligence services, their focus of operations, the APT groups attributed to them and some specific cyber operations (Cheravitch, 2021; Bowen, 2021, 2022; Wilde and Sherman, 2023; Melella, Ferazza and Mersinas, 2024; SSSCIPU, 2025)

5. Case-Studies

5.1 Ukraine Power Grid (2015)

Affecting 225,000 customers across three power-distribution territories, the December 23, 2015, cyberattack on the Ukrainian power grid is the first known case of a power outage caused by a cyber operation against critical infrastructure. The tools employed revealed high sophistication, with the attackers delivering BlackEnergy 3, a malware associated with GRU-affiliated Sandworm, through a phishing campaign (Hultquist, 2016; Lee, Assante and Conway, 2016; Greenberg, 2019). The strategic motive, as suggested by Baezner (2018), was to influence the population and the authorities, demonstrating the risks of escalation and resistance. This is evidenced through i) the hindering of crisis response capabilities by executing a telephone denial-of-service campaign (Hultquist, 2016); ii) the nature of a blackout at a time when no ground attack was taking place, as at the time the conflict between Ukraine and Russia was limited to few clashes, with the Second Minsk Accords still in place; iii) the timing (close to the Winter holidays).

Thus, the cyberattack aligns with Russian state objectives (H1), as the operation aimed to weaken Ukraine's resolve through infrastructure disruption. However, the attack's strategic impact was limited, contrary to what is stated in H2, as power was restored within hours (Kolodii, 2024), and no strategic objective in Ukraine was reached, as Kyiv continued to resist Russian pressure, even learning from this experience for the future 2022 conflict (Kolodii, 2024).

5.2 SolarWinds Attack (2020)

Between 2019 and 2020, SVR-aligned unit CozyBear infiltrated the supply chain of Orion, a data-managing software developed by SolarWinds. At the time, Orion was used by numerous entities worldwide, particularly in the U.S., where it was employed by key players such as Cisco, Microsoft, and at least twelve federal agencies (Devanny, Martin and Stevens, 2021). The malware spread through an update, resulting in a massive digital espionage campaign that affected over 18,000 SolarWinds clients (Willett, 2021).

Among the infected targets were also the U.S. Departments of Homeland Security and of the Treasury. While the exfiltrated information included counterintelligence information, Microsoft highlighted the access to data on sanctions via the Department of the Treasury as the primary objective of the operation (Menn and Bing, 2021).

The SolarWinds attack demonstrates coordination with state strategic objectives, supporting H1, as CozyBear targeted specific policy-relevant intelligence aligned with Russian priorities regarding U.S. sanctions policy. However, the operation provoked several reactions in the United States, resulting in heightened sanctions and a more robust cyber defence structure (Devanny, Martin and Stevens, 2021), limiting strategic gains regarding sanctions, despite the intelligence value of the exfiltrated data, which also included code, high-level correspondence and tools (Willett, 2021). These results contradict what was posited in H2, pointing to null strategic gains and only limited tactical ones.

5.3 APT Groups During the war in Ukraine (2022-)

During the 2022 invasion of Ukraine, Russian-sponsored APT groups subordinated to the GRU, FSB, and SVR were mobilised according to each intelligence service's distinct operational mandates and target sets.

GRU-linked units executed some of the most strategically timed attacks in the early phases of the war. Sandworm deployed AcidRain against KA-SAT satellite modems in February 2022, disrupting Ukrainian military communications at the onset of the kinetic operations (Boschetti, Falco and Gordon, 2022; Miron and Thornton, 2024; MITRE ATT&CK®, 2025). The attack on Viasat coincided with cyber operations targeting ISPs operating in the areas that were the main focuses of the invasion (NetBlocks, 2022). The impact was, however, offset by the redundancy of communication systems enjoyed by the Ukrainian military and civilian population across ISPs, mobile telephone providers, and secure radio communications (Brantly and Brantly, 2024).

Sandworm was later responsible for Industroyer2, an updated malware launched in April 2022, specifically designed to disrupt the industrial control systems of energy providers, with the potential to plunge over two million people into darkness (Wright, 2022); however, the attacks failed. These were synchronised with physical strikes on key logistical nodes in Kyiv, Vinnytsia, and Odesa (Kolodii, 2024), and were aimed at degrading physical infrastructure, causing confusion and eroding confidence, while also delaying decision-making in the field during offensive operations.

FancyBear, also GRU-affiliated, maintained a focus on credential harvesting, spear-phishing, and document exfiltration, targeting Ukrainian military and government institutions throughout 2022 and 2023. While not as technically destructive as Sandworm, FancyBear played a critical role in acquiring sensitive information, which was later exploited through information-psychological warfare (SSSCIPU, 2025).

