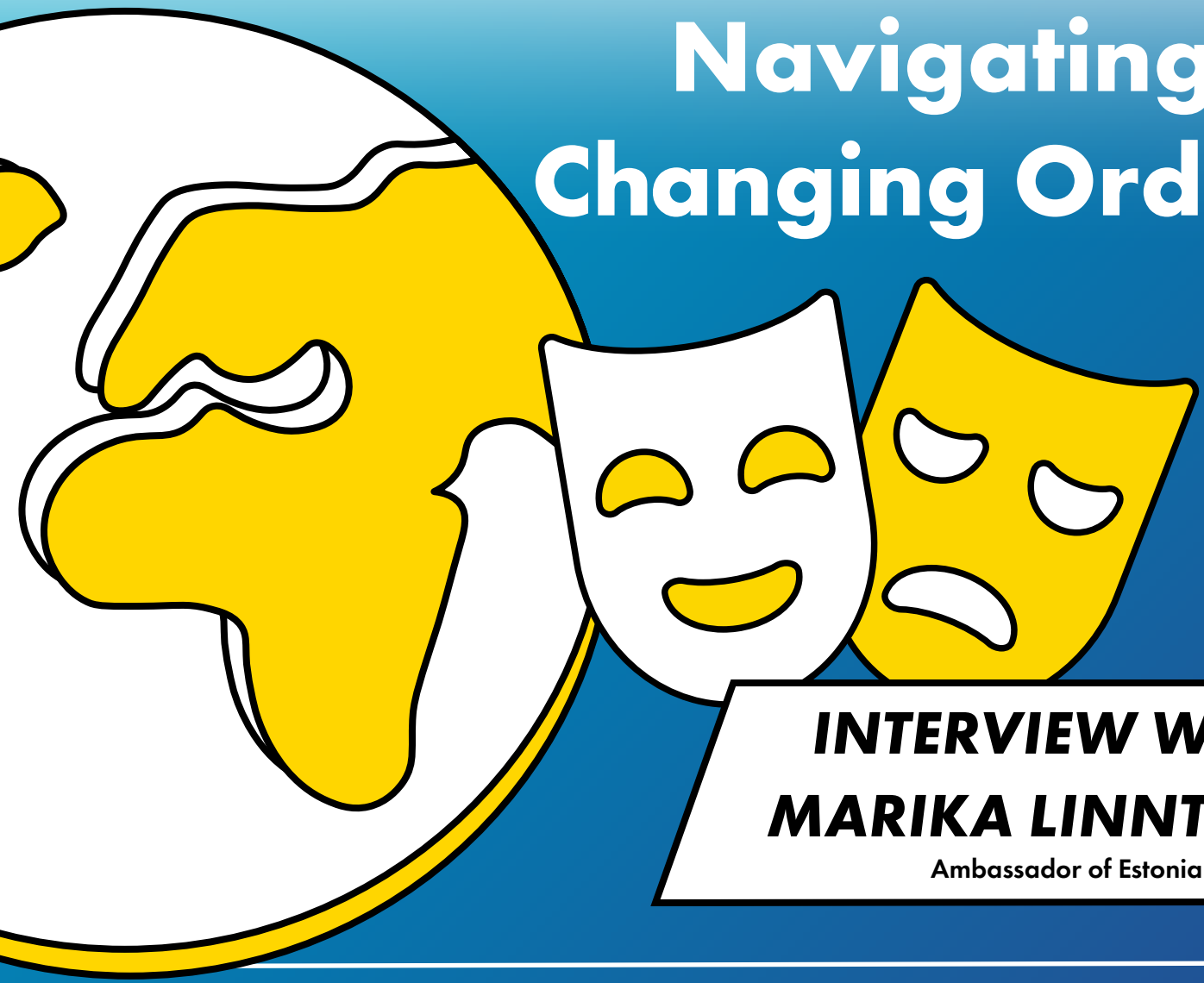
EPIS Thinktank
foreign affairs & security policy

Issue VI
March 2025
epis-thinktank.de

Navigating a Changing Order



INTERVIEW WITH MARIKA LINNTAM

Ambassador of Estonia to Berlin

Contemporary Sabotage Operations

State-led sabotage remains a key tool of influence, mirroring Cold War doctrines despite shifting justifications. Malte Koppermann's essay argues that while ideological motives have faded, the core objective—disrupting adversaries' policies and capabilities—remains unchanged. Both the U.S. and Russia continue to use proxies, uphold plausible deniability, and adapt to new technologies, including cyber sabotage. The recent rise in Russian sabotage underscores its ongoing relevance in geopolitical competition.

The Future of Democracy

Democracy faces growing cybersecurity threats in the digital age. Zhala Mammadli explores how cyberattacks, misinformation, and AI-driven manipulation undermine electoral integrity and public trust. While digital platforms expand political participation, they also expose democracies to hacking, disinformation, and algorithmic bias. Strengthening cyber defenses, digital literacy, and regulatory frameworks is crucial to safeguarding democratic governance in an era of evolving cyber threats.

Table of Contents

Guest Contributions

Interview

Columns

Editorial

Theodor Himmel

Theodor Himmel is pursuing an advanced legal education as a Rechtsreferendar at the Regional Court of Baden-Baden. His expertise includes international arbitration and mediation, as evidenced by his Advanced LL.M. from Leiden University, where he focused on the EU and Singapore Mediation Conventions. As Chair of the EPIS Thinktank e.V., he leads international collaborations on foreign affairs and security policy, while also contributing to legal scholarship and policy advisory roles with government affairs.

Alvin Karl Bürck

Alvin Karl Bürck is a German-Estonian aspiring social scientist pursuing an M.Sc. in International Political Economy at the London School of Economics (LSE). His research focuses on the political economy of climate change and quantitative social science. In addition to editing the EPIS Magazine, he serves on the Editorial Board of the Millennium Journal of International Studies and as a Postgraduate Student Academic Representative at LSE. He has prior professional experience in public affairs and public sector consulting.

Navigating a Changing Order

The world is in flux. The assumptions that shaped the past decades—on security, alliances, and stability—are being challenged by geopolitical tensions, military innovation, and economic realignments. As great power competition intensifies and new security threats emerge, states, institutions, and individuals must constantly adapt. Whether in military doctrine, energy policy, or digital governance, strategic choices made today will shape the world for years to come.

This issue of EPIS Magazine explores these shifting dynamics. Malte Koppermann analyses state-led sabotage, revealing how Cold War-era tactics persist in contemporary geopolitical competition. Dmytro Sochnyev challenges misconceptions about military obsolescence, demonstrating that technological and logistical factors—not battlefield survivability—determine the relevance of military systems. Nils A. Neubert examines the Sahel's strategic realignment, as Mali, Niger, and Burkina Faso move away from Western security partnerships towards new alliances with Russia and Turkey. Joschka Menge scrutinises Germany's shift from Russian gas to LNG through the lens of European cooperation, energy security, and policy contradictions. Meanwhile, Zhala Mammadli delves into the vulnerabilities of digital democracy, highlighting the rising threats posed by cyberattacks, misinformation, and AI-driven manipulation. Finally, Donát Oláh analyses the geopolitical contest in the Pacific, where China's growing influence challenges Western alliances. Additionally, we are pleased to feature guest contributions from Dr. Markus Schiller, Mr. Ferdinand Gehringer, and Dr. Johann Schmid, alongside an interview with Marika Linntam, Estonian Ambassador to Germany, whose expertise provides further insight into the evolving nature of international security.

We extend our gratitude to our authors and our designer Cira Scherenberger for their dedication to this issue. and to the many members—new and old—of the EPIS Think Tank for their motivation and continued interest in foreign affairs and security policy. As we move into 2025, we do so with a keen awareness of the challenges ahead but also with confidence that informed discussion and rigorous analysis will help us navigate an increasingly complex world. We hope you enjoy this issue of EPIS Magazine

Theodor Himmel
Chairman of EPIS Think Tank

Alvin Karl Bürck
Editor of the EPIS Magazine

About the Article

State-led sabotage remains a key tool of influence, mirroring Cold War doctrines despite shifting justifications. Malte Koppermann's essay argues that while ideological motives have faded, the core objective—disrupting adversaries' policies and capabilities—remains unchanged. Both the U.S. and Russia continue to use proxies, uphold plausible deniability, and adapt to new technologies, including cyber sabotage. The recent rise in Russian sabotage underscores its ongoing relevance in geopolitical competition.

About the Author

Malte Koppermann is pursuing an M.A. in Intelligence and Security studies at Kings College London (UK). His research focuses on national defense, hybrid warfare and open-source intelligence (OSINT). Currently, he posts daily updates on the war in Ukraine on X. Driven by a passion for safeguarding democracies, Malte Koppermann is eager to leverage his academic background to protect them from foreign and domestic adversaries.

1. Introduction

To advance and defend their national interests, states make use of the comprehensive toolkit of influence. On the one hand, traditional tools of influence include imposing sanctions, military exercises, or public diplomacy. On the other hand, states may opt to employ non-traditional measures of influence that are widely regarded as illegitimate in order to enhance traditional measures of influence (Hoffman, 2018). One such measure is sabotage. This essay argues that contemporary state-led sabotage mirrors Cold War-era sabotage doctrines. The persistence of sabotage operations since the end of World War Two demonstrates the centrality of this tool in the repertoire of statecraft to advance and protect national interests. Despite changes in the narratives that justify covert action and the means of conducting sabotage, the key objective of defending national interests has remained constant. The prevalence and significance of sabotage operations is reflected in contemporary media reporting, where Russian sabotage plots against the West have made repeated headlines. While Russian drones, bombs, and missiles continue to cause destruction across Ukraine, Russia is waging a non-lethal war against NATO. From weaponising migration to jamming the GPS signals vital to civilian aviation, Russia seeks to undermine and effectively halt Europe's support for Ukraine. Additionally, mysterious fires at arms manufacturing plants and severed or damaged undersea data cables in the Baltic Sea have been attributed to the Kremlin (Helsinki Commission, 2024). This shows that sabotage is a frequently used covert action tool. Despite Russian sabotage being on the rise, it is not unique to Russia but has been employed by the United States (U.S.) as well. During the Cold War, sabotage was embedded in the ideological struggle between the capitalist United States and the communist Soviet Union. Both superpowers have employed covert action to frustrate the policies, economies and military capabilities of their systemic opponent and their respective allies. At the same time, they attempted to uphold plausible deniability for their actions to avoid a direct military confrontation. Although both refrained from ever conducting such operations directly on each other's territories, they were frequently carried out on the soil of their respective allies. Since the collapse of the Soviet Union, ideological motivations have made way for pragmatic considerations of national security. Transcending this shift in narratives is their persistent reliance on proxies to execute sabotage operations. Whether Operation Mongoose in the 1960s or hiring of saboteurs through social media, intelligence services would commit significant effort in order to evade direct attribution. At the same time, state-led sabotage adapts to technological advancements. Sophisticated cyber-enabled sabotage has given states the opportunity to disrupt critical infrastructure and military facilities remotely, achieving greater plausible deniability. The critical examination of the extent to which contemporary state-led sabotage mirrors the Cold War-era sabotage doctrine reveals a significant continuation of its role in the pursuit of long-term strategic objectives. Due to the brevity of this essay, the analysis and comparison of state-led sabotage operations in light of Cold War-era sabotage doctrines is restricted to the United States and the Soviet Union, later the Russian Federation.

2. Cold War-era sabotage doctrines

Rovner (2023) defines sabotage as "the weaponization of friction." Here, friction is understood as all negative effects on the routine performance of organisations, including computer errors or mechanical defects. Sabotage, then, seeks to exploit and exacerbate these frictions in order to make them unbearable for the organisation. In the military-political complex, targets for sabotage are military assets and facilities, information systems, communication networks or intelligence agencies. It must be borne in mind that sabotage generally does not focus on short-term results. Rather, it "gradually increases friction in the service of long-term objectives" (Rovner, 2023). The U.S. Department of Defense defines sabotage in military terms as "an act or acts with intent to injure, interfere with, or obstruct the national defense of a country by

willfully injuring or destroying [...] any national defense or war materiel, premises, or utilities, to include human and natural resources" (2010, p. 209). Although this essay employs both definitions, it is restricted to those operations that cause or intend to cause physical harm to life and property. In the immediate aftermath of the Second World War, the Cold War quickly began to divide the world into the Eastern and Western blocs. As for the Soviet Union, Donnelly claimed that the USSR would use "any and every political tool" (1980, p. 35) in order to destroy global capitalism. According to documents shared between the Soviet KGB and East German and Czechoslovak intelligence agencies, Soviet sabotage pursued three objectives. It would aim to frustrate the Western bloc's pursuit of policies the Kremlin viewed as hostile, firstly, in the domestic context and, secondly, in the context of NATO. Thirdly, sabotage operations would try to downgrade the West's economic basis and military capabilities. Importantly, the intensity and severity of these operations would depend on the level of escalation with the West (Richterova, 2024). A special focus would be on sabotaging key military logistics hubs, airfields, and reserve forces in times of war (Sherfrey, 1987). Another key characteristic of the Soviet sabotage doctrine to amplify the fallout of sabotage activities by accompanying them with "active measures." In order to maximise the disruptive potential of kinetic operations, information warfare tactics, such as propaganda and disinformation, would seek to escalate the fallout of sabotage (Richterova, 2024). This highlights that sabotage does not appear in a vacuum. Instead, it is embedded in wider covert action or "active measures." On the other side of the Iron Curtain, on May 4, 1948, the U.S. Policy Planning Staff ushered in U.S.-led organised political warfare in order to pursue and protect national objectives using all means available. Ostensibly, it would serve as the answer to Soviet political warfare that had "become the most refined and effective of any in history" (Thorne & Patterson, 1996, p. 669). On the one hand, the realisation of this doctrine would rely on overt actions, meaning traditional statecraft such as diplomacy and economic tools. On the other hand, the United States would also engage in covert operations. The National Security Council Directive on Covert Action specified that "propaganda; economic warfare; preventive direct action, including sabotage [...]" (NSC 10/2, 1948) were permissible in order to fight "International Communism." Crucially, these actions were to be conducted in a manner that offered the U.S. Government plausible deniability. This precaution was undertaken in order to avoid a direct military confrontation with the Soviet Union or its allies. The declassified 1976 Church Report found that the Central Intelligence Agency (CIA) had conducted 900 major covert action projects between 1961 and 1976 (Select Committee to Study Governmental Operations, 1976). However, the report did not specify how many of these were sabotage. The analysis of both doctrines highlights that sabotage does not appear in a vacuum. Instead, it is embedded in a wider array of covert actions or "active measures." An analysis of sabotage operations must appreciate the clandestine context in which sabotage operations in tandem with other covert actions are executed. Looked at individually, any one covert action may have limited impact. However, as Rovner (2023) describes, sabotage is not a game-changer but a gradual exploitation of friction in service of long-term objectives. . Additionally, "when augmented with other coercive operations," (Reed, 2021, p. 22), it can have a strategic impact.

Sabotage:
Harming national defence by intentionally injuring or destroying personnel or materiel

3. Same objective, different narrative

Although the narratives that legitimise sabotage have shifted, the objectives have remained unchanged. The key motivation behind sabotage is to frustrate the opponent's capabilities and resolve in order to defend and advance one's own national interests. The Cold War was characterised by a competition of ideologies. The capitalist United States was fighting communism while the communist

Soviet Union wanted to dispose of the imperialist West. However, in the contemporary era, state-led sabotage has shifted from being embedded in a confrontation of ideological systems towards pragmatic considerations. The United States have leveraged strategic sabotage to advance their foreign policy objectives since the Directive on Covert Action. During the Vietnam War, the two superpowers were in a proxy war against each other. While the United States supported the South Vietnamese regime in its fight against communism in Vietnam, the Soviet Union aided North Vietnam and the Viet Cong. In the 1950s and 1960s, the CIA actively conducted sabotage operations behind enemy lines in North Vietnam. Targets included "trains, buses, contaminating fuel and oil, organizing two hundred Vietnamese commandos trained by the CIA, and burying weapons in the cemeteries of Hanoi" (Weiner, 2007, p. 211). More than four decades later, the United States was at war with Iraq in 2003. Here, the CIA organised and led a group of Iraqi paramilitaries - the Scorpions - to conduct sabotage missions around the start of the war (p. 492). The justifying narrative was no longer the fight against international communism but the alleged possession of weapons of mass destruction by the Iraqi regime and the global war on terrorism. The continued use of sabotage shows that it does not depend on ideological justifications. Instead, it is an available means in the toolkit of statecraft and warfare in order to disrupt governments and their policies that are seen as obstructive to United States strategic interests. In 1968, Chairman of the KGB, Yuri Andropov, issued the order "On tasks of State security agencies in combating ideological sabotage by the adversary" (Andrew, 1999, p. 7). The Soviet Union became obsessed with combating domestic dissent and foreign policies it perceived as antagonistic to the regime. Even human rights were perceived as a weapon of the imperialist West to subvert Moscow. This "ideological subversion" by the West was to serve as a narrative to justify Soviet kinetic operations. This twentieth-century narrative has largely made way to more generic justifications under President Putin. In 2023, he issued a new foreign policy against the "hostile" West that was supposedly waging a hybrid war against the Russian Federation (Bloomberg, 2023). After the relative absence of sabotage post-Cold War, one may argue that the recent intensification of sabotage activities is a departure from the Soviet sabotage doctrine. Granted, since the full-scale invasion in Ukraine on February 24, 2022, there have been almost 150 Russian hybrid attacks on NATO territory, of which a third were sabotage operations targeting critical infrastructure (Helsinki Commission, 2024). However, as noted above, the intensity of sabotage operations was tied to the level of escalation (Richterova, 2024). As the war against Ukraine has continued and Western military, economic, and humanitarian aid has increased, so has Russian sabotage. Contrary to a departure from the Cold War, the intensification of sabotage activities represents the continuation of Soviet sabotage doctrine into the modern-day Russian Federation. What is more, contemporary sabotage mirrors its Cold War predecessor because it is accompanied by information warfare. The increase in sabotage activities has been coupled with a large-scale propaganda and disinformation campaign. By relying on the penetration of social media platforms in Western societies, the Kremlin has been adamant about sowing discord and skewing the discourse on the war in Ukraine. While the European Union has banned Russian government outlets RT, formerly Russia Today, and Sputnik (Council of the EU, 2022), Russia has made ingenious use of social media, botnets, and fake websites to distribute its narratives. As the Atlantic Council (2024) writes, although the Russian effort to justify the invasion of Ukraine has fallen short of expectations, Western societies have been highly responsive to the narrative that blames NATO for the war in Ukraine.

Hence, sabotage is about the protection of national interests at the expense of the policies and capabilities of "hostile" governments. The shift in narratives from ideology to geostrategy notwithstanding, the objectives driving state-led sabotage have remained unchanged across decades.

4. Persistent use of proxies

In order to avoid direct military confrontation with one another or their allies, the United States and Soviet Union

relied and continue to rely on proxies to conduct sabotage. Both superpowers used their intelligence services to train, equip and direct foreigners to conduct clandestine operations on their behalf. On the one hand, as for the United States during the Cold War, arguably the most prominent operation that included sabotage was Operation Mongoose, authorised by President Kennedy in 1961. One year before the Cuban missile crisis, President Kennedy was convicted to dispose of Cuba's communist leader, Fidel Castro. There were many options to achieve that goal. One such option would have been for the CIA to stage an attack on the U.S.-held Guantanamo Bay as a pretext to invade Cuba. However, the Kennedy Administration discarded that idea as an outright escalation that may have resulted in nuclear war (Weiner, 2007, pp. 192–193). The alternative was Operation Mongoose, the largest U.S. intelligence effort within a Communist state (Thorne et al., 1996, p. 666). Sabotage would play a crucial role in enhancing the efforts to recruit the local population for guerilla warfare. A concrete sabotage plot would have been to contaminate Cuban strategic assets such as petroleum, oil, and lubricants. Although the United States would have been able to "liberate" Cuba in an amphibious invasion by itself, it preferred relying on Cubans (Lansdale, 2004, pp. 540–541). This had two benefits. While it provided the United States with some deniability, it also prevented a direct military confrontation with Cuba, or worse, the Soviet Union.

Sabotage adapted to shifting narratives, strategic considerations, and technological advancement

On the other hand, the Russian Federation, as did the Soviet Union, relied on proxy forces for sabotage operations. During the Cold War, the Soviet Union hired "agent-executioners" or "agents-saboteurs" from abroad to conduct a variety of sabotage activities (Richterova, 2024). However, two factors led to the departure from that practice. First, Russia has lost much of its personnel under diplomatic cover in Europe. Whereas 1,500 Soviet officials had been expelled from Western states between 1946 and 1991, since the start of the Russian full-scale invasion of Ukraine in 2022, more than 700 diplomats have been asked to leave Europe and North America (Riehle, 2024, p. 1238). Second, recent developments in information communication technologies (ICT) have facilitated the hiring, handling, and payment of saboteurs. Taken together, Richterova et al. (2024) argue that Russia has taken notes from the gig economy in the outsourcing of sabotage operations. The ease of hiring saboteurs, the lack of direct connections to Russian intelligence services, and the anonymity in payments through cryptocurrencies at least partially offsets the sabotage potential lost through the expulsion of diplomats and agents under diplomatic cover. Richterova et al.'s (2024) argument is being corroborated by recent acts of sabotage across Europe. For example, in 2024, Russia recruited around ten Estonian nationals via social media to conduct sabotage against government officials inside Estonia (Tucker, 2024). This demonstrates the persistent outsourcing of clandestine activities to gain (im)plausible deniability. Furthermore, those attacks were directly aimed at disrupting and degrading governments that pursued policies that were perceived as hostile to the United States or Russia. From a strategic standpoint, the two examples highlight that sabotage itself is no silver bullet. Rather, they are embedded in a wider context, intended to support traditional military action or the suppression of policies by adversarial governments.

5. The growing toolkit of sabotage

The exploitation of both new technologies and vulnerabilities showcases the continuation of advancing national interests by all means necessary. On the one hand, cyber- and cyber-enabled sabotage now constitute a central role in contemporary sabotage strategies. Unlike Cold War sabotage methods, cyber sabotage requires neither physical presence nor complex logistical and personnel arrangements. The contemporary interconnected world enables intelligence agencies to disrupt and even destroy critical infrastructure and military assets through

RETYPED BY COMMITTEE STAFF FROM
INDISTINCT ORIGINAL

16 October 1962

MEMORANDUM FOR: Special Group (Augmented)

SUBJECT: Operation MONGOOSE/Sabotage Proposals

1. The Director of Central Intelligence proposes that CIA undertake as soon as possible the following listed sabotage operations:

a. Demolition by an eight-man raider team of the railroad bridge near Calafre, Pinar del Rio Province

b. An underwater demolition attack by two Cuban frogmen against shipping and port facilities at the port of La Isabella, Las Villas Province

c. Grenade attack on the Chinese communist embassy in Havana, to be carried out by a recruited Cuban agent who has access to a roof overlooking the embassy garden and who has volunteered for this mission.

d. Mine with moored oil drum mines the approaches to one or more of the following harbors: Moa Bay, Nicaro, Banes, Neuvitas, Mariel, Bahia Conda

e. A demolition attack by a hit-and-run raider team on the Matanzas power plant

f. A hit-and-run mortar and gunfire attack on the Soviet SAM site near Santa Lucin, Pinar del Rio Province

g. Incendiary sabotage by a raider team of the wooden cooling tower, wooden docks, and sulphur stockpile at the Nicaro nickel plant. A parallel attempt will be made against the sulphur stockpile using [redacted] intermediate agent assets.

h. Set afire by gunfire an oil tanker off Havana or Matanzas harbor. This operation will be mounted from a small, fast boat using recoiless rifles and rackets.

CIA HAS NO OBJECTION TO DECLASSIFICATION AND/OR RELEASE OF THIS DOCUMENT AS SANITIZED 2 Aug 94

NO OBJECTION NATIONAL SECURITY COUNCIL defer to CIA 7/15/94

Figure 1: Sabotage proposals during Operation Mongoose (Kennedy Administration vs. Castro's Cuba)
National Archives, JFK Assassination Records, Document No. 157-10004-10154. CIA, Marshall Carter, Memorandum for Special Group (Augmented), "Operation MONGOOSE/Sabotage Proposals," October 16, 1962. https://nsarchive.gwu.edu/document/19628-national-security-archive-doc-17-cia-marshall

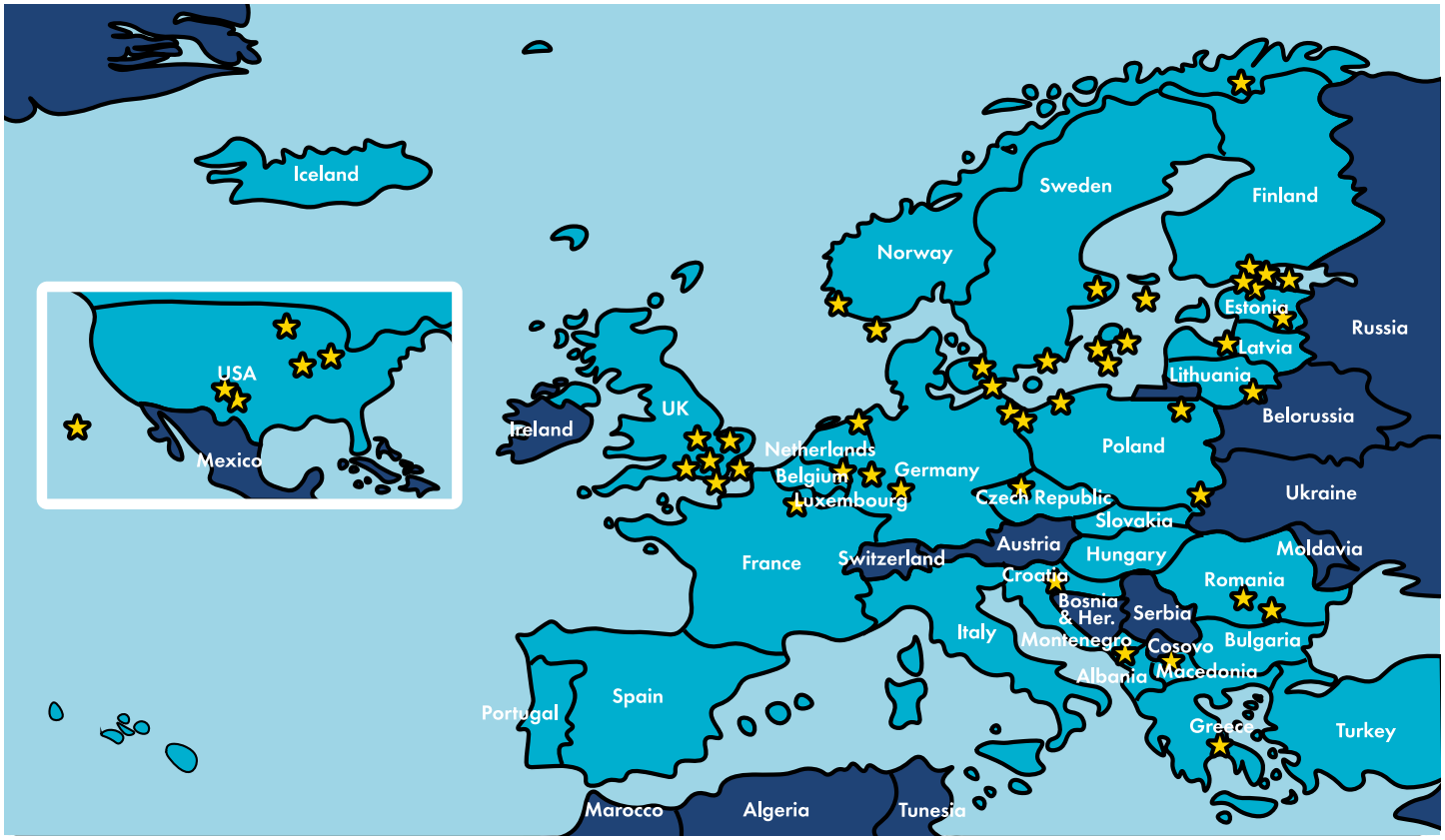


Figure 2: Map of Europe (and the US): indication of Russian hybrid warfare attacks on critical national infrastructure
Commission on Security and Cooperation in Europe, U.S. Helsinki Commission. https://www.csce.gov/publications/spotlight-on-the-shadow-war-inside-russias-attacks-on-nato-territory/

offensive cyber means. Regarding the United States, the most infamous example of cyber sabotage is the Stuxnet computer worm, targeting Iran's nuclear program. Although there is no concrete evidence of who exactly perpetrated the attack, the biggest beneficiaries of disrupted Iranian nuclear ambitions are the United States and Israel (Congressional Research Service, 2010, p. 5). The way the worm operated was through sabotaging the routine Siemens industrial control process technology that manages the speed of the motors (Farwell & Rohozinski, 2011, p. 25). This sabotage attack demonstrates how cyber capabilities can be used to generate a high impact without risking direct military confrontation with Iran. A high-risk alternative would have been an airstrike on nuclear enrichment facilities. Instead, the United States were able to protect their strategic objectives in the region while at the same time upholding plausible deniability. As for the Russian Federation, cyber and cyber-enabled sabotage has been increasingly employed as part of the hybrid warfare campaign against the states providing aid to Ukraine. One example, the military intelligence (GRU) Unit 29155, is responsible for large-scale cyber sabotage operations, including the destruction of data and website defacements. U.S. authorities have observed more than 14,000 instances across 26 NATO and EU member states, where Unit 29155 has scanned domains for potential vulnerabilities (Cybersecurity & Infrastructure Security Agency, 2024). The number of successful cyber sabotage operations is not publicly available information. As for another example, in late 2024, Polish authorities discovered a network of Russian and Belarussian-linked hackers. The group had been responsible for cyber sabotage activities against the Polish government, military, and economy (Antoniuk, 2024). Poland, one of the biggest military aid supporters to Ukraine, is a prime target for Russian subversive activities. As a member of NATO, Poland is not an attractive target for conventional attacks. In order to mediate the aggressive efforts to disrupt Polish support for Ukraine while staying below the threshold of war, Russia is using sabotage operations to frustrate Polish resolve. However, these attacks have hitherto not effectively undermined Polish determination in

supporting Ukraine. This example showcases that Russia will use any means at its disposal to stop policies it deems hostile towards its national interest. The same is true for the Stuxnet example. Taken together, the United States and Russia adapt their sabotage activities to technological advancements. In particular, cyber and cyber-enabled sabotage can be operated remotely. While United States saboteurs would have found it difficult to access Iranian nuclear enrichment facilities, Russia is facing increasing difficulty to keep its agents under diplomatic cover inside target countries. Where the recruitment of saboteurs fails, cyber sabotage offers a high-impact alternative that retains plausible deniability.

6. Concluding thoughts

State-led sabotage operations as a tool of statecraft have adapted to shifting political narratives, strategic considerations, and technological advancements. Irrespective of the time period, the core objective of this clandestine activity has remained consistent. It is used to advance and protect the national interest by frustrating, disrupting, and destroying the adversaries' military and economic policies and capabilities. Whereas Cold War-era sabotage was justified by ideological competition between the United States and the Soviet Union, contemporary efforts show a shift towards calculated strategic motivations. Despite this change, the reliance on proxies, upholding plausible deniability, and the incremental accumulation of short-term friction in the pursuit of long-term strategic objectives closely mirrors the Cold War-era sabotage doctrine. The recent intensification of sabotage by the Russian Federation underscores persistent use of sabotage in geopolitical competition. Since the operations must be understood in a wider context of political or hybrid warfare, there is a high probability of these attacks to continue. Future research may benefit from investigating the actual impact of sabotage activities. Concretely, a comprehensive study of these operations has the potential to reveal their tactical, operational, and strategic value. Furthermore, it would be insightful to clearly distinguish between peace- and wartime sabotage, not only to analyse the impact but also.

References

Andrew, C. (1999). The sword and shield: The mitrokhin archive and the secret history of the KGB. New York, United States: Perseus Books Group.

Antoniuk, D. (2024, September 9). Poland dismantles cyber sabotage group linked to Russia, Belarus. Retrieved from https://therecord.media/poland-dismantles-cyber-sabotage-group-russia-belarus

Atlantic Council. (2024, November 26). Russia's evolving information war poses growing threat to the west. Retrieved from https://www.atlanticcouncil.org/blogs/ukrainealert/russias-evolving-information-war-poses-a-growing-threat-to-the-west/

Congressional Research Service. (2010, December 9). The stuxnet computer worm: Harbinger of an emerging warfare capability. Retrieved from https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-040.pdf

Council of the EU. (2022, March 2). EU imposes sanctions on state-owned outlets RT/Russia Today and Sputnik's broadcasting in the EU. Retrieved from https://www.consilium.europa.eu/en/press/press-releases/2022/03/02/eu-imposes-sanctions-on-state-owned-outlets-rtrussia-today-and-sputnik-s-broadcasting-in-the-eu/

Cybersecurity & Infrastructure Security Agency (2024, September 5). Russian military cyber actors target US and global critical infrastructure. Retrieved from https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-249a#:~:text=Since%20early%202022%2C%20the%20primary,European%20Union%20(EU)%20countries.

Donnelly, C. N. (1980). Operations in the enemy rear: Soviet doctrine and tactics. International Defense Review, 13(1), 35-41.

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. Survival, 53(1), 23-40. DOI: https://doi.org/10.1080/00396338.2011.555586

Hoffman, F. G. (2018). Examining complex forms of conflict: Gray zone and hybrid challenges. PRISM, 7(4), 30-47.

Putin signs new Russia foreign policy against 'hostile' west (2023, March 31). Bloomberg. Retrieved from https://www.bloomberg.com/news/articles/2023-03-31/putin-signs-new-russia-foreign-policy-against-hostile-west

Reed, G. K. (2021). Assessing the effectiveness of strategic sabotage in supporting United States national security objectives (master's thesis). USMC Command and Staff College, Quantico, United States.

Richterova, D. (2024). The long shadow of Soviet sabotage doctrine? Retrieved from https://warontherocks.com/2024/08/the-long-shadow-of-soviet-sabotage-doctrine/

Richterova, D., Grossfeld, E., Long, M., & Bury, P. (2024). Russian sabotage in the gig-economy era. The RUSI Journal, 169(5), 10-21 DOI: 10.1080/03071847.2024.2401232

Riehle, K. P. (2024). Soviet and Russian diplomatic expulsions: How many and why? International Journal of Intelligence and CounterIntelligence, 37(4), 1238-1263. DOI: https://doi.org/10.1080/08850607.2023.2272216

Rovner, J. (2023). Theory of sabotage. Études françaises de renseignement et de cyber, 1(1), 139-153. doi: https://doi.org/10.3917/efrc.231.0139

Sherfrey, L. W. (1987). Operational employment of airborne forces: The Soviet approach and the implications for NATO (Monograph). Fort Leavenworth: School of Advanced Military Studies.

Thorne, C. T., & Patterson, D. S. (1996). Foreign relations of the United States: 1945-1950: Emergence of the intelligence establishment. Washington, D.C.: United States Government Printing Office.

Tucker, P. (2024, February 20). Russian hybrid operations on the rise in Estonia, Moldova: Similar Russian attempts to exploit ethnic divisions in democratic nations have preceded more aggressive action. Retrieved from https://www.defenseone.com/threats/2024/02/russian-hybrid-operations-rise-estonia-moldova/394318/

U.S. Department of Defense. (2019, November 8). Dictionary of military and associated terms. Retrieved from https://irp.fas.org/doddir/dod/jp1_02.pdf

U.S. Helsinki Commission. (2024). Spotlight on the shadow war: Inside Russia's attacks on NATO territory. Retrieved from https://www.csce.gov/publications/spotlight-on-the-shadow-war-inside-russias-attacks-on-nato-territory/

U.S. National Security Council. (1948, June 18). NSC 10/2. National security council directive on covert action. Retrieved from https://www.cia.gov/readingroom/docs/CIA-RDP80B01676R001100070002-3.pdf

Weiner, T. (2007). Legacy of ashes: The history of the CIA. New York, United States: The Doubleday Broadway Publishing Group.

Greetings from our contributors

friedrich 30

Founded in 2009, we have ever since been operating for our clients in Germany and beyond.

We represent interests

friedrich30 represents security and diplomatic interests around the world, including in countries with challenging political and security conditions.

Our company has four business areas:

I. Political Lobbying
II. Business Development
III. Multi-track Diplomacy
IV. Security & Protection from Economic Damage

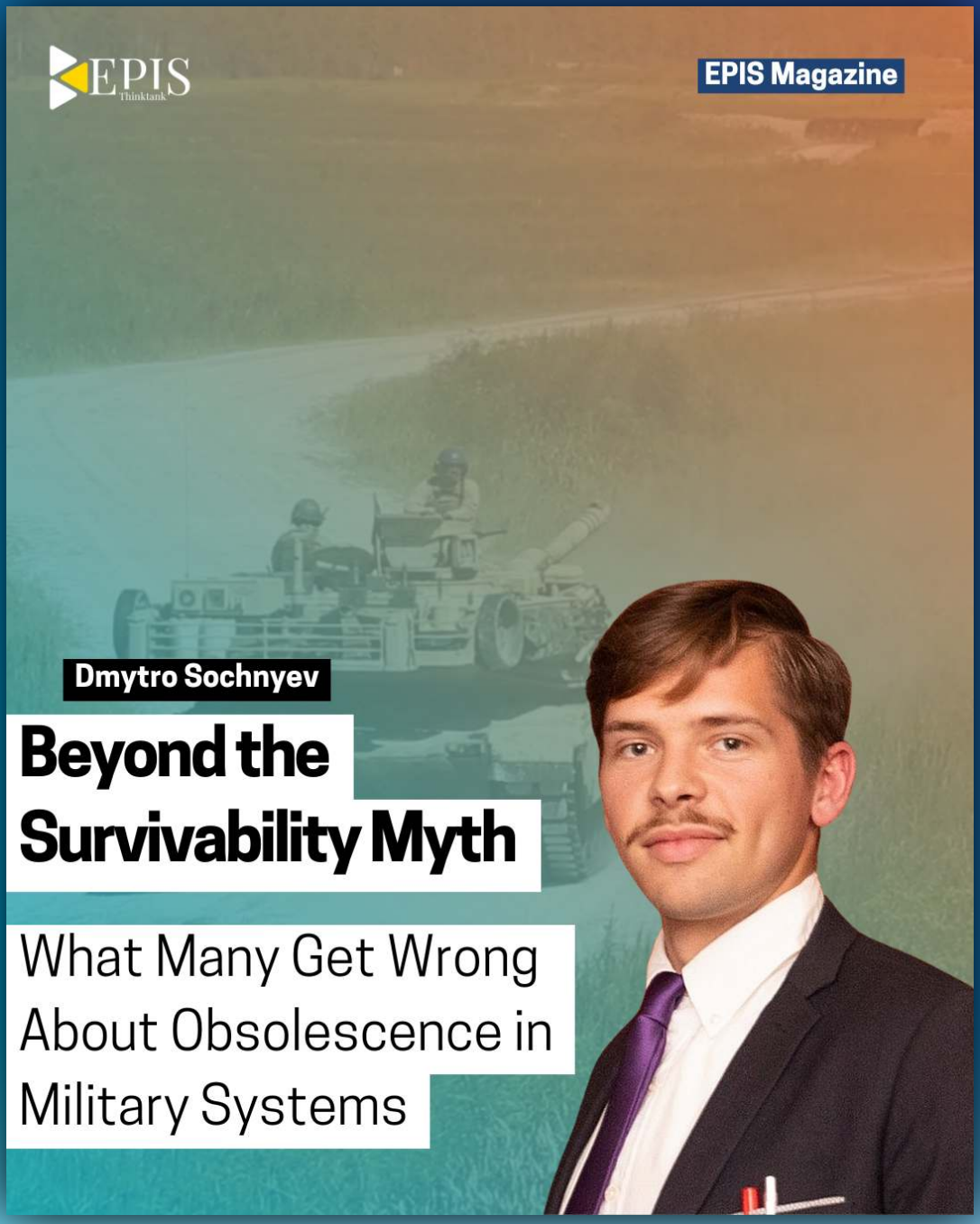
Our Network – friedrich30 team members include former policemen, high-ranking intelligence officers, diplomats, government officials and IT-experts.

Locations – With offices in Berlin, Brussels and Mainz, our operating range covers Germany, the EU as well as selected countries around the world.

Contact us – info@friedrich30.com

We especially enjoy collaborating with motivated students and supporting think tanks in their important work at the focal point of policy and research!

friedrich30.com



About the Article

Many misunderstand military obsolescence, assuming battlefield survivability dictates a system's relevance. Dmytro Sochnyev attacks that myth, arguing that obsolescence stems from the emergence and availability of superior alternatives, not mere vulnerability. Through historical and modern examples, the author reveals why even „outdated" weapons persist—proving that survivability alone is not the key determinant of military evolution, but rather technological and logistical realities.

About the Author

Dmytro Sochnyev is pursuing an MIA at the Hertie School (DE). His research focuses on international relations and contemporary security. Driven by a passion for uncovering data-driven and innovative solutions to security challenges, Dmytro Sochnyev aims to address existential issues.

1. Introduction

What makes a military technology obsolete? In late November 2024, the mercurial oligarch Elon Musk took to X (Twitter) to severely criticise the "idiots" building the F-35, a multirole fighter jet developed and manufactured by Lockheed Martin (Hambling, 2024). As the chair of the incoming Department of Government Efficiency tasked with slashing government spending, Musk did not just complain that the aircraft was overdesigned and overpriced. He also questioned the very necessity of fighter jets in the future. "Crewed fighter jets are an inefficient way to extend the range of missiles or drop bombs," Musk posted. „A reusable drone can do so without all the overhead of a human pilot [...] Manned fighter jets are obsolete in the age of drones." He added that fighter jets are "laughably easy to take down" because their "stealth means nothing if you use elementary AI with lowlight sensitivity cameras" and thus "will be shot down very quickly if the opposing force has sophisticated SAM or drones."

There is an increasingly common public perception, and even in some military commentary, that the inability of a weapons system itself or its user to survive on the battlefield is the critical cause of its obsolescence. This 'survivability' narrative has driven charges of obsolescence against the full spectrum of military technology available, challenging us to reflect on whether the tools we have to fight the next major war with are sufficient. One article in March 2022 questioned if tanks were still worthwhile investments as endless footage of their destruction by anti-tank missiles and drones was published (O'Brien, 2022). "Tanks, fighter jets, and warships are being pushed into obsolescence," argued an Atlantic article in May 2022 because drones and various missiles were causing significant losses among those systems (Cumming, 2022). These arguments, based on published footage and other media describing the loss of large and expensive equipment, seem so intuitive that it might be puzzling why many major militaries have and continue to procure similar equipment. This is because much of the public commentary is getting a crucial fact about the battlefield incorrect. It is not survivability that drives technological obsolescence. Instead, superior performance in the relevant battlefield role and sustained availability are the primary determinants of technological obsolescence.

2. Killing the Survivability Narrative

Understanding the intersectional complexities and nuances of modern warfare begins with tremendous effort and broad research, which is not always possible on all levels of debate. Making accurate statements about the battlefield requires in-depth technical knowledge of a dizzying range of technologies, but also how they interact with variables like tactics, environment, and quantity. Often, certain erroneous claims are driven by misconceptions about warfare, war economics, and even physics.

Many experts, for example, responded to Musk's criticisms by explaining the basic economic and physics constraints that make it impossible for smaller drones to detect, chase, or engage modern aircraft. Others pointed out that modern air defence, like those employed by the Islamic Republic of Iran, was helpless against airstrikes launched by stealthy Israeli F-35Is back in October (Epstein, 2024). Likewise, Ukrainian ground air defences have decimated the Russian Air Force, but have lacked the range to prevent the relentless bombardment of glide bombs by Russian jets operating dozens of kilometres behind the front. Above all, the surest indicator of the fighter jet's and any other weapons system's continued relevance is to follow the money. The dramatic reveal of two new Chinese next-generation aircraft (Jensen, 2025), four years after the first US Next-Generation Air Dominance prototype flight (Insinna, 2020), underscored how major militaries continue to believe that fighter jets and other large piloted aircraft will play a critical defence role in the next few decades at the very least. Certainly, even military officials with experience and technical expertise have made similarly incorrect assessments. Consider, for example, some 20th-century claims that put into question the future survivability of the aircraft carrier. After US Navy testing of

anti-ship bombers in 1925, for example, Lt. Commander G.B. Vroom claimed that the plane could only defeat the battleship through "too much publicity" and that "dropping bombs on ships undefended by planes merely proves that V2 equals 2 Gs" (Vroom, 1925). In 1940, Nazi German naval leadership likewise believed that carrier-launched combustion engine planes would eventually "not be usable in this war" and thus never seriously invested in carriers (Polmar, 2008, p. 418). Lt. General James H. Doolittle, who relied extensively on carriers in the Pacific campaign against Imperial Japan, argued before a US Senate Committee that "the carrier has two attributes: one attribute is that it can move about; the other is that it can be sunk" (Polmar, 2008, p. 2). And yet, in 1993, former US President Bill Clinton would remark that the first reaction in Washington to an international crisis breaking out would be to ask where the nearest carrier was (Cohen, 2010). It is uncertain why this narrative of survivability persists, but it has proliferated during the Russian full-scale invasion of Ukraine, as drone cameras reveal more than ever the attrition of modern equipment in large-scale peer-to-peer combat. At first glance, the narrative provides a palatable argument: if the multirole fighter jet is easily shot down by existing or anti-air and the aircraft carrier is easily sunk by submarines or anti-ship cruise missiles, then these expensive systems provide minimal value since they cannot survive to deliver on their intended purpose. To continue using them would be to needlessly risk valuable human lives and capital. But war necessarily involves a varying risk of loss, after all, whether it be by enemy or friendly fire (Lagrone, 2024). One might take the Kantian perspective, wherein the constituents of democratic societies are incentivised to prioritise survivability in the procurement of defence technologies in case they must consent to war. Perhaps, as a Chinese military document assesses regarding the US (Sullivan, 2025), it is the "inherent nature of its bourgeois army" that creates a persistent fear of casualties in democracies. Maybe the argument is just logical enough in theory to be palatable to a wide audience. Whatever the reason, in practice the survivability narrative invariably fails to predict which kinds of military technologies persist or not. Consider how the lens of survivability views the relationship between infantry and armour as an unsolvable cycle. In the era of mechanised armour, infantry are too slow to deploy to battlefields without transportation, putting pressure on defence ministries to procure mechanised transport wherever possible. Yet the proliferation of automatic fire and artillery leaves infantry too vulnerable in unarmoured trucks and cars, so it follows that armoured personnel carriers are used instead. Still, the lack of significant armament on armoured personnel carriers could leave them dangerously defenceless, so perhaps an infantry fighting vehicle with an autocannon as its primary armament is better. Yet the thin armour still leaves infantry inside vulnerable to enemy mines and larger guns, so a tank's increased armour and firepower are imperative to maintain survivability. At each step, the additional weight from additional armour and ammunition decreases speed, affordability, and—most importantly—transport capacity. Such survivability-driven procurement leaves the infantry trailing the tank on foot, seemingly beginning the cycle anew. In the reality of mechanised assault, however, neither of these systems is considered in isolation but as part of a larger tactical approach that ideally involves the full spectrum of terrestrial and airborne systems. Instead, the task of the typical commander is to combine the capabilities of systems at their disposal—such as mobility, protection, firepower, and disruption—to hide their respective deficiencies and complete the mission. The machine-gun-laden and thinly armoured personal carrier is not made obsolete by the tank, for it contributes to a completely different tactical profile. In fact, the infantryman, owing to their inherent lack of natural protection against blades, bullets, and other dangerous battlefield implements, has long been rendered obsolete if survivability was the crucial factor of obsolescence. In the past, the common soldier could rely upon worn or wielded armour, and some of

Survivability myth:
The belief that a battlefield system is obsolete when itself or its user is vulnerable.

Figure 1: Despite the proliferation of drones, tanks like this Ukrainian T-64 have opted for improvised protective cages rather than disappear from frontline combat altogether. АрміяInform, CC 4.0

the wealthier knights could equip themselves in full armour suits that were virtually impenetrable to the crossbows and the guns of the time. Later, the proliferation and evolution of gunpowder weapons left chainmail and metal armour—for those that could afford it—helpless against projectiles. As armies nationalised and began fielding their infantry in regular uniforms absent any substantial protection, the essential vulnerability of the infantryman was acquiesced to by modernising militaries around the world. With the development and spread of shell artillery, this vulnerability has become horrifically acute over time. Infantry increasingly avoid direct combat with each other because their primary threat is now the artillery. During the American Civil War, around 12% of casualties came from artillery (McIntire, 2022), and in the First World War, the war of the 'big guns' pounding troops trapped in trenches, that figure rose to over sixty percent (Jones, 2016). In the battlefields of Ukraine, however, every four out of five casualties (Watling, 2024) came from artillery fires. Casualties among infantry are not only expected but even incorporated into strategies of relative attrition (Gady & Kofman, 2024). Infantry are less survivable than ever, yet are no less relevant than they have ever been.

3. Good is Better than Bad, but Bad is Better than None

What makes these systems, like the infantryman or the armoured tank, persist in the modern army despite visually observed evidence of their vulnerabilities? There is indeed a much more accurate explanation: the lack of available superior alternatives. Superiority means that an alternative system either (1) fulfils the same battlefield role as the previous system but with better efficiency or performance, or (2) transforms or replaces the previous battlefield role by creating a new capability. For example, weapons systems whose evolution is measured in "generations" of systems, such as fighter jets or tanks, become superior through superior range of engagement, speed, armament, and/or numerous other capabilities. Generally speaking, the newer systems of newer generations dominate those of previous generations, such as when the US Air Force and allies decimated the hundreds of older aircraft of Saddam Hussein's Iraqi regime during the Gulf War. Likewise, the carrier demonstrated its superiority over the battleship by replacing its gun-based fire support with air-based fire support. As a sophisticated platform for

naval aircraft, carriers exploited them to strike farther and with greater precision—even though they were no more survivable against the anti-ship weapons of the time than battleships. Simultaneously, the superior alternative must also be available. A military must be able to procure and maintain a weapons system, which is not possible under budget constraints, under sanctions regimes, or in the absence of infrastructure for it, such as sufficient replacement parts or ammunition. Yet if a weapons system is expensive enough, it cannot replace other systems that are inferior since even the wealthiest of militaries are limited by economic constraints and budgetary pressures from other departments. For example, a regular unguided munition is inferior in most characteristics, such as range and accuracy, to most modern precision missile systems. Nonetheless, their cost makes them prohibitively expensive for strikes against less-valuable but still important targets like trench defences and heavy equipment. In other cases, a weapon system might, on paper, be superior to its peers but locally or fundamentally lack important supporting elements in sufficient quantity, like a consistent supply of ammunition, fuel, or proprietary replacement parts. In other circumstances, a military simply does not have sufficient quantities of the most modern systems but still requires specific battlefield roles to be fulfilled. Nowhere is this more apparent today than in Ukraine. The Russian Armed Forces, for example, continue to require armour to protect assaults and transport infantry quickly, but stockpiles of T-80 and T-72 series tanks have been severely attrited or emptied, and production and modernisation of newer armour have not kept pace with loss rates. As a result, the Russian Ministry of Defence continues to draw down equipment reserves for older tanks and artillery, even pieces better suited for museum exhibitions than frontline combat. Ukrainians, for their part, have relied extensively on underarmoured donations, like the myriad Humvees and Mine-Resistant Ambush Protected vehicles (Axe, 2023), leftover from decades of counterinsurgency warfare, for frontline assaults in the absence of sufficient donated or domestic armour. Likewise, some of the qualitative advantages of Western-donated artillery systems like the German Panzerhaubitze 2000 or the French Caesar self-propelled guns over older Soviet systems, in light of the paucity of 155mm artillery shells, could not be exploited as intended. In other circumstances, Russian units have used golf carts (Axe, 2024) and motorcycles (Segura, 2024)—which are completely devoid of any direct protection—to at least maximise the mobility of infantry. That most of these systems lack survivability does not preclude their use, for even an older tank presents a threat. As commentators mock the "outdated" and "obsolete" systems in use by the Russians, they ignore that the same conditions of mass attrition cause similar equipment problems for Ukrainians. Without alternatives, the standards for obsolescence fall dramatically. For a weapons system to be truly obsolete, there evidently must be alternative systems that fulfil the same or a better tactical purpose, and they must be available in sustainable quantities. Certainly, some historical military technologies appear to have fallen into irrelevance because of their survivability. Defensive technologies, like castles and the intricate star forts that later replaced them, or steel armour and shields, are no longer survivable against modern explosive artillery and high-calibre ammunition. Yet in so far as their role was their survivability—to be able to consistently repel the various contemporary projectile and melee threats of their time—and this was made generally impossible by the aforementioned weapons, their obsolescence was still distinctly caused by a change in their battlefield role, one that overlapped with survivability. This is not to argue that the bicycle or the early Cold War tank is not obsolete, but it reaffirms how much more nuanced the contribution of technology is to strategic planning than is presented within the neat vacuums of academic debate. Although firearms immediately presented a kinetic advantage over bolts and arrows, it took centuries of improvements in fuse safety, barreling, and reload mechanism design for them to become the

Infantry are less survivable than ever, yet are no less relevant than they have ever been.

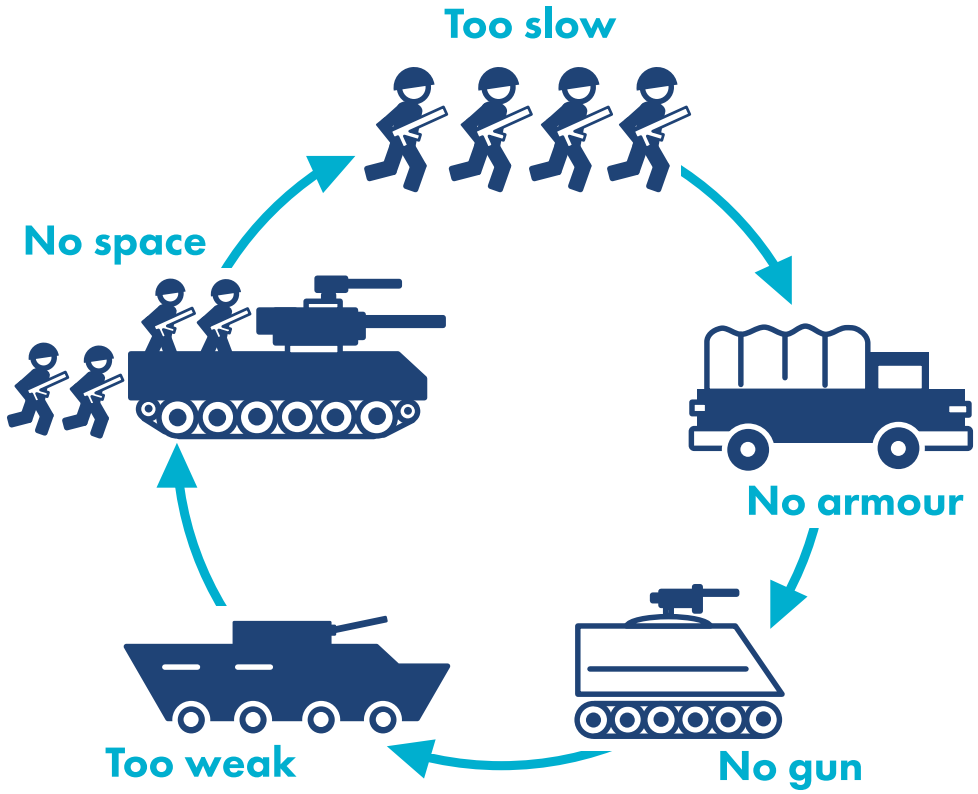


Figure 2: Development Cycle of War Machinery

universal weapon of the infantryman. Still today, some militaries employ modernised crossbows for niche situations where noise discipline is crucial. Likewise, even the widespread proliferation of ranged weapons did not immediately spell the end of melee combat. Bayonets, knives, and clubs were common in the trenches of the First World War, and as late as 1945, Imperial Japanese defence procurement insisted on bayonet lugs for the Type 96 and Type 99 light machine guns and other main firearms.

Technology thus absolutely drives the development of new tactics, but tactical thought likewise influences the adoption of technology. Until advancements in artificial general intelligence facilitate human-machine teaming, or even machines by themselves capable of assaulting and occupying territory, militaries will continue to plan offensive action around infantry in mechanised armour supported by long-range fires and air support. This likely means the persistence of many contemporary systems, like tanks or aircraft. Drones provide a tantalising, cost-effective answer to fighter jets and their missiles in theory. But can you design a combat drone that can fly as far and as fast as a fighter jet, equip it with sufficiently strong sensors to detect the jet, and carry capable enough ordinance to engage it without simply making another expensive aircraft whose decision-making is slowed down by remote piloting or still unreliable algorithms? The anecdote of the Russian S-70 Okhotnik-B unmanned combat drone, which was shot down by friendly aircraft over Ukrainian territory after a catastrophic control failure (Newdick, 2024), perhaps hints at why major militaries have not yet changed their tactical approach completely away from piloted combat aircraft.

4. Conclusion

Military procurement has long been seen as a distant realm of government policy, more the target of disdainful lip service for its wastefulness in light of pressing civil and environmental needs than any meaningful debate. Indeed, the procurement of technologies and the construction of supply chains, conducted on a national level far away from constituents, do not synergise well with a transparency that can create sensitive vulnerabilities for armies. But if we are to have meaningful public debate on specific military procurement and the social opportunity costs of sixth-generation fighter jets and other systems, we have to understand the need for nuance, avoid reductive conceptualisations with little external validity, and accept that

Figure 3: German forces pull 10.5cm howitzers on horseback in occupied Norway, 1940. Although trucks would have been a much more efficient transport for artillery, horses were often in more abundant supply than either trucks or their fuel. National Library of Norway, CC 4.0

the survivability lens oversimplifies the battlefield into a narrow, game-like mentality. Warfare is not a rock-paper-scissors match wherein the existence of gaps in specifications and capabilities of certain weapons systems leads to catastrophically one-sided engagements. This may prove difficult in an era of pervasive social media that provides the user with an unprecedented access to both battlefield information and their political representatives. Some private citizens, influenced by public online debates, even directly affect the outcome of national budget proposals (Gold et al., 2024). Musk and his like-minded colleagues are certainly far from being authoritative experts on military affairs, but they might still have a wide public audience and access to key government actors. Some might even be investors in emerging miltech and Silicon Valley darling firms like Anduril, which sells drone prototypes to the US Department of Defence, and thus have clandestine motivations to influence the distribution of billions of dollars in military contracts. Regardless, individuals with access to the internet are now privy to a wealth of readily available open-source information that intelligence agencies once expended a tremendous amount of resources and effort to obtain. Satellite imagery lets users speculate on the rate of equipment loss and specifications of nuclear submarines, driving security analysis without relying on experts with insider information or direct military publications. Telegram and other platforms publish endless streams of media from current conflicts, whose biased selection makes the vulnerabilities of military technologies more visible than ever before. Occasionally, confidential specifications are leaked online for sometimes the most trivial of reasons. Such a flood of information easily facilitates erroneous narratives and obscures the nuanced reality in military affairs as it does in other realms. Citizens certainly can and should expect their military officials to have more in-depth and accurate assessments necessary for strategic procurement. Yet the slow death of the Pax Americana and the return of conventional war require sustained increases in defence budget spending, which means sacrifices elsewhere. If citizens are to understand the necessity of procurement decisions in the coming future, they must understand that survivability does not necessarily drive obsolescence.

References

Axe, D. (September 2023). The Ukrainians Are Using Their MRAP Armored Trucks in Direct Assaults On Russian Positions. Forbes. https://www.forbes.com/sites/davidaxe/2023/09/20/the-ukrainians-are-using-their-mrap-armored-trucks-in-direct-assaults-on-russian-positions/

Axe, D. (March 2024). Russia's Golf Cart Troops Don't Stand A Chance. Forbes. https://www.forbes.com/sites/davidaxe/2024/03/22/russias-golf-cart-troops-dont-stand-a-chance/

Boot, M. (April 2024). Weapons of War: The Race Between Russia and Ukraine. Council on Foreign Relations. https://www.cfr.org/expert-brief/weapons-war-race-between-russia-and-ukraine
Cancian, M. F., Park, C. H. (March 2024). Can South Korean 105-Millimeter Ammunition Rescue Ukraine? Center for Strategic & International Studies. https://www.csis.org/analysis/can-south-korean-105-millimeter-ammunition-rescue-ukraine

Cohen, S. (2010). Where are the Carriers? Forbes. https://www.forbes.com/sites/stevecohen/2010/10/25/where-are-the-carriers/

Cumming, E. (March 2022). Is this the end of the tank? The Telegraph UK. https://www.telegraph.co.uk/news/2022/03/14/end-tank/

Epstein, J. (December 2024). Israel showed the ‚power' of F-35s in destroying nearly all of Iran's air defenses without a loss, UK admiral says. Business Insider. https://www.businessinsider.com/israel-showed-power-of-f-35s-iran-strikes-uk-admiral-2024-12

Insinna, V. (September 2020). The US Air Force has built and flown a mysterious full-scale prototype of its future fighter jet. DefenseNews. https://www.defensenews.com/breaking-news/2020/09/15/the-us-air-force-has-built-and-flown-a-mysterious-full-scale-prototype-of-its-future-fighter-jet/

Gady, F-S. & Kofman, M. (February 2024). Making Attrition Work: A Viable Theory of Victory for Ukraine. International Institute for Strategic Studies. https://www.iiss.org/online-analysis/survival-online/2024/01/making-attrition-work-a-viable-theory-of-victory-for-ukraine/

Gold, H., et al., (December 2024). Elon Musk comes out swinging against government spending package in early test of his political might. CNN Business. https://edition.cnn.com/2024/12/18/media/elon-musk-government-spending-bill-doge/index.html

Hambling, D. (November 2024). Elon Musk Calls F-35 Builders 'Idiots', Favors Drone Swarms. Forbes. https://www.forbes.com/sites/davidhambling/2024/11/26/elon-musk-calls-f-35-builders-idiots-favors-drone-swarms/

Jensen, B. (January 2025) What China's New Fighter Jet Really Signals. Foreign Policy. https://foreignpolicy.com/2025/01/16/china-new-fighter-jet-military-capabilities/

Jones, E. (2016). Terror Weapons: The British Experience of Gas and Its Treatment in the First World War. National Library of Medicine. https://pmc.ncbi.nlm.nih.gov/articles/PMC5131841/

McIntire, T. (June 2022) "We Bury Our Dead" – The Effects of Civil War Artillery. National Museum of Civil War Medicine. https://www.civilwarmed.org/effects-of-artillery/

Newdick, T. (October 2024). Russia's S-70 Hunter Drone Was Armed When Shot Down By Friendly Fighter Over Ukraine. The Warzone. https://www.twz.com/air/russias-s-70-hunter-drone-was-armed-when-shot-down-by-friendly-fighter-over-ukraine

Lagrone, S. (December 2024). U.S. Super Hornet Shot Down Over Red Sea in Friendly Fire Incident; Aviators Safe. US Naval Institute News. https://news.usni.org/2024/12/21/u-s-super-hornet-shot-down-over-red-sea-in-friendly-fire-incident-aviators-safe

O'Brien, P.P. (May 2022). War Will Never Be This Bulky Again. The Atlantic. https://www.theatlantic.com/ideas/archive/2022/05/ukraine-russia-putin-war/638423/

Polmar, N. (2008). Aircraft Carriers: A History of Carrier Aviation and Its Influence on World Events, Volume II: 1946-2006 (Vol. II). Potomac Books, Inc.

Segura, C. (June 2024). Russian army develops motorcycle assault units to carry out lightning attacks on the front lines. Él Pais. https://english.elpais.com/international/2024-06-18/russian-army-develops-motorcycle-assault-units-to-carry-out-lightning-attacks-on-the-front-lines.html

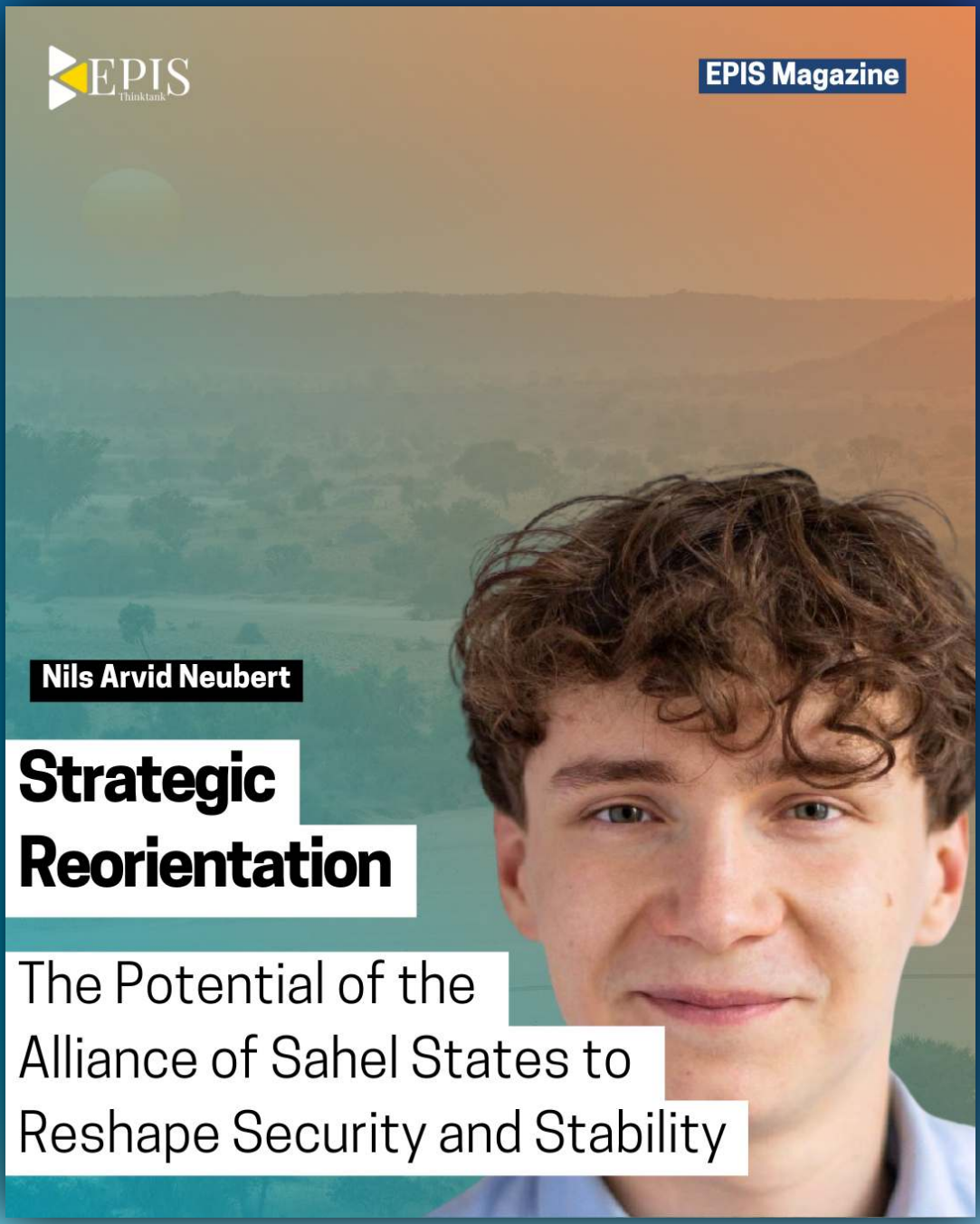
Sullivan, J. F. (January 2025). Twitter/X Thread. https://x.com/JohnF_Sullivan/status/1876738289492795889

Watling, J. (February 2024). The Peril of Ukraine's Ammo Shortage. Time Magazine. https://time.com/6694885/ukraine-russia-ammunition/

West, B. (August 2024). Has High Tech Made Artillery Obsolete? Hoover Institution. https://www.hoover.org/research/has-high-tech-made-artillery-obsolete

Vroom, G. B. (1925). Strategic Value of the Aircraft Carrier. Proceedings. U.S. Naval Institute. https://www.usni.org/magazines/proceedings/1925/january/strategic-value-aircraft-carrier

Zabrodskyi, M., Watling, J. Oleksandr V. D., Reynolds, N. (2022). Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022. Royal United Services Institute for Defence and Security Studies.