FSB-controlled groups operated more diffusely across Ukraine's administrative and civilian structures, with the APT group Gamaredon being long focused on regional intelligence collection, with the number of phishing activities for espionage and intelligence-gathering purposes being high at the end of 2021 and the beginning of 2022, also scaling up after the beginning of the invasion, to the point where they became the most active APT group in Ukraine since the beginning of the war, with 829 attributed incidents (SSSCIPU, 2025).

Other FSB-linked APTs such as Callisto and Turla pursued credential theft and espionage campaigns against state institutions and civil society targets (CERT-UA, 2023).

What emerges from this brief analysis is that APT operations were deeply coordinated with the tactical and strategic objectives of the Russian Federation, rather than the groups acting as independent units, or "patriotic

hackers". This element supports H1 in proving the coordination of APT units with Moscow and the doctrine of IPb. However, while initial fears of a Russian "Bitskrieg" mounted before the beginning of the invasion (Brantly and Brantly, 2024), the experience shows that even the disruptive attacks that were successfully deployed had either temporary and limited impact; this is accounted by the Ukrainian defense capabilities as well as their lessons learnt throughout the previous periods of cyber warfare since 2014 (Kolodii, 2024). Therefore, H2 is not supported, with Russia being unable to deliver a cyber "kill-blow" to Ukraine.

6. Analysis and Conclusions

Table 1: Structured focused comparison of the case-studies

Questions	2015 Ukraine power grid	2020 SolarWinds	2022 Ukraine war
i) APT group and agency	Sandworm (GRU)	CozyBear (SVR)	Multiple: Sandworm, FancyBear (GRU); CozyBear, Turla (SVR); Gamaredon, Callisto (FSB)
ii) Context-specific Russian strategic objectives	To maintain pressure on Ukraine during the stalemate of the Minsk Accords, and showcase their capability to inflict damage without open war.	Gather intelligence on U.S. sanction policy; evade sanctions.	Degrade and disrupt Ukrainian C2 capabilities and critical infrastructure during the full-scale invasion of the country.
iii) coordination	Yes, to maximise psychological effects.	Yes.	Yes, with multiple instances of kinetic operations.
iv) Achieved tactical, strategic or response effects	Tactically, the operation resulted in a wide blackout. Strategically, the power was restored within hours, no policy change was registered and Ukraine hardened its cyber defences.	Tactically, important data was exfiltrated from U.S. institutions. Strategically, this resulted in a wider range of sanctions.	Tactically, disruptions only limitedly helped gains on the ground. Strategically, Ukrainian redundancies were able to offset the gains.

The case-studies showcase a consistent pattern of APT behaviour within Russian information confrontation doctrine: across all three instances, APT units systematically align with state objectives, rather than acting autonomously: the power grid attack targeted Ukrainian resolve at a critical time of competition between Kyiv and Moscow; CozyBear's infiltration of SolarWinds targeted the U.S. sanctions policy apparatus, reflecting Moscow's strategic priorities; finally, the 2022 campaigns demonstrated coordination between cyber operations and kinetic military actions. Thus, H1 is supported: APT groups function as institutionalised instruments of IPb, coordinated with state strategic objectives through their embedding within GRU, SVR, and FSB structures.

However, H2 reveals a gap between investments and outcomes. Despite Russia's substantial investment in APT capabilities, operations achieve tactical, rather than strategic effects, and limited ones at that (see Table 1). In the 2015 case-study, power was restored within hours, and Ukraine hardened its defences against future attacks, leading to the "pedagogy of cyber-war" reported by (Kolodii, 2024). In the case of SolarWinds, while intelligence exfiltrated, the discovery triggered heightened sanctions and expanded U.S. cyber defences, which offset the gains. In the wider 2022 campaign in Ukraine, initial "Bitskrieg" expectations were unmet, as Ukrainian resilience, communications redundancy, and allied support thwarted operations. Despite tactical differences across agencies, all APT groups faced similar strategic constraints when their operations prompted defensive adaptations or diplomatic retaliation.