About the Article

The Sahel is undergoing a profound geopolitical shift. Nils A. Neubert examines how the Alliance of Sahel States (AES)—Mali, Niger, and Burkina Faso—has broken from Western security partners, turning instead to Russia and Turkey. While AES's joint military force improves operational flexibility, authoritarian counterterrorism and ethnic militias risk fueling jihadist recruitment. Without political inclusion and sustainable governance, Neubert argues, lasting stability remains elusive.

About the Author

Nils A. Neubert is a student of Political Science and African Studies at the University of Leipzig. His research focuses on security policy in Africa, with a regional emphasis on the Sahel, and the nexus between development and security.

1. Introduction

In an increasingly multipolar world where many states are diversifying their international relations, the Sahel is by no means an exception. After years of more or less close alignment with the West, the last French troops have now left the region. In particular, the three countries of Mali, Niger, and Burkina Faso are strategically realigning, as they pursue membership in the BRICS within the framework of the Alliance des États du Sahel (AES) and are increasingly turning to partners such as Russia and Turkey for security cooperation. This alliance also aims to foster closer military collaboration among their members themselves, including the formation of a joint force. Given the deteriorating security situation in Mali, Burkina Faso, and Niger – largely driven by a multitude of jihadist actors – the question arises as to whether the AES and its new partners have the potential to reshape security in the Sahel region. This essay argues that while the AES offers several operational advantages, the disadvantages currently outweigh these benefits. Although the AES countries receive external support, particularly from Russian Wagner Group/Africa Corps, the exclusion and repression of significant portions of the population prevent the mitigation of security threats in the region. Unless current anti-terror strategies of AES states are complemented by political components, the situation is likely to remain precarious. Furthermore, self-defense militias often exacerbate existing ethnic tensions, thereby perpetuating the alignment of certain population groups with Islamist militias. The relevance of this essay is derived primarily from the catastrophic security situation in the focal countries under analysis. Equally important, however, is the context of shifting geostrategic partnerships among African states, particularly in the security sector, and the ensuing implications thereof.

2. Breakup With the West - A Step Towards Genuine Sovereignty?

Traditionally, the former colonial power France has been deeply embedded in the region. In 2013, as part of Opération Serval, France supported the Malian government in countering an offensive by militant Islamists from northern Mali's Azawad region. Subsequently, from 2014 onward, France contributed to combating transnational jihadist terrorism and stabilising the region through Opération Barkhane—albeit with limited success. Germany also took part in counterterrorism efforts in the Sahel through the UN stabilisation mission MINUSMA, first mandated in 2013, and was, at times, the second-largest non-African troop-contributing country after Bangladesh (UN, 2020). Due to growing disagreements with the Malian military junta, which has been in power since 2020, France, previously involved in counterterrorism efforts in Mali through Opération Barkhane with up to 4,500 soldiers, withdrew its troops from the country as early as August 2022 (Spiegel, 2022). The junta's differences with other nations participating in the United Nations peacekeeping mission in Mali (MINUSMA), such as Germany also intensified, for instance through the denial of overflight rights by Malian authorities (Gebauer, 2022). While Germany had already decided in November 2022 to withdraw its troops by May 2024 (Monath, 2022), the Malian junta demanded in June 2023 the withdrawal of MINUSMA "without delay" (Diop cit. in Al Jazeera, 2023), citing its perceived inefficiency. In response, the UN Security Council, two weeks later, mandated the immediate termination of the mission and its withdrawal by the end of the year (UNSC, 2023). With Burkina Faso terminating its military cooperation agreement with France in February 2023 (Ndiaga, 2023), Niger also increasingly turned towards Russia, prompting French, American and German contingents to leave the country (Reuters, 2023; DW, 2024; Mackinnon, 2024). In July 2023, when the Nigerien military staged a coup against the incumbent president Bazoum, Niger became the third country in the Sahel, after Mali and Burkina Faso, to fall under the rule of a military junta. In response to the coup, the Economic Community of West African States (ECOWAS) announced plans to intervene in Niger to restore constitutional democratic order. Together, the military juntas of Niger, Mali, and Burkina Faso

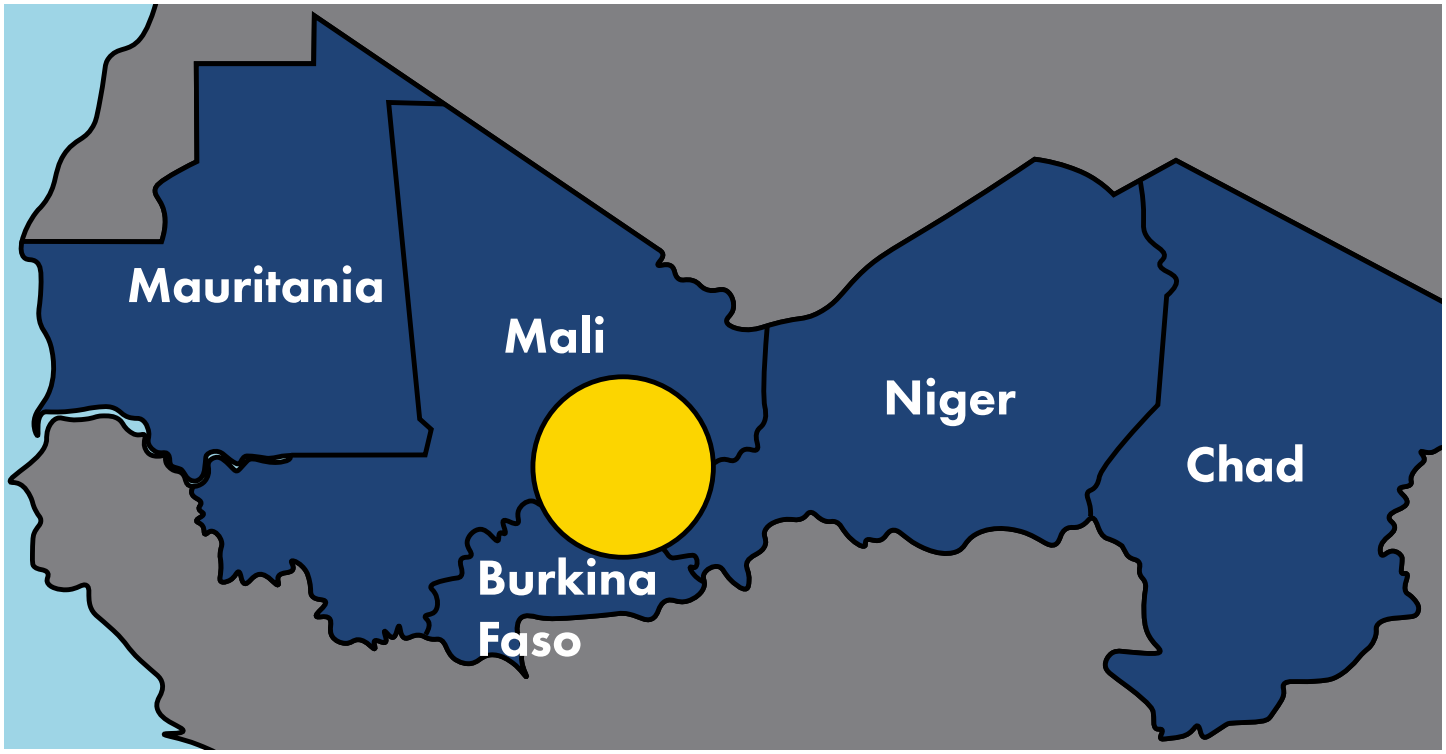


Figure 1: The Liptako-Gourma Region in Mail, Burkina Faso and Niger - PRIF BLOG, Source: ECFR, 2024

subsequently established the Alliance of Sahel States (AES) as a "mutual defense pact against external and internal threats, including terrorism" (Sow & Koné 2024). Although no intervention of ECOWAS ultimately occurred, the most significant security challenge currently facing the three Sahel countries remains the rampant threat of terrorism, particularly prevalent in the tri-border region of Liptako-Gourma. Initially founded as a defensive alliance against intervention from ECOWAS, the leading military juntas of the three countries soon announced the establishment of a confederation (Le Faso, 2024). This measure is part of a broader trend of reorientation towards "genuine independence and self-determination" among many states in the Sahel, which is understood here as comprising the countries of Mauritania, Mali, Burkina Faso, Niger, and Chad. Especially French activities in the region are frequently interpreted as neocolonial. Demands for the withdrawal of Western troops from Mali, Niger, and Burkina Faso should also be understood in this context. The turn away from Western powers is further highlighted by increasingly deepening ties of the Alliance of Sahel States with Russia and their desire to join BRICS (Kohnert, 2024). As part of an increasing rapprochement between Mali, Niger and Burkina Faso and a strategic reorientation away from traditional Western security partners, the establishment of a joint combat force represents a key project of the newly founded AES confederation. The announcement of closer cooperation in the field of security occurs within the context of increasing insecurity due to terrorists and rebel group activities (ACLED, 2024). Particularly active groups in this regard are the Islamic State in the Greater Sahara (ISGS) as well as the Al-Qaeda affiliated Jama'at Nusrat ul-Islam wa al-Muslimin (JNIM), a coalition formed in 2017 of several jihadist groups such as al-Mourabitoun, Katiba Macina, and Ansar Dine. While both control large swaths of Burkinabé territory – JNIM approximately 40% and ISGS about 10% (Brown, 2024) – the potential of those groups to openly challenge the state militaries of AES countries is further exemplified by the unprecedented attack that JNIM fighters launched on Malian military infrastructure near its capital in September (Jezequel, 2024). In this context, the question arises as to what extent deeper collaboration among AES countries and a reorientation away from Western partners hold the potential to reshape security and stability in a region severely affected by terrorism. This question is particularly relevant given that the hotbed of West African terrorism is located in the tri-border region of Liptako-Gourma, at the geographical nexus of the three AES countries (see Figure 1).

3. Increasing Interoperability and Flexibility: Advantages of Regional Security Integration

Closer regional cooperation, especially in the face of a transnational threat, offers numerous advantages in terms of interoperability and (geographical) operational flexibility of national contingents. Thus, one of the obvious advantages of an AES cross-border joint force, that is according to the Nigerien Minister of Defense Mody operational since January 2025 (AP News, 2025), lies in the pooling of resources and troops (Bassou, 2024), which can enhance flexibility and lead to more effective utilisation of existing resources. Additionally, the establishment of a legal framework that permits the pursuit of terrorists across borders, as suggested by Coulibaly, appears particularly beneficial in the context of the transnational nature of security threats in the Liptako-Gourma region (Baele et al., 2020; Touré, 2024). Furthermore, an increase in interoperability among the three national militaries would be advantageous, as it would significantly facilitate the execution of joint operations, especially in border areas. Closer collaboration regarding the sharing of intelligence information and aerial capabilities, as well as the exchange of liaison officers, demonstrates the progress already made towards greater cohesion and enhanced interoperability (Abba, 2024). The joint military exercise Tarhanakal, which involved not only the three AES states but also contingents from Chad and Togo (ibid.; ActuNiger, 2024), illustrates not only the commitment to a joint interoperable force but also accounts for the necessity of embedding a counter-terrorism strategy within a broader regional context, considering the "inexorable descent" (Toulemonde, 2022) of terrorist groups towards the Gulf of Guinea. While Ghana remains the only country in the region that has not yet experienced attacks by JNIM or ISGS, significant potential exists for terrorist groups to exploit grievances stemming from marginalised ethnic minorities in the northern part of the country to establish a presence there (Brown, 2024). In this context, the call by Ghana's newly elected President, John Mahama, to provide greater support to AES states in their fight against terrorism must be understood. In his appeal, he specifically referenced Benin and Côte d'Ivoire (Daily Post Nigeria, 2024), both increasingly targeted by jihadist activities (Boeke, 2021; Vines, 2024b).

The Sahel:
A semi-arid African region south of the Sahara, spanning from the Atlantic to the Red Sea, facing droughts and conflicts.

4. Western Withdrawal: Russia and Turkey Able and Ready to Fill the Gaps?

Following the withdrawal of Western partners from the three AES states of Mali, Burkina Faso, and Niger, these countries are increasingly turning to Russia as a partner in the fight against terrorism. Although the withdrawal of MINUSMA and Western troops from the AES countries has led to a 'capacity drain' in the fight against terrorism, other external partners stand ready to fill those gaps. Notably, Russian Wagner troops are supporting the Malian military (FAMa) (Elischer, 2022; Spearin, 2024), while troops from the Russian Africa Corps are mainly present in Burkina Faso and Niger for training purposes (Spearin 2024; Karr & Gianitsos, 2024). The Africa Corps, which seems to be now active in all AES countries (Spearin, 2024; Karr & Gianitsos, 2024), does not stand in opposition to Wagner. It was formed to replace Wagner and to align its independent operations more closely with Russian state strategies, particularly in response to the growing uncontrollability exemplified most notably by the Prigozhin-led uprising in June 2023. Unlike Wagner, it is subordinated to Russian state institutions such as the Ministry of Defense or the military intelligence agency GRU (Bryjka & Czerep, 2024). Nevertheless, the Africa Corps in many ways represents a continuation of Wagner's tradition (Lechner, 2024) and primarily recruits from its former fighters (Wolkov et al., 2023). In addition to personnel support, recent arms deliveries to Burkina Faso and Niger countries have been reported (Peltier, 2024), while Russia had

already sent fighter jets and helicopters to Mali in 2022 (Al Jazeera, 2021). The delivery of Turkish Bayraktar drones to the armies of the AES countries (Le Figaro, 2024; Le Monde, 2024; RFI, 2022) could also significantly contribute to effective counter-terrorism efforts – especially following the withdrawal of American forces from Niger, particularly from Base 201 (Tait, 2024), which served as a launchpad for intelligence gathering on terrorist movements and the liquidation of key terrorist leaders (Peltier & Schmitt, 2024; Schmitt, 2018).

5. Authoritarian Conflict Management: A Strategy That Does Not (Yet) Pay Out

However, it is highly questionable whether these advances are sufficient to address the volatile security situation within the territory of the AES countries. The Wagner forces notably lack important capabilities compared to their French counterparts, such as the ability to operate or even move autonomously. Furthermore, the withdrawal of western air capabilities from Mali and Niger represented – at least temporarily – significant vulnerabilities (Nasr, 2022), leaving it unclear to what extent these withdrawals have since been compensated. The reliance on Russian support seems to be further detrimental regarding the long-term goal of stability concerning the anti-terror strategy of Russian forces, which have been described as "iron-fist" (Jezequel, 2024) or "brutal and indiscriminate counterinsurgency efforts" (Nasr, 2022, p. 21), characterized by the "application of violence" (Spearin, 2024, p. 3). This is exemplified by the fact that the Wagner Group was involved in 71% of all "Organized Political Violent Events Targeting Civilians" in the first seven months of 2022 in Mali (Serwat et al., 2022). Malian forces were frequently complicit in severe human rights violations committed by Wagner (Spearin, 2024), with the massacre in Moura, resulting in between 300 and 600 (civilian) deaths (Faulkner, 2022), being the most egregious example. Civilian targeting significantly contributes to the fact that affected population segments, particularly semi-nomadic herders of the already marginalized ethnic Fulani group, increasingly turn towards terrorist groups. In this context, Amadou Koufa, leader of the jihadist group Katiba Macina, also noted that civilian targeting of the Fulani "contributes directly to the engagement and recruitment of the Fulani in the ranks of jihadists" (Koufa cit. in France24, 2024).

Reliance on Russian support seems to be detrimental regarding the long-term goal of stability.

6. 'Self-Defense'-Militias: Operating Along the Lines of Ethnic Tensions

The targeting by state militaries and/or Russian forces is further exacerbated by the states' partial reliance on local 'self-defense' militias, which have been employed to provide intelligence and low-threshold security measures to villages threatened and attacked by terrorist groups. Several massacres, with each resulting in hundreds of civilian Fulani victims, can be attributed to such self-defense militias. In 2019, more than 130 Fulani were killed by Dan Na Ambassagou, a self-defense militia of the Dogon ethnic group, in the Bankass area of the Mopti region in southern Mali (France24, 2019), which consequently led to the group's ban (RFI, 2019), although some cells still appear to be active (HRW, 2024). In Burkina Faso, however, since President Ibrahim Traoré assumed office in 2022, the use of auxiliary corps has been significantly intensified (ICG, 2023), although under his predecessor Kaboré, efforts were made in 2016 to integrate local self-defense militias into state structures (Soré et al., 2021). However, regarding the Koglweogo, one of the most active self-defense alliances in Burkina Faso and with approximately 45,000 members by far exceeding the size of the national army, those efforts remained unsuccessful (ibid.; Gabriel, 2024). While it should be emphasised that different "Koglweogo groups emerge from diverse historical and socio-political realities" (Soré et al., 2021, p. 130), most of their members belong to the Mossi ethnic group (Haavik 2022; da Cunha Dupuy, 2019; Demuynck, 2021). While the Mossi predominantly represent a sedentary

agricultural population, the Fulani are often semi-nomadic herders. This distinction, particularly in the context of numerous droughts over the past decades, population growth (Boukhars & Pilgram, 2023), southward migration of many Fulani in search of viable grazing land (Tiegna, 2021; Ansorg, 2021), and the resulting intensified pressure on available land, has contributed to a broader 'crisis of pastoralism' (Boukhars & Pilgram, 2023) and resource conflicts. The Koglweogo gained prominence in 2015-16 for their efficiency in combating (armed) criminality, albeit through the extensive use of violence and human rights violations (Haavik, 2022). As such, they provided at least a partial response to the security void created by the low level of state governance in rural areas. Even if the Koglweogo occasionally operate in conjunction with the army and police, their activities are guided by their own system of justice, which they independently administer and enforce (Piombo et al., 2021). This includes detaining individuals, publicly (physically) punishing them (Tiegna, 2021), and imposing fines on identified suspects. Especially in the regions of northern and eastern Burkina Faso where the Koglweogo operate, the Fulani constitute a significant minority often depicted as ethnically aligned with terrorist organizations, with the Koglweogo considerably contributing to such narratives (Quidelleur, 2021; Haavik, 2022). Through frequent and brutal targeting of Fulani communities (Kim & Kim, 2024; Demuynck, 2021), the strategies employed by the Koglweogo further contribute to the ethnicisation of complex conflicts over land and resource use, significantly exacerbating the security situation. A striking example in this regard is the Yirgou massacre: In January 2019, in the Barsalogho department of northern Burkina Faso, after a village chief was killed by individuals allegedly speaking Fula, local Koglweogo launched a retaliatory attack on nearby Fulani settlements, resulting in several hundred fatalities (Tiegna, 2021). Consequently, 19,000 people were displaced from the region (ibid.; da Cunha Dupuy, 2019). Despite these events, no punishments were meted out to the perpetrators, as Koglweogo not only undermine state authority but also challenge its capacity to enforce the rule of law, increasingly operating beyond the state's control (Haavik, 2022). Frequent attacks by local vigilante groups, state armies, or external fighters indeed lead marginalised groups to turn towards criminal and terrorist organizations in order to seek protection and/or revenge (Ansorg, 2021; Boukhars & Pilgram, 2023). This, in turn, transforms the narrative that they are terrorists into a self-fulfilling prophecy, further fueling the proliferation of violence. The "intersection of ethnicity and occupation" (ibid., p. 4) facilitates terrorist organizations to exploit these social cleavages (ICG, 2017) by positioning and portraying themselves as protectors of marginalised communities, for instance, through the reorganisation of land-use rights in territories under their control (Boukhars & Pilgram, 2023). The increasing reliance on local self-defense militias, as well as the brutal approaches of Malian and Russian troops, appears to exacerbate rather than sustainably resolve the complex "cycle of revenge and retaliation exacerbated by ethnic polarization" (ibid., 6). The Fulani are by no means the only ethnic community actively courted by terrorist organisations due to their "history of repression" (Vines & Wallace, 2022). Other ethnic groups, such as parts of the Tuareg or the Songhai, are also targeted by jihadist groups seeking to exploit "the deep resentment of the communities [...] towards their respective central governments" (Kazeem, 2024). This is further illustrated by the fact that, despite increasing calls for national unity in the name of comprehensively understood 'forces vives de la nation' [vital forces of the nation] to strengthen social and societal cohesion (Grütjen, 2024), rebels from the northern Malian Azawad region resumed their fighting in the summer of 2023, driven, according to the rebels, by continued provocations and ceasefire violations from the Malian side contrary to the provisions of the 2015 Algiers Agreement (RFI, 2023; Le Figaro, 2023).

7. Russian Supply Routes At Stake in Syria With No Viable Alternatives In Sight

While the question arises as to whether the approach to counterterrorism adopted by the military governments of the AES countries, characterised by an Authoritarian

Percentage of Organized Political Violence Events Targeting Civilians by Actor and Country During Wagner Deployment

Timeframe in Mali: 1 December 2021 - 31 July 2022
Timeframe in Central African Republic: 1 January 2018 - 31 July 2022

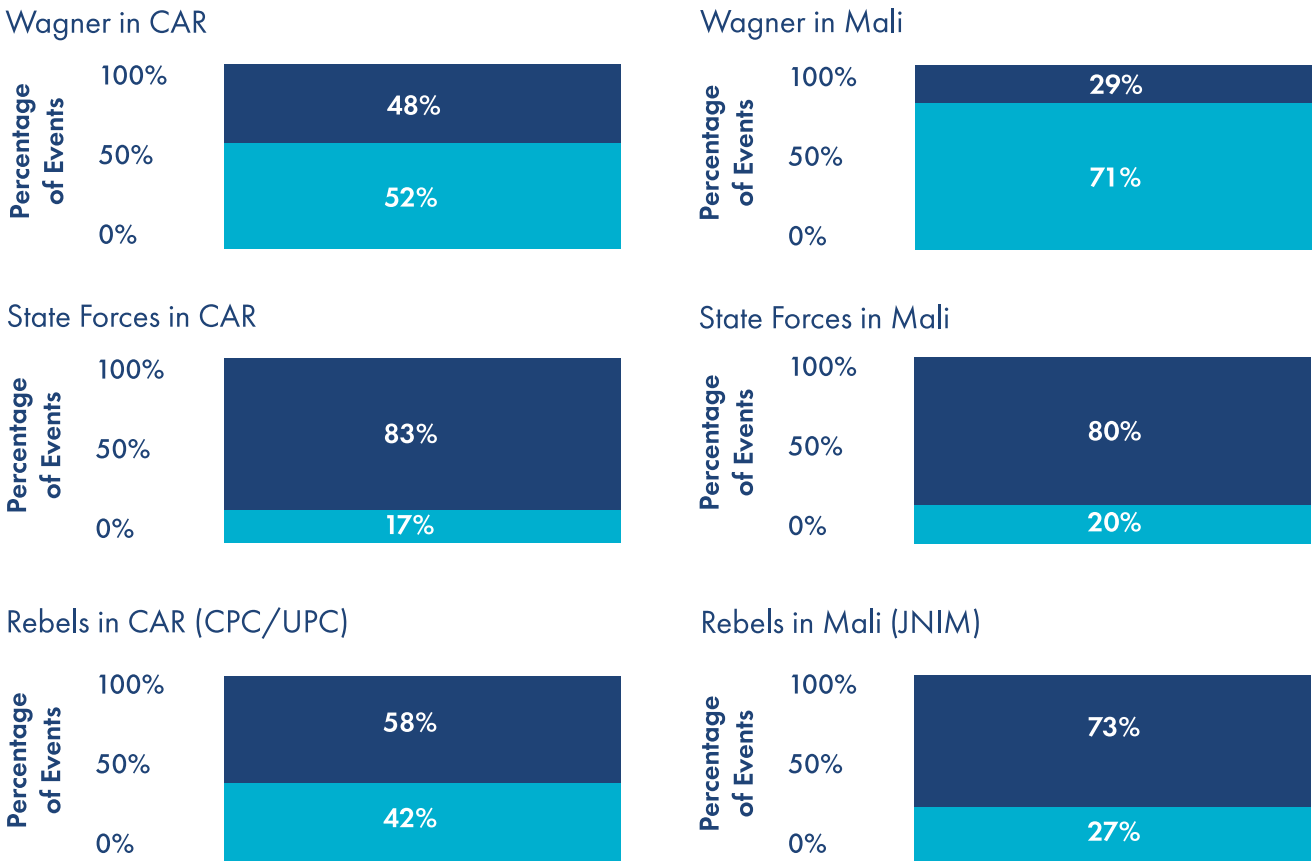


Figure 2: (Serwat et al. 2022)

Conflict Management approach (Spearing, 2024) and the use of local self-defense militias as the Koglweogo, plays into the hands of terrorist groups, Russian support for Sahelian efforts in this regard appears to be experiencing a significant blow in Syria: Following the fall of Syria's decades-long dictator Assad, Russian support for AES countries in counterterrorism efforts could face increasing constraints, as the future of Russian bases in the western Syrian region of Latakia, vital logistic hubs for Russia's power projection into Africa, remains, at the time of writing, uncertain. Specifically, the port of Tartus and the Khmeimim Air Base have served as critical nodes for Russian supply routes and logistics toward Africa. Their loss would therefore have considerable strategic implications for Russia's ability to project power into the region. Although Russia has repeatedly demonstrated its capability in handling radical Islamist groups such as the Houthis or the Taliban and could potentially lend international legitimacy to the new state authority of the radical Islamist Hay'at Tahrir al-Sham (HTS) (Smagin, 2024), it remains doubtful whether HTS would allow a military force to operate from Syrian territory that had supported their main opponent, Assad, militarily for nine years – notably through bombings targeting HTS positions (ibid.). Furthermore, HTS is likely to view critically that Russia has granted asylum to Assad (Al Jazeera, 2024). An alternative strategic hub and operational base for activities in Africa could be the eastern part of Libya, controlled by Russian-backed General Haftar (Wehrey, 2024). Some reports already point to the transfer of various Russian military assets to this region (Faucon & Seligman, 2024; Ebrahim & Lister, 2024). However, Haftar, wary of Turkey's growing involvement in the area, might view an exclusive dependency on Russia with skepticism (Wehrey, 2024).

Moreover, the geographical proximity of Libya to NATO territory could significantly complicate Russia's efforts to establish a major military hub there for its operations in Africa. Another potential option, Port Sudan, which has long been a focus of Russian considerations (Karr, 2024), appears less viable due to the ongoing civil war in Sudan. The substantial material demands of the Sudanese army – likely driving up the cost of hosting a Russian base (Knipp, 2024) – and the significant geographical distance from Russia are additional factors that make the location appear less favorable as a military hub in comparison. Although the future of Russian troops in Syria remains unclear at the time of writing, and the search for alternatives is fraught with numerous contingencies, Assad's fall in Syria highlights the precarious nature of Russia's supply lines to sub-Saharan Africa. In the event of a withdrawal or significant weakening of the Russian presence in the Sahel due to volatile supply routes, an increased reliance on security providers from other countries, such as the already present mercenaries of the Turkish Sadat PMC, could present an alternative for the ruling juntas of the AES countries. However, this eventuality also appears unlikely to offer any improvement, given the "horrific human rights record" (Kohnert, 2024, p. 6) of Turkish armed groups, which could trigger similarly exacerbating dynamics as the activities of the Wagner Group.

8. Conclusion

Anti-terror strategies embedded in the logic of authoritarian conflict management, rather than being complemented with political peacebuilding components, will not contribute to sustainably curbing the problem of terrorism in the AES states. The formation of an interoperable joint force consisting of the armed forces of the three AES countries, along with external material support, could indeed lead to a mid-term strengthening of counterterrorism efforts, particularly in the Liptako-Gourma region. However, it should be noted that the sheer ineffectiveness of current strategies regarding long-term peacebuilding measures suggests that an end to terrorist groups activities and instability is not discernible. Furthermore, given the shaky structure of Russia's logistical hubs to Africa, it remains questionable to what extent the current "iron-fist" strategy can be materially sustained. An inclusive political process is essential as a key component of a counter-terrorism strategy to address the political and economic grievances of currently marginalised ethnic groups like the Fulani or the Tuareg, thereby removing breeding ground for NSAGs in the long term. Thus it cannot be assumed that a (sustainable) peace will occur in the contexts of terrorism in AES countries and especially the Liptako-Gourma region. It became evident all too often that violence is an inherent component of the current counter-terrorism strategies employed by these states, involving cooperation with brutally operating Russian troops and local self-defense militias, which frequently act along pre-existing ethnic and occupational divisions. The reasons why individuals join terrorist groups can certainly be traced to weak state governance structures (Apau & Banunle, 2019), as well as economic hardships and a lack of opportunities, particularly among young people (Agbiboa, 2019; Vines, 2024a). However, human rights abuses, discrimination, and (political) exclusion increasingly serve as significant driving factors for joining jihadist groups, particularly among members of ethnic minorities. The establishment of an inclusive dialogue with marginalised (ethnic) communities and their traditional authorities to improve their living conditions is thus essential for effective and long-term peacebuilding and stabilisation of the Sahel region. As long as this is not ensured, the potential of the Alliance of Sahel States (AES) to reshape security and stability in the Sahel remains limited, despite a profound strategic reorientation.

References

Abba, S. (2024). AES-Cedeao: vivre ou mourir ensemble. Jeune Afrique. Online: https://www.jeuneafrique.com/1623833/politique/aes-cedeao-vivre-ou-mourir-ensemble/ [last accessed: 25.10.2024, 22:44].

ACLED (2024). The Sahel: Mid-year metrics 2024. Online: https://acleddata.com/acleddatanew/wp-content/uploads/2024/08/Mid-year-metrics-2024-Sahel.pdf [last accessed: 25.10.2024, 22:31].

ActuNiger (2024). Exercice militaire "TARHANAKL": à Tillia, l'Armée mène des manoeuvres d'envergure avec les forces de l'AES, du Tchad et du Togo. Online: https://www.actuniger.com/societe/20131-exercice-militaire-tarhanakal-a-tillia-larmee-mene-des-manoeuvres-denvergure-avec-les-forces-de-laes-du-tchad-et-du-togo.html [last accessed: 25.10.2024, 22:53].

Agbiboa, D. E. (2015). Youth as Tactical Agents of Peacebuilding and Development in the Sahel. In: Journal of Peacebuilding & Development, 10(3), pp. 30-45.

Al Jazeera (2021). Mali receives helicopters and weapons from Russia. Online: https://www.aljazeera.com/news/2021/10/1/mali-receives-helicopters-weapons-from-russia [last accessed: 25.10.24, 23:41].

Al Jazeera (2023). Mali asks UN to withdraw its peacekeeping mission 'without delay'. Online: https://www.aljazeera.com/news/2023/6/16/mali-asks-un-to-withdraw-its-peacekeeping-mission-without-delay [last accessed: 18.12.2024, 18:16].

Al Jazeera (2024). Russia gave asylum to deposed Syrian President al-Assad, Kremlin confirms. Online: https://www.aljazeera.com/news/2024/12/9/russia-gave-asylum-to-deposed-syrian-president-al-assad-kremlin-confirms [last accessed: 01.01.2025, 15:06].

Ansorg, N. (2021). Burkina Faso. Bundeszentrale für politische Bildung. Online: https://www.bpb.de/themen/kriege-konflikte/dossier-kriege-konflikte/327266/burkina-faso/ [last accessed: 11.12.2024, 22:04].

AP News (2025). West Africa's junta-led nations announce deployment of a joint force as extremist violence spikes. Online: https://apnews.com/article/alliance-sahel-mali-niger-burkina-faso-joint-force-3e40c22ad8a90bf351b4ed0cd5648abf [last accessed: 28.01.2025, 23:36].

APA News (2024). Sahel states to form confederation, establish parliament. Online: https://apanews.net/sahel-states-to-form-confederation-establish-parliament/ [last accessed: 28.12.2024, 21:51].

Apau, R. & Banunle, A. (2019). Terrorism, Violent Extremism and Insurgency in the Sahel Region: An Assessment. In: African Journal on Terrorism, 8(1), pp. 1-20.

Baele, F., Baudais, V., Deb, S., Diarra, T., Hamani, O. & Ouédraogo, T. (2020). Humanitarian protection in the Liptako-Gourma region Local protection mechanisms and humanitarian response. Stockholm: SIPRI.

Bassou, A. (2024). From the Alliance of Sahel States to the Confederation of Sahel States: The Road is Clear, But Full of Traps. Policy Brief Nr. 19. Rabat: Policy Center for the New South.

Boeke, S. (2021). Pathways out of the Quagmire? Perspectives for al-Qaeda in the Sahel. The Hague: International Centre for Counter-Terrorism.

Boukhars, A. & Pilgram, C. (2023). In Disorder, They Thrive: How Rural Distress Fuels Militancy and Banditry in the Central Sahel. Washington D.C.: Middle East Institute.

Brown, W. (2024). Aligned in the Sand. How Europeans Can Help Stabilise the Sahel. Berlin: European Council on Foreign Relations.
Bryjika, F. & Czerep, J. (2024). Africa Corps - A New Iteration of Russia's Old Military Presence in Africa. Warszawa: Polski Instytut Spraw Międzynarodowych.

Courtright, J. (2023). Ethnic Killings by West African Armies Are Undermining Regional Security. Foreign Policy. Online: https://foreignpolicy.com/2023/03/07/mali-burkina-faso-fulani-ethnic-killings-by-west-african-armies-are-undermining-regional-security/ [last accessed: 25.10.2024, 23:11].

Da Cunha Dupuy, R. (2019): Logiques d'un maintien de l'ordre moral : le cas des groupes d'autodéfense Koglweogo au Burkina Faso. Bulletins de l'Observatoire international du religieux, n° 30-31. Online: https://sciencespo.hal.science/hal-03456049v1/document [last accessed: 11.12.2024, 21:43].

Daily Post Nigeria (2024). John Mahama urges greater support for Sahel countries in combating terrorism. Online: https://dailypost.ng/2024/12/21/john-mahama-urges-greater-support-for-sahel-countries-in-combating-terrorism/ [last accessed: 28.12.2024, 19:10].

Demuynck, M. (2021): Civilians on the Front Lines of (Counter-)Terrorism: Lessons from the Volunteers for the Defence of the Homeland in Burkina Faso. Den Haag: International Centre for Counter-Terrorism.

Deutsche Welle (2024). Germany withdraws troops from junta-run Niger. Online: https://www.dw.com/en/germany-withdraws-troops-from-junta-run-niger/a-70097640#:~:text=Germany%27s%20army%2C%20the%20Bundeswehr%2C%20has%20officially%20withdrawn%20its,the%20capital%2C%20Niamey%2C%20arriving%20in%20Germany%20late%20Friday. [last accessed: 31.12.2024, 15:59].

Ebrahim, N. & Lister, T. (2024). Spike in Russian flights from Syria to Libyan desert base as Moscow eyes new Mediterranean hub. CNN. Online: https://edition.cnn.com/2024/12/31/middleeast/spike-russian-flights-libya-desert-base-intl/index.html [last accessed: 01.01.2025, 16:21].

ECOWAS (2024). Extraordinary Summit of the ECOWAS Authority of Heads of State and Government on the Political, Peace and Security Situation in the Region: Final Communiqué. Online: https://www.ecowas.int/wp-content/uploads/2024/02/EXT-ORD-SUMMIT-FINAL-COMMUNIQUE-ENGLISH-_240225_160529.pdf [last accessed: 28.12.2024, 19:57].

Elischer, S. (2022). Populist Civil Society, the Wagner Group, and Post-Coup Politics in Mali. West African Papers, No. 36. Paris: OECD Publishing.

European Council on Foreign Relations (2024). Mapping Armed Groups in Mali and the Sahel. Online: https://ecfr.eu/special/sahel_mapping/isgs [last accessed: 31.12.2024, 15:08].

Faucon, B. & Seligman, L. (2024). Russia Withdraws Air-Defense Systems, Other Advanced Weaponry From Syria to Libya. Wall Street Journal. Online: https://www.wsj.com/world/russia-air-defense-bases-syria-libya-25810db0 [last accessed: 01.01.2025, 15:08].

Faulkner, C. (2022). Undermining Democracy and Exploiting Clients: The Wagner Group's Nefarious Activities in Africa. In: CTC Sentinel, 15(6), pp. 28-37.

France24 (2019). More than 130 Fulani massacred as ethnic and jihadist violence escalates in Mali. Online: https://www.france24.com/en/20190323-mali-100-fulani-herders-massacred-donzo-ogossagou-ethnic-violence [last accessed: 29.12.2024, 17:40].

France24 (2024). Al-Qaïda, ONG, communautés peules ... le point sur la situation au Sahel. Online: https://www.france24.com/fr/afrique/20241023-al-qa%C3%AFda-ong-communaut%C3%A9s-peules-le-point-sur-la-situation-au-sahel [last accessed: 25.10.2024, 23:07].

Gabriel, A. O. I. (2024): A Historical Analysis of Banditry and Human Security in Some West African Countries in the Sahel Region (2010-2023). In European Journal of Theoretical and Applied Sciences, 2(4), pp. 1028-1041.

Gebauer, M. (2022). Streit mit Putschregime in Mali: Bundeswehrmaschine muss nach Gran Canaria abdrehen. Spiegel. Online: https://www.spiegel.de/politik/mali-bundeswehr-maschine-muss-nach-gran-canaria-abdrehen-a-96f17233-649a-4f30-aeba-44a3d31b9594 [last accessed: 28.12.24, 18:11].

Grütjen, K. (2024). Current developments in West Africa's regional integration: Challenges for the future design of foreign and development policy. IDOS Policy Brief, No. 6/2024. Bonn: German Institute of Development and Sustainability (IDOS).

Haavik, V. (2022): Self-Defence Militias and State Sponsorship in Burkina Faso. Conflict Trends. Online: Accord+Conflict+Trends_2021+(4)+Self-defence+Militias+and+State+Sponsorship+in+Burkina+Faso.pdf [last accessed: 11.12.24, 22:54], pp. 24-31.

Human Rights Watch (2024). Mali: Atrocities by the Army and Wagner Group. Online: https://www.hrw.org/news/2024/12/12/mali-atrocities-army-and-wagner-group [last accessed: 31.12.2024, 15:25].

International Crisis Group (2023). Burkina Faso: Arming Civilians at the Cost of Social Cohesion? Africa Report N°313. Brussels: International Crisis Group.

International Institute of Strategic Studies (2023). From Global Jihad to Local Insurgencies: the Changing Nature of Sub-Saharan Jihadism. In: IISS (ed.), The Armed Conflict Survey 2023. London: IISS. Pp. 160-165.

Jezequel, J.-H. (2024). The 17 September Jihadist Attack in Bamako: Has Mali's Security Strategy Failed? International Crisis Group. Online: https://www.crisisgroup.org/africa/sahel/mali/attaque-jihadiste-du-17-septembre-bamako-lechec-du-tout-securitaire-au-mali [last accessed: 25.10.2024, 22:32].
Karr, L. (2024). Africa File, May 31, 2024: Russian Red Sea Logistics Center in Sudan. Institute for the Study of War. Online: https://www.understandingwar.org/backgrounder/africa-file-may-31-2024-russian-red-sea-logistics-center-sudan [last accessed: 01.01.2025, 15:13].

Karr, L. & Gianitsos, M. (2024). Africa File Special Edition: Russia's Africa Corps Arrives in Niger. What's Next? Institute for the Study of War. Online: https://www.understandingwar.org/backgrounder/africa-file-special-edition-russia%E2%80%99s-africa-corps-arrives-niger-what%E2%80%99s-next [last accessed: 25.10.2024, 23:05].

Kazeem, O. S. (2024). Dynamics of Conflict in the Sahel: Mali, Burkina Faso and Niger. In: FUOYE International Journal of Criminology and Security Studies, 3(2), pp. 58-79.

Kim, E. K. & Kim, K.-S. (2024): The Effect of Violent Extremism on Local Conflicts and Vice Versa: Differences and Similarities among Mali, Burkina Faso, and Niger. In Insight on Africa, 16(2), pp. 192-210.

Kohnert, D. (2024). Naviguer dans les rivalités: perspectives de coexistence entre la CEDEAO et l'AES en Afrique de l'Ouest. Hamburg: GIGA-Institute for African Affairs.

Le Faso (2024). Sommet des chefs d'Etat de l'AES : Le traité instituant la „Confédération AES" adopté. Online: https://lefaso.net/spip.php?article131446 [last accessed: 01.01.2025, 21:48].

Le Figaro (2023). Mali : l'ex-rébellion touareg quitte Bamako, nouveau signe de tension avec la junte. Online: https://www.lefigaro.fr/international/mali-l-ex-rebellion-touareg-quitte-bamako-nouveau-signe-de-tension-avec-la-junte-20230810 [last accessed: 01.01.2025, 16:40].

Le Figaro (2024). Mali : des drones turcs Bayraktar livrés à la junte au pouvoir. Online: https://www.lefigaro.fr/international/mali-des-drones-turcs-bayraktar-livres-a-la-junte-militaire-20240104?msockid=367eb9ff17e86459319cad6b16e865e2 [last accessed: 25.10.24, 23:49].

Knipp, K. (2024). Russia's military presence in Sudan boosts Africa strategy. Deutsche Welle. Online: https://www.dw.com/en/russias-military-presence-in-sudan-boosts-africa-strategy/a-69354272 [last accessed: 01.01.2025, 15:15].

Le Monde (2024). L'armée du Burkina Faso reçoit une douzaine de drones turcs pour lutter contre les groupes djihadistes. Online: https://www.lemonde.fr/afrique/article/2024/04/09/l-armee-du-burkina-faso-recoit-une-douzaine-de-drones-turcs-pour-lutter-contre-les-groupes-djihadistes_6226793_3212.html [last accessed: 25.10.24, 23:49].

Lechner, J. A. (2024). Is Africa Corps a Rebranded Wagner Group? Foreign Policy. Online: https://foreignpolicy.com/2024/02/07/africa-corps-wagner-group-russia-africa-burkina-faso/ [last accessed: 25.10.2024, 23:26].

Mackinnon, A. (2024). The U.S. Military Is Getting Kicked Out of Niger. Foreign Policy. Online: https://foreignpolicy.com/2024/04/26/niger-military-withdrawal-us-counterterrorism-russia/ [last accessed: 31.12.2024, 16:01].

MaliJet (2024). AES: La force conjointe est opérationnelle (Ministre). Online: https://malijet.com/actualite-sur-afrique/293866-aes--la-force-conjointe-est-operationnelle-ministre.html [last accessed: 25.10.2024, 22:35].

Monath, H. (2022). Ampel beendet Auslandseinsatz: Bundeswehr verlässt Mali bis Mai 2024. Tagesspiegel. Online: https://www.tagesspiegel.de/politik/ampel-beendet-auslandseinsatz-bundeswehr-verlasst-mali-bis-mai-2024-8907592.html [last accessed: 28.12.2024, 18:13].

Nasr, W. (2022). How the Wagner Group Is Aggravating the Jihadi Threat in the Sahel. In: CTC Sentinel, 15(11), pp. 21-30.

Ndiaga, T. (2023). Burkina Faso marks official end of French military operations on its soil. Reuters. Online: https://www.reuters.com/world/africa/burkina-faso-marks-official-end-french-military-operations-its-soil-2023-02-19/ [last accessed: 31.12.2024, 15:54].

Peltier, E. & Schmitt, E. (2024). After Niger Coup, U.S. Scrambles to Keep a Vital Air Base. The New York Times. Online: https://www.nytimes.com/2024/01/06/world/africa/niger-us-air-base.html [last accessed: 25.10.2024, 23:08].

Piombo, J., Kallel, L. & Englebert, P. (2024): Understanding the Dynamics of State Responses to Security Threats in the Sahel. In African Security. Online: https://www.tandfonline.com/doi/pdf/10.1080/19392206.2024.2429281?casa_token=hGQz3lkI-L4AAAAA:08aDR4R1lM-9kQGRvqDSuPyya-qnIjgR0oV_6Rf3OzwyIrPBcCAt2BzWD66cVz8Rfzk6Yp-nMX72M [last accessed: 11.12.2024, 21:43], pp. 1-27.

Quidelleur, T. (2024): Arming Civilians in Burkina Faso: The State, the War on Terror and the Militarisation of Society. Megatrends Afrika. Policy Brief 22. Berlin: Stiftung Wissenschaft und Politik.

Raffinot, M. & Giovalucchi, F. (2024). Une monnaie commune au Sahel : derrière la logique politique, un risque économique. The Conversation. Online: https://theconversation.com/une-monnaie-commune-au-sahel-derriere-la-logique-politique-un-risque-economique-227246 [last accessed: 29.12.2024, 11:08].

Reuters (2023). Last French troops leave Niger as military cooperation officially ends. Online: https://www.reuters.com/world/africa/last-french-troops-leave-niger-military-cooperation-officially-ends-2023-12-22/ [last accessed: 31.12.2024, 15:57].

RFI (2019). Massacre au Mali: IBK remplace son état-major et dissout la milice dogon. Online: https://www.rfi.fr/fr/afrique/20190324-mali-consternation-secours-massacre-centre-peuls-ogossagou [last accessed: 29.12.2024, 11:37].

RFI (2022). La Turquie livre six drones Bayraktar TB2 au Niger. Online: https://www.rfi.fr/fr/afrique/20220524-la-turquie-livre-six-drones-bayraktar-tb2-au-niger [last accessed: 25.10.24, 23:41].

RFI (2023). Mali: les ex-rebelles de la CMA accusent l'armée et Wagner d'une attaque tuant deux de ses membres. Online: https://www.rfi.fr/fr/afrique/20230809-mali-les-ex-rebelles-de-la-cma-accusent-l-arm%C3%A9e-et-wagner-d-une-attaque-tuant-deux-de-ses-membres [last accessed: 01.01.2025, 16:42].

Schmitt, E. (2018). A Shadowy War's Newest Front: A Drone Base Rising From Saharan Dust. The New York Times. Online: https://www.nytimes.com/2018/04/22/us/politics/drone-base-niger.html [last accessed: 25.10.2024, 23:08].

Serwat, L., Nsaibia, H., Carbone, V. & Lay, T. (2022). Wagner Group Operations in Africa: Civilian Targeting Trends in the Central African Republic and Mali. ACLED. Online: https://acleddata.com/2022/08/30/wagner-group-operations-in-africa-civilian-targeting-trends-in-the-central-african-republic-and-mali/ [last accessed: 25.10.2024, 23:11].

Smagin, N. (2024). Can Russia Reach a Deal With Syria's New Rulers?. Carnegie Endowment. Online: https://carnegieendowment.org/russia-eurasia/politika/2024/12/syria-russia-new-relationships?lang=en&utm_source=carnegieemail&utm_medium=email&utm_campaign=autoemail [last accessed: 01.01.2025, 15:04].

Soré, Z., Cote, M. & Zongo, B. (2021): Politiser le "Vide Sécuritaire": À Propos des Groupes d'Autodéfense Koglweogo au Burkina Faso. In Politique Africaine, 163(3), pp. 127-144.

Sow, D. & Koné, H. (2024). As AES and ECOWAS drift apart, dialogue on the fundamentals is vital. Institute for Security Studies. Online: https://issafrica.org/iss-today/as-aes-and-ecowas-drift-apart-dialogue-on-the-fundamentals-is-vital [last accessed: 25.10.2024, 22:29].

Spearin, C. (2024). Russia's Wagner Group/Africa Corps: an authoritarian conflictmanagement examination. In: Conflict, Security & Development. Online: https://www.tandfonline.com/doi/epdf/10.1080/14678802.2024.2415659?needAccess=true [last accessed: 25.10.2024, 23:02].

Spiegel (2022). »Opération Barkhane« beendet: Frankreich zieht letzte Soldaten aus Mali ab. Online: https://www.spiegel.de/ausland/mali-frankreich-zieht-letzte-soldaten-ab-a-0ba4ab33-c0d6-4dc3-83d2-088aea466df4 [last accessed: 28.12.2024, 18:05].

Tait, R. (2024). US to withdraw from Niger after security pact fails in strategic victory for Russia. The Guardian. Online: https://www.theguardian.com/world/2024/apr/20/us-withdrawal-niger-security-pact-russia [last accessed: 25.10.24, 23:41].

Tiegna, J. (2021): L'impact de groupes d'autodéfense et vigilantes dans l'extrémisme violent. In V. Rouamba-Ouedraogo (Ed.): Crise sécuritaire dans les pays du G5 Sahel : comprendre pour agir. Paris: L'Harmattan. pp. 287-320.

Tisseron, A. (2021). Pandora's box. Burkina Faso, self-defense militias and VDP Law in fighting jihadism. Dakar: Friedrich-Ebert-Stiftung Peace and Security - Competence Centre Sub-Saharan Africa.

Topona, E. (2024). Les pays de l'AES vont se doter d'un passeport biometrique. Deutsche Welle. Online: https://www.dw.com/fr/mali-niger-burkina-faso-aes-passeport-biom%C3%A9trique-colonel-assimi-goita-issaka-souar%C3%A9/a-70236279 [last accessed: 28.12.2024, 21:34].

Toulemonde, M. (2022). Jihadisme au Sahel : l'inexorable descente vers le Golfe de Guinée. Jeune Afrique. Online: https://www.jeuneafrique.com/1358991/politique/jihadisme-au-sahel-linexorable-descente-vers-le-golfe-de-guinee/ [last accessed: 25.10.2024, 22:56].

Touré, J. (2024). Alliance des États du Sahel : une nouvelle dynamique de sécurité collective ? Institut d'études de géopolitique appliquée. Online: https://www.institut-ega.org/l/alliance-des-etats-du-sahel-une-nouvelle-dynamique-de-securite-collective/ [last accessed: 25.10.2024, 22:41].

United Nations (2020). Summary of Contribution to UN Peacekeeping by Mission, Country and Post: Police, UN Military Experts on MIssion, Staff Officers and Troops 31/12/2020. Online: https://peacekeeping.un.org/sites/default/files/04_mission_and_country_33_dec2020.pdf [last accessed: 25.10.2024, 23:24].
United Nations Security Council (2023). Resolution 2690 (2023) / adopted by the Security Council at its 9365th meeting, on 30 June 2023. Online: https://digitallibrary.un.org/record/4014208?v=pdf [last accessed: 18.12.2024, 18:18].

Vines, A. & Wallace, J. (2022). Terrorism in Africa. Chatham House. Online: https://www.chathamhouse.org/2021/09/terrorism-africa [last accessed: 25.10.2024, 23:24].

Vines, A. (2024a). What's at stake for Africa in 2024? Chatham House. Online: https://www.chathamhouse.org/2024/01/whats-stake-africa-2024 [last accessed: 25.10.2024: 23:28].

Vines, A. (2024b). Combatting Terrorism in Africa. In Nicolas Stockhammer (Ed.): EICTP Vienna Research Papers on Transnational Terrorism and Counter-Terrorism: Recent Manifestations of Anti-Government Extremism and Transnational Terrorism in Europe, Africa and Beyond - Volume VI. Vienna: European Institute for Counter Terrorism and Conflict Prevention. pp. 59-69.

Wehrey, F. (2024). Assad's Downfall Echoes Across the Mediterranean. Carnegie Endowment. Online: https://carnegieendowment.org/middle-east/diwan/2024/12/assads-downfall-echoes-across-the-mediterranean?lang=en [last accessed: 01.01.2025, 15:10].

Wolkov, N., Harward, C., Hird, K., Stepanenko, K., Barros, G. & Kagan, F. W. (2023). Russian Offensive Campaign Assessment, December 20, 2023. Institute for the Study of War. Online: https://www.understandingwar.org/sites/default/files/Russian%20Offensive%20Campaign%20Assessment%2C%20December%2020%2C%202023%20%28PDF%29.pdf [last accessed: 25.10.2024, 23:11].

epis ThinkTank

International Politics Shaped By **You**

EPIS Thinktank

Who We Are

EPIS is a young think tank on foreign affairs and security policy. We publish scientific articles, send members to international conferences, and maintain a network of: students & young professionals.

The deal:

- You professionalize yourself in your field
- We help you start your career

What We Do

EPIS Magazine

- In-Depth Analyses of Political Issues of Your Choice
- 80 Pages
- 3x/Year

EPIS Working Groups

- Monthly Briefings on Political Developments in Eight World Regions

EPIS Talks

- Deep Dive into the Articles of our Magazine with the Authors

EPIS Blog

- Short Analyses of Political Issues of Your Choice
- Weekly Release

About the Article

Germany's shift from Russian gas to LNG aligns with EU energy security goals but reveals contradictions. Joschka Menge examines how Germany diversified suppliers, invested in LNG infrastructure, and strengthened European cooperation. However, indirect Russian LNG imports and environmentally questionable investments raise concerns. While Germany meets EU guidelines on diversification and cooperation, its long-term reliance on LNG and hidden Russian gas ties highlight policy inconsistencies.

About the Author

Joschka Menge is pursuing an B.A. in European Studies at Maastricht University (NL).

1. Introduction

Under the goal of improving Energy Security, the EU has changed its approach to energy policy since the Russian invasion of Ukraine. Europe's heavy reliance on Russian energy and especially gas imports has made the EU subject to Russian weaponization of energy. Especially countries like Germany, the biggest economy in the EU, which had tight bilateral bonds with Russia in the gas sector were heavily reliant on Russian gas. With the Russian invasion of Ukraine and the EU's following sanctions, the issues that came with this kind of reliance became ever so more apparent. Buying its energy from an illiberal country like Russia now had severe impacts on European Energy Security. Since then, increasing European Energy Security and becoming less dependent on Russia have been major goals of the EU and countries like Germany. Already more than 15 years ago, scholars like Garibaldi (2008, p.4) identified that "The EU is chronically incapable of reaching a common position on energy security". More recently, scholars like Mišík and Nosko (2023) argued that there is a severe solidarity problem within the EU highlighting Germany and France as a driver of the issue. For example, in 2022 when countries were supposed to voluntarily reduce their gas consumption, many member states showed significant opposition. Further, instances like Germany's involvement in the Nord Stream pipelines and differing responses to the 2009 gas crisis reveal internal divisions and a preference for bilateral agreements over a collective EU strategy. The EU aims to solve these issues by creating new energy policies that help to diversify the European energy portfolio with more reliable trade partners, cooperate more intensively within the European Community, and push for sustainable energy alternatives (European Commission, 2022a). In my article, I will be focusing on the shift away from Russian gas imports to Liquified Natural Gas (LNG). In the center of my analysis will be Germany as it has always played an important role in the European gas sector and has been heavily affected by the Russian war. I will answer the question: "To what extend did Germany's heavy investment into LNG follow the European policy objectives like further European cooperation as well as new partnerships with reliable countries?"

2. EU Strategy

As a reaction to the war in Ukraine, the EU launched the REPowerEU strategy, in which they showcase how they aim to improve the so-called European Energy Security. Throughout the document, the term Energy Security is being used to justify changes in the European energy policy, without giving a clear definition of the term. The goal to improve European Energy Security includes but is not limited to: "save energy; diversify supplies; quickly substitute fossil fuels by accelerating Europe's clean energy transition; smartly combine investments and reforms." (European Commission, 2022e, p.1). In the long run the EU aims to foster further integration among the European member states. By improving European energy security, the EU becomes a more independent and authentic actor in the global arena. By not relying on non-democratic and even autocratic countries for energy, the EU strengthens its position as a normative power in the world. For those outlined goals, countries like Germany play an important role in following European guidelines and further driving European integration, strengthening European Energy security, while also being an example for all the other Member States.

3. Analytical framework

Measuring whether member states are following European guidelines as well as an increase in Energy Security is a difficult thing to do. Nevertheless, to be able to measure an increase in Energy Security and to operationalize the concept of Energy Security, I will use the terms of measurement: diversification; stable supply; saving gas; reduced dependence on Russia; as well as cooperation among Germany and its fellow member states, to analyze whether Germany is meeting European goals and whether its LNG investments help Europe's Energy

1. Diversification with like-minded partners	**Spreading out the German energy, specifically, gas portfolio, to reduce dependencies on unreliable partners and build relationships with like-minded partners.**
2. Reduced dependence on Russia	**Reducing the reliance on Russian gas imports to be less of a subject to Russia's weaponization of energy.**
3. Cooperation among Member states	**Enhanced cooperation between Germany and other member states regarding Energy Policy, to ensure a stable and secure supply of energy within the Union. Especially important for this thesis are economic partnerships in gas policy like LNG investments.**
4. Stable supply	**Ensuring partnerships as well as using mechanisms, to secure a stable supply of energy for European countries.**
5. Saving Energy	**Building mechanisms and policies that help save- gas consumption. Building up gas storages to be prepared for future supply cuts.**

Figure 1: Terms of measurement

Security to increase. Each quality will be looked at from a perspective of change, looking at the pre-war situation versus the situation now as well as the outlook for the near future. These terms are derived from what the Commission outlined in the REPowerEU document, as well as from my definition of what Energy Security is (European Commission, 2022e). As the term "cooperation" is not listed among those, I will explain its importance under section Analysis A.

a. Terms of measurement:

In my analysis, I first look at documents and publications by the European Union to go in-depth about how the EU's energy policy has changed (3.a) and what changes the EU expects from its member states. To do that, I mainly look at publications by the European Commission like the document on the REPowerEU, on EU action to address the energy crisis, as well as documents on LNG and secure gas supplies. Secondly, I will analyze the changes in German gas policy (4.b) after the Ukraine war and how these changes align with the European goals. For the third and fourth part I will go more in depth on German gas policy and put my focus on LNG. The third part will look at Germanys LNG import (3.c) and the way the country substituted Russian gas with LNG. Fourthly, I will look at the investments in LNG (3.d) that Germany has committed itself to and how those help to fulfill the European ideals.

4. Analysis

a. Change in European Energy Policy

As a direct response to the Russian war in Ukraine, the Commission launched the REPowerEU strategy, defining the three main maxims that would lead the change in European energy policy: Save energy; Produce clean energy; Diversification of energy supply (Commission, 2022a). The result of reducing dependency on Russian gas was already visible within the first 8 months after the beginning of the war, as 80% of Russian pipeline gas had been replaced already. Since September 2022, Russian

gas accounts for only 8% of all pipeline gas imported into the EU, compared to 41% of EU imports from Russia in August 2021. While Russian pipeline gas imports decreased drastically, the EU had more than doubled its LNG imports by the beginning of 2023, rising from 20% to up to 42% (Commission, 2022a). Additionally, European countries started to cooperate between each other in regional groups to assess common supply risks (Common Risk Assessments) and to develop joint preventive and emergency measures (European Commission, 2021). The very regulation EU/2017/1938 facilitating this, does not only ensure safe energy by assessing risks to the supply collectively, but it also enhances cooperation between member states. For example, it introduces EU-wide simulations of gas supply and infrastructure disruption, which help to gain a greater understanding of possible risks and weaknesses related to the energy sector. The regulation also introduces a mechanism of solidarity that can be used if an extreme gas crisis occurs. It ensures that even under extreme circumstances households will have access to gas (European Commission, 2021). Additionally, under regulation 2022/1032 member states gas storages must be filled to 80% by November 2022 and 90% by November 2023, ensuring energy safety in cases of gas import shortages. A report published by the Commission in 2024 shows that this regulation enhanced Europe's Energy Security, its supply security, helped stabilize energy prices, and therefore helped European competitiveness (European Commission, 2024). The not explicitly mentioned, but underlying goal of cooperation among member-states can be seen in the regulations mentioned above. For example, the regulation EU/2017/1938 animated member states to exchange information on assessing risks cooperatively. Especially after the beginning of the war, the Commission proposed regulations COM/2022/360 and COM/2022/361 introducing plans for the EU to save gas collectively to be better prepared for a supply cut (European Commission, 2021). Further, shortly after the invasion, the EU proposed a common gas purchasing, which incorporates buying a share of the European gas together. This would help European competitiveness, as European countries do not have to compete among each other, and the EU has greater leverage when negotiating gas deals. Using its combined purchasing power will lower prices, reduce risks to member states, and protect smaller European states, using cooperation to prioritize the notion of solidarity. To summarize, the EU launched new policies and its REPowerEU strategy to outline new goals for the EU and its member states to enhance Energy Security. Part of these policies was to cut Russian gas imports and find new energy suppliers.

b. Change in Germanys Gas Policy

After the beginning of the war in Ukraine, Germany completely overhauled its gas policy with Russia, marking Russia as a not friendly and secure trading partner. Russian gas imports were cut completely by the end of August 2022, while only a few month earlier more than half of imported gas came from Russia (Bundesnetzagentur, 2024). Still, in 2022, 22% of all-natural gas imported to Germany came from Russia (Bundesnetzagentur, 2022). In 2023, it had been fully substituted by gas imports from mainly Norway and the Netherlands (Bundesnetzagentur, 2023). Not only did Germany substitute the Russian gas imports, but it also cut its entire gas import volume by almost a third, from 1.437 TwH in 2022 to 968 TwH in 2023. In addition, the German state opened several LNG hubs through which in 2023 almost 70.000 GwH (7% of the annual import volume) had been imported (Bundesnetzagentur, 2023). The federal government passed a law in June of 2022 that aims to help a fast transition away from Russian gas imports (Die Bundesregierung, 2023). The LNG-Beschleunigunggesetz (LNG acceleration law) is an answer to the unlawful war on Ukraine, aiming to accelerate European independency from Russian gas imports. Making permits and other procedures less bureaucratic and making exceptions for environmental regulations possible, the law opened the door for the first new LNG infrastructure to be built in the summer of 2022. The law also included specific locations for the LNG hub to make the construction of LNG terminals easier (Die Bundesregierung, 2023b). In 2023, Germany imported a total of 968 TWh of natural gas. 43 percent of that total volume was imported from Norway,

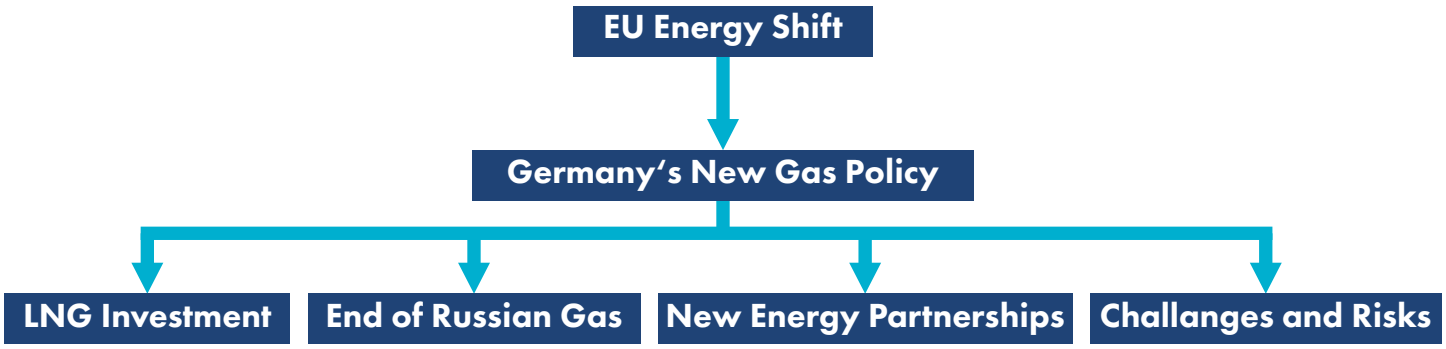


Figure 2: The shift in the EUs energy policy and germany's compliance to those new guidelines

26 percent from the Netherlands, and 22 percent from Belgium. To rely predominantly on imports from other European countries shows Germany's commitment to intra-European cooperation and reduced dependence on third countries. Germany's one-third cut in imported gas also led to significant cuts in its export volume of natural gas, with the Czech Republic being the biggest buyer of these exports (Bundesnetzagentur, 2024). Even though the gas imports were reduced significantly, Germany managed to adhere to the gas storage terms. In 2023, Germany even managed to overshoot the goals and had its gas storages filled with 85% already in June (1st of October 85% were EU guidelines) and managed to fill them up further to 95% on September 25th (1st of November 95% were EU guidelines). Unexpectedly, Germany had its storages filled a 100% on November 4th, surpassing European expectations. One can already see the trend of diversification (1) away from Russia towards more like-minded partners like other European countries, which is in line with the ideals of the EU. Further, the massive cut in gas imports did not affect Germanys capability to adhere to the gas storage guidelines by the EU. On the contrary, Germany managed to surpass the European timetable and fill its storages up months earlier than required. The country was able to do so by saving massive amounts of energy (5), both in the private and public sectors (Bundesnetzagentur, 2024). To help that along, the government passed a so-called Energieffizienzgesetz (energy efficiency law) in April of 2023, which aimed to put the saving of energy in the industry as well as the private sector into legislation (Die Bundesregierung, 2023). Lower energy consumption (5) does not only make Germany less dependent (2) on its energy importers and helped it move away quickly from Russian gas, but also has an environmental aspect to it. Burning less gas means a lower CO2 output. Even though it does not directly adhere to the goal of the EU to produce clean energy, it does have a notion of environmental protection when less energy is being used. Germany's general trend to cut gas imports, save energy, and cut gas deals with its fellow member states seems to comply with the European goal of diversification and cooperation (3) between member states. Importing gas from neighboring European countries like Belgium and the Netherlands also ensures a stable supply (4) of energy for Germany. Further, the cutting of gas consumption positively affects the environment, following the broader notion of environmental protection outlined by the EU in its goal to produce clean energy.

c. Germanys LNG imports

On second glance, data by Kpler shows that the EU is still importing significant amounts of Russian LNG from the Yamal, Portovaya, and Vysotsk LNG terminals, and Germany is profiting from it (IEEFA, 2023). In 2022, European countries still imported 18.5 billion cubic meters (bcm) of Russian LNG, while in the first nine months of 2023 close to 14 bcm were imported. The main importing countries are France, Spain, Belgium, and the Netherlands with Spain and Belgium having their imports increased by 50% in 2023. After these increases in Russian LNG imports, Russia is Spain's second-largest LNG exporter after the US. Spain also re-exports parts of its imported LNG with Germany being the second-largest recipient of Spanish LNG exports. As mentioned before, among Germany's biggest LNG imports are the Netherlands with 26% and Belgium with 22%. Although the

Netherlands have cut their LNG imports by more than 50% in 2023, they still import Russian LNG via the Yamal terminal (IEEFA, 2023). Even though it is unclear, to what amount the Russian gas imported to Belgium and the Netherlands is being re-exported again, it is likely that some of the LNG that Germany is importing from these countries has Russian origins. Germany's second-hand dependence on Russian gas seems to be well hidden behind the diversification and newly found trade partners Belgium and Spain but is ever so evident. Especially in light of Germany's heavy investment in LNG infrastructure, addressed in the next section, ongoing dependence on Russia is risky, as one might have learned from the past. Looking at the websites and publications by the German government, the hypocrisy is hard to overlook. "Russia's war of aggression against Ukraine, which violates international law, has led the federal government to reassess the energy and security policy situation in Germany" (Die Bundesregierung, 2023, Flüssiggas-Anbindungen schneller bauen, para. 3), claiming that the war in Ukraine led to rethinking of the German energy and gas policy, logically leading to a distancing to Russia. While this might have happened on an official level, meaning no direct imports from Russia, Russian gas is still flowing into Germany through this backdoor. These findings contradict the previous conclusion about Germany becoming less dependent on Russia (2), as Germany seems to still import Russian gas through third countries, making Germany second hand depend on Russian gas exports. While it still holds true that Germany does not import Russian gas directly anymore and therefore has significantly reduced its dependence, other European countries that Germany imports gas from have not shown the same commitment. Nevertheless, terms 1, 3, 4, and 5 still hold true to the conclusion under section b.