From an offensive realist perspective, these findings reveal both the framework's explanatory power and its limitations. Offensive realism successfully explains why Russia organises and employs APT groups: as a revisionist power in anarchic cyberspace, Russia has institutionalised sophisticated cyber capabilities to maximise relative power through low-cost, deniable operations. The organisational embedding, target selection, and persistent employment align precisely with offensive realist logic about state behaviour in competitive domains. However, the expectation that sophisticated offensive tools yield cumulative strategic advantages proves limited. Rather, a more consistent pattern emerges: tactically successful operations trigger balancing responses, which then constrain the advantages gained during the operations. These constraints align with realist scholarship that remains sceptical of cyberattacks' "revolutionary" potential (Gartzke, 2013; Rid, 2013; Smeets, 2018), while also going further: even when operations coordinate with state objectives, employ sophisticated capabilities, and synchronise with conventional force, they achieve limited tactical effects without decisive strategic outcomes.

These findings clarify the role of APT groups in information confrontation. Russian-sponsored APTs remain sophisticated instruments that systematically pursue state objectives while achieving tactical rather than strategic effects. The gap between IPb doctrine's vision of cyber operations as tools of decisive power projection and their constrained operational reality reveals a significant gap: offensive realist imperatives drive Russia to maximise cyber capabilities and employ them persistently, yet the cyber domain characteristics, such as the adaptability of cyber defence, limit the strategic yield of even sophisticated operations. APT groups thus occupy a paradoxical role, remaining indispensable tactical instruments whose employment generates the very balancing responses that constrain their strategic value.

AI declaration: Grammarly was used for spelling/proofreading. All research content and analysis are entirely the authors' original work.

Ethics declaration: This research did not involve human participants or personal data and therefore did not require ethics approval.

References

Abrams, S. (2016) "Beyond Propaganda: Soviet Active Measures in Putin's Russia", *Connections: The Quarterly Journal*, 15(1), pp. 5–31.

Allen, P.D. and Gilbert, D.P. (2009) "The Information Sphere Domain Increasing Understanding and Cooperation", in C. Czosseck and K. Geers (eds) *The Virtual Battlefield: Perspectives on Cyber Warfare*. Tallin: CCDCOE, NATO Cooperative Cyber Defence Centre of Excellence.

Baezner, M. (2018) *Cyber and Information Warfare in the Ukrainian Conflict*. ETH Zurich.

Boschetti, N., Falco, G. and Gordon, N. (2022) "Space Cybersecurity Lessons Learned from The ViaSat Cyberattack", in. *AIAA Ascend 2022*, Las Vegas.

Bowen, A.S. (2021) *Russian Military Intelligence: Background and Issues for Congress*. R46616. Congressional Research Service.

Bowen, A.S. (2022) *Russian Cyber Units*. IF11718. Congressional Research Service.

Brantly, A.F. and Brantly, N.D. (2024) "The bitskrieg that was and wasn't: the military and intelligence implications of cyber operations during Russia's war on Ukraine", *Intelligence and National Security*, 39(3), pp. 475–495.

CERT-UA (2023) *Targeted attacks by Turla using CAPIBAR and KAZUAR malware*, *cert.gov.ua*.

Chekinov, S.G. and Bogdanov, S.A. (2013) 'The Nature and Content of a New Generation War', *Military Thought*.

Cheravitch, J. (2021) *The Role of Russia's Military in Information Confrontation*. Center for Naval Analyses.

Devanny, J., Martin, C. and Stevens, T. (2021) 'On the strategic consequences of digital espionage', *Journal of Cyber Policy*, 6(3), pp. 429–450.

Eriksson, J. and Newlove-Eriksson, L.M. (2021) 'Theorizing technology and international relations: prevailing perspectives and new horizons', in G. Giacomello, F.N. Moro, and M. Valigi (eds) *Technology and International Relations: The New Frontier in Global Power*. Edward Elgar Publishing.

Gartzke, E. (2013) "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth", *International Security*, 38(2), pp. 41–73.

George, A.L. and Bennett, A. (2005) *Case studies and theory development in the social sciences*. Cambridge, Mass: MIT Press.

Giles, K. (2011) "'"Information Troops" – a Russian Cyber Command?", in. *3rd International Conference on Cyber Conflict*, Tallinn, Estonia: CCDCOE, NATO Cooperative Cyber Defence Centre of Excellence, pp. 45–60.

Giles, K. (2016) *Handbook of Russian Information Warfare*. Rome: NATO Defense College (Fellowship Monograph, 9).

Greenberg, A. (2019) *Sandworm: a new era of cyberwar and the hunt for the Kremlin's most dangerous hackers*. New York: Doubleday.

Grisé, M. *et al.* (2022) *Rivalry in the Information Sphere: Russian Conceptions of Information Confrontation*. RAND Corporation.

Haataja, S. (2017) "The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach", *Law, Innovation and Technology*, 9(2), pp. 159–189.

Hultquist, J. (2016) *Sandworm Team and the Ukrainian Power Authority Attacks*. Mandiant.