Energy Security:
The reliable and stable supply of energy at affordable prices, minimizing dependency on risky or hostile suppliers.

d. Germany's investments in LNG infrastructure

After the start of the war in Ukraine, Germany started to heavily invest in LNG. This involves constructing new LNG terminals and connecting them to the existing network, with a total projected investment requirement of around 45 billion euros by 2032 (Bundesnetzagentur, 2023). As part of this investment plan Germany plans to build close to 1000km of new LNG pipelines as well as several compressor stations. Through the commitment to the European environmental goals, Germany plans to convert existing gas pipelines to hydrogen and construct new ones, covering approximately 6,365 km, indicating a significant commitment to hydrogen as a future energy carrier. Contrary to this investment in hydrogen infrastructure to support the green transition; are the loans German banks are giving out for US LNG export terminal construction. Over the past decade, German banks have provided close to 5 billion dollars in loans. From January 2022 to April 2023 alone, support from German banks totalled $2.94 billion. Major financiers include Deutsche Bank, Landesbank Baden-Württemberg (LBBW), KfW IPEX-Bank, and Siemens. 60% of loans have been given out since the beginning of the war in Ukraine with the loans being almost 60% carried by Deutsche Bank (1.9 billion) and Landesbank Baden-Württemberg (LBBW) (1.4 billion). The loans supported the construction of seven American LNG export sides, passively supporting the LNG fracking industry by facilitating increased sales. It's estimated that those seven LNG export sides with their connection to fracking, produce more than 400 million tons of CO2, which is more than 50% of Germany's emitted greenhouse gases in 2022. This poses a significant contradiction to the German commitment to fulfil European environmental goals, as private German banks support the of fracking abroad. Further, the LNG contracts that have been cut with the American LNG export companies are 20 years long, compromising Germany's goal to be carbon neutral by 2045 (Gheorghiu, A., & Richter, R., 2023). These investments by German banks must be looked at from two different angles. On the one hand, these investments fulfil almost all my terms of measurement. Heavily investing in American LNG exporters is

undoubtedly an act of diversification (1) away from Russian gas, especially since the investments have skyrocketed since the beginning of the war. Further, the LNG deals cut with American LNG exporters for the next 20 years also help reduce dependency (2) on Russia quite a lot. Long-lasting economic bonds with the US as well as the EU/Germany and the US having a similar set of values suggest that the US is a safe trade partner, and a stable supply (3) is being ensured. With the upcoming presidential elections, this is something that might need to be reevaluated, but that goes beyond the scope of this thesis. On the other hand, these investments are an environmental disaster. As shown above, the American LNG fracking projects emit more than 50% of Germany's annual greenhouse gases (Gheorghiu & Richter, 2023). Further, the practice of fracking is illegal in most European countries, with Germany banning fracking already in 2017 (Peigné, 2022). Considering the illegality of fracking in the investor's own country, the investments can be critiqued, as they do not align with the European environmental protection goals. The German Association of Gas Transmission Network Operators (FNB Gas) released a draft for the 2022–2032 gas network development plan which includes future investments in the LNG sector. FNB Gas plans to invest close to 4.5 billion euros in the expansion of the gas and LNG network, including almost 1000 km of new gas pipelines. Additionally, they aim to expand the import infrastructure for LNG from the Netherlands and Belgium (FNB Gas, 2024). Even though the 'Netzentwicklungsplan Gas 2022–2032' still needs to be approved by the Bundesnetzagentur, the trend of heavy investments in the German LNG infrastructure trade with fellow member states by the private sector is continuing. The European Commission already approved a €40 million German support measure for constructing and operating a new land-based LNG terminal in Brunsbüttel to enhance energy security and diversify supplies, aiming to reduce dependence on Russian fossil fuels (European Commission, 2023). The claim by the Commission is that this support aligns with the European Green Deal, REPowerEU Plan, and broader EU efforts to reduce dependency on Russian energy imports, contributing to the EU's Energy Security and climate goals. The project's beneficiaries are RWE (a German energy operator) and Gasunie (a Dutch energy network operator), with the terminal to be built and operated by German LNG Terminal GmbH, jointly owned by KfW (50%), Gasunie (40%), and RWE (10%) (European Commission, 2023). This marks a significant step in the direction of the broader goal of the EU to enhance cooperation among member states. Such a pan-European project makes sense in light of economic prosperity and enhances European Energy Security by friend-shoring investments. Collective investments in institutions like LNG hubs help member states be less dependent on external parties and countries. Further, these investments facilitate intra-European cooperation.

The Tree Energy Solutions' (TES) Wilhelmshaven terminal by the German company E.ON cooperated with the French company France's Engie in planning the terminal. Additionally, all of the three terminals aim to transition to green energy in the future and align with the German net zero plans (Global LNG Hub, 2024). Further, the German Association of Gas Transmission Network Operators (FNB Gas) released a draft for the 2022–2032 gas network development plan on 31 March 2023, committing to 4.4 billion euro investment in in gas networks. Significant investments in connecting to neighbouring countries' LNG hubs are also planned (Centre for Eastern studies, 2023). These projects highlight Germany's efforts to cooperate with its fellow member states. German companies are switching from their Russian business partners like Gaz-Prom towards other European companies with their headquarters in like-minded countries. This process of friend-shoring aligns with the European goal of diversification and cooperation and enhances European economic unity by using the advantages of the common market. In addition, the terminals are designed to later be used for green energy like ammonia storage and e-methane production, aligning with the goal of clean energy outlined

Germany drives further European integration and is complying with European guidelines.

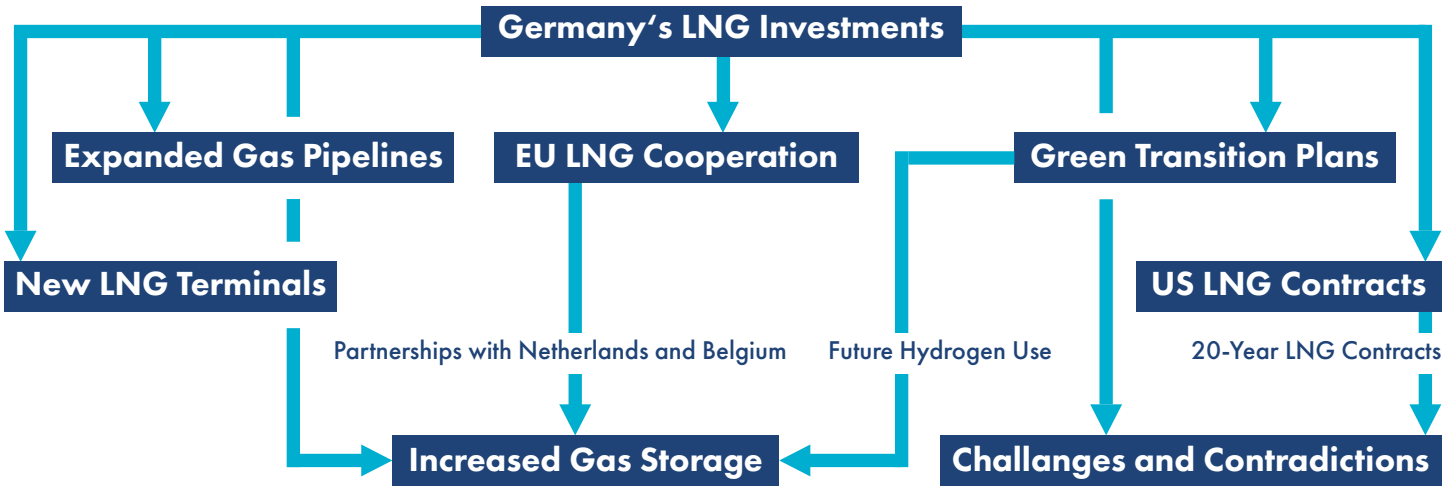


Figure 3: The pros and cons of germany's LNG investments

by the EU (Global LNG Hub, 2024). Looking at the terms of measurement, all five of them are being fulfilled by the investments of the terminals looked at above. To sum up: Diversification (1): Germanys cooperation with several fellow European member states; Reduced dependency (2): Germanys investments in infrastructure to be able to diversify away from Russian gas, is helping to reduce dependency on Russia; Cooperation (3): German companies cut gas deals with other European companies, as well as common investments in LNG infrastructure like the HEH facilitate intra-European cooperation; Secure supply (4): by cutting deals with like-minded countries and relocating investments to friendly countries, supply security is being enhanced; Save Energy (5): By preparing the German LNG infrastructure to later be able to be used for hydrogen, the saving of fossil energy is being prepared for the future.

5. Conclusion

Looking back at the research question of this paper: To what extend did Germany's heavy investment into LNG follow the European policy objectives like further European cooperation as well as new partnerships with reliable countries? as well as my terms of measurement (1) Diversification with likeminded partners, (2) Reduced dependence on Russia, (3) Cooperation, (4) Stable supply, and (5) saving energy, I will now answer to what extent Germany and its investments are in line with the guidelines given by the EU. The EU clearly outlined its energy goals in the REPowerEU strategy and other, mostly Commission documents, analysed above. Germany, having been so very dependent on Russian gas, did a complete reversal in its energy policy following the Russian invasion of Ukraine. As a substitute for the cutting of the gas imports from Russia, Germany started to import heavily from Norway, the Netherlands, and Belgium, strengthening European trade and facilitating European cooperation. Looking deeper into the origins of the LNG Germany is importing from Belgium and Spain, the still existing bonds to Russia as a gas exporter become apparent. Russia is still exporting significant amounts of gas and LNG to European countries, on which Germany is now directly dependent. This means that Germany is also indirectly still very dependent on Russia, which is quite the opposite of what they aimed for when stopping all Russian energy imports. Looking at the LNG investments, a great pattern of cooperation between German companies and other European and American companies can be seen. Germany is planning major LNG onshore terminals, for which other European companies have bought stakes in. The EU clearly outlined its energy goals in the REPowerEU strategy and other, mostly Commission documents, analysed above. Germany, having been so very dependent on Russian gas, did a complete reversal in its energy policy following the Russian invasion of Ukraine. As a substitute for the cutting of the gas imports from Russia, Germany started to import heavily from Norway, the Netherlands, and Belgium, strengthening European trade and facilitating European cooperation. Furthermore, Germany

managed to meet all European timelines to fill German gas storages and even managed to fill the storages up faster and with a higher volume than demanded. Following this pattern, Germany further passed legislation to save energy, adhering to the broader notion of environmental protection outlined by the EU. The country managed to fulfil all legal requirements given by the EU and started cooperating with its fellow member states more frequently. It successfully diversified its energy portfolio away from Russia, reducing dependency on unsafe trade partners. Looking back at my terms of measurement, in all three instances (Gas policy ;LNG imports ;LNG investment) Germany has fulfilled all of them, except for the questionable investments in US LNG sides and the exporting of Russian LNG through third countries. One can say that Germany does fulfil European guidelines to the best of its ability and shows great effort in becoming independent from Russian gas imports. It helps to drive further European integration and in comparison, to other member states, Germany is doing a great job in complying with European guidelines Further, its commitment to LNG investments shows a real paradigm shift in Germany's energy policy.

References

Apostolicas, P. (2020). EVOLVING MARKETS: Evolving markets: LNG and Energy Security in Europe. Harvard International Review, 41(2), 6–10. https://www.jstor.org/stable/26917294

Atlantic Council. (2023). Two years on, what the Russian invasion of Ukraine means for energy security and net-zero emissions. https://www.atlanticcouncil.org/.

Bowen, G. A. (2009). Document analysis as a qualitative research method. Qualitative research journal, 9(2), 27-40.

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen. (2023, December). Änderungsverlangen: Details zum Netzentwicklungsplan Gas 2022–2032. https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/NetzentwicklungUndSmartGrid/Gas/NEP_2022/Aenderungsverlangen.pdf?__blob=publicationFile&v=2

Bundesnetzagentur. (n.d.). Information on Securing Energy for Europe GmbH. https://www.bundesnetzagentur.de/EN/Areas/Energy/Treuhand/Gazprom/LetterOfComfort.pdf?__blob=publicationFile&v=1

Bundesnetzagentur. (2024). Gasimporte. https://www.bundesnetzagentur.de/DE/Gasversorgung/aktuelle_gasversorgung/_svg/Gasimporte/Gasimporte.html

Centre for Eastern Studies. (2023). Germany plans to adjust its gas network to a rapid increase in LNG imports. https://www.osw.waw.pl/en/publikacje/analyses/2023-04-07/germany-plans-to-adjust-its-gas-network-to-a-rapid-increase-lng

Deese, D. A. (1980). Energy: Economics, politics, and security. International Security, 4(3), 140-153.

Die Bundesregierung. (2023a). Flüssiggas-Anbindungen schneller bauen. https://www.bundesregierung.de/breg-de/schwerpunkte/klimaschutz/sichere-gasversorgung-2037912

Die Bundesregierung. (2023b). Klimafreundlich und krisensicher. https://www.bundesregierung.de/breg-de/schwerpunkte/klimaschutz/energieversorgung-sicherheit-2040098

ECFR. (2023). Keeping the lights on: The EU's energy relationships since Russia's invasion of Ukraine. https://ecfr.eu/publication/keeping-the-lights-on-the-eus-energy-relationships-since-russias-invasion-of-ukraine/

European Commission. (2014). European Energy Security Strategy. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014DC0330

European Commission. (2022a). REPowerEU. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal/repowereu-affordable-secure-and-sustainable-energy-europe_en

European Commission. (2022b). EU action to address the energy crisis. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal/eu-action-address-energy-crisis_en

European Commission. (2022c). Liquefied natural gas. https://energy.ec.europa.eu/topics/oil-gas-and-coal/liquefied-natural-gas_en
European Commission. (2022d). State aid: Commission approves €6.3 billion German measure to recapitalise energy company SEFE GmbH in context of Russia's war against Ukraine. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7828

European Commission. (2022e). REPowerEU Plan. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A230%3AFIN&qid=1653033742483

European Commission. (2022f). Seventh report on the state of the energy union. https://energy.ec.europa.eu/system/files/2022-10/state_of_the_energy_union_report_2022.pdf

European Commission. (2024). Report from the Commission to the European Parliament and the Council on certain aspects concerning gas storage based on Regulation (EU) 2017/1938 of the European Parliament and of the Council. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52024DC0089&qid=1709919504520

FNB Gas. (2024). Netzentwicklungsplan Gas 2022–2032. https://fnb-gas.de/wp-content/uploads/2024/03/2024_03_20_NEP-2022_Gas_FINAL_DE.pdf

Foreign Policy Research Institute. (2023). Synchronized: The Impact of the War on Ukraine's Energy Landscape. https://www.fpri.org/article/2023/12/the-impact-of-the-war-on-ukraines-energy-landscape/
Garibaldi, I. (2008). NATO and European Energy Security. American Enterprise Institute, 1, 1-6.

Gheorghiu, A., & Richter, R. (2023). Investing in climate chaos. Andy Gheorghiu Consulting, urgewald, and Deutsche Umwelthilfe e.V.

Giuli, M., & Oberthür, S. (2023). Assessing the EU's Evolving Position in Energy Geopolitics under Decarbonisation. The International Spectator, 58(3), 152–170. https://doi.org/10.1080/03932729.2023.2199648

Goldthau, A., & Sitter, N. (2022). Whither the Liberal European Union Energy Model? The Public Policy Consequences of Russia's Weaponization of Energy. EconPol Forum, 23(6), 4-7.

Hafner, M., & Noussan, M. (2019). The Geopolitics of the Global Energy Transition. Global Energy Journal.

Hafner, M., & Noussan, M. (2021). The geopolitics of the global energy transition. In The Geopolitics of Renewable Energy (pp. 182-206). Springer.

Jaller-Makarewicz, A. (2023). EU turns a blind eye to 21% of Russian LNG flowing through its terminals. Institute for Energy Economics and Financial Analysis.

Jerzyniak, T., & Herranz-Surrallés, A. (2024). EU Geoeconomic Power in the Clean Energy Transition. Journal of Common Market Studies. https://doi.org/10.1111/jcms.13590

Kucharski, J. (2023). Outlook for European energy security. In European Energy Security: An uncertain road ahead amid a triple crisis (pp. 37–40).

Mišík, M., & Nosko, A. (2023). Each one for themselves: Exploring the energy security paradox of the European Union. Energy Research & Social Science, 99, 103074. https://doi.org/10.1016/j.erss.2023.103074

Ozawa, M. (2022). The Russia-Ukraine war and the European energy crisis. NATO Defense College. https://www.jstor.org/stable/resrep41406.9

Peigné, M. (2022). Europe's energy crisis is reviving the fracking industry. Investigate Europe. https://www.investigate-europe.eu/posts/europes-energy-crisis-is-reviving-the-fracking-industry

Scholten, D., Criekemans, D., & Van de Graaf, T. (2020). An energy transition amidst great power rivalry. Journal of International Affairs, 73(1), 195-204. Retrieved from https://hdl.handle.net/10067/1667250151162165141

Yergin, D. (1991). The prize: The epic quest for oil, money, and power. Simon & Schuster.
Yergin, D. (2006). Ensuring Energy Security. Foreign Affairs, 85(2), 69–82. https://doi.org/10.2307/20031912

About the Article

This article emphasizes the duality of China's position—as both an economic partner and a potential disruptor to the status quo—while addressing the underlying uncertainties about its long-term intentions in the Arctic.

About the Author

Zhala Mammadli holds an M.A. in EU International Relations and Diplomacy Studies from the College of Europe (BE). Her research focuses on the potential effects of climate change on security and international relations.

1. Introduction

Democracy, a concept that has endured for centuries, has been a beacon of political ideals, rooted in citizens' right to participate in governance and hold leaders accountable (Dahl, 1989; Held, 2006). However, as the world continues to digitalise, the methods through which citizens engage with their political systems have drastically transformed, bringing with them both unprecedented opportunities and critical risks (Bennett, 2012; Papageorgiou, 2016). Democracy is no longer confined to the physical space of voting booths and town halls; it has expanded to social media platforms, online petitions, and real-time discussions, allowing citizens to participate in more dynamic ways (Shirky, 2011; Castells, 2012). These advancements have provided greater accessibility to political processes, particularly for marginalized communities, thereby empowering voices that were once silenced (Graham, 2014; McKenna & Pole, 2018).

However, the digital era also opens new avenues for manipulation, posing unique threats to democratic systems. As political engagement has migrated online, so too have the threats to its integrity. Cyberattacks, misinformation, and the weaponization of technology by state actors are increasingly destabilizing democratic processes around the globe (Norris, 2018; Tufekci, 2018). In the context of elections, for instance, cyberattacks on voting infrastructure or the spread of fake news can compromise the fairness and transparency of elections, ultimately eroding public trust in democratic institutions (Gagliardone, 2020; Howard & Parks, 2012). The 2016 U.S. presidential election, for example, illustrated how foreign interference can sway public opinion and undermine electoral integrity, prompting a reevaluation of how to safeguard elections in the digital age (Mueller, 2019; Margetts et al., 2018). As technology continues to evolve, the security of democratic systems and processes must be prioritized to ensure they remain resilient against increasingly sophisticated cyber threats (Binns et al., 2020; Geers, 2019). This essay seeks to explore the intersection between democracy and cybersecurity, examining the risks posed by digital technologies to democratic governance and evaluating strategies to protect democratic processes. In particular, it will address the research question: How do digital technologies, such as social media platforms and AI, influence the spread of misinformation and its impact on electoral integrity? By analyzing these challenges, we can begin to understand the potential future trajectory of democratic governance and the steps necessary to safeguard it from emerging cybersecurity threats.

2. The Digital Age and Political Engagement

2.1 The Rise of Digital Platforms for Political Participation

In the 21st century, the rise of digital platforms has reshaped political engagement, fostering greater interaction between the public and political systems (Van Dijck, 2013; Shirky, 2011). Political participation has traditionally been defined by voting and attending physical rallies or meetings (Putnam, 2000). However, with the proliferation of social media platforms, the internet, and digital communication tools, citizens now have new ways to interact with political content, express opinions, and even mobilize around causes (Bessi et al., 2016; Tufekci, 2017). Social media, in particular, has served as a primary venue for political discourse, where individuals, organizations, and even governments can engage directly with one another (Chadwick, 2013). The increasing ease of access to information on digital platforms has also democratized knowledge, allowing individuals to educate themselves on political matters without the constraints of geography or socio-economic status (Shirky, 2011; Rheingold, 2002). For example, Twitter hashtags like #BlackLivesMatter, #MeToo, and #ClimateStrike have allowed individuals to organize globally and bring attention to critical social and political issues (González-Bailón, 2013; Jackson & Foucault Welles, 2015). The role of digital platforms in organizing political action was evident in the Arab Spring, where platforms like Facebook, Twitter, and YouTube allowed activists to organize protests, document state

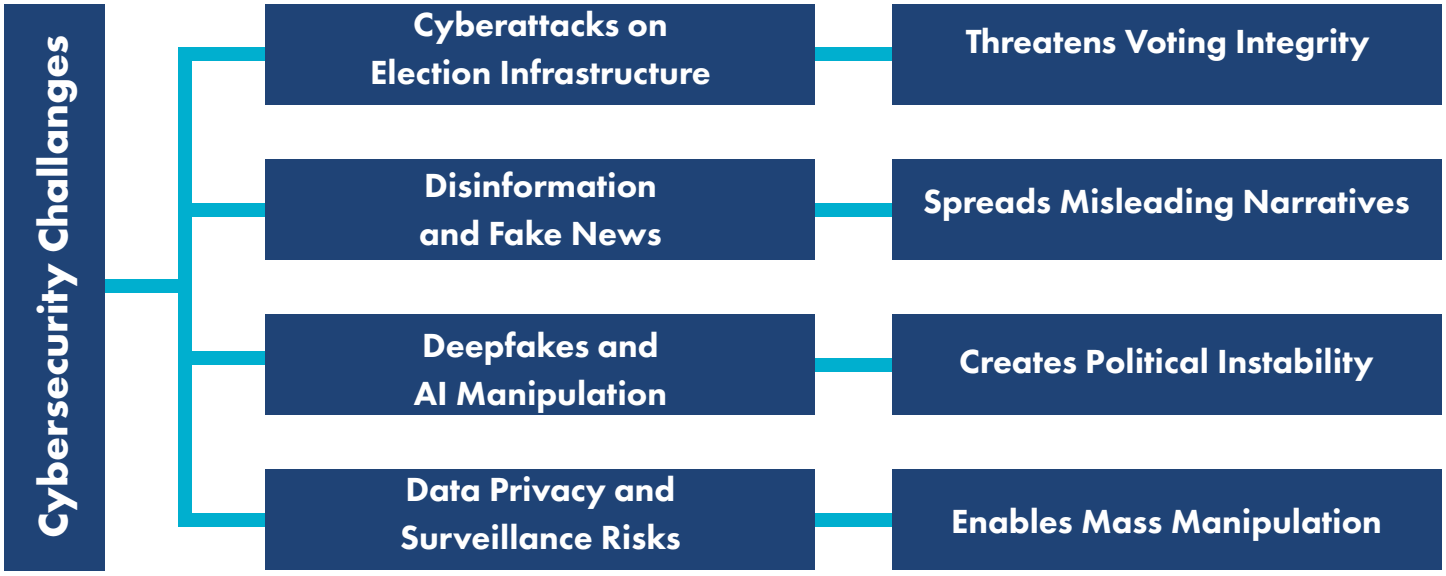


Figure 1: Cybersecurity Challenges in Modern Democracy

violence, and share their struggles with the international community, ultimately resulting in significant political upheaval in the Middle East (Howard & Hussain, 2013; Howard et al., 2011). These digital tools allow individuals to bypass traditional gatekeepers, such as government-controlled media outlets, and gain more direct access to the political process (Benkler, 2017). In turn, digital engagement fosters a sense of collective action, enabling ordinary citizens to shape political narratives and demand change (Tufekci, 2014). Moreover, the rise of digital political engagement has contributed to the proliferation of online petitions, crowdfunding for political campaigns, and even e-petitions to government officials (Schneider et al., 2013; Zuckerman, 2014). This access to new forms of participation not only encourages greater involvement in the political sphere but also facilitates political dialogue in real-time (Tufekci, 2017). For example, platforms such as Change.org and GoFundMe have become critical spaces where citizens can rally support for political causes and mobilize resources for political movements (Bennett & Segerberg, 2013). Such innovations in digital participation have fundamentally altered the way citizens interact with political issues, increasing the reach of campaigns and enabling individuals to actively contribute to political discourse (Chadwick, 2013). However, while the growth of digital engagement brings greater inclusivity, it also comes with a complex set of challenges, particularly in how political participation is regulated and protected from digital manipulation (Bradshaw & Howard, 2018). The ease of access to these platforms, while democratizing, has raised concerns regarding the vulnerability of digital political processes to manipulation, including bot-driven campaigns, data privacy issues, and coordinated misinformation efforts (Morris, 2017; Howard et al., 2018). For instance, crowdfunding platforms and online petitions are susceptible to being hijacked by malicious actors seeking to manipulate public opinion, whether by flooding petitions with fraudulent signatures or diverting donations to unauthorized causes (Binns et al., 2020). These challenges necessitate stronger regulatory frameworks to protect the integrity of digital political engagement (Gagliardone, 2020; Zuckerman, 2014).

2.2 The Risks of Online Political Engagement

The digital age has undoubtedly expanded the possibilities for political participation, but it has also introduced new vulnerabilities, particularly regarding the integrity of the political process. As political discourse increasingly shifts to online platforms, the risks of misinformation and disinformation campaigns become more prevalent. Misinformation refers to the unintentional spread of false information, whereas disinformation is deliberate, with the intent to mislead or manipulate public opinion (Bennett & Livingston, 2018; Lazer et al., 2018). Both

phenomena have become significant threats to democratic engagement, particularly in the context of elections, as false or misleading information can sway public opinion and impact voter behavior (Friggeri et al., 2014; Vosoughi et al., 2018). Social media platforms, despite their democratizing potential, have become a breeding ground for the rapid dissemination of false information (Pennycook & Rand, 2018). During the Brexit referendum in 2016, for instance, the campaign to leave the European Union was characterized by false claims and misleading narratives that were propagated across social media channels (Cummings, 2016; Walker & Broersma, 2019). Similarly, in the 2016 U.S. presidential election, a coordinated disinformation campaign by Russian actors exploited social media platforms to sow division and influence the electoral outcome (Bastos et al., 2018). In this case, fake news stories were shared widely, manipulating public perceptions of candidates, policies, and issues. These fabricated stories were often amplified by automated bots, which exacerbated the spread of misinformation (Ferrara et al., 2016). The implications of such disinformation are far-reaching, eroding public trust in democratic processes and distorting the political landscape (Allcott & Gentzkow, 2017). The risks associated with online political engagement are compounded by the phenomenon of "echo chambers," where individuals are exposed primarily to information that aligns with their pre-existing beliefs, often leading to increased polarization (Pariser, 2011). In these environments, disinformation thrives, as users are less likely to critically evaluate information that reinforces their views (Friggeri et al., 2014). This online fragmentation of political discourse is particularly harmful to democracy, as it makes it more difficult to find common ground or engage in productive debate (Tucker et al., 2018). As digital platforms continue to play an outsized role in political participation, the spread of misinformation poses a significant threat to the integrity of democratic processes and public trust in the media and government institutions (Levinson, 2017; Sunstein, 2017).

Cybersecurity in Democracy
The use of digital technologies to enhance political participation, governance, and democratic processes.

2.3 Cybersecurity Risks in Political Engagement

As political engagement increasingly moves into the digital realm, the cybersecurity risks to democratic institutions become ever more pressing. In particular, the threat of cyberattacks targeting election systems has risen to the forefront of cybersecurity concerns. These attacks range from simple data breaches to more sophisticated interference campaigns aimed at disrupting electoral processes or influencing public opinion (Gartzke, 2019). For instance, the 2017 French presidential election witnessed cyberattacks on Emmanuel Macron's campaign, with hackers targeting the candidate's email accounts to release sensitive information in an effort to undermine his candidacy (Hughes, 2017; Greenberg, 2017). The 2016 U.S. presidential election, however, remains one of the most high-profile examples of cyber interference in democratic processes. Russian operatives not only hacked into the Democratic National Committee's email servers but also engaged in a campaign of disinformation aimed at influencing voter sentiment (Mueller, 2019). Social media platforms were flooded with divisive and misleading content designed to manipulate voters and stoke political polarization (Bradshaw & Howard, 2018). This attack demonstrated the vulnerability of democratic systems to cyber threats and highlighted the challenges of securing election infrastructure against increasingly sophisticated and persistent adversaries (Cavelty, 2017).

Moreover, as elections around the world become increasingly reliant on digital technologies—such as electronic voting machines and online voting systems—the potential for cyberattacks grows. Malicious actors can target vulnerabilities in these systems to manipulate results or undermine voter confidence (Adelstein, 2020). In 2020, for instance, while no significant evidence of voter fraud or interference emerged, concerns about the security of electronic voting systems were raised in the United States, especially in light of the persistent threat of cyberattacks (Pomerleau, 2020). These risks make it imperative that governments invest in secure, transparent, and

resilient electoral systems that are resistant to manipulation (Mueller et al., 2020). To address these vulnerabilities, countries must implement strong cybersecurity measures to safeguard their democratic processes, ensuring that election-related systems and communication channels are protected from interference (Anderson et al., 2020). With increasing digitalization comes the need for enhanced vigilance and preparedness in securing electoral systems, not just against external threats but also against the rise of cybercrime, insider threats, and other cybersecurity risks (Friedberg, 2018).

3. The Role of Artificial Intelligence in Cybersecurity and Democracy

3.1 AI in Detecting Cyber Threats

The integration of Artificial Intelligence (AI) into cybersecurity practices offers significant potential for detecting and mitigating emerging threats. AI technologies are capable of analyzing vast amounts of data at unparalleled speeds, allowing for the detection of patterns, anomalies, and suspicious behavior that would be otherwise undetectable through traditional methods (Shrestha et al., 2019). For example, machine learning algorithms can be employed to identify phishing attacks, suspicious network traffic, and malware in real-time, helping prevent or mitigate damage caused by cyberattacks (Binns et al., 2020; Hsu & Hsu, 2021). The use of AI in detecting cybersecurity threats also extends to election security. AI-powered tools can be used to monitor online political discourse for signs of disinformation campaigns or coordinated social media manipulation (Lazer et al., 2018). For instance, machine learning algorithms can identify fake news, deepfake videos, and the presence of bot-driven accounts, which are commonly used to spread misleading narratives during election periods (Shao et al., 2018). AI tools can also monitor changes in voting patterns and detect anomalies that may indicate attempts to manipulate election results (Tufekci, 2018). Additionally, AI is increasingly being used to protect critical infrastructure, including election systems, from potential attacks (Hathaway et al., 2020). Governments can implement AI-powered threat detection systems that can identify and respond to intrusions or vulnerabilities in real time, preventing malicious actors from compromising the electoral process (Zhao & Li, 2021). AI's ability to continuously learn and adapt to new threats is a key advantage in the ongoing fight to secure democratic processes from cyber threats (Dastin, 2019).

Protecting democracy today requires strong defences against cyber threats and disinformation.

3.2 The Dark Side of AI: Weaponizing Technology

While AI offers tremendous benefits in cybersecurity, it also introduces new risks, particularly when weaponized for malicious purposes. AI-driven technologies such as deepfakes, bots, and algorithmic manipulation have the potential to disrupt democracy in unprecedented ways (Chesney & Citron, 2018). Deepfake technology, which uses AI to generate hyper-realistic but fake video and audio content, can be used to create fabricated narratives that manipulate public opinion and destabilize political campaigns (Brundage et al., 2018; West, 2019). Deepfakes, which are increasingly difficult to detect, can portray political figures making false statements or engaging in compromising behavior, leading to widespread misinformation and confusion among the electorate (Franks, 2020). Furthermore, AI-powered bots and automated algorithms can amplify disinformation campaigns, creating an illusion of widespread support or opposition for particular political causes (Binns et al., 2020). These bots can flood social media platforms with misleading content, shaping public discourse by drowning out opposing voices or pushing specific political agendas (Howard et al., 2018). The use of bots in the 2016 U.S. election demonstrated how easily they can influence political outcomes, amplify extremist views, and undermine the integrity of democratic processes (Helbing, 2019; Zeng, 2019). As AI becomes more sophisticated, the potential for its misuse to undermine democratic processes only increases (Brynjolfsson

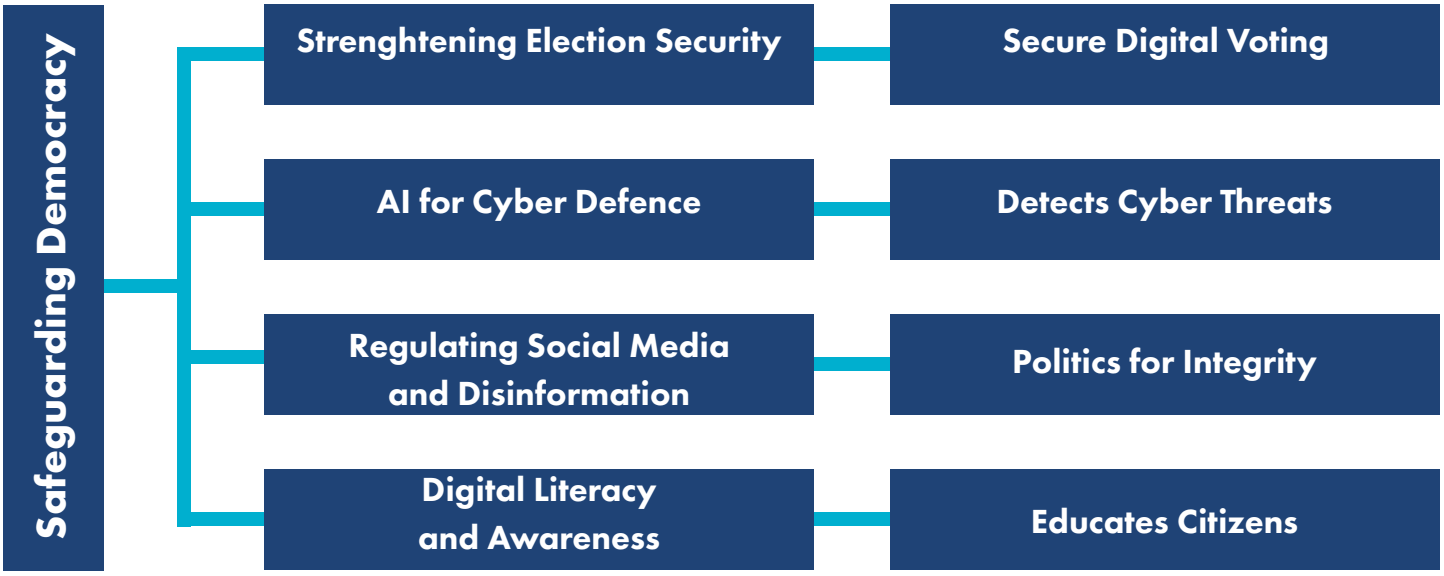


Figure 2: Safeguarding Democracy from Cyber Threats

& McAfee, 2017). The challenge moving forward will be to strike a balance between harnessing AI's capabilities for cybersecurity and ensuring that it is not exploited to manipulate elections or erode public trust in democratic institutions (Sullivan & Bailey, 2021).

4. Protecting Democracy in the Digital Age

4.1 Comprehensive Cybersecurity Strategies

To protect democracy in the digital age, comprehensive cybersecurity strategies must be developed and implemented at both the national and international levels. These strategies should focus on protecting critical infrastructure, including voting systems, communication networks, and election-related databases (Kshetri, 2017). Furthermore, governments must prioritize investments in advanced technologies and cybersecurity practices that are designed to detect, prevent, and respond to cyberattacks that threaten the integrity of democratic processes (Gagliardone, 2020; Zetter, 2019). The inclusion of blockchain technology in electoral processes, for example, offers a promising avenue for securing votes and preventing fraud. Blockchain's decentralized and tamper-proof structure makes it an ideal candidate for building transparent, secure voting systems that are resistant to hacking (Ferrara et al., 2016; Tapscott & Tapscott, 2017).

In addition to technological solutions, cybersecurity strategies must include robust protocols for identifying and mitigating disinformation campaigns. Social media platforms can work alongside governments to identify coordinated attempts to spread false narratives or manipulate public opinion (Tufekci, 2018). However, these partnerships must be carefully regulated to ensure that efforts to combat disinformation do not infringe on freedom of speech or undermine democratic values (Gillespie, 2018). Governments must also invest in educating citizens about the importance of cybersecurity in maintaining democratic integrity. This includes providing digital literacy education that empowers individuals to recognize misinformation, protect their personal information, and engage with political discourse in a responsible and informed manner (Mossberger et al., 2012).

4.2 Promoting Digital Literacy

In order to effectively safeguard democracy from digital threats, it is crucial to promote digital literacy across all sectors of society. Digital literacy is the ability to use digital tools effectively while understanding the risks associated with online engagement (Dahlberg, 2018). By teaching citizens how to recognize misinformation, evaluate sources critically, and navigate digital platforms safely, we can create a more resilient electorate (Norris, 2001; Rheingold, 2012). Digital literacy education should

be embedded in school curriculums from an early age, ensuring that future generations are well-equipped to engage in online political discussions and make informed decisions (Bennet & Livingston, 2018). Public awareness campaigns can also play a significant role in empowering individuals to identify and combat disinformation. These campaigns can educate citizens on the tactics used by malicious actors, such as bots, deepfakes, and fake news, and provide strategies for verifying information before sharing it (Franks, 2020). A digitally literate electorate is less likely to fall victim to manipulation and more likely to participate meaningfully in democratic processes (Shao et al., 2018).

5. Conclusion

5.1 The Future of Democracy in the Cyber Age

This essay explored the impact of cybersecurity challenges on democratic governance, posing the research question: "How do digital technologies, such as social media platforms and AI, influence the spread of misinformation and its impact on electoral integrity?" This question is particularly relevant in today's geopolitical climate, where cyberattacks, disinformation campaigns, and digital surveillance shape political discourse and election outcomes (Bessi et al., 2016; Howard & Hussain, 2013). The analysis reveals that cybersecurity threats undermine democracy by eroding public trust, enabling foreign interference, and disrupting electoral processes (Tufekci, 2018). To counter these risks, governments must implement robust cybersecurity policies, enhance public awareness, and foster international cooperation (Brundage et al., 2018). Ultimately, the future of democracy depends on adapting to technological advancements while upholding core democratic principles such as transparency, fairness, and accountability (Zhao & Li, 2021). By strengthening cybersecurity, promoting digital literacy, and fostering international collaboration, societies can protect democratic institutions from emerging cyber threats and ensure the resilience of democratic values in the digital age (Bennett, 2016). Beyond these findings, several implications and open questions remain. How can democracies balance security with digital freedoms? What role should private tech companies play in safeguarding democratic institutions? Addressing these concerns will be crucial in ensuring resilient and secure democratic governance in the digital age.

References

Adelstein, J., 2020. Cybersecurity and elections: A new front for electoral integrity. Oxford University Press.

Allcott, H. and Gentzkow, M., 2017. Social media and fake news in the 2016 election. Journal of Economic Perspectives, 31(2), pp. 211-236.

Anderson, C., Bell, D., Gagliardone, I. and Howard, P., 2020. Cybersecurity in elections: Protecting democracy in the digital age. Journal of Information Technology & Politics, 17(3), pp. 1-15.

Bastos, M.T., Ferrara, E. and Garcia, D., 2018. The spread of fake news by social media in the 2016 U.S. election. Scientific Reports, 8(1), pp. 1-11.

Benkler, Y., 2017. The wealth of networks: How social production transforms markets and freedom. Yale University Press.

Bennett, L., 2012. The personalization of politics: Political identity, social media, and changing patterns of political participation. Journal of Political Communication, 29(1), pp. 30-47.

Bennett, L. and Segerberg, A., 2013. The logic of connective action: Digital media and the personalization of contentious politics. Information, Communication & Society, 16(5), pp. 1-21.

Bessi, A., et al., 2016. Social media and the spread of misinformation. Journal of Political Communication, 33(3), pp. 247-268.

Binns, R., et al., 2020. Cybersecurity and elections: Safeguarding democratic processes in the digital age. Cybersecurity Journal, 24(2), pp. 43-65.

Blum, D. (2020) Defending the Digital Election Infrastructure; Security Architect.

Bradshaw, S. and Howard, P., 2018. The global disinformation order: 2019 Global inventory of organized social media manipulation. Oxford Internet Institute.

Brundage, M., et al., 2018. The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. arXiv preprint arXiv:1802.07228.

Cavelty, M.D., 2017. Cybersecurity and the future of democracy: The challenges ahead. Cambridge University Press.

Castells, M., 2012. Networks of outrage and hope: Social movements in the internet age. Polity Press.

Chadwick, A., 2013. The hybrid media system: Politics and power. Oxford University Press.

Chesney, R. and Citron, D., 2018. Deepfakes: A looming challenge for privacy, democracy, and national security. California Law Review, 107(4), pp. 1753-1819.

Cummings, D., 2016. The Brexit campaign: The role of misinformation in political processes. Political Analysis, 43(2), pp. 205-227.
Dahl, R., 1989. Democracy and its critics. Yale University Press.

Dastin, J., 2019. Artificial intelligence in cybersecurity: A boon or a threat?. Harvard Business Review, 97(5), pp. 124-135.

Ferrara, E., et al., 2016. The rise of social bots. Communications of the ACM, 59(7), pp. 96-104.

Franks, D., 2020. The deepfake threat: Weaponizing artificial intelligence. Journal of Artificial Intelligence & Society, 28(2), pp. 45-61.

Friggeri, A., et al., 2014. Rumor cascades. Proceedings of the 2014 ACM Conference on Computer-Supported Cooperative Work, pp. 157-167.

Geers, K., 2019. Cybersecurity and the future of democratic governance. Springer.

Giles, M.W., 2018. The role of AI in protecting democracy. In: L. Thompson and M. Anderson, eds. Artificial Intelligence and Political Change. Oxford University Press, pp. 119-130.

González-Bailón, S., 2013. The dynamics of online political participation. Journal of Communication, 63(5), pp. 667-684.

Graham, M., 2014. The digital divide and political participation: An analysis of the impact of internet access on democratic engagement. Journal of Political Science, 34(3), pp. 123-145.

Greenberg, A., 2017. The hacks that changed the election: Cyberattacks on the 2016 U.S. election. Wired, 22(6), pp. 34-45.

Held, D., 2006. Models of democracy. Stanford University Press.

Helbing, D., 2019. How AI will affect politics and society: Political dimensions of the digital revolution. Springer.

Hsu, L., and Hsu, J., 2021. AI in cybersecurity: Techniques and applications. IEEE Transactions on Network and Service Management, 18(2), pp. 198-207.

Howard, P.N., et al., 2011. The Arab Spring: A study of social media in the Middle East. Journal of International Affairs, 63(1), pp. 67-88.

Howard, P.N. and Hussain, M., 2013. Democracy's Fourth Wave? Digital Media and Political Change. Oxford University Press.

Howard, P.N. and Parks, M., 2012. Social media and political mobilization in the 21st century. Journal of Political Science, 40(3), pp. 21-35.

Jackson, S.J. and Foucault Welles, B., 2015. #BlackLivesMatter: A critique of social media activism. The Information Society, 31(3), pp. 227-241.

Kshetri, N., 2017. Cybersecurity and the economics of digital democracy. International Journal of Internet Technology and Secured Transactions, 7(4), pp. 289-307.

Lazer, D., et al., 2018. The science of fake news. Science, 359(6380), pp. 1094-1096.

Levinson, R., 2017. The impact of digital platforms on political participation: A global overview. Political Studies, 65(3), pp. 479-498.

Liva, G., Codagnone, C., Misuraca, G., Gineikyte, V. & Barcevičius, E. (2020) 'Exploring digital government transformation: a literature review', 13th International Conference on Theory and Practice of Electronic Governance, pp. 502–509.

Margetts, H., et al., 2018. Political influence in the digital age. Cambridge University Press.

McKenna, K.Y.A. and Pole, A., 2018. Social media and political mobilization: How digital platforms are reshaping democracy. Journal of Politics and Technology, 27(2), pp. 50-67.

Morris, M., 2017. Digital democracy: The intersection of technology and political participation. Routledge.

Mueller, R., 2019. The Mueller report: The investigation into Russian interference in the 2016 election. U.S. Government Printing Office.

Norris, P., 2001. Digital divide: Civic engagement, information poverty, and the internet worldwide. Cambridge University Press.

Norris, P., 2018. Cyberattacks and their impact on democratic processes. Harvard International Review, 39(4), pp. 72-80.

Papageorgiou, A., 2016. The role of social media in political engagement. Journal of Political Science, 42(1), pp. 123-140.

Pennycook, G. and Rand, D., 2018. Fighting fake news: A computational social science approach. Science, 359(6380), pp. 1094-1096.

Putnam, R., 2000. Bowling alone: The collapse and revival of American community. Simon & Schuster.

Shirky, C., 2011. The political power of social media. Foreign Affairs, 90(1), pp. 28-41.

Shrestha, R., et al., 2019. AI and cybersecurity: The emerging role of artificial intelligence in digital protection. Journal of AI Security, 2(1), pp. 3-19.

Shao, C., et al., 2018. The role of AI in detecting and mitigating disinformation campaigns. Social Media + Society, 4(2), pp. 1-14.

Sunstein, C., 2017. #Republic: Divided democracy in the age of social media. Princeton University Press.

Tufekci, Z., 2014. Social media and the decision to participate in political protest: Observations from the Arab Spring. Journal of Political Science, 51(2), pp. 264-280.

Tufekci, Z., 2017. How social media shapes political movements. Social Media + Society, 3(1), pp. 1-10.

Tufekci, Z., 2018. The impact of algorithmic manipulation on democracy. Journal of Digital Politics, 12(4), pp. 90-105.

Van Dijck, J., 2013. The culture of connectivity: A critical history of social media. Oxford University Press.

Walker, M. and Broersma, M., 2019. Misinformation campaigns in the Brexit referendum. Political Science and Politics, 41(2), pp. 245-258.

West, S., 2019. Deepfake technology and its implications for politics. Technology and Society, 38(3), pp. 113-128.

Zhao, Z. and Li, L., 2021. AI-powered cybersecurity: Addressing the future of digital governance. Journal of Cybersecurity, 9(4), pp. 45-62.

Zeng, J., 2019. The political weaponization of artificial intelligence. Oxford Review of Political Economy, 36(1), pp. 23-47.

Zuckerman, E., 2014. Rewire: Digital cosmopolitans in the age of connection. W.W. Norton & Company.

epis ThinkTank

International Politics Shaped By **You**

EPIS Thinktank

Why Join Us?

- Make Your Voice Heard Through Our Various Formats and Participate in International Politics
- Publish Articles from Early on in Your Academic Career
- Receive Valuable Guidance throughout the whole Writing Process
- Become a Part of Our Network of Likeminded Students and Young Professionals in International Affairs

Interested? *Reach Out!*

Contact us on Instagram or LinkedIn or learn more about our work on our website!

@episthinktank

/epis-thinktank

epis-thinktank.de

About the Article

The Pacific is a stage for an unfolding geopolitical contest, where global powers compete for influence through diplomacy and aid. Donát Oláh explores how the U.S. and Australia strive to maintain dominance while China aggressively expands its reach. Pacific nations leverage this competition to secure financial and developmental support. Although China's presence is growing, Western alliances remain strong, ensuring that the region remains a focal point of strategic rivalry for years to come.

About the Author

Donat Olah is pursuing a B.A. in Economics and Management at Paris Dauphine University (FR). His research focuses on economics, foreign policies, and supranational organisations.

1. Introduction

The Pacific region is marked by its vast geographic expanse and the isolation of its island nations. These countries, despite their sovereignty, remain heavily dependent on external support across various sectors, including defence, infrastructure, and agriculture. Limited natural resources and small, dispersed populations further constrain their economic development, necessitating reliance on international aid and unconventional economic activities. Examples include Nauru's operation of migrant processing centres for Australia and Vanuatu's practice of selling citizenship for $130,000. Although these nations maintain higher levels of human development than the world's poorest states, their long-term growth prospects remain hindered by geographical and economic limitations. Stretching between Japan, California, and Australia, the Pacific Ocean contains only a handful of islands capable of sustaining human settlements. Many of these have been inhabited for only a few centuries, and their integration into global economic and political networks has been relatively recent. While colonial powers such as the United States, France, the United Kingdom, and New Zealand still maintain territories in the Pacific, 11 island nations have gained sovereignty, primarily in the southwestern region of the ocean. However, despite their political independence, these countries remain vulnerable to external influence. What drives global powers' diplomatic engagement with Pacific nations? The United States seeks to uphold its strategic dominance in the Pacific, ensuring the stability of its alliances and countering geopolitical rivals. Similarly, regional actors like Australia and New Zealand aim to maintain strong diplomatic and security ties with their Pacific neighbours. Meanwhile, China has become increasingly assertive in its efforts to secure influence in the region, particularly by strengthening its position in key economic sectors such as fisheries and maritime trade routes. This paper examines the strategic interests that major global and regional powers pursue in their relations with Pacific island nations—specifically focusing on Fiji, the Solomon Islands, Vanuatu, Samoa, Kiribati, Micronesia, Tonga, the Marshall Islands, Palau, Nauru, and Tuvalu. The analysis will centre on the roles played by the United States, China, and Australia, as these three actors have been the most engaged in the Pacific in recent decades, shaping the region's diplomatic and economic landscape.

2. Interests and Methods of Global Powers in the Pacific

Most global powers have limited direct economic interests in Pacific nations due to their lack of significant natural resources and small internal markets. Establishing large-scale industrial or manufacturing facilities in remote islands, where populations often number in the thousands, is economically unfeasible. However, despite their small size, these nations hold full UN membership, granting them voting rights on resolutions and influence in global affairs. Their strategic location along key maritime trade routes between the United States, Hawaii, and Southeast Asia further elevates their geopolitical importance. Diplomatic engagement with Pacific nations is often characterised by "chequebook diplomacy", a term used to describe foreign policy strategies where economic aid or investments are exchanged for diplomatic support. Essentially, financial incentives are leveraged to secure political alliances and favourable policy decisions. Despite their small populations, Pacific nations remain focal points of foreign diplomatic interest due to their strategic positioning and political significance. The objectives of global powers in the Pacific vary. The United States seeks to maintain its military dominance and strategic foothold in the region. China aims to expand its sphere of influence, challenging traditional Western hegemony. Meanwhile, Australia and New Zealand, as the most influential regional actors, strive to preserve their strong ties with neighbouring island nations, ensuring stability and alignment with their broader strategic interests. There are numerous instances of chequebook diplomacy in the Pacific, ranging from relatively low-profile financial contributions to large-scale aid packages worth

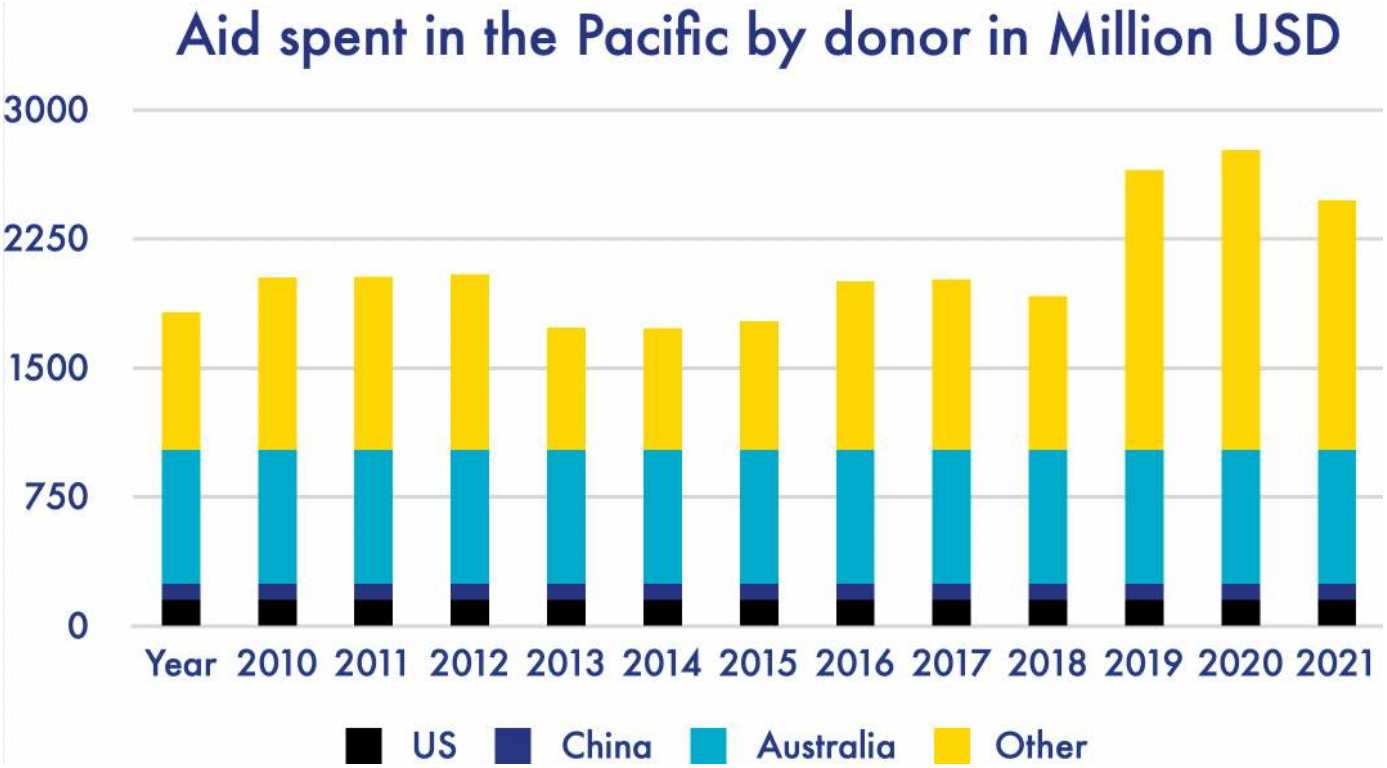


Figure 1: Source : Lowy Institute, Note : Most of „other" is from the World Bank, the Asian Development Bank, the EU and New Zealand

hundreds of millions of dollars. In 2016, Kuwait provided approximately $620,000 to Vanuatu and several other Pacific nations to secure support for its bid for a UN Security Council seat the following year. In 2012, Slovenia contributed $44,000 to improve water quality in the Marshall Islands, Micronesia, and Palau in exchange for diplomatic backing for its own Security Council bid—an effort that ultimately failed. While such financial incentives are not exclusive to the Pacific, the scale of foreign aid received by these nations is remarkable. In 2022, Micronesia received $122 million in aid from the United States, amounting to roughly 25% of its GDP. In 2020, Vanuatu secured $200 million in Official Development Assistance (ODA) and Other Official Flows (OOF) grants, equivalent to approximately 20% of its GDP. The Pacific remains the most aid-dependent region in the world, with seven out of the top ten highest per capita recipients of net ODA being Pacific nations. The lowest-ranked among the 11 countries studied in this paper still placed 16th globally in terms of net ODA received per capita. The primary sources of foreign aid in the Pacific, in order of contribution, are Australia, Japan, New Zealand, China, and the United States. Additionally, both China and Japan have provided substantial loans to Pacific nations over the past 15 years, further shaping the region's economic landscape. The motivations and mechanisms behind this financial assistance vary from country to country, reflecting the diverse strategic priorities of external powers operating in the Pacific.

2.1 Australia

Australia is committed to ensuring that its regional neighbours remain aligned with its strategic interests, prioritising stability and security. A peaceful Pacific is essential for Canberra, particularly given its geographic proximity to Indonesia, Papua New Guinea, the Solomon Islands, and Vanuatu—all of which lie within 1,500 kilometres of its coastline. While this may seem like a significant distance, history has demonstrated the region's strategic importance. During World War II, Japanese forces occupied parts of Papua New Guinea and the Solomon Islands, launching bombing raids on Darwin with the goal of pressuring and isolating Australia. This historical precedent underscores the necessity for Canberra to maintain influence over its northern and eastern neighbours. Beyond defence concerns, Australia also has significant economic interests in the region. A considerable portion of its exports passes through Pacific waters, making it

vital that shipping lanes remain secure and under the control of friendly states. To achieve this, Australia has established formal and informal security agreements with several Pacific nations, including Nauru, Kiribati, and Tuvalu, assuming varying degrees of responsibility for their defence. Additionally, many Pacific nations rely on Australian-supplied weaponry, further embedding Canberra's role as the region's primary security provider. Similarly, New Zealand plays a comparable role in ensuring the defence of Samoa. Australia has historically been the most significant donor to Pacific nations, providing both financial aid and various non-monetary contributions. Its strong regional ties and geographic proximity make it the largest benefactor, but in recent years, Canberra has had to intensify its diplomatic efforts to counter China's growing influence. Over the past 15 years, Beijing has aggressively expanded its presence in the Pacific, prompting Australia to adopt a more assertive approach to prevent China from dominating the region. To reinforce its position, Australia has financed several major infrastructure projects, including the installation of undersea telecommunications cables for multiple Pacific nations. This initiative serves both economic and security objectives by limiting Chinese involvement in regional telecommunications networks. In 2019, Canberra established the Infrastructure Financing Facility for the Pacific (AIFFP), a fund designed to compete with Chinese infrastructure loans. The AIFFP provides approximately 1.9 billion euros in loans and an additional 600 million euros in direct grants, ensuring that Pacific nations have alternatives to Chinese financing. One of Australia's most high-profile commitments in the Pacific is the Australia-Tuvalu Falepili Union. This treaty guarantees Tuvalu's statehood and sovereignty despite the existential threat posed by climate change-induced sea level rise. Additionally, Australia has pledged to welcome a significant number of Tuvaluan citizens annually as climate refugees. The agreement gained substantial media attention for being one of the first formal recognitions of climate-induced displacement. While the treaty is significant in its own right, it also serves as a strategic move by Canberra to signal to other Pacific nations that Australia is prepared to support and protect them in the face of climate-related challenges, strengthening diplomatic ties and countering China's influence in the region. Climate change poses an existential threat to Pacific nations, many of which lie only a few meters above sea level. As sea levels continue to rise, the very survival of these islands is at stake, with devastating consequences expected in the coming decades. The intensifying effects of climate change make Pacific nations particularly vulnerable, yet they are often underprepared to deal with the crisis. In response, governments in Kiribati, Tuvalu, and the Marshall Islands have already begun relocating populations from smaller islands that face immediate threats from rising waters. In March 2023, Vanuatu was struck by a powerful tropical cyclone, causing damages estimated at more than 400 million euros—approximately 30% of the country's GDP—primarily affecting infrastructure. Earlier that same year, another cyclone hit the island nation, leading to damages amounting to about 40% of its GDP and devastating up to 90% of crops in certain provinces. These extreme weather events highlight the urgent need for climate resilience strategies. However, Pacific nations lack the financial and infrastructural capacity to handle these disasters alone and must seek international assistance. Australia, through its friendship treaty with Tuvalu, has positioned itself as a key ally in addressing climate-related challenges. The agreement demonstrates Canberra's commitment to the region's stability and future, reinforcing its diplomatic standing. By offering support and protection, Australia ensures that Pacific nations look to it for assistance rather than turning to China. This strategic positioning not only enhances Australia's influence in the Pacific but also safeguards its broader security interests. If Canberra fails to maintain its reputation as a generous and reliable partner, there is a risk that Pacific nations could shift their alliances toward China, potentially undermining Australia's long-term strategic objectives. Australia remains the dominant power in the Pacific, leveraging its deep financial resources and historical ties

Checkbook Diplomacy:
Using financial aid or loans to secure diplomatic support and influence.

with island nations. Its extensive military presence and strategic alliances serve to establish a defensive perimeter around its territorial waters. Canberra's primary objective is to ensure regional stability and maintain the alignment of Pacific states with its broader strategic interests. By securing its influence, Australia seeks to protect vital shipping lanes and telecommunications networks that connect it to global markets. Ensuring that regional neighbours remain stable and aligned with Australian security policies is a key component of its long-term defence and economic strategy.

2.2 The United States of America

The United States maintains a significant presence in the Pacific, primarily through the Compact of Free Association (COFA), an agreement signed in 1982 with the Marshall Islands, Palau, and Micronesia. Under COFA, these nations receive financial assistance and enjoy easy access to the U.S., while Washington gains exclusive military rights and assumes responsibility for their defence. The agreement ensures that the U.S. is the only country permitted to establish military bases in Palau, Micronesia, and the Marshall Islands, effectively granting it control over vast maritime territories. At present, the U.S. military footprint in COFA states remains minimal, as there are no immediate security threats in the region. However, escalating tensions in the South China Sea over the past decade could prompt Washington to strengthen its presence for strategic and power-projection purposes. While COFA represents a considerable financial commitment—exceeding $200 million in 2022 alone—the benefits far outweigh the costs. By securing influence over several million square kilometres of ocean and maintaining unrestricted access to critical locations, the U.S. solidifies its strategic dominance in the Pacific. The deep economic and financial ties between the COFA nations and the U.S. further reinforce this alliance. All three countries use the U.S. dollar as their official currency, and their economies are heavily reliant on American aid. The prospect of severing ties with Washington is highly improbable, as doing so would result in the loss of substantial financial support and long-term economic repercussions. This ensures that the U.S. can sustain its military presence in the region without fear of losing its strategic foothold.

Access to these nations provides Washington with a direct link between its military bases in South Asia, Hawaii, and the U.S. mainland. Such logistical connections could prove crucial for American military supply chains in the event of a conflict in the region. Additionally, the agreement ensures that the countries surrounding U.S. overseas territories remain strategically aligned with Washington, reducing the risk of foreign powers gaining influence near America's most remote territories. From the perspective of the three Pacific nations under the Compact of Free Association (COFA), the agreement offers substantial benefits. They receive significant foreign aid with minimal obligations while also securing their defence under U.S. protection. Furthermore, Washington's financial assistance and continued interest in the region contribute to political and economic stability, reinforcing their long-term security. As a result, COFA remains a mutually advantageous arrangement, allowing both parties to maintain strategic and economic stability while strengthening regional alliances. The United States remains committed to countering China's expanding influence in the Pacific. Beijing's assertive foreign policy in the region took Washington by surprise, prompting an increased American presence. In response, the U.S. has strengthened diplomatic ties by opening new embassies, dispatching Vice President Kamala Harris to engage with Pacific leaders, and hosting high-level summits at the White House. These efforts serve two key objectives: preventing China from gaining new allies and preserving America's strategic advantages in the region.

Beijing's assertive foreign policy in the region took Washington by surprise, prompting an increased American presence.

2.3 China

Pacific nations play a key role in the ongoing diplomatic battle over the recognition of the Republic of China

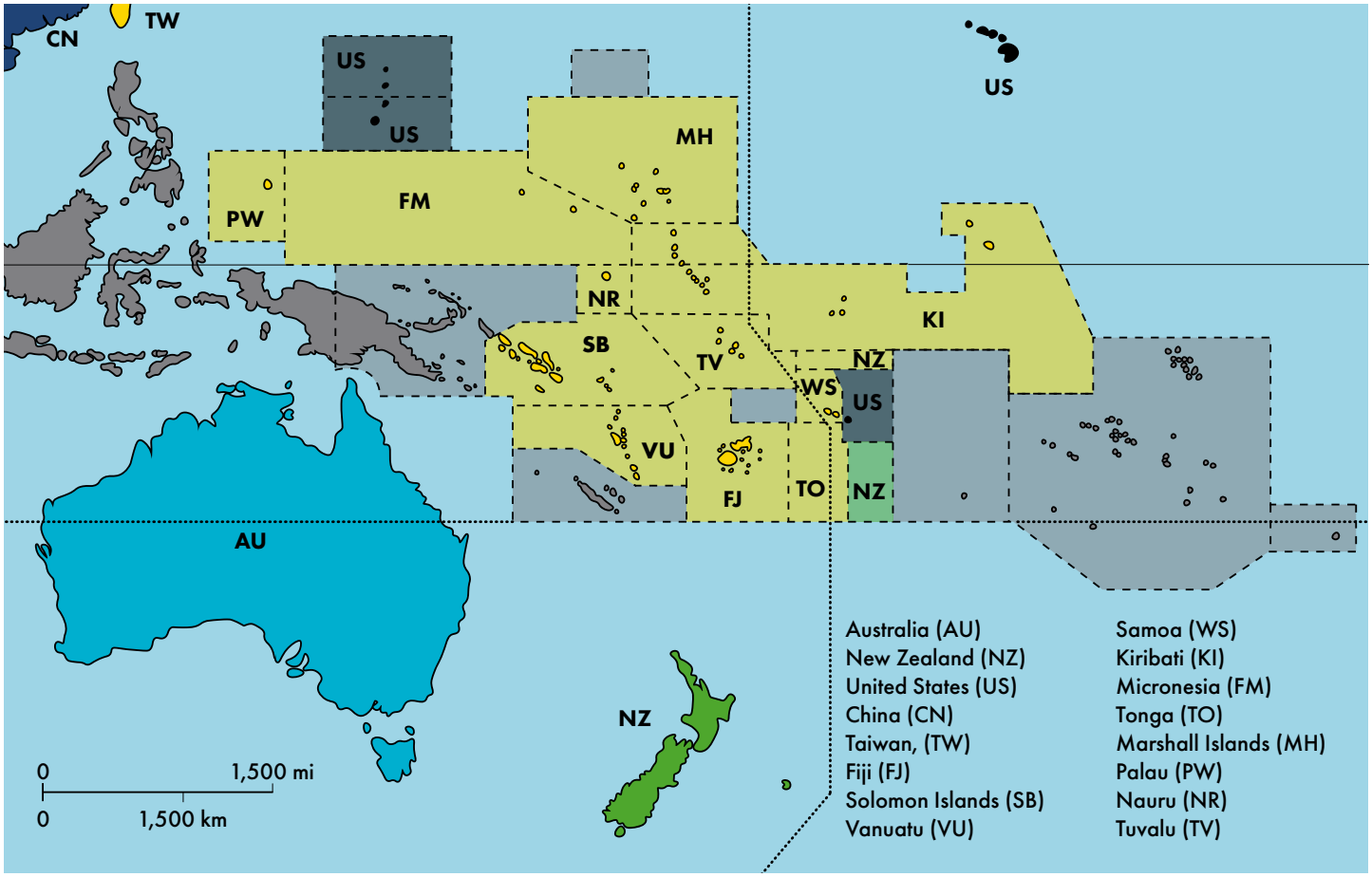


Figure 2: Map of Oceania, Taken and modified from: https://commons.wikimedia.org/wiki/File:Oceania_ISO_3166-1.svg

(Taiwan). Currently, only 12 countries recognize Taiwan as a sovereign state, three of which—Palau, the Marshall Islands, and Tuvalu—are in the Pacific. Nauru withdrew its recognition of Taiwan in early 2024, while both the Solomon Islands and Kiribati switched allegiance to the People's Republic of China (PRC) in 2019. The broader international community largely adheres to the principle that only one of the two Chinas can be officially recognized, and over the past five decades, most countries have shifted their recognition to the PRC. For Taiwan, securing diplomatic recognition from UN member states is critical to its legitimacy. It actively seeks to maintain and expand its list of supporting countries, while the PRC works to diplomatically isolate it. This struggle for recognition is a reflection of China's efforts to extend its global influence and Taiwan's fight to preserve its limited international standing. Countries that still recognize Taiwan tend to be smaller states, often with little to gain or lose from aligning with Beijing. These nations can also be swayed through diplomatic and financial incentives, leading to a dynamic often described as a bidding war between Taipei and Beijing. Reports suggest that China provided approximately 75 million euros in aid to Nauru as part of the deal that led to its recognition shift. Similarly, until the Solomon Islands withdrew its recognition in 2019, Taiwan provided more than $10 million annually in aid—an amount that ultimately proved insufficient to retain their support. The stakes are high, and allegations of bribery attempts by both China and Taiwan to influence officials in the Solomon Islands further underscore the significance of this diplomatic contest. The question of diplomatic recognition in the Pacific often comes down to which side can offer the largest financial incentive. Both the People's Republic of China (PRC) and the Republic of China (Taiwan) engage in a bidding war, with the highest offer securing a diplomatic victory and the recipient nation benefiting from financial aid. This dynamic is particularly pronounced in the Pacific, where many nations are highly dependent on foreign assistance. The 75 million euros reportedly provided to Nauru by Beijing represent nearly half of the country's GDP, highlighting the scale of these financial incentives. Larger nations with significant trade

relationships with China are generally reluctant to engage in this bidding process, as the economic benefits of maintaining ties with Beijing far outweigh any direct aid that Taiwan might offer. However, for smaller nations with limited economic ties to China, diplomatic recognition can be leveraged for financial gain. Over the past few decades, the PRC has successfully outbid Taiwan, securing recognition from all but three Pacific nations—Tuvalu, Palau, and the Marshall Islands. As the 21st century unfolds, China is actively expanding its economic, cultural, political, and military influence across the globe. While the Pacific is not among the most economically significant regions—lacking major internal markets for Chinese goods, unlike Africa—Beijing has pursued greater influence there for reasons similar to those of Western powers. The region represents an extension of China's strategic sphere, with critical shipping lanes running through or near it, making its stability and alignment with Chinese interests a priority. More importantly, China seeks to expand its zone of influence and break out of what it perceives as U.S.-led encirclement by regional adversaries such as the Philippines, Japan, South Korea, and Taiwan. The Pacific islands lie beyond the contested South China Sea, making them strategically relevant to China's broader geopolitical ambitions. The United States has surrounded China with military bases in these neighbouring countries and routinely patrols nearby waters. From Beijing's perspective, strengthening ties with Pacific nations is a necessary countermeasure to enhance its own security. Initially, China's push into the Pacific focused on securing diplomatic recognition in the One China policy dispute, a strategy that has largely succeeded, with most Pacific nations now recognising the People's Republic of China (PRC) over Taiwan. However, China's most significant diplomatic breakthrough came in 2023 with the signing of the China-Solomon Islands security pact. The agreement has the potential to establish China's second overseas military base, following its first in Djibouti. This deal was widely covered in international media, as it marked China's first major security agreement in the Pacific. If fully implemented, the pact could allow for the deployment of Chinese troops just a few hundred kilometres from Australia's northern coast, separated only by the Coral Sea. This development served as a wake-up call for both the United States and Australia, highlighting that their dominance in the region is no longer unchallenged. Despite China's growing presence in the Pacific, most countries in the region remain primarily aligned with the West. The shift in diplomatic recognition from Taiwan to China among some Pacific nations can largely be attributed to global trends, as nearly all countries now recognise the People's Republic of China (PRC). Additionally, China's status as a significant trading power makes it an economic partner that Pacific nations cannot afford to alienate. Given their vulnerability, these countries are wary of being caught in trade disputes, knowing that their economies are too small for China to consider their losses significant. China's presence in the Pacific is firmly established, but its influence is not absolute. In recent years, Beijing has scaled back its spending in the region, concentrating its resources on countries already aligned with its interests, particularly the Solomon Islands and Kiribati. Expansion into more diplomatically neutral or Western-leaning states has slowed. Overall, Chinese aid to the Pacific has declined significantly, dropping to roughly a third of its peak level of $325 million in 2016. Despite its efforts, China's influence in the region remains relatively limited. Most Pacific nations either maintain strong ties with the West or pursue a policy of "friends to all, enemies to none," seeking deeper engagement with any willing partner while avoiding firm commitments to one side. Their primary focus is not taking sides in geopolitical rivalries but securing much-needed support for economic development and climate change mitigation. The growing competition between global powers benefits them, as China's emergence has heightened international attention on the region, increasing the overall flow of aid and investment.