Katagiri, N. (2024) "Advanced persistent threats and the "big four": State-sponsored hackers in China, Iran, Russia, and North Korea in 2003–2021", *Comparative Strategy*, 43(3), pp. 280–299.

Kello, L. (2017) *The Virtual Weapon and International Order*. New Haven: Yale University Press.

Kello, L. (2022) *Striking back: the end of peace in cyberspace - and how to restore it*. New Haven: Yale University Press.

Kolodii, R. (2024) "The Pedagogy of Cyber-War: Explaining Ukraine's Resilience Against Russian Cyber-Aggression", *Defense & Security Analysis*, 40(2), pp. 270–291.

Kvachkov, V. (2004) *Russia's Special Purpose Forces*. Voyennaya Literatura.

Lee, R., Assante, M. and Conway, T. (2016) *Analysis of the Cyber Attack on the Ukrainian Power Grid*. E-ISAC.

Lilly, B. and Cheravitch, J. (2020) "The Past, Present, and Future of Russia's Cyber Strategy and Forces", in. *2020 12th International Conference on Cyber Conflict (CyCon)*, IEEE, pp. 129–155.

Lindsay, J.R. (2013) "Stuxnet and the Limits of Cyber Warfare", *Security Studies*, 22(3), pp. 365–404.

Lynch III (2025) "Forward Persistence in Great Power Cyber Competition", *The Cyber Defense Review*, 9(3), pp. 81–103.
Lysenko, V. and Brooks, C. (2018) 'Russian Information Troops, Disinformation, and Democracy', *First Monday*.
Martino, L. (2018) "La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale", *Politica & Società*, (1), pp. 61–76.
Mearsheimer, J.J. (2001) *The Tragedy of Great Power Politics*. 1st edn. New York: Norton.
Melella, C., Ferazza, F. and Mersinas, K. (2024) 'Disjointed Cyber Warfare: Internal Conflicts among Russian Intelligence Agencies', *Applied Cybersecurity & Internet Governance*, 4(2).
Menn, J. and Bing, C. (2021) "Hackers of SolarWinds stole data on U.S. sanctions policy, intelligence probes", *Reuters*, 8 October.
Ministry of Defense of the Russian Federation (2011) "Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space".
Miron, M. and Thornton, R. (2024) "The Use of Cyber Tools by the Russian Military: Lessons from the War against Ukraine and a Warning for NATO?", *Applied Cybersecurity & Internet Governance*.
MITRE ATT&CK® (2025) *AcidRain, Software S1125*.
NetBlocks (2022) *Internet disruptions registered as Russia moves in on Ukraine - NetBlocks*.
Nye, J.S. (2011) "Diffusion and Cyberpower", in Nye, J. S., *The future of power*. 1. ed. New York: PublicAffairs.
Rid, T. (2013) *Cyber war will not take place*. Oxford ; New York: Oxford University Press.
Security Council of the Russian Federation (2014) "The Military Doctrine of the Russian Federation".
Smeets, M. (2018) "The Strategic Promise of Offensive Cyber Operations", *Strategic Studies Quarterly*, (Fall 2018), pp. 90–113.
Smeets, M. (2022) *No shortcuts: why states struggle to develop a military cyber-force*. London: Hurst & Company (Oxford scholarship online Political Science).
SSSCIPU (2025) *War and Cyber: Three Years of Struggle and Lessons for Global Security*. Kyiv: State Service of Special Communications and Information Protection of Ukraine.
Steffens, T. (2020) *Attribution of Advanced Persistent Threats: How to Identify the Actors Behind Cyber-Espionage*. Berlin, Heidelberg: Springer Berlin Heidelberg.
Thomas, T. (2019) *Russia's Reflexive Control Theory: Manipulating an Opponent to One's Advantage*. MITRE.
Voo, J. and Singh, V.V. (2025) *Russia's Information Confrontation Doctrine in Practice (2014–Present): Intent, Evolution and Implications*. International Institute for Strategic Studies, p. 36.
White, S.P. (2018) *Understanding Cyberwarfare: Lessons from the Russia-Georgia War*. Modern War Institute at West Point.
Wilde, G. and Sherman, J. (2023) *No Water's Edge: Russia's Information War and Regime Security*. Washington, DC: Carnegie Endowment for International Peace (Working Papers).
Willett, M. (2021) "Lessons of the SolarWinds Hack", *Survival*, 63(2), pp. 7–26.
Wright, R. (2022) *Industroyer2: How Ukraine avoided another blackout attack*, *TechTarget*.