3. Conclusion

For global and regional powers, relations with Pacific nations are primarily driven by geopolitical considerations, with economics playing a secondary role. The United States and Australia seek to maintain and reinforce

their dominance in the South Pacific, a position they have held since World War II. They have long been the region's dominant military, diplomatic, and economic forces. However, over the past two decades, China has aggressively sought to expand its influence, challenging this long-standing balance of power. For both the U.S. and Australia, retaining control over the South Pacific is a key element of their broader global strategy. Their historical advantage in the region, once largely uncontested, has now been disrupted by China's growing presence. This has forced them to refocus on a region that was once considered secure under their influence. Beijing's engagement has injected new competition into the Pacific, compelling Western powers to respond with increased diplomatic and financial commitments. Pacific nations, in turn, have leveraged this competition to their advantage. They have long faced pressing challenges, from climate change to economic underdevelopment, due to their geographic isolation and limited resources. The influx of foreign aid—whether from the West or China—has provided them with much-needed financial support. However, their growing role in global power dynamics raises an important question: are they trading their sovereignty for financial assistance? Despite their small size, these island nations remain fully sovereign UN members with nearly the same voting rights as larger nations like Germany or Japan. Their strategic value in global diplomacy ensures that the bidding war for their allegiance is unlikely to slow in the coming years. With China continuing to grow in economic and military power, and deep-sea mining set to become a reality, securing the vast Exclusive Economic Zones (EEZs) of Pacific nations will become an increasingly critical issue in global politics.

References

Australian Infrastructure Financing Facility for the Pacific, 2022, October Budget 2022-23: Unlocking opportunities and boosting connectivity through quality, climate-resilient infrastructure

Australia, Tuvalu, 2023 Australia-Tuvalu Falepili Union

BBC, 2022, Tonga volcano: New images reveal scale of damage after tsunami

Cameron S., Lowy Institute, 2021, Palau faces the dragon

CIA, 2024, The World Factbook

Dayan A., Keen M., Rajah R., Lowy Institute, 2023, Chinese ait to the Pacific: decreasing but not disappearing

Dayan A, Moyle E., Lowy Institute, 2020, Chequebook diplomacy in the Pacific: Not just the big fish

Duke R., De Gorostiza G., 2023, Measuring the climate cost to development

Government of Vanuatu, Department of Strategic Policy, Planning & Aid Coordination, 2023, National Recovery Plan

Hammond J, 2023, China's Security Agreement with the Solomon Islands Lowy Institute, 2025, Pacific Aid Map

Salem S, Rosencranz A., 2020, Climate Refugees in the Pacific

Sora M., 2023, Digital dominoes: Australia's strategic play in the Pacific

The Guardian, 2018, China and Taiwan offered us huge bribes, say Solomon Islands MPs

United Nations, 2024, Human Development Reports

United States Department of State, United States Agency for International Development, 2024, Foreign Assistance by country

Woo R., Reuters, 2024, Former Taiwan ally Nauru re-establishes diplomatic ties with China

World Bank, 2024, World Bank Open Data

About the Article

Space exploration has always been driven by military interests. Markus Schiller examines how the arms race shaped spaceflight, from Cold War-era missile programs to modern satellite warfare. As China, Russia, and the U.S. expand military space capabilities, Europe lags behind. While commercial actors like SpaceX may reshape the landscape, Schiller argues that security concerns remain the primary force behind space innovation—just as they always have been.

About the Author

Dr. Markus Schiller is an expert in aerospace engineering and missile technology. He holds degrees in mechanical and aerospace engineering from the Technical University of Munich and a doctorate in astronautics. In 2015, he founded ST Analytics GmbH. He has held roles at Schmucker Technologie and the RAND Corporation and is a Senior Researcher at SIPRI. Dr. Schiller teaches missile technology at the Bundeswehr University and advises NATO, the German government, and the EU on security and aerospace matters.

Ein glitzernder Sternenhimmel wölbt sich über einen fremden Planeten. Ein gigantischer Sternenkreuzer zieht über den Beobachter hinweg, während er aus allen Rohren mit seinen Laserkanonen auf ein anderes Raumschiff feuert. Untermalt wird alles mit Explosionsgeräuschen und düsterer Orchestermusik. Solche Bilder sind häufig die ersten unbewussten Assoziationen, die sich einstellen, sobald man das Wettrüsten im Weltall anspricht. Jahrzehnte der Berieselung aus Hollywood und unzählige Darstellungen in Büchern, Comics oder Videospielen haben dazu beigetragen, dass sich die breite Bevölkerung unter Waffen im Weltraum zuerst bemannte Raumschiffe mit Lasern vorstellt, das ganze also der fernen Zukunft zuordnet. Jedoch ist das Thema weitaus aktueller, als viele vermuten würden. Die Bewaffnung des Weltraums ist mit dem Aufstreben Chinas als Supermacht und der Polarisierung der Welt – rapide beschleunigt durch den Einmarsch Russlands in die Ukraine – in den letzten Jahren wieder zu einem brisanten Thema geworden. Weltweit werden verschiedenste neue Projekte angeschoben, anhand derer sich heute ein Wettrüsten im Weltall festmachen lässt. Auch die globale Debatte darüber, wie aus sicherheitspolitischer und juristischer Sicht damit umgegangen werden sollte, hat wieder an Fahrt aufgenommen. So wurde erst im Mai 2024 bei der Generalversammlung der Vereinten Nationen diskutiert, wie damit umzugehen sei, dass Russland kurz zuvor einen Antrag von Japan und den USA im Sicherheitsrat blockiert hatte, der vorsah, dass alle Staaten, vor allem jene mit Zugang zum Weltraum, aktiv zur friedlichen Nutzung des Weltraums und einer Verhinderung eines Rüstungswettlaufs im All beitragen sollten. Russland hatte juristische Bedenken angemahnt und den Antrag abgelehnt; China enthielt sich. Die wahren Hintergründe sind unklar. Klar ist aber, dass China seit Jahren intensiv seine Präsenz im All ausbaut. Schon 2011 wurde die erste chinesische Raumstation in die Umlaufbahn geschossen, seit 2021 bereits die dritte Station aufgebaut. 2019 startete China erstmals mehr Weltraumraketen als jede andere Nation, inzwischen ist man nach den USA fest etablierte Nummer 2. Erst im November 2024 mahnte die US Space Force an, dass China erst kürzlich mehr als 970 Satelliten im Weltraum stationiert hätte, die Angriffe auf US-Flugzeugträger unterstützen sollten. Russland wurde gleichzeitig vorgeworfen, ein nukleares Waffensystem zu bauen, das in großem Stil Satelliten zerstören könne. Gleichzeitig treiben die USA selbst Programme voran, in deren Rahmen bis 2026 mehr als 1000 Satelliten verschiedenste militärische Unterstützungsaufgaben übernehmen sollen. Europa plant derzeit zwar mit, viel mehr aber auch nicht. Satellitenkonstellationen für militärische Anwendungen werden untersucht, aber mehr als 2 Weltraumstarts schaffte man im Jahr 2024 nicht. Zum Vergleich (Stand 3.12.2024): Japan startete 6 Raketen ins All, Russland 15, China 59, die USA 142. Selbst Indien lag mit 3 Starts um 50% über den Leistungen Europas. Auch dort bemüht man sich verstärkt um eine Rolle im Weltraum, deutlich ausgedrückt durch einen erfolgreichen Test einer Anti-Satellitenwaffe in 2019. Neu ist das alles jedoch nicht. Raumfahrt ist seit ihren frühesten Anfängen engstens mit Rüstung und militärischer Nutzung verwoben, wie ein detaillierter Blick darauf verrät. Ein Streifzug durch die Entwicklungsgeschichte der Raumfahrt verdeutlicht das.

Disclaimer:
Please take note, that this article has also been published in the Rotary Club Magazine in January 2025, which is why it's written in German.

Der Umweg über die Waffe

Obwohl sich die wahren Beweggründe der Raumfahrtpioniere, die in der ersten Hälfte des 20. Jahrhunderts die Tür zum Himmel aufstießen, gerne den Träumereien eines Jules Verne oder anderer Visionäre zurückverfolgen lassen, so war doch stets das Militär die treibende Kraft, die das nach Abraham Maslow definierte menschliche

Grundbedürfnis nach Sicherheit als Triebfeder nutzte, um die gewaltigen finanziellen Ausgaben zu rechtfertigen, die die Entwicklung der Raumfahrt überhaupt erst möglich machten: Der Weg führte über Waffen in den Weltraum. Die bekanntesten, die sich in diesen faustischen Pakt begaben, um ihre Visionen der Raumfahrt mit dem Umweg über das Militär zu ermöglichen, waren Wernher von Braun und sein Team. Heute wird häufig übersehen, dass die Wahl dieses Weges noch vor der Machtergreifung durch die NSDAP geschah: Bereits 1932 verpflichtete das Heereswaffenamt unter Walter Dornberger mehrere Raketenenthusiasten, die zuvor im Berliner „Verein für Raumschifffahrt" erste Erfahrungen im Raketenbau gesammelt hatten. Unter technischer Leitung von Brauns wurden damals von der Reichswehr Arbeiten zu einer Reihe von Raketen aufgenommen, die einmal Sprengladungen über mehrere hundert Kilometer transportieren sollten. So war die Umgehung der Versailler Verträge geplant, die zum Ende des ersten Weltkriegs Deutschland die Beschaffung weitreichender Artillerie verboten hatten, Raketen aber nicht erwähnten. Von Braun und seine Mitstreiter sahen darin zunächst die einzige Möglichkeit, um ausreichend Geld für ihre Pläne zur Entwicklung der Technologien zu erhalten, die später einmal das Tor zum Weltraum aufstoßen sollten. Nach der Machtübernahme der Nazis 1933 wurde das Programm mit Hochdruck weiterbetrieben. Man umgarnte die politisch-militärische Führung, um das Programm mehrfach vor dem Aus zu retten, und 1942 erfolgte schließlich der erste Flug eines Aggregat 4, das unter seinem Propagandanamen Vergeltungswaffe 2 (V2) traurige Berühmtheit erlangen sollte. Der Urahn aller heutiger Raumtransportsysteme war erschaffen, ermöglicht durch den Umweg über die Rakete als Waffe. Zum Kriegsende entwickelten die Siegermächte USA und Sowjetunion die erbeuteten Technologien weiter, erstmal aber wieder nur als Waffen. Der Kalte Krieg war bereits voll entflammt. In den USA wurde zunächst nur halbherzig versucht, sich das Know-How der deutschen Ingenieure einzuverleiben; Stalin aber sah das Potenzial der Atomrakete als ultimative Waffe, mit der man – im Gegensatz zu Flugzeugen oder anderen Rüstungsgütern, bei denen die Amerikaner einen uneinholbaren technologischen Vorsprung besaßen – mit den USA nicht nur gleichziehen konnte, sondern den Amerikanern überlegen wäre.
Die Sowjetunion trieb daher mit gewaltigem Aufwand die Entwicklung leistungsstarker Raketen zur Waffennutzung voran, angefangen mit einem Nachbau der deutschen V2 unter dem Namen R-1. Nach einem Jahrzehnt gipfelten die Anstrengungen in der R-7, der ersten Interkontinentalrakete der Welt, die mit einem atomaren Sprengkopf bis zur amerikanischen Ostküste reichen sollte. Und diese Waffe sollte nun endlich das Zeitalter der Raumfahrt einläuten. Denn zu ihrem fünften Testflug, am 4. Oktober 1957, konnte sich der Chefingenieur Sergei Koroljow mit seinem Vorschlag durchsetzen, ein leichtes Objekt mit der Rakete zu starten, welches – bei erfolgreichem Flug – als künstlicher Satellit Sputnik 1 die Erde umkreisen würde. Das Unterfangen gelang, und dass das Politbüro die Tragweite dieses Ereignisses völlig verkannte, zeigt sich am besten dadurch, dass dieser Erfolg dem sowjetischen Leitmedium Prawda zunächst nur eine Randnotiz wert war. Erst das gewaltige Medienecho aus dem Westen sorgte schließlich dafür, dass auch die Sowjets den Erfolg des Sputniks für ihre Zwecke ausschlachteten. Das Potenzial des Weltraums als Propagandavehikel war erkannt, und der Wettlauf ins All endlich in vollem Gange.

Mit Waffenraketen ins All

Die Amerikaner setzten nun alles daran, mit den Sowjets gleichzuziehen, während diese versuchten, ihren Vorsprung zu halten. Im Hintergrund wurden weiter neue Generationen von Atomraketen sowie erste Spionagesatelliten entwickelt, für alle Welt sichtbar war jedoch das „Race into Space": Dem ersten Flug eines Menschen ins All – Gagarin 1961 auf einer sowjetischen Atomrakete des Typs R-7 – folgten die Flüge der US-amerikanischen Astronauten Shepard auf der Mittelstreckenrakete Redstone 1961 und Glenn auf der Interkontinentalrakete Atlas 1962. Dieser Wettlauf sollte bald in der erfolgreichen Mondlandung der USA 1969 gipfeln, durchgeführt von der neunten Raketengeneration, die Wernher von Brauns Team federführend entwickelte: Der Saturn 5, die zwar noch wesentliche technische Parallelen zur alten V2

aufwies, aber ausnahmsweise nicht mehr als Waffenträger entwickelt worden war. Doch auch das Apollo-Mondprogramm konnte seine enge Verbundenheit mit der Rüstung nicht abschütteln. So war beispielsweise von den zwölf Astronauten, die bis 1971 den Mond betraten, nur ein einziger Zivilist; alle anderen waren Soldaten, die für die NASA temporär freigestellt wurden. In der Sowjetunion wurden dagegen ausschließlich umfunktionierte Waffenraketen für die Raumfahrt genutzt. Die Proton, Arbeitspferd der unbemannten russischen Raumfahrt bis in die Gegenwart hinein, flog erstmals 1965, damals entwickelt als schwere Interkontinentalrakete UR-500. Die Sojus, die heute noch Astronauten zur Internationalen Raumstation fliegt, ist eine mäßig modernisierte Version der Atomrakete R-7. Und selbst zur erfolglosen russischen Mondrakete N1 gibt es Berichte, nach denen sie ursprünglich als superschwere Interkontinentalrakete entworfen worden sei.

Weitgehend unbemerkt vom Westen hatte währenddessen die Sowjetunion mit großem Aufwand Technologie und Expertise zu den Waffenraketen an den Nachbarn China transferiert, der sich nun auch der Entwicklung immer leistungsstärkerer Großraketen verschrieb – primär zur Waffennutzung, wie zum Beispiel mit der Interkontinentalrakete DF-5, die aber nebenher auch in modifizierter Version als Langer Marsch Chinas erste Satelliten ins All brachte. Bis heute fliegen Chinas Taikonauten mit dieser Technik in die Erdumlaufbahn.

Space exploration was never independent from the military—rather, military funding made civilian spaceflight possible in the first place.

Rüstung als treibende Kraft

Nach der Mondlandung wurden in Amerika die Weichen in Richtung wiederverwendbarer Raumtransporter gestellt. Dieser baute weitgehend auf den Entwicklungen auf, die zunächst während des Zweiten Weltkriegs rudimentär unter Eugen Sänger zu seinem Projekt Silbervogel durchgeführt wurden, einem wiederverwendbaren Raumtransporter, der als „Fernbomber" von Deutschland aus die USA angreifen und nach einer Erdumrundung wieder in Deutschland landen sollte. Dieser Ansatz wurde nach dem Krieg in den USA in diversen Projekten weitergeführt, beispielsweise in Boeings X-20 Dyna-Soar, bei dem eine Interkontinentalrakete des Typs Titan eine geflügelte bemannte Kapsel auf eine Bahn schießen sollte, die man heute als „hypersonisch" bezeichnen würde. Die X-20 sollte dabei zur militärischen Aufklärung sowie zur gezielten Bombardierung genutzt werden. Das Projekt war weit fortgeschritten, wurde jedoch 1963 abgebrochen. Die Erkenntnisse daraus bildeten aber die Basis für die nachfolgende Entwicklung des Space Shuttle, welches mit einer rieseigen Ladebucht versehen wurde, um die neuesten Spionagesatelliten der USA in die Umlaufbahn transportieren zu können – die US Air Force bestand auf diesen Dimensionen, wodurch das Projekt deutlich teurer als zunächst erhofft wurde. Möglich war das, da die Air Force selbst eine Flotte von mehreren Raumfähren bestellt hatte und damit neben NASA Kunde war. Gestartet werden sollten diese vom kalifornischen Vandenberg, wo heute noch die dafür gebaute Startrampe steht. Es sind noch viele weitere Rüstungsprojekte aus Zeiten des Kalten Krieges bekannt, die nie verwirklicht wurden. Schon 1948 wurde in den USA über bemannte Militärbasen auf dem Mond nachgedacht, ernsthafte Projekte hierzu entstanden aber erst nach dem Sputnik-Schock. Ab 1958 untersuchte die US Air Force Möglichkeiten, ab 1967 eine bemannte Atomraketenbasis auf dem Mond zu unterhalten, um den USA im Fall eines sowjetischen Überraschungsangriffs eine Fähigkeit zum Vergeltungsschlag zu garantieren. Auch Möglichkeiten zum Bau von Spionageeinrichtungen auf dem Mond zur Beobachtung der Erde wurden untersucht. In einem konkreten Fall schlug beispielsweise Boeing vor, ab 1963 die Mondoberfläche mit Astronauten nach geeigneten Bauplätzen zu untersuchen, und bis 1973 schon 116 Menschen auf den Mond gebracht zu haben. Andere Konzepte wurden ebenfalls verworfen, wie etwa Project Thor aus den 1950er Jahren, das in den 1980ern im Rahmen von Brilliant Pebbles nochmals aufgewärmt wurde. Hierzu wollten die USA

hunderte massive Metallstäbe aus Wolfram in der Größe von Telefonmasten in niedrigen Erdumlaufbahnen stationieren. Im Bedarfsfall sollten diese zu einem kontrollierten Wiedereintritt gebracht werden und als Wuchtstab mit mehrfacher Schallgeschwindigkeit beim Aufschlag Ziele auf der Erdoberfläche ausradieren.

In Wirklichkeit fürs Militär

Andere Projekte wurden jedoch vom und fürs Militär verwirklicht, ohne dass dies heute weithin bekannt ist. Die ersten bemannten Raumstationen wurden beispielsweise in der Sowjetunion unter dem Namen Saljut gebaut und geflogen, ursprünglich aber ab 1965 als Almaz zur rein militärischen Nutzung entworfen. Zunächst wurden ab 1971 neun dieser Stationen gestartet. Zwei davon erreichten die Umlaufbahn nicht, die anderen wurden aber unter den Namen Salyut 1 bis 7 bis Mitte der 1980er Jahre teils zivil, teils militärisch genutzt. Die Kernmodule der legendären Raumstation Mir sowie der Internationalen Raumstation waren beziehungsweise sind modernisierte Varianten dieser Weltraumlabore. Auch im Bereich der Satellitentechnik lassen sich zahlreiche Beispiele für militärische Hintergründe scheinbar ziviler Programme finden. Bekanntestes Beispiel hierfür ist wahrscheinlich das US-amerikanische Satellitennavigationssystem GPS, das ab 1973 vom Pentagon als Navstar für das Militär entwickelt wurde und bis heute von der US Space Force, einem Ableger der US Air Force, betrieben wird. Mit dem Abschuss eines koreanischen Verkehrsflugzeugs im Jahr 1983, das sich in sowjetischen Luftraum verirrt hatte, und bei dem 269 Menschen ihr Leben verloren, stellten die USA die Nutzung von GPS auch für zivile Anwendungen frei. Von den heute existierenden vier großen Satellitennavigationssystemen ist nur das europäische Galileo in erster Linie zivil durch die EU finanziert, die anderen Systeme (US-GPS, Glonass aus Russland und Beidou aus China) unterstehen mehr oder weniger direkt dem Militär. Die Liste an Raumfahrtprojekten mit militärischem Hintergrund ließe sich noch beliebig verlängern, beispielsweise mit der bemannbaren russischen Kampfstation Polyus, die 1987 bei einem Fehlstart verloren ging, oder mit der nahen Verwandtschaft zwischen dem Weltraumteleskop Hubble und den US-amerikanischen Spionagesatelliten des Typs Keyhole. Die Raumfahrt war nie unabhängig vom Militär. Vielmehr haben die Geldtöpfe des Militärs die uns bekannte zivile Raumfahrt überhaupt erst ermöglicht, und auch den wahren Grund für den gewaltigen Aufwand geliefert: Nämlich das Bedürfnis nach Sicherheit. Inwiefern sich dies durch den großen Erfolg des US-amerikanischen Unternehmens SpaceX ändern könnte, muss sich erst noch zeigen. Die Falcon-Raketen, die inzwischen wöchentlich fliegen, wurden in ihrer frühen Phase durch hochpreisige Starts von US-amerikanischen Militärsatelliten mitsubventioniert, und das (auch militärisch genutzte) Satellitennetzwerk Starlink hat inzwischen einen militärischen Ableger namens Starshield bekommen. Eine völlige Loslösung von der militärischen Seite sieht anders aus. Und während Europa im Weltraum auf absehbare Zeit nur noch eine untergeordnete Rolle spielt, und Russland derzeit andere Schwerpunkte setzt, muss man über die treibenden Faktoren der chinesischen Weltraumaktivitäten keine Worte verlieren. Es ist, wie es immer schon war: Der Krieg ist nun mal der Vater aller Dinge.

Greetings from our contributors

friedrich 30

We represent interests

Founded in 2009, we have ever since been operating for our clients in Germany and beyond.

friedrich30 represents security and diplomatic interests around the world, including in countries with challenging political and security conditions.

Our company has four business areas:

I. Political Lobbying
II. Business Development
III. Multi-track Diplomacy
IV. Security & Protection from Economic Damage

Our Network – friedrich30 team members include former policemen, high-ranking intelligence officers, diplomats, government officials and IT-experts.

Locations – With offices in Berlin, Brussels and Mainz, our operating range covers Germany, the EU as well as selected countries around the world.

Contact us – info@friedrich30.com

We especially enjoy collaborating with motivated students and supporting think tanks in their important work at the focal point of policy and research!

friedrich30.com

About the Article

Germany faces escalating cyber threats from state and non-state actors, targeting businesses and critical infrastructure. Ferdinand Gehringer argues that Germany's cybersecurity framework is outdated and inefficient, requiring urgent reforms. He advocates for a stronger, independent BSI, enhanced public-private partnerships, streamlined cyber defense structures, and better legal frameworks for digital forensics. Strengthening education and training is crucial for building long-term cyber resilience.

About the Author

Ferdinand Gehringer is a security policy advisor at the Konrad Adenauer Foundation, a lawyer, and a certified mediator. He advises members of the German Bundestag and the European Parliament, as well as international organizations and governments, primarily on cyber and information security, hybrid threats, and the protection of critical infrastructure

In the past 12 months, approximately 81 percent of German companies have been affected by data theft, digital industrial espionage, or sabotage (Bitkom, 2024). Concurrently, the warnings issued by the Federal Office for the Protection of the Constitution and the Federal Intelligence Service regarding cyber activities from states such as Russia, China, and Iran have intensified annually (BfV, 2025; PC-SPEZIALIST, 2024). The 2024 Situation Report by the Federal Office for Information Security (BSI) describes the situation as alarming, with Germany being a primary target (BSI, 2024). Given the increasing risk of major digital disruptions, as well as (digital) sabotage and espionage, it is imperative that Germany responds to developments in cyberspace and enhances its cyber capabilities.

Escalating Threats in Cyberspace

The cyber threat landscape has deteriorated significantly in recent years. Cyberspace has evolved into a complex and dynamic environment where various actors pursue different objectives. While cyberattacks were previously often opportunistic, they have now become more targeted and technologically sophisticated. The use of artificial intelligence (AI) and machine learning has significantly increased the effectiveness and sophistication of these attacks (BSI, 2024).

The Convergence of State and Non-State Actors

Cyber actors can broadly be categorized into state and non-state groups, though distinguishing between them has become increasingly challenging. Non-state actors frequently operate on behalf of state actors, executing their strategic objectives. State actors include national governments, as well as their military and intelligence agencies. These entities leverage cyberspace for espionage, sabotage, and the pursuit of geopolitical interests. The United States, Israel, China, Russia, Iran, and North Korea are particularly active in cyberspace and possess advanced cyber capabilities (CISA, 2021).

Non-state actors encompass criminal organizations, hacker groups, and individuals (Chaudhury, 2021). These actors typically pursue financial gains through ransomware attacks or ideological motives, as seen in hacktivism. Frequently, non-state actors are contracted by state entities for specific objectives, receiving financial compensation or state approval for their (criminal) activities in return (Maurer, 2016, p. 383f.). Cybercrime groups are often highly organized and structured similarly to corporate entities. They maintain a hierarchical structure, with leadership overseeing operations while specialized members execute tasks such as malware development, phishing, or data exfiltration. Payments are sometimes issued monthly, akin to conventional employment contracts. These groups employ sophisticated technologies and infrastructures to support their illicit activities, generating substantial revenue through ransomware attacks, the sale of stolen data, and fraud. To safeguard their identities and evade law enforcement, they utilize encryption techniques, anonymization services, and cryptocurrencies (Sancho & Fuentes, 2023). This level of organization makes cybercrime groups a significant threat to businesses and governments worldwide. One particularly notable example is the ransomware group „LockBit," which carried out numerous attacks on businesses worldwide in 2022 and 2023. Operating as a Ransomware-as-a-Service (RaaS), LockBit recruits affiliates to conduct ransomware attacks using its proprietary tools and infrastructure. These attacks result in the encryption of data on compromised systems, with victims being extorted for ransom payments to regain access to their files (CISA, 2023). A case in point is the 2022 attack on the DAX-listed company Continental, which suffered significant financial losses and required several weeks to restore its systems. LockBit affiliates have targeted companies globally, spanning industries such as financial services, food and agriculture, education, energy, government and emergency services, healthcare, manufacturing, and transportation (BlackFog, 2025).

Critical Infrastructure as a Target

Globally, cyberattacks frequently aim to disrupt critical infrastructure, inflict economic damage, or foster political instability. A prominent example is the Russian cyberattack on Ukraine's power grid in 2015 (Süddeutsche, 2016). The extensive Russian military aggression against Ukraine has demonstrated the integral role of cyberattacks in modern warfare, with Russian state-sponsored hackers repeatedly attempting to destabilize Ukrainian infrastructure through DDoS attacks. Notably, in the early stages of the war, these attacks targeted Ukraine's critical infrastructure alongside conventional military operations.

The Geopoliticization of Cyberspace

Digital demobilization poses a substantial challenge, as cyberspace has become a battleground for geopolitical conflicts. Real-world political events manifest in cyberspace, where their implications and consequences are increasingly severe. Cyber operations are now integral to modern military strategies and hybrid warfare.Simultaneously, non-state groups and hacktivists exploit cyberattacks to advance ideological and political agendas.

Germany's current cybersecurity architecture is insufficiently aligned with existing threats and proves inefficient.

Strengthening Germany's Cyber Capabilities

To effectively respond to developments in cyberspace, Germany must enhance its cyber capabilities. The country's current cybersecurity architecture is insufficiently aligned with existing threats and proves inefficient. Redundant structures at federal and state levels, along with unclear jurisdictional responsibilities among various institutions, exacerbate the issue. Small and medium-sized enterprises (SMEs) and operators of critical infrastructures (KRITIS) face particular challenges in this regard, especially concerning the upcoming implementation of the European NIS2 Directive (European Parliament, 2022) and the Cyber Resilience Act (European Parliament, 2024).

A Central Role for the BSI

The Federal Office for Information Security (BSI) should assume a more central and independent role, particularly in advisory and certification functions. To meet future challenges, the BSI must receive additional personnel and financial resources. Simultaneously, the interests of federal states and municipalities must be equitably considered when restructuring cybersecurity frameworks.

Cybersecurity as a Collective Responsibility

Cybersecurity is a shared responsibility among all stakeholders. Beyond government agencies, the private IT security sector must be more actively involved. Germany possesses a robust base of SMEs specializing in IT security services, which could significantly contribute to strengthening cybersecurity while alleviating the burden on public institutions such as the BSI. Establishing a resilient public-private partnership is crucial, supported by targeted incentives such as tax benefits for companies investing in cybersecurity or funding programs for innovative security solutions.

Optimizing Cyber Defense

Germany's current cyber defense mechanisms are inadequate for addressing the existing threat landscape. The Federal Criminal Police Office (BKA) should be designated as the central authority for cyber threat prevention due to its well-developed and scalable structures. Furthermore, the National Cyber Defense Center (C-AZ) should be upgraded and placed under the jurisdiction of the Federal Chancellery, with stronger involvement from federal states. A nationwide real-time cyber threat intelligence

system, maintained at the C-AZ and accessible to all relevant stakeholders, is essential.

Enhancing Digital Forensic Capabilities

Germany's prosecution authorities must also be adequately equipped for the digital transformation. Cybercrime is escalating, with cybercriminal groups becoming increasingly sophisticated. Legal frameworks should be revised to enable secure confiscation of digital attack infrastructures such as servers and IT networks. Additionally, a reform of cybercrime laws is necessary. Notably, ethical security researchers should no longer face prosecution for identifying and mitigating security vulnerabilities. Establishing an official register for security researchers would provide them with greater legal clarity. For non-researchers, voluntarily reporting vulnerabilities to the BSI, the Federal Commissioner for Data Protection and Freedom of Information, the Federal Ministry of Justice, or Central Cybercrime Contact Points (ZAC) could yield mitigating legal benefits.

Strengthening Cybersecurity Education and Training

These reforms alone will not render Germany fully cyber-capable. Future crises cannot be entirely prevented. Therefore, alongside a more robust cybersecurity education and training framework for the general population, regular cybersecurity exercises should be conducted to enhance preparedness and resilience.

Strengthening Digital Sovereignty

Germany must also place greater emphasis on strengthening its digital sovereignty. This includes not only diversifying risks and reducing dependencies but also promoting sustainable and secure digitalization based on the principle of „Security by Design." According to a survey by Bitkom, four-fifths of German companies view their digital dependence on the USA and China as problematic. The dependency is particularly high in the areas of semiconductors and end devices: 83 percent of companies consider Germany to be highly dependent on third parties. This dependence poses a significant risk, as many companies see no way to counteract political pressure on their foreign business partners (Bitkom, 2025). National and European innovations should be promoted more intensively, and investments should be strengthened. Start-ups must be supported in product development in the German market and encouraged to compete in international markets such as the USA or Israel. For the federal administration, state institutions, municipalities, and critical infrastructures, this means relying on uniform digital solutions „Made in Germany." A first step could be the development of a national cloud infrastructure and a German cloud solution.

Germany Must Act Quickly

To address developments in cyberspace, the increasingly professionalized state and non-state actors, and the growing damage potential, several adjustments must be made. Germany is currently not sufficiently prepared. Successfully tackling these challenges requires close cooperation between the government, society, and the economy. The key issues and necessary measures are clear: adapting the cybersecurity architecture, strengthening the Federal Office for Information Security (BSI), building an effective cyber defense, improving education, and promoting digital sovereignty. Only in this way can hostile actors in cyberspace be stopped and Germany become cyber-capable."

References

Bitkom. (2024). Wirtschaftsschutzstudie 2024. Abgerufen von https://www.bitkom.org/sites/main/files/2024-08/240828-bitkom-charts-wirtschaftsschutz-cybercrime.pdf (zuletzt aufgerufen am 24.01.2025).

Bitkom. (2025). Deutschlands digitale Abhängigkeit steigt. Abgerufen von https://www.bitkom.org/Presse/Presseinformation/Deutschlands-digitale-Abhaengigkeit-steigt (zuletzt aufgerufen am 24.01.2025).

BlackFog. (2025). LockBit's 2024 Attacks – An Overview. Abgerufen von https://www.blackfog.com/lockbit-attacks-2024/ (zuletzt aufgerufen am 24.01.2025).

Booz Allen Hamilton. (2023). China's Cyberattack Strategy Explained. Abgerufen von https://www.boozallen.com/insights/cyber/chinas-cyberattack-strategy-explained.html (zuletzt aufgerufen am 24.01.2025).

Bundesministerium des Innern und für Heimat (BMI). (2024). Cyberangriffe auf die SPD und auf Rüstungs-, IT- und Luftfahrtunternehmen sind APT 28 und damit dem russischen Militärgeheimdienst GRU zuzuordnen. Abgerufen von https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2024/05/aktuelle-Cyberangriffe.html (zuletzt aufgerufen am 24.01.2025).

Bundesministerium des Innern und für Heimat (BMI). (2024) II.

Bundesamt für Verfassungsschutz (BfV). (2025). Akteure und Angriffsmethoden.
Abgerufen von https://www.verfassungsschutz.de/DE/themen/cyberabwehr/akteure-und-angriffsmethoden/akteure-und-angriffsmethoden_node.html (zuletzt aufgerufen am 24.01.2025).

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2024). Die Lage der IT-Sicherheit in Deutschland 2024. Abgerufen von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.pdf?__blob=publicationFile&v=5 (zuletzt aufgerufen am 24.01.2025).

Chaudhury, D. R. (2021, April 12). States' use of non-state actors in cyberspace. Observer Research Foundation. https://www.orfonline.org/expert-speak/states-use-of-non-state-actors-in-cyberspace (zuletzt aufgerufen am 24.01.2025).

CrowdStrike. (2024). Global Threat Report 2024. Abgerufen von https://www.crowdstrike.com/en-us/global-threat-report/ (zuletzt aufgerufen am 24.01.2025).

Cybersecurity and Infrastructure Security Agency (CISA). (2021). Nation-State Threats. Abgerufen von https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors (zuletzt aufgerufen am 24.01.2025).

Cybersecurity and Infrastructure Security Agency (CISA). (2023). Understanding Ransomware Threat Actors: LockBit. Abgerufen von https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a (zuletzt aufgerufen am 24.01.2025).

Europäisches Parlament. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union. Abgerufen von https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555 (zuletzt aufgerufen am 24.01.2025).

Europäisches Parlament. (2023). Cybersecurity in the EU: Threats, challenges and policy responses. Abgerufen von https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf (zuletzt aufgerufen am 24.01.2025).

Europäisches Parlament. (2024). Regulation (EU) 2024/2847 of the European Parliament and of the Council of 14 December 2024 on measures for a high common level of cybersecurity across the Union. Abgerufen von https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847 (zuletzt aufgerufen am 24.01.2025).

Maurer, T. (2016). Cyber Proxies and the Crisis of International Relations. Journal of Conflict and Security Law, 21(3), 383-403. https://carnegie-production-assets.s3.amazonaws.com/static/files/JConflictSecurityLaw-2016-Maurer-383-403.pdf (zuletzt aufgerufen am 24.01.2025).

Merics. (2023). Cyber Security in China (II): Neue politische Führung setzt auf Stärkung der nationalen Sicherheit. Abgerufen von https://merics.org/sites/default/files/2020-05/China%20Monitor%20No%2020.pdf (zuletzt aufgerufen am 24.01.2025).

PC-SPEZIALIST. (2024). Digital Defense Report 2024: Zahl der Cyberangriffe steigt. Abgerufen von https://www.pcspezialist.de/blog/2024/11/04/digital-defense-report-2024/ (zuletzt aufgerufen am 24.01.2025).

Sancho, D., & Fuentes, M. R. (2023, April 3). Unpacking the structure of modern cybercrime organizations. Trend Micro. Abgerufen von https://www.trendmicro.com/en_us/research/23/d/unpacking-the-structure-of-modern-cybercrime-organizations--.html (zuletzt aufgerufen am 24.01.2025).

Spiegel. (2023). Vulkan Files. Abgerufen von https://www.spiegel.de/politik/deutschland/vulkan-files-enthuellungen-wie-putins-cybersoldaten-den-krieg-ins-internet-tragen-a-bb241ad9-a9c3-422e-af57-ffe59986a1d8 (zuletzt aufgerufen am 24.01.2025).

Süddeutsche Zeitung. (2016, Januar 11). Ukraine: Bundesamt geht von Hackerangriff auf ukrainisches Stromnetz aus. Süddeutsche.de. Abgerufen von https://www.sueddeutsche.de/wirtschaft/ukraine-bundesamt-geht-von-hackerangriff-auf-ukrainisches-stromnetz-aus-1.2830197 (zuletzt aufgerufen am 24.01.2025).

The Cyber Express. (2023). Hacktivist Groups Target G20 Summit. Abgerufen von https://thecyberexpress.com/g20-summit-2023-cyber-attack-infrastructure/ (zuletzt aufgerufen am 24.01.2025).

About the Article

Hybrid warfare is shaping the future of conflict by expanding battlefields beyond the military domain, leveraging political, economic, and societal pressures. Drawing from Clausewitz, Johann Schmid argues that defense remains stronger than offense, but hybrid strategies exploit grey areas and strategic ambiguity to circumvent strong defenses. As warfare blurs the lines between war and peace, military and civilian targets, nations must prepare holistically to counter hybrid threats.

About the Author

Colonel Dr. Johann Schmid is the project officer for the subject matter of hybrid warfare at the Center for Military History and Social Sciences of the Bundeswehr (ZMSBw). He is also a lecturer at the Chair of Military History and Cultural History of Violence at the University of Potsdam and a non-resident fellow at the Institute for Peace Research and Security Policy at the University of Hamburg (IFSH).

Abstract

Anyone who understands the DNA of war can look a little way into its future. Hybrid warfare will shape this future to a considerable extent. Its strategists are expanding the battlefield horizontally, operating in gray areas and using unorthodox combinations of means and methods. Nonetheless, military combat will not lose any of its importance. However, in future it will have to be increasingly placed in the overarching context of hybrid warfare.

Keywords: Hybrid warfare, Clausewitz, On War, Russian-Ukrainian war

The DNA of war

Much is written about the future of war. The half-life of such considerations is generally limited. However, one work stands out in terms of its significance across time, even though it does not explicitly deal with the future of war. It is called "On War" and was written by the Prussian general and philosopher of war Carl von Clausewitz (1780-1831). The background was the social upheavals of the French Revolution and the revolutionary changes in warfare that accompanied it. The Napoleonic wars of conquest were the result. They also provided the empirical background for "On War". But what is the significance of this work for the future of war? It lies in Clausewitz's interest in understanding the unchanging nature of war. He sought to fathom this in "On War", detached from the manifold and ever-changing empirical manifestations of war. In other words, "On War" is about decoding the DNA of war. In doing so, Clausewitz identifies principles, connections and interactions that transcend time and develops a method of thinking that corresponds to the nature of war. On this basis, it is possible to look a little way into the future of war in order to understand its contours and recognize basic constants and protect one's own judgment from major deviations.

Clausewitz and the future of war

Following Clausewitz's analysis of the nature of war, war will continue to be a continuation of politics by other means. It will also continue to be an act of violence in order to force the opponent to fulfill one's own will. Uncertainty, chance and friction, as well as psychological and moral factors, will continue to play a decisive role in the future and thus make war impossible to be calculated mathematically. Last but not least, war will continue to be more a matter for the defender than the aggressor. After all, it is only with the defense that the battle begins and with it the war. The "peace-loving" aggressor, Clausewitz refers in this context to Napoleon Bonaparte's self-portrayal, generally wants to conquer, dictate or unilaterally use force, but not necessarily fight. It is therefore particularly up to the defender to prepare for war.

Figure 1: Carl von Clausewitz 1780-1831

„War serves the purpose of the defense more than that of the aggressor. It is only aggression that calls forth defense, and war along with it. The aggressor is always

peace-loving (Bonaparte); he would prefer to take over our country unopposed. To prevent his doing so one must be willing to make war and be prepared for it." (Clausewitz, On War, VI, 5, p. 444).

The greater strength of the defense

After all, the war of the future will also be characterized by two main forms: attack and defense. Clausewitz has a special message to convey in this regard. It is his theorem of the fundamentally greater strength of the defense at both the tactical and strategic levels. This strength results, among other things, from the support of the theater of war (terrain, fortresses, bases), the people (population, use of conscription) and great moral forces (motivation, willingness to make sacrifices, ability to suffer), which a legitimate war of popular defense against an external invasion is particularly capable of arousing. Without this inner strength, Ukraine's successful defense against the Russian attack would have been almost inconceivable. It is the single most important factor in explaining the war in and over Ukraine since 2014 and increasingly so since February 2022.

Hybrid warfare blurs the lines between war and peace, leveraging military and non-military means to achieve strategic goals.

Battle for Ukraine

One of the reasons why Ukraine was not able to derive far greater benefit from the strength of its defense was its lack of preparation, particularly for the military escalation since February 2022. For example, the crossings from Crimea to the Ukrainian mainland were not sustainably defended, there were no larger bodies of troops in defensive positions between Kiev and the Belarusian border, and a (potentially deterrent) partial mobilization was not carried out. Despite the transparency of the Russian deployment and the relevant warnings, Ukraine's political leadership failed to recognize the danger. In the summer of 2023, Ukraine had to learn the hard way how difficult or even impossible it can be to overcome a well-prepared military defense. Despite Western weapons assistance, its long-prepared counter-offensive became bogged down after a few kilometers in the minefields and in the fire of the well-organized Russian defense. This confirmed the principle that the better prepared a defense is, the stronger it is.

State of weapons technology

In addition, the greater internal strength of the defense described by Clausewitz is massively reinforced by the current state of weapons technology. The battlefield has become transparent thanks to drone-supported continuous observation from the air. Real-time data transmission enables responsive precision fire from artillery, drones, attack helicopters and air forces. Fire dominates movement on the ground to an unprecedented degree, allowing defense to dominate offense. Paradoxically, the war in Ukraine today is more like at the Western Front of the First World War than at the Eastern Front of the Second. This raises a fundamental question in relation to war: how can a well-prepared military defense be overcome?

Hybrid overcoming of military defense

The strategists of hybrid warfare have found very different answers to this. If it is not possible to defeat the enemy's armed forces militarily, as is currently the case in the war between Russia and Ukraine, the war can be extended horizontally and along the time axis. In this case, strategies of denial of victory, personnel and material attrition and devastation as well as psychological and moral exhaustion are pursued. Not only the armed forces but also the economy, industry, society, science and technology come into play. Soft dimensions such as psychology, morale, legitimacy and the political will to endure a war despite sacrifices and burdens are equally important. Morality, willingness to make sacrifices and the ability of

society to suffer are important, as are the economic, financial and resource-related resilience of a state. Finally, the resourcefulness with which new technologies can be quickly harnessed for warfare can also be of great importance. Even without its own navy, Ukraine has succeeded in challenging the Russian fleet for control of the western part of the Black Sea. The decisive factor in this was Ukrainian military intelligence in conjunction with the innovative use of new technologies. This made it possible to quickly develop far-reaching means of action (including naval drones) to combat the Russian fleet, inflict substantial losses on it and thus keep it at a distance.

Hybrid delimitation of the battlefield

In hybrid warfare, the battlefield is expanded horizontally. The war is waged simultaneously on different domains, which can be regarded as "partial battlefields". The military "shooting war" is one of these sub-domains. The information and propaganda war, the economic and resource war, the struggle in the diplomatic arena and the fight for legitimacy and international support are also part of the war as a whole. The same applies to the battle of the secret services and the cultural struggle within society. As a rule, it is not possible to predict ex ante on which field such a hybrid war will be decided. In the event of a military stalemate, the opponent can also be forced to comply with its own will via other fields of action (domains), e.g. politically, diplomatically, economically, socially or technologically.

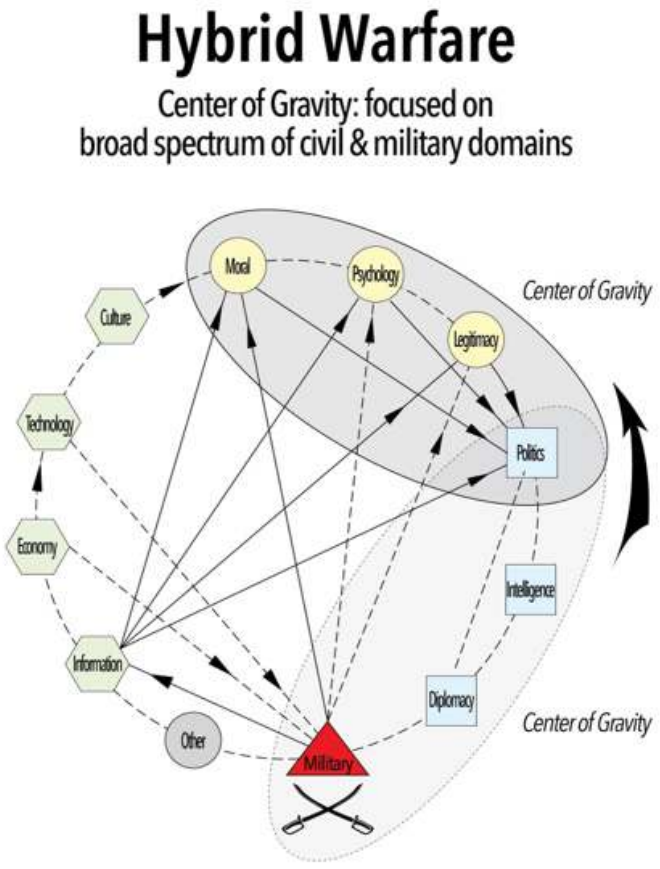


Figure 2: Non-hierarchical / dynamic / flexible Structure Multiple and shifting Centers of Gravity

Society as a target

Hybrid actors take the path of least resistance whenever possible and prefer to operate in the gray areas of interfaces. As societies are more vulnerable than their armed forces, the former can already be effectively attacked using non-military hybrid methods. The instrumentalization of irregular migration flows to destabilize and disintegrate the society of a target country ("weaponized migration") is currently the sharpest weapon in this context. Ideological radicalization of an Islamist nature, clan-criminal disintegration as well as the targeted infiltration of an aggressor's "fifth column" in the form of agents, agitators, saboteurs and terrorists can go hand in hand with this. EU Europe has been exposed to such hybrid attacks on a massive scale since 2015. Some of these attacks (including in the direction of Poland, Lithuania and Finland) are part of the Ukraine-Russia war and are directed against supporters of Ukraine. However, even without its own EU external border, Germany is the main target country for this method of attack. The lack of awareness of this danger, the pull effect of the easy accessibility of its social systems and the lack of political will to protect its own population from this danger make Germany an "Eldorado" for such hybrid attacks. It should be borne in mind that those who fail to protect their society from non-military attack vectors also jeopardize their military defense capabilities. Germany's declared aim of making its armed forces "fit for war" and preparing its own country and society for "total defense" is thus thwarted.

Implications / conclusions

- Anyone who wants to understand the future of war must come to terms with its nature. Clausewitz offers an excellent approach to this with "On War".

- War will continue to be more a matter for the defender than the aggressor. It is therefore crucial for peace-loving nations to prepare for war.

- In the future, war will continue to be characterized by the fundamentally greater strength of the defense. This is currently being massively reinforced by the state of weapons technology. But only those who prepare the defense can also use these strengths.

- Hybrid warfare is accompanied by three central challenges that must be considered with regard to resilience building, defense and counteraction:

    - Firstly, the horizontal dissolution of the boundaries of the battlefield in conjunction with the use of non-military centers of gravity for decision-making (including politics, diplomacy, economics, society, culture, technology, the military, information and legitimacy).

    - Secondly, deliberately operating in the grey areas of interfaces between traditional categories of order and areas of responsibility (e.g. war - peace, friend - foe, internal - external security, civil - military areas of responsibility, state - non-state actor categories) in order to create ambiguity and paralyze decision-making processes.

    - Thirdly, the creative and unorthodox combination of means, methods, tactics and strategies that in a more traditional understanding would tend to be separated from each other (regular and irregular, symmetrical and asymmetrical, overt and covert, legal and illegal, hard and soft).

- In times of hybrid warfare, the boundaries between war and peace, friend and foe and between internal and external security are becoming blurred. In addition to a strong military defense, the protection of one's own society against non-military attack vectors (including "weaponized migration", ideological radicalization, criminal disintegration, enemy infiltration) is therefore of central importance.

- Hybrid warfare is the more holistic and diverse form of warfare. With its unorthodox approaches, it also offers the possibility of circumventing or undermining a strong military defense. In many cases, it will be the simpler, cheaper and more intelligent alternative. The future of war to a large degree will therefore be hybrid.

epis ThinkTank

International Politics Shaped By **You**

EPIS Thinktank

Who We Are

EPIS is a young think tank on foreign affairs and security policy. We publish scientific articles, send members to international conferences, and maintain a network of: students & young professionals.

The deal:

- You professionalize yourself in your field
- We help you start your career

What We Do

EPIS Magazine

- In-Depth Analyses of Political Issues of Your Choice
- 80 Pages
- 3x/Year

EPIS Working Groups

- Monthly Briefings on Political Developments in Eight World Regions

EPIS Talks

- Deep Dive into the Articles of our Magazine with the Authors

EPIS Blog

- Short Analyses of Political Issues of Your Choice
- Weekly Release

About the Interview

Marika Linntam, Estonian Ambassador to Germany, discusses her career, Estonia's digital leadership, and security policies. Estonia pioneered digitalization, offering nearly all government services online. Cyber security is crucial, especially after Russian cyber-attacks in 2007. Estonia strongly supports Ukraine and sees NATO as essential for security. Relations with Germany are strong, based on shared values and cooperation. Linntam encourages young people, especially women, to pursue diplomacy with passion.

About the Interviewee

Marika Linntam has been Estonia's Ambassador to Germany since September 27, 2023. She studied law at the University of Tartu, European law at the University of Trier, and earned a master's degree from the University of Rennes 1. Joining the Ministry of Foreign Affairs in 2001, she held key positions, including leading the European Law Division and representing Estonia at the European Court of Justice. From 2018 to 2023, she served as Director General of the European Affairs Department.

About the Interviewer

Carolin Hochstrat is pursuing a double degree in Germany and France. Alongside her studies, she brings a strong journalistic background, having worked for WELT TV-Axel Springer, and currently manages public relations in the Bundestag. She is actively engaged in political organizations and think tanks, including DGAP and GSP, contributing to discussions on foreign policy and security. Her multidisciplinary expertise bridges media, politics, and international relations.

Carolin Hochstrat:
Would you like to tell us a little about yourself?

Marika Linntam:
I have been the Estonian Ambassador to Germany for a little over a year now, a role I take on with great honor and responsibility, as Germany is one of Estonia's main partners and allies. Germany's role in Europe is incredibly important. I have worked in the Estonian foreign service since 2001. My academic background is in law, particularly European law. I studied it in Germany at the University of Trier in some courses and completed a longer master's program in France. My career has consistently been focused on Europe. Over the years, I've held various positions, including postings to Brussels, where I was involved during Estonia's presidency of the European Union. Before that, I served as Estonia's state agent at the European Court of Justice. Since 2014, security issues have been a significant part of any European diplomat's work, and certainly for Estonian diplomats. Before coming to Germany, I spent five years as the Director General for Europe at the Estonian Ministry of Foreign Affairs, overseeing bilateral relations with European countries and key EU policies.

Carolin Hochstrat:
That's a remarkable path to becoming an ambassador! What would you say have been the biggest milestones and challenges in your career?

Marika Linntam:
The biggest milestones often revolve around major postings. For example, my time in Brussels allowed me to work closely on high-level EU affairs and engage with critical topics that even heads of state were discussing. Being responsible for relations with other European countries at the Ministry of Foreign Affairs was a tremendous honor. Of course, becoming Estonia's ambassador to Germany is an important milestone.

Carolin Hochstrat:
How do you handle the responsibility that comes with being a diplomat?

Marika Linntam:
I genuinely enjoy my work, so I embrace the responsibility that comes with it. Managing international relations, especially for Estonia, is a key role in ensuring the country's place in the world. It's a privilege to contribute to that.

Carolin Hochstrat:
What has your experience been like as a woman in the diplomatic and international field?

Marika Linntam:
Personally, I haven't found gender to be a decisive factor in my career. The Estonian foreign service maintains a good gender balance, and in my various postings, I haven't noticed significant differences in how male and female diplomats are treated.

Carolin Hochstrat:
How would you describe Estonia in three words?

Marika Linntam:
Innovative, digitalised, and beautiful—especially its landscape. Estonia is an amazing destination for tourism because of its stunning nature. We have a long coastline, around 2,000 islands (many of which are inhabited and fascinating to explore), as well as marshlands, forests, and lakes. The people are friendly, though some might say that people in the north take a bit longer to open up. Overall, we are very welcoming.
Carolin Hochstrat: Estonia is often seen as a pioneer in digitalisation. Could you tell me more about that and your e-government system?

Marika Linntam:
After regaining independence in 1991, Estonia faced economic challenges and needed deep reforms. Our leaders had the foresight to focus on digitalisation early. In the 1990s, we introduced the "Tiger Leap" program, which brought computer classes to all schools and integrated IT education into the curriculum. Today, nearly all government services are available online, with the exception of getting married. Citizens can securely access services using their ID cards, which also enable digital signatures. This digital transformation has been a significant advantage for Estonia, fostering innovation and a strong startup culture. We now have the highest number of unicorns per capita in Europe. Estonia also actively shares its digital expertise with other countries.

Carolin Hochstrat:
You've touched on cyber security. Could you explain Estonia's approach, especially in light of its history with cyber-attacks?

Marika Linntam:
Cyber security is the flipside of digitalisation. In 2007, Estonia experienced severe cyber-attacks from Russia, which served as a wake-up call. We've since built a robust cyber security system. Tallinn hosts NATO's Center of Excellence for Cyber Security, and Estonia actively promotes responsible state behavior in cyberspace, emphasising international law and security.

Carolin Hochstrat:
How would you describe Estonia's relationship with Russia, particularly in the context of the war in Ukraine?

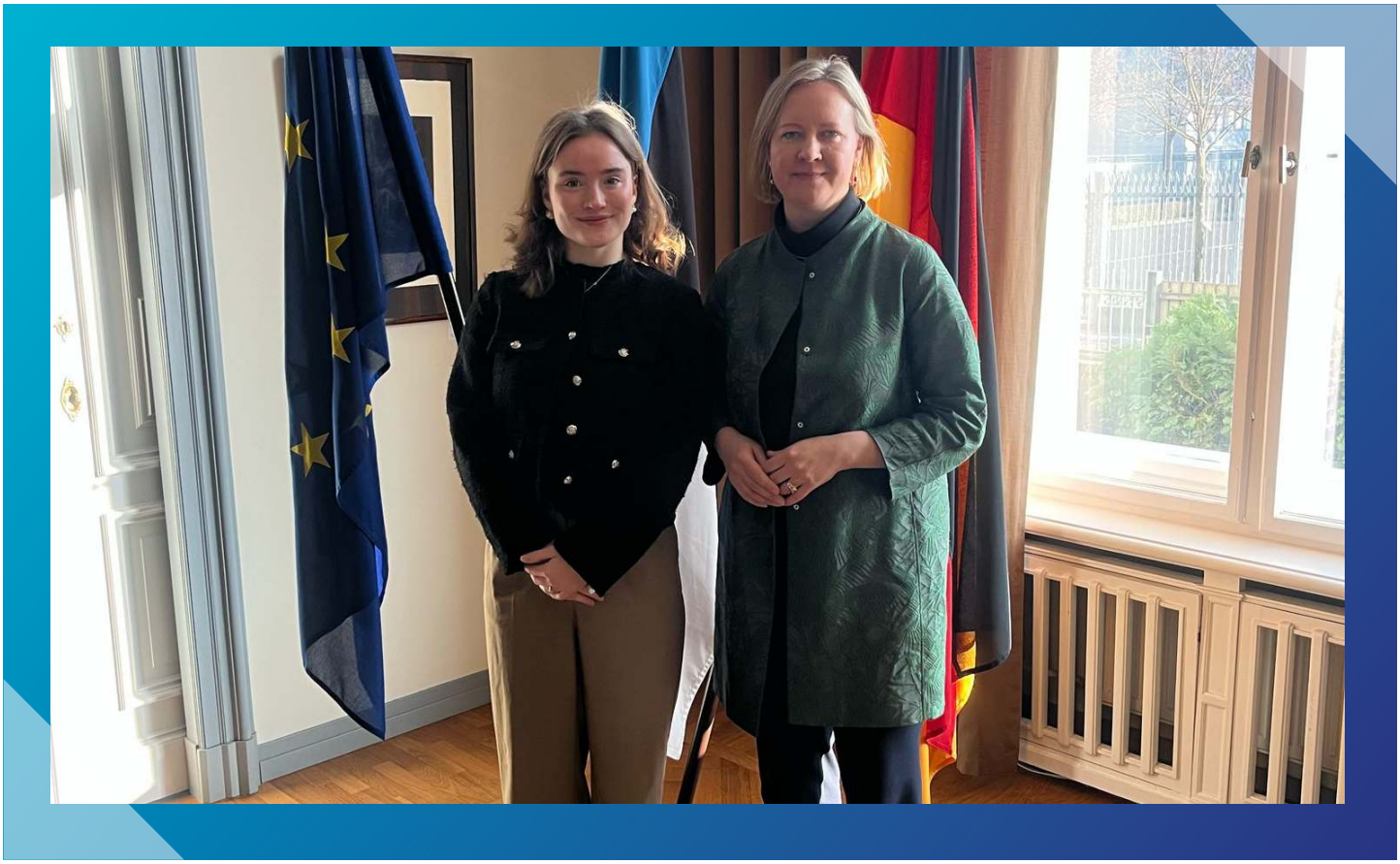
Marika Linntam:
Estonia values good relations with its neighbors, but this also depends on the other side. Our membership in the European Union and NATO has been crucial for our security. Russia's actions—annexing Crimea in 2014 and its full-scale invasion of Ukraine in 2022—are grave concerns for us. Such actions threaten European and global security. Estonia strongly supports Ukraine, as we believe allowing Russia to benefit from aggression would undermine the rules-based international order.

> **We encourage other NATO countries, especially in Europe, to strengthen their contributions.**

Carolin Hochstrat:
How significant is NATO for Estonia?

Marika Linntam:
NATO is vital for our security. Estonia contributes significantly, with defense spending at 3.4% of GDP. We also encourage other NATO countries, especially in Europe, to strengthen their contributions.

Carolin Hochstrat:
What about strengthening Europe's defense capabilities within the EU?



Marika Linntam:
NATO is the cornerstone of our collective security, but the EU also has a role, particularly in areas like hybrid threats and supporting the defense industry. Strengthening these areas complements NATO's efforts.

Carolin Hochstrat:
How would you describe Estonia's role within the European Union?

Marika Linntam:
Estonia is a constructive and engaged member. We focus on areas where we can lead, such as digitalisation and cyber security, and work collaboratively to ensure EU policies benefit all member states.

Carolin Hochstrat:
As Estonia's ambassador to Germany, how would you describe the relationship between the two countries?

Marika Linntam:
Estonia and Germany share close ties, rooted in historical connections like the Hanseatic League and strengthened by common values. Germany plays a key role in Europe, and we highly value our cooperation across various areas.

Carolin Hochstrat:
What advice would you give to young people, particularly women, aspiring to a diplomatic career?

Marika Linntam:
Follow your own path. Diplomacy offers many areas of focus, so it's important to find the one you're passionate about. Commitment and inspiration are essential in this field, as it requires genuine interest and dedication.

Carolin Hochstrat:
Thank you so much for this insightful conversation and for your time.

Marika Linntam:
Thank you for having me.

EPIS BASICS:

THE ORIGIN OF THE MILITARY-INDUSTRIAL COMPLEX, IT'S ASPECTS, AND OUTLOOK TODAY

In EPIS Basics, our authors explain basic knowledge of international foreign affairs and security policies. This encompasses basic theories, organisations and events This series is presented in depth here in the magazine. You can also find other smaller contributions on our Instagram page

Dominic Perfetti

As I am currently studying War Studies at King's College London, I have always had an interest in geopolitics within and outside of academia. My career goal is to do intelligence analysis within the scope of geopolitical risk.

1. Military Industrial Complex

Russians in Ukraine, Israelis in Gaza, and American threats to leave NATO. Increasing tensions and rising military budgets have given rise to concerns over what Eisenhower called the "military-industrial complex". The military-industrial complex (MIC) was first mentioned almost 70 years ago by President Eisenhower in his farewell speech, "In the councils of government, we must guard against the acquisition of unwarranted influence, whether sought or unsought, by the military-industrial complex. The potential for the disastrous rise of misplaced power exists and will persist" (Eisenhower, 1961, para. 15). Eisenhower warned against the MIC, which describes a strong relationship between a state's government and its defence industry, wherein defence companies benefit from government contracts, and officials benefit politically from increased defence spending. The fears of the MIC to which Eisenhower alluded are inflated military spending, erosion of democratic institutions, and environmental and humanitarian concerns.

2. Ratchet Effect

The MIC can create an economic ratchet effect, whereby once a state's military budget has increased, it can be difficult to lower it in the future. Governments invest in the defence sector by procuring military equipment.For countries like the United States, the defence sector represents a relatively large portion of the economy. U.S. military spending as a percentage of GDP was 3.4 per cent in 2023 (World Bank Group, n.d.), and the defence sector represents 1.6 per cent of American employment (Aerospace Industries Association, 2021).

As such, it can be difficult to reduce defence spending without facing political opposition. An inability to lower the defence budget can cause problems like increasing national debt or an inability to allocate funds for other projects.

3. Socio-Political Consequences

The consequences of the ratchet effect of the MIC are the undermining of democracy and social issues. MIC can undermine liberal democratic values because of lobbying efforts of defence firms for an increased military budget. This lobbying means that politicians represent the interests of these companies rather than the concerns of the citizens who voted them into office. Social concerns like arms control and environmental protection also arise from the MIC, as having more guns does not necessarily make the world safer. Moreover, the defence industry creates a significant amount of pollution.

4. The Military-Industrial Complex Today

Though global defence spending as a percentage of GDP has steadily decreased over time, many states have seen a rise in their own defence spending in recent years. Since the outbreak of the war in Ukraine, Russia's defence spending as a per cent of GDP rose from 3.6 per cent in 2021 to 6.3 per cent in 2025 (Al Jazeera, 2024). Among security concerns, advancements in technology drive increased defence spending. New military technologies, such as those that utilise artificial intelligence, have attracted greater defence budgets. Finally, MIC concerns have been raised from President Trump's calls for NATO allies to spend at least 5 per cent of their GDP on defence. (Kayali et al., 2025). Although humanitarian and environmental efforts may challenge the MIC, it will be a hard-fought battle.


Donate
About us
Network
Working Groups
Formats
Report Groups
Apply
EPIS Thinktank
The Think Tank for Foreign- and Security Policy
episthinktank
EPIS ThinkTank | Foreign- & Security Policy
222 posts
531 followers
49 following
Political Organization
Thinktank & Network for Students
Connect with Experts & Publish your Articles
Based in
Join EPIS Now
See Translation
www.epis-thinktank.de/en and 3 more
Follow
Message
Email
Delegations
W.Groups
Basics
Blog
Berlin Security Conference 2024
Join our Team
EPIS Report on Climate Policy & Environment
Read Now!

Imprint

Editor-in-chief: Alvin Karl Bürck
ViSdP: Theodor Himmel
Publisher: EPIS ThinkTank e.V.
Contact: kontakt@epis-thinktank.de
ISSN: 2942-6030

Are you interested in our work?

EPIS is both a network and a think tank in foreign and security policy. The EPIS Network connects students and graduates, supporting their careers. The EPIS Think Tank produces publications in various formats on different regions and topics. Together, they form EPIS—where you can join passively as a network member or actively contribute to publications. Interested? Apply now for an onboarding meeting & follow us on social media!

Find out more on: www.epis-thinktank.de

or visit us on: