AKADEMIA SZTUKI WOJENNEJ

AKADEMICKIE CENTRUM
ANALIZ STRATEGICZNYCH

MYŚL STRATEGICZNA

Nr 1 (5) 2026

Warszawa 2026

ISSN 3071-9305

Adres wydawcy/redakcji
Akademickie Centrum Analiz Strategicznych
Akademia Sztuki Wojennej w Warszawie
Al. gen. A. Chruściela „Montera" 103
00-910 Warszawa

Skład, druk i oprawa: Wydawnictwo Akademii Sztuki Wojennej, zam. nr 14/26, nakład 120 egz.

Contents

War is merely the continuation of policy by other means

C. Von Clausewitz, *On war*, Princeton 1873

Introduction

This first English issue of Strategic Thought is conceived as an intervention into a rapidly shifting security environment in which the boundaries between war and peace, internal and external security, and civilian and military innovation are increasingly porous. Our guiding premise, in methodological and theoretical terms, is that contemporary strategic studies and security studies must (I) integrate multi-level analysis – linking structural drivers and institutional architectures with meso-level organisational practices and micro-level operational methods; (II) adopt mixed methods commensurate with hybrid threats – combining doctrinal analysis, content/discourse analysis, process tracing, and policy evaluation; and (III) remain problem-driven, policy-relevant, and empirically grounded. Recent escalations in Eastern Europe and the Middle East, the weaponisation of supply chains and energy flows, and the diffusion of dual-use technologies underscore the need for such an integrated approach. Against this backdrop, the contributions assembled here examine the logics and instruments of contemporary statecraft - from proxy networks and disinformation ecosystems to air and missile defence architectures, cybercrime governance, narcotics-conflict nexuses, and the politics of European defence integration.

The volume has been curated to illuminate four cross-cutting problem sets. First, the rise of indirect instruments of power (proxy agency, disinformation, criminalised logistics), which challenge classical deterrence and attribution. Second, the technological acceleration of security dilemmas (dual-use

innovation, AI governance, cybercrime), which collapses the civilian–military boundary. Third, the institutional adaptation of states and alliances (air/missile defence integration, legal/doctrinal updates) to compressed warning timelines and saturation threats. Fourth, the regional interdependence of theatres (MENA–Europe), which binds domestic vulnerabilities to transnational conflict economies. The selection of texts is informed by these priorities, which together provide an analytically coherent and empirically diverse map of contemporary strategic risks and response options, grounded in security studies, political science, and the political economy of technology.

Proxy agent networks as an instrument of contemporary intelligence

Dr Anna Grabowska-Siwiec theorises „proxy agent networks" as a distinct modality of intelligence action that outsources risk and cost to intermediaries while preserving plausible deniability for the state sponsor. Conceptually, the article distinguishes proxy networks from classical agents of influence and anchors key terms in Polish and EU legal frameworks. Empirically, it links the proliferation of such networks in Poland to the post-February 2022 context and Warsaw's robust support for Ukraine. Methodologically, it combines doctrinal/legal analysis with open-source indicators (institutional communiqués) to specify operational signatures and counterintelligence implications. The piece advances security studies debates by clarifying categories, specifying mechanisms (digital recruitment, tasking, and remuneration), and deriving policy-ready recommendations for resilience and law enforcement practice.

Characteristics of Russian disinformation in Lebanon

Dr Blanka Katarzyna Dżugaj investigates Russian disinformation in Lebanon as a nested strategy that operates across traditional and social media, exploiting sectarian fragmentation, weak regulation, and patronage-based media ownership. The article employs discourse analysis and media monitoring (2022–2025) to identify narrative families (anti-Western moral delegitimation, multipolarity claims, Ukraine-focused denialism) and their conduits (local platforms, Arabic-language repackaging, proxy amplification). It contributes theoretically by situating disinformation within a political economy of media capture, and it contributes methodologically through a transparent design that links macro-level crisis indicators (such as currency collapse and governance paralysis) to meso-level messaging practices and micro-level audience effects.

Policy-wise, the paper cautions that short-term soft-power gains for Moscow may entail reputational overreach as literacy about manipulation grows.

China's Made in China 2025 and the dual-use turn

Dominika Sikorska's article presents a structured analysis of Made in China 2025 (MIC-2025) as a blueprint for technological hegemony through the fusion of civilian and military sectors. Theoretically, it mobilises state-capacity and industrial-policy frameworks to situate MIC-2025 within a phased national strategy (to 2049), and analytically unpacks the program's ten strategic sectors. Methodologically, it triangulates primary policy documents with international scholarship to map targets (e.g., 70% self-sufficiency in core components), instruments (SOEs, subsidies, talent programs), and vulnerabilities. The distinctive contribution to strategic studies lies in specifying the transfer channels by which civilian innovation (AI, semiconductors, advanced manufacturing, space, energy systems, new materials, biotech) is routinised into PLA modernisation via institutionalised Military-Civil Fusion—recasting deterrence, supply-chain security, and export-control debates in dual-use terms.

Computer crime in the information society

Julia Czajka's study provides a conceptually careful and policy-focused overview of computer crime as a constitutive threat to an information society premised on ubiquitous connectivity and data flows. The piece clarifies definitional boundaries (INTERPOL, criminological literature), classifies offence categories (hacking, sniffing, sabotage, espionage, malware/cracking, phishing), and links them to critical-infrastructure risks. Methodologically, it employs content analysis to synthesise legal-doctrinal sources and applied guidance (e.g., police practice notes), thereby translating abstract categories into operational prevention and response typologies. The contribution is twofold: normatively, it centres on societal resilience and rights protection; analytically, it reframes "cyber" as a systemic risk whose mitigation requires both criminal law enforcement and organisational hygiene across public and private sectors.

Poland's air and missile defence in transformation

Lieutenant General (ret.) Lech Majewski examines the Polish Air Defence System (PL ADS) as an ecosystemic, layered, network-centric architecture

designed for interoperability with NATO's Integrated Air and Missile Defence. The article blends organisational analysis (governance split between operational and general commands) with capability mapping across tiers (Wisła/Patriot; Narew/CAMM-ER; Pilica/Pilica+; MANPADS; Poprad; counter-UAS; radiotechnical forces and next-gen radars), and integrates recent milestones (e.g., IOC achievements, live-fire events in 2024–2025; IBCS integration; financing instruments; European missile-shield initiatives). Methodologically, it offers a template for capability assessment that ties sensors, effectors, C2, and financing to strategic effects. It concludes with sequencing choices for closing priority gaps-precisely the sort of actionable analysis strategic-studies journals should foreground.

Captagon, conflict economies, and the Sudan–Libya border triangle

My contribution examines Captagon as a structuring node in the Sudan–Libya–Sahel conflict economy, linking clandestine manufacture and supply chains to revenue generation for armed groups, institutional erosion, and cross-border governance gaps. Theoretically, the piece engages with literature on illicit markets and hybrid warfare, examining the causal impact of narcotics economies on structural governance failure. Methodologically, it advances a case-study design that is attentive to production/trafficking mechanisms (precursor access, clandestine lab geographies, and route diversification) and to multi-scalar effects - financing of armed actors, social harms through addiction, and feedback loops of institutional erosion. The article's central payoff is to embed narcotics-driven insecurity within regional conflict systems, thereby warning against security-only responses and highlighting the co-necessity of public health, development, and conflict resolution instruments.

Strengthening the EU's CSDP and transatlantic frictions

Marek Rohr-Garztecki interrogates whether efforts to reinforce the EU's Common Security and Defence Policy (CSDP) risk generating new fault lines in transatlantic relations—especially amid Europe's post-2022 rearmament, persistent procurement fragmentation, and Washington's shifting tolerance for allied "burden-sharing." Conceptually, the article situates CSDP dynamics within alliance-management logics and the political economy of defence supply chains; empirically, it traces the interplay between U.S. leverage (market dominance, basing, and export timelines) and Europe's search for greater industrial autonomy (SAFE/EDIRPA/EDIP). The core finding is

deliberately non-alarmist: in the short-to-medium term, CSDP strengthening does not yet threaten U.S. defence primacy and thus is unlikely, by itself, to trigger major transatlantic rupture – provided Europe avoids exclusionary clauses, vanity duplications of superior U.S. systems, and rhetorical escalation, while expanding pragmatic co-production and standardisation. For Poland, the piece recommends criteria-led participation in European programmes, priority partnerships (notably with Nordics), and tighter congressional-level engagement in Washington – an agenda that aligns industrial policy with alliance cohesion.

Taken together, these contributions operationalise several core ideas in contemporary strategic thought: that the indirectness of contemporary statecraft - manifested in proxy agency, disinformation, and criminalised markets – extends action into the grey zone and therefore demands theories attentive to delegation, deniability, and diffusion, alongside methods capable of working with partial observability while maintaining legal-doctrinal precision; that technological duality has fused industrial policy and innovation systems with defence planning, as dual-use diffusion compresses policy cycles and elevates the importance of anticipatory governance, export controls, and alliance-level standardisation; that systems thinking in defence is indispensable, because air and missile defence effectiveness derives less from platform inventories than from the integration of networks, sensors, command-and-control, financing, and legal interoperability – an insight readily generalisable to cyber governance and AI oversight; and that political economies of insecurity – from narcotics and extractives to smuggling – constitute systems of violence and de facto governance, requiring multi-sectoral counter-measures that judiciously combine coercive tools with public-health, development, and institutional-reform logics.

The objective of this issue is not simply to describe emerging risks but to translate theoretical clarity and methodological discipline into decision-grade insight. Scholars will find conceptual refinements (e.g., proxy agent networks, dual-use transfer channels). At the same time, practitioners and policymakers gain structured diagnostics and sequenced recommendations (e.g., counterintelligence posture, media-ecosystem hardening, capability integration). The editors have selected texts that are (I) empirically anchored, (II) explicit about methods and sources, and (III) oriented toward

implementable policy pathways. That is the standard we regard as necessary for strategic thought in an era of compressed time, contested cognition, and accelerated technology.

I extend my sincere thanks to the contributing authors – Dr Anna Grabowska-Siwiec, Dr Blanka Katarzyna Dżugaj, Dominika Sikorska, Julia Czajka, Lt. Gen. (ret.) Lech Majewski, and Marek Rohr-Garztecki – for their intellectual rigor, methodological transparency, and exemplary responsiveness to peer review and editorial guidance. Their willingness to refine arguments, deepen empirical substantiation, and align formats under compressed timelines made this issue possible. I am equally grateful to our anonymous reviewers for their incisive, field-shaping critiques; to the editorial board and copy-editing team for steady, meticulous support; and to colleagues and practitioners who shared data, documents, and case insights that strengthened several articles.

Magdalena El Ghamari, PhD – Issue Editor

Anna Grabowska-Siwiec
University of Bialystok
ORCID: 0000-0003-0788-4171
a.grabowska-siwiec@uwb.edu.pl

Threats to Poland and NATO member states posed by proxy agent networks

Abstract

The article examines the phenomenon of proxy agent networks as an instrument of contemporary intelligence activity, focusing on operational modalities and the associated threats to the security of Poland and NATO member states. The aim is to provide an in-depth analysis of proxy agent networks, with a particular focus on the practices employed by the Russian Federation. The text identifies the consequences of using proxy agents in the context of hybrid and information warfare. It explains why this form of agent network constitutes an effective tool for achieving intelligence objectives, enabling the aggressor to conduct destabilising operations. It also sets out recommendations for state services on how to build societal resilience to this category of intelligence threat.

Key words

agents, proxy, intelligence, counterintelligence, subversion

Introduction

In this article, I employ the term "proxy agent networks" to denote the indirect conduct of intelligence operations, whereby a state sponsor tasks non-state actors or third parties to achieve informational and active effects while maintaining distance and plausible deniability. At first mention, it is useful to note near-synonyms that may appear in the literature – "such as proxy agency, operations using intermediaries (proxy)", or "indirect/outsourced intelligence operations" – but for the sake of terminological consistency, I use only proxy

agent networks throughout. For clarity, I also distinguish this concept from agents of influence, which are primarily oriented towards shaping perceptions, narratives, and decision-making within media, culture, academia, or politics; they may feature within long-term classical intelligence architectures without necessarily operating in a proxy mode. By contrast, proxy agent networks describe a mode of execution (intermediation/outsourcing of risk and cost) that can encompass both influence work and task-oriented operations (reconnaissance, arson, sabotage, etc.).

The word "proxy" derives from English and denotes an agent or a power of attorney. When coupled with the term from the lexicon of security and intelligence services – *agent*, understood (following NATO usage)[1] as a person recruited, trained, directed, and employed to collect and transmit information – the combined notion of the proxy agent emerges[2]. In practice, proxy agent networks enable state services to act by proxy or instead of traditional agent handling (identifying, developing, recruiting, training, and maintaining liaison with assets over a sustained period). The constitutive features of proxy agent networks, to which this article will repeatedly refer, include: (1) indirectness of action, (2) plausible deniability for the sponsor, (3) variegated actors (individuals, loose groups, criminal intermediaries), (4) operational flexibility and scalability across jurisdictions, and (5) transnational reach often facilitated by digital communications.

The etymology of "proxy agent" is commonly linked to the concept of proxy warfare, which has deep historical roots. In the scholarly literature, a proxy war is defined as "an armed conflict in which a third party intervenes indirectly in order to influence the strategic outcome in favour of its preferred faction"[3]. A more specific military definition describes it as "a conflict in which the belligerents employ third parties as an additional means of waging war or as a substitute for the direct use of their own armies"[4]. The concept assumed

1 *Słownik terminów i definicji NATO*, https://wcnjik.wp.mil.pl/u/AAP6PL.pdf [access: 5.08.2025].

2 J.K. Wither, *Outsourcing warfare: Proxy forces in contemporary armed conflicts*, „Security and Defence Quarterly" 2020, vol. 31, no. 4, p. 17.

3 Ibidem.

4 C. A. Kozera et. al., *Game of Proxies – Towards a new model of warfare: Experiences from the CAR, Libya, Mali, Syria, and Ukraine*, „Security and Defence Quarterly" 2020, vol. 31, no. 4, p. 77–97.

particular significance during the Cold War, when the United States and the Soviet Union sought to conduct their rivalry without risking direct military confrontation or nuclear escalation. The USSR supported anti-colonial and revolutionary movements opposed to the West, while the USA backed anti-communist leaders and counter-revolutionaries.

The use of proxy agent networks has also been incorporated into the activities of security and intelligence services, particularly foreign intelligence. The term "security service" has not yet been defined in normative terms in Poland; however, in academic discourse, it is commonly understood to refer to services responsible for performing intelligence and counterintelligence tasks. The principal instruments of their activity are operational and reconnaissance measures designed to gather information. Historically, the data collected have served military ends; over time, active measures were added to informational tasks. These include, inter alia, shaping situations advantageous to the state (deception/disinformation), acquiring agents of influence, compromising opponents and targeted killings, as well as sabotage and subversion, and the orchestration of acts with a terrorist character.

Terminological and legal precision. In what follows, I treat "subversion/dywersja", "sabotage", and "terrorism" as legal categories, not colloquial labels. Their use is anchored in the Polish Criminal Code (e.g., the post-2023 wording of Art. 130 on espionage and forms of activity on behalf of a foreign intelligence service; the legal definition of a terrorist offence in Art. 115 §20) and in Directive (EU) 2017/541 on combating terrorism. Accordingly, I employ these terms only where they reflect official qualification by competent authorities, or—where such qualification is pending – use cautious formulations such as "actions of a subversive/sabotage character", explicitly attributing claims to ABW/Prokuratura Krajowa communiqués. This distinction also underlines that not every arson constitutes terrorism, and that legal assessment depends on statutory elements (intent to intimidate a population, coerce public authorities, scale of endangerment, etc.).

Each successive conflict has compelled the security services to expand their areas of operation. The apogee of remit expansion is typically dated to the Cold War, during which – as Tomasz R. Aleksandrowicz observes – "it is difficult to identify any area that would remain outside the sphere of interest

of the security services"[5]. Thus, the functions and tasks of the services are conditioned by the security environment and by the state's interpretation and perception of threats; changes in that environment drive changes in scope and methods. Analysing the tasks and objectives assigned to proxy agent networks allows us to identify them as a contemporary tool (notably in recruitment and digital tasking) employed by the Russian intelligence services. In Poland, the application of proxy agent networks is directly linked to the outbreak of war in Ukraine in February 2022 and to Poland's robust provision of military and international support to the Ukrainian authorities. Actors recruited into such networks pursue strategic aims aligned with those of the Russian state, including, among other objectives, the erosion of support for Ukraine and the reassertion of Russian influence.

Aleksandrowicz also draws attention to the problem of defining the adversary with whom the security services contend. Current hybrid-warfare practices suggest that state intelligence services are appropriating behaviors characteristic of non-state organisations – or masquerading as them – precisely to obscure the identity of the principal. This pattern satisfies the logic of proxy action and further justifies the analytical separation between agents of influence and proxy agent networks as distinct, though sometimes overlapping, categories.

The purpose of this article is to identify and conceptualise proxy agent networks as a contemporary instrument of Russian security and intelligence services, to describe their methods of operation (including digital recruitment, tasking and remuneration), to delineate their targets and effects in Poland and across NATO member states, and to propose avenues for counter-action – from legal-doctrinal clarity and strategic communications to operational counter-intelligence and international cooperation.

5 T.R. Aleksandrowicz, *Służby specjalne w strategicznym zapewnieniu bezpieczeństwa państwa*, [in:] *Strategia bezpieczeństwa narodowego Polski*, ed. J. Gryz, Warszawa 2013, p. 257.

Proxy agent networks in Poland

In 2024, the Internal Security Agency (Agencja Bezpieczeństwa Wewnętrznego – ABW) published a communiqué characterising subversive (dywersyjne) activities directed against the Republic of Poland[6], as well as against member states of the European Union and NATO, which were initiated and coordinated by Russian special services. It is worth noting here why ABW is the body addressing this category of criminal activity. This follows from the Agency's statutory powers to identify, prevent and combat threats to the state's internal security and constitutional order in the civilian sphere, as well as to identify, prevent and detect the offence of espionage[7]. Espionage is defined in Art. 130 of the Polish Criminal Code[8]. It involves participating in the activities of a foreign intelligence service or acting on its behalf against the Republic of Poland or its partner countries. The 2023 amendment to Art. 130 also enumerates, as categories of activity on behalf of a foreign intelligence service, such conduct as subversion (dywersja), sabotage or offences of a terrorist character (§ 7)[9]. In the military domain, responsibility for prosecuting this kind of activity on behalf of a foreign intelligence service lies with the Military Counterintelligence Service (Służba Kontrwywiadu Wojskowego – SKW).

In the public domain, only ABW[10], together with the National Public Prosecutor's Office (Prokuratura Krajowa), disseminates information relating to the above-mentioned activities. This is linked to the Agency's competence in both identifying and countering this type of threat. One of the first public

6 *Komunikat dotyczący działalności dywersyjnej FR z dn. 25.10.2024 r.*, https://www.abw.gov.pl/pl/informacje/2569,Komunikat-dotyczacy-dzialalnosci-dywersyjnej--FR.html [access: 18.08.2025].

7 Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, t.j., Dz.U. 2025, poz. 902, art. 5.

8 Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, t.j., ibidem, poz. 383, art. 130.

9 S. Hoc, *Szpiegostwo w znowelizowanym Kodeksie karnym*, „Nowa Kodyfikacja Prawa Karnego" 2023, no. 67, p. 119–143; P. Burczaniuk, *Przestępstwo szpiegostwa po nowemu, czyli w świetle nowelizacji Kodeksu karnego z 17 sierpnia 2023 roku*, „Przegląd Bezpieczeństwa Wewnętrznego" 2024, no. 30, p. 49–78.

10 It should be noted that the oldest communication published on the abw.gov.pl website currently dates back to 12.10.2023. It is not possible to read the communications from previous years relating to the activity of this service in the context of sabotage activities carried out for the benefit of foreign intelligence.

statements (since the outbreak of the regular armed conflict in Ukraine in 2022) concerning subversive operations conducted for a foreign intelligence service was the communiqué of 16 March 2023 regarding the actions of 12 persons suspected of cooperating with the Russian special services (it later transpired that the group numbered 16)[11]. The communiqué stated that "the group carried out monitoring of railway routes. Its tasks included, inter alia, identifying, monitoring and documenting consignments of armaments destined for Ukraine. The suspects were also preparing diversionary actions aimed at paralysing deliveries of equipment, weapons and aid for Ukraine"[12]. ABW further indicated that the group had also been tasked with propaganda activities designed to destabilise Polish-Ukrainian relations, to inflame and amplify in Poland sentiments hostile to NATO member states, and to attack the policy of the Government of the Republic of Poland towards Ukraine.

The only available report (more precisely, an infographic) presenting the scope of ABW's activities for the period 2015–2019[13], in identifying intelligence threats to the Republic of Poland, links them to "so-called hybrid warfare". The report underscores that "at present [2019] the boundary is becoming blurred between externally generated intelligence threats and hostile actions carried out within the state". It defines the most serious challenges in the security sphere as those that are associated with the aggressive policy of the Russian Federation. In the last four years [2015–2019], five diplomats of the Russian Federation were expelled from Poland, including four in response to the attempt to poison Sergei Skripal. Five individuals were also detained on espionage charges – three for Russia and two for China." At no point does this report refer to intelligence threats to Poland in the form of subversive or sabotage operations. It follows clearly that the first subversive activities, conducted on behalf of the Russian special services, to be detected and defined by ABW and disclosed publicly were those of the "16-person spy network" in 2023.

The last publicly known information about the activity of spy networks in Poland after the Second World War dates from the 1940s and 1950s. This

11 *ABW rozbiła siatkę szpiegowską*, https://www.gov.pl/web/sluzby-specjalne/abw-rozbila-siatke-szpiegowska [access: 19.08.2025].

12 Ibidem.

13 *Podsumowanie działań ABW*, https://www.gov.pl/web/sluzby-specjalne/podsumowanie-dzialan-abw [access: 19.08.2025].

concerned the network of André Robineau (an official of the French Consulate in Szczecin), who was detained in 1949 and convicted in 1950, together with six other individuals, for activities on behalf of French intelligence. Robineu was pardoned in 1953. Since the entry into force of Art. 130 of the Criminal Code in 1997, there have been no recorded cases of the disclosure of spy networks in Poland[14]. One cannot, however, exclude the existence of a dark figure[15]. The first spy network uncovered in the Third Republic numbered 16 persons, of whom 13, as announced by the National Public Prosecutor's Office in December 2023, were convicted by the Regional Court in Lublin and received aggregate custodial sentences ranging from 1 year and 1 month to 6 years' imprisonment, together with fines. The prosecutor charged the defendants with participation in an organised criminal group under Art. 258 §1 of the Criminal Code and acting for the benefit of a foreign intelligence service against the interests of the Republic of Poland under Art. 130 § 1. The investigation established that the group operated from January 2023 to March 2023 in various locations, including Biała Podlaska, Chełm, Medyka, Przemyśl, Rzeszów, Warsaw, and other localities across the country. The defendants undertook activities, including reconnaissance of critical infrastructure, such as military facilities and seaports. They continuously informed their principals of the results of their intelligence-gathering efforts, for which they received remuneration. The bill of indictment covered a total of 16 individuals belonging to a spy network that was cooperating with Russian special services. The accused were identified as foreign nationals from beyond Poland's eastern border (13 Ukrainian citizens, 2 Belarusian citizens and one Russian – an ice-hockey player). They conducted intelligence as well as propaganda activities against Poland and prepared acts of subversion on the instructions of Russian intelligence. The remaining three individuals were tried in separate proceedings[16].

14 S. Hoc, *Siatki szpiegowskie w kontekście art. 130 kk*, [in:] *Prawo karne na przełomie wieków. Księga jubileuszowa profesora Ryszarda A. Stefańskiego*, eds. M. Rogalski, J. Kosonoga, J.A. Dąbrowski, Warszawa 2025, p. 269.

15 A dark figure is a criminological concept that refers to the number of crimes actually committed that are not included in official crime statistics due to their failure to be disclosed by law enforcement agencies or reported by victims.

16 S. Hoc, *Siatki szpiegowskie*…, p. 283.

In subsequent years, the National Public Prosecutor's Office, in cooperation with the Internal Security Agency and in collaboration with partner countries, identified further subversive operations carried out at the instruction of Russian special services. These include, inter alia:

1. Arson attacks in May 2024 on two construction depots in the Masovian Voivodeship. The operations were commissioned, supervised and financed by an individual linked to the Russian special services – a Colombian national. The suspect received detailed instructions regarding targets and modes of execution via the Telegram messenger. He has already been convicted by a Czech court and sentenced to eight years' imprisonment for the arson of a bus depot in Prague. A Joint Investigation Team was established in the case with the participation of Poland, the Czech Republic, Romania and Lithuania[17];

2. In July 2024, Kristina S. (a Ukrainian national) took part in sending a courier parcel containing explosive materials: nitroglycerin, military electric detonators, an initiation device, a metal vacuum flask with a shaped-charge insert, and powdered aluminium. The device constituted a so-called shaped-charge bomb. The consignment was detected and secured in the warehouses of a courier company in the Łódź Voivodeship. She acted in concert with a Ukrainian national and two Russian citizens. ABW charged the Ukrainian woman with the offence of complicity in bringing about a direct danger of an explosion of explosive materials (sabotage activity)[18];

3. On 6 August 2025, an indictment was filed against three Belarusian nationals and three Polish nationals engaged in organising and carrying out acts of subversion on the territory of Poland. They were accused of setting fire to a building materials warehouse in Gdańsk and attempting to set fire to a company in Marki, near Warsaw. In addition, the group was involved in the illicit trade in weapons, ammunition, explosives and narcotic drugs.

17 *Działał na rzecz obcego wywiadu przeciwko RP. 21 lipca br. Kolumbijczyk usłyszał zarzuty*, https://www.abw.gov.pl/pl/informacje/2662,Dzialal-na-rzecz-obcego-wywiadu-przeciwko -RP-21-lipca-br-Kolumbijczyk-uslyszal-z.html [access: 21.08.2025].

18 *Akt oskarżenia w sprawie planowania działań sabotażowych*, https://www.abw.gov.pl/pl/informacje/2665,Akt-oskarzenia-w-sprawie-planowania-dzialan-sabotazowych.html [access: 21.08.2025].

The investigation revealed the mechanisms by which subversive actions were commissioned and executed on the instructions of foreign services, as well as the routes used to smuggle illicit materials from Ukraine into EU member states[19];

4. On 12 May 2025, the National Public Prosecutor's Office announced that the fire at the shopping centre on ul. Marywilska 44 in Warsaw on 12 May 2024 had been the result of arson commissioned by the intelligence service of the Russian Federation. The evidentiary material gathered in the case allowed charges to be brought against two Ukrainian citizens who acted in concert with the perpetrators of the arson. The group's objective was to carry out arson attacks on large-format facilities within EU member states. This group is also responsible, inter alia, for the arson of an IKEA store on 9 May 2024 in Vilnius[20].

Communiqués issued by ABW and the National Public Prosecutor's Office reveal the systematic activity of foreign special services – primarily Russian and Belarusian – using proxy agents against Poland and its allies. The activities include:

– Arson attacks on civilian and industrial facilities;

– Dispatch of consignments containing explosive materials transported by courier companies;

– Propaganda operations aimed at polarising society;

– Classical espionage against defence-significant facilities (so-called external reconnaissance, conducted chiefly on behalf of the Belarusian special services);

– Operations targeting Russian and Belarusian opposition figures.

The majority of perpetrators – particularly of subversive acts – are young people originating from Belarus and Ukraine; they are most commonly financially motivated and recruited via internet messengers (Telegram).

19 *Akt oskarżenia w sprawie działań dywersyjnych na rzecz obcego wywiadu*, https://www.abw.gov.pl/pl/informacje/2666,Akt-oskarzenia-w-sprawie-dzialan-dywersyjnych-na-rzecz-obcego-wywiadu.html [access: 21.08.2025].

20 *Zarzuty w związku z pożarem hali przy ul. Marywilskiej 44*, https://www.gov.pl/web/prokuratura-krajowa/zarzuty-m44 [access: 21.08.2025].

Proxy agent networks targeting NATO member states

Subversive operations conducted by proxy agents on the instructions of Russian intelligence are taking place not only on the territory of Poland but are also directed against other NATO member states. In April 2024, two individuals (German citizens of Russian origin) were detained in Germany for preparing, at the behest of Russian intelligence, attacks on military installations, arms factories, industrial facilities and transport infrastructure used to supply Ukraine. The planned actions took the form of arson and the detonation of explosive devices, and one of the intended targets comprised installations of the United States Armed Forces in Bavaria, where Ukrainian soldiers[21] are being trained. In Lithuania, Latvia, Estonia and the United Kingdom, saboteurs inspired by Russia have primarily attacked so-called soft civilian targets (e.g., industrial halls, shops, warehouses)[22]. In May 2022, persons preparing an attack on the Lielvārde military air base were detained in Latvia[23].

As indicated above, once selected and tasked, a given individual may carry out similar activities across several countries. Such was the case, inter alia, with the Colombian national who operated in the Czech Republic and Poland, while the perpetrators of the fire at the shopping centre on ul. Marywilska 44 in Warsaw are also responsible for the arson of an IKEA store on 9 May 2024 in Vilnius.

Characteristic features of the intelligence use of proxy networks

When characterising proxy agent networks in the context of special services' activities, attention should be paid to features such as the utilisation of non-state actors or individuals motivated ideologically and/or financially to achieve intelligence objectives without the direct involvement of official intelligence structures. The term "proxy agent network" may also refer to systems and mechanisms whereby intelligence services employ intermediaries to collect

21 F. Bryjka, *Rosyjskie działania dywersyjne wobec państw NATO*, „Biuletyn PISM" 2024, no. 112.
22 Ibidem.
23 Ibidem.

information, conduct operations or perform tasks that, for various reasons, they cannot or do not wish to undertake directly through official structures.

The characteristic features of proxy networks include:

1) Structural features:

a) Indirect mode of operation – the principal (here understood as the commissioning party) acts through intermediaries, allowing it to retain distance from the operations conducted,

b) Diversity of actors – proxy networks may encompass a wide range of non-state entities, individuals or groups who may or may not be in some form of mutual dependency,

c) Operational flexibility – proxies enable action in the "grey zone" between peace and war, exploiting information activities, cyber operations, clandestine actions by the special services or ordinary criminal conduct;

2) Functional features:

a) Plausible deniability – although contemporary proxy operations often do not conceal the sponsor's involvement, they still afford a degree of deniability in the event of failure,

b) Cost-effectiveness – employing proxies is significantly cheaper than directly engaging regular armed forces or official intelligence structures by recruiting so-called classical agents,

c) Risk minimisation – proxies allow the sponsor to avoid the negative political consequences associated with direct involvement;

3. Strategic features:

a) Long-term horizon – the use of proxy networks frequently presupposes long-term strategic relationships. Actions taken today may yield the desired effect for the sponsor in a decade or more'

b) Multidimensionality – contemporary proxy networks encompass not only military aspects but also technical, cyber and informational dimensions (disinformation, propaganda),

c) Adaptability – proxy agents can be rapidly adjusted to the sponsor's changing operational and strategic requirements.

Attention should also be drawn to the targets of proxy attacks in Poland, which have primarily been civilian facilities, including warehouses and large retail outlets, with arson as the principal method employed. Hostile activity is increasingly taking on the characteristics of terrorist conduct.

Conclusion and Recommendations

As is unambiguously evident from official ABW and National Public Prosecutor's Office communiqués, an intensification of subversive activity carried out by proxy networks in Poland has been observed since 2023. The ABW communiqué of 25 October 2024 is the first to provide a synthetic summary of such operations on behalf of a foreign intelligence service and marks a watershed in ABW's official public communications. For the first time, it directly employed the term "subversive activities" in the context of Russian special services, thereby introducing a new category of threats into the public discourse on the state's internal security. The communiqué presents a comprehensive analysis of Russian subversive operations, highlighting their systematic and coordinated nature. It discloses details of operational methodology, including the use of internet messengers for recruitment and handling, payments to contractors in cryptocurrencies, and the recruitment of individuals from countries such as Ukraine and Belarus[24].

The strategic objectives of Russian subversive activity were also identified: to intimidate citizens of Poland and of Western states and to discourage support for Ukraine and its people. An important aspect is the drive to foment chaos, a sense of insecurity, distrust of state authorities, social unrest and internal destabilisation. The long-term consequences of such actions may also include a crisis of democratic values, deep societal polarisation, and the entrenchment of anti-immigrant and extreme nationalist attitudes.

It is noteworthy that neither ABW nor the National Public Prosecutor's Office uses the term "proxy network" in their communiqués. This may be linked to an avoidance of terminology reserved for operational practice and associated with classified operational guidelines. In many countries, the terms "agent" and "agent network" are professional designations drawn from the operational vocabulary of the special services.

The publication of the communiqué also signifies ABW's formal recognition of a new dimension of Russian hybrid activities directed against

24 The use of the term "coming from former USSR countries" by the Internal Security Agency is noteworthy, which, in the author's opinion, is a measure aimed at not directly pointing to Ukrainian citizens so as not to incite social antagonisms between Ukrainians and Poles.

Poland – subversive and sabotage operations with a terrorist character. In the Author's assessment, these do not replace traditional intelligence operations, such as the cultivation of durable agents of influence, work under non-official cover, diplomatic cover or the exploitation of walk-ins. The aforementioned classical intelligence activities may proceed in parallel with newer tools such as proxy networks. Cyberspace and the widespread use of social media have been integrated into intelligence operations as inexpensive and practical tools, enabling the recruitment and effective deployment of proxy agents in areas such as subversion, sabotage, and terrorist activity.

In building resilience to proxy-network operations, the activity of state institutions – including services responsible for counterintelligence tasks – is of cardinal importance. Beyond the October 2024 communiqué, there is a lack of information materials from ABW promoted through widely accessible channels commonly used by the public, such as social media (e.g., TikTok and Instagram) and podcasts. It is worth noting the niche character of sources such as the abw.gov.pl website. Research conducted by the Author on a defined cohort of students showed that potential audiences seeking knowledge about Polish special services via their websites amounted to between 30% and 50% (depending on gender and year of study)[25]. Notably, these were individuals who already possessed preliminary knowledge of Poland's special services and were self-motivated to expand it.

To date, Poland has not seen a public-awareness campaign informing citizens about the threats posed by proxy networks and the desired patterns of behaviour. Citizens do not know how to react when they observe individuals behaving suspiciously – for example, installing cameras along railway routes. The fact that ABW, which most frequently issues statements on this subject, does not employ the term "proxy network" has a desensitising effect: the phenomenon lacks rigorous, clear and socially recognisable definitional framing.

The detection, prosecution and prevention of proxy-network activity conducted on behalf of foreign intelligence services also requires appropriate tools and personnel resources on the part of ABW and SKW. Staffing continuity

25 A. Grabowska-Siwiec, *Służby specjalne – czy są atrakcyjnym miejscem pracy dla młodych Polaków?*, „Special OPS" 2023, no. 2, p. 28–33.

in Poland's special services, including counterintelligence, is subject to cyclical disruption associated with the electoral cycle. This does not favour effective action against foreign intelligence services operating in the country, whose activities are inherently long-term – an aspect often poorly understood by both political decision-makers and the general public. As Stanisław Hoc argues, it is essential to enhance counterintelligence effectiveness in combating espionage by ensuring a proper standard of operational work, utilising both technical and human assets, and fostering close cooperation between the operational and investigative branches, among other measures[26].

The prosecution of proxy networks – which also exhibit transnational characteristics – requires cooperation between Polish special services, the Police, and the prosecutor's office, as well as their counterparts in NATO and EU member states. ABW declares intensive international cooperation, including with the authorities of Lithuania, Germany and the United Kingdom. The exchange of experience and knowledge regarding the adversary's modus operandi is crucial to preventing and combating proxy-network activity.

Bibliography

Aleksandrowicz T.R., *Służby specjalne w strategicznym zapewnieniu bezpieczeństwa państwa*, [in:] *Strategia bezpieczeństwa narodowego Polski*, ed. J. Gryz, Warszawa 2013.

Bryjka F., *Rosyjskie działania dywersyjne wobec państw NATO*, „Biuletyn PISM" 2024, no. 112.

Burczaniuk P., *Przestępstwo szpiegostwa po nowemu, czyli w świetle nowelizacji Kodeksu karnego z 17 sierpnia 2023 roku*, „Przegląd Bezpieczeństwa Wewnętrznego" 2024, no. 30.

Grabowska-Siwiec A., *Służby specjalne – czy są atrakcyjnym miejscem pracy dla młodych Polaków?*, „Special OPS" 2023, no. 2.

Hoc S., *Siatki szpiegowskie w kontekście art. 130 kk*, [in:] *Prawo karne na przełomie wieków. Księga jubileuszowa profesora Ryszarda A. Stefańskiego*, eds. M. Rogalski, J. Kosonoga, J.A. Dąbrowski, Warszawa 2025.

Hoc S., *Szpiegostwo w znowelizowanym Kodeksie karnym*, „Nowa Kodyfikacja Prawa Karnego" 2023, no. 67.

26 S. Hoc, *Szpiegostwo w znowelizowanym…*, p. 120.

Kozera C.A. et al., *Game of Proxies – Towards a new model of warfare: Experiences from the CAR, Libya, Mali, Syria, and Ukraine*, „Security and Defence Quarterly" 2020, vol. 31, no. 4.

Wither J.K., *Outsourcing warfare: Proxy forces in contemporary armed conflicts*, „Security and Defence Quarterly" 2020, vol. 31, no. 4.

Blanka Katarzyna Dżugaj
Institute for Turkey Studies
ORCID: 0000-0002-3794-9194
blanka.k.dzugaj@gmail.com

Characteristics of Russian Disinformation in Lebanon: Causes, Strategies, Consequences[1]

Abstract

This study examines the phenomenon of Russian disinformation in the Lebanese media landscape, focusing on its underlying causes, strategic mechanisms, and broader consequences. The analysis identifies a range of political, economic, and socio-cultural factors that create fertile ground for disinformation in Lebanon, including the country's complex sectarian dynamics, weak media regulation, and external influence from global powers. This study outlines the main strategies employed by pro-Russian media outlets in Lebanon, such as the selective framing of international events, amplification of anti-Western narratives, and the use of local proxies to increase credibility. Particular attention is paid to how these strategies aim to shape public opinion, foster distrust of Western institutions, and position Russia as a reliable geopolitical partner in the region. The article concludes by assessing the impact of such disinformation on Russia's image in the Middle East, arguing that while it contributes to short-term soft power gains, it also risks long-term reputational damage due to the growing awareness of manipulative tactics among regional audiences.

Key words

Lebanon, Russia, disinformation, Ukraine, war

1 The article is based on the report "Russian Disinformation in Lebanon", created as part of a public task funded by the Ministry of Foreign Affairs of the Republic of Poland in the „Public Diplomacy 2024–2025 – European Dimension and Counteracting Disinformation" competition.

Introduction

The reasons behind Russia's interest in Lebanon is geopolitical and ideological. Situated at the crossroads of the Middle East, Lebanon offers strategic value regarding access, alliances, and influence. Russia's presence in Lebanon is part of Moscow's broader strategy in the Middle East. Lebanon itself is of strategic and political importance to Russia, primarily due to its geographical location, which is a potential bridgehead of influence in the Mediterranean, in the immediate vicinity of NATO's southern flank, and at the same time a country that allows it to maintain channels of influence on Syrian affairs, which are very important for Russia even after the fall of Bashar al-Assad's regime. Good relations with Hezbollah, on the other hand, constitute a bargaining chip in dialogue with Israel. Hence, attempts to maintain influence in Lebanon, a country marked by political fragmentation, sectarian divides, and a complex media landscape, have emerged as fertile ground for Russian disinformation efforts. This study explores the characteristics of Russian disinformation in Lebanon, focusing on its underlying causes, strategic objectives, and tangible consequences. This study identifies the primary methods employed by Russian-linked media and proxies, including the use of local platforms, Arabic-language content, and exploitation of societal cleavages. The methodology implemented in this study relies on combining discourse analysis, media monitoring, and desk research to examine the characteristics, motivations, and effects of Russian disinformation activities in Lebanon. This research focuses on the period from 2022 to 2025, the period of full-scale Russian aggression against Ukraine, to show how Russian disinformation exploits this conflict to weaken Western influence in Lebanon.

The concept of disinformation has not been clearly defined in the scientific literature, but it is assumed to be an intentional misleading of recipients, often in political, religious, and ideological contexts[2]. An important element of the definition of disinformation is intention: disinformation is a deliberate action that is intended to result in the author achieving their own benefits (political, social, financial, etc.). In scientific discourse, there is also the concept of

2 K. Kaczmarek, *Konsekwencje dezinformacji: przegląd wybranych narzędzi i technik manipulacji*, „Bezpieczeństwa Narodowe" 2024, no. 45, p. 12.

misinformation, which is false information that can be disseminated by people who have been misled themselves[3]. For disinformation to find fertile ground, there must be several or even a dozen factors. In the case of the state, these are among others:

1. Difficult political and/or economic situation: deep social divisions, internal conflicts on ethnic, religious, or political grounds, and weakness of the authorities;
2. High levels of anxiety and uncertainty, for example, as a result of economic crises, wars, or instability of state power;
3. Weak institutions, and high levels of corruption;
4. Poverty and social inequality;
5. Low level of media education, and lack of critical thinking skills;
6. Underdeveloped, polarized, or corrupt media;
7. Lack of strong international alliances[4].

Most of these factors are present in Lebanon, and Russian disinformation exploits the weaknesses of the system. Lebanon has been experiencing one of the most devastating financial crises in modern history since 2019, which has seen the country become insolvent. The economy has shrunk by approximately 34 percent since 2019, and GDP has fallen by 70–75% compared to pre-crisis levels[5]. The Lebanese pound has lost 90 percent of its value since October 2019, inflation has risen to 890 percent, and food prices have risen by more than 1000 percent[6]. According to the United Nations, almost 80 percent of Lebanon's population lives below the poverty line, and more than half, that is, more than three million people, are in need of humanitarian aid. The

3 *Dezinformacja – czym jest i jak ją zweryfikować*, https://cyberprofilaktyka.pl/blog/dezinformacja---czym-jest-i-jak-ja-zweryfikowac_i23.html [access: 27.09.2025].

4 *Harvard Kennedy School – raport: Who is afraid of fake news?*, „Harvard Kennedy School Misinformation Review" 2022, vol. 3, no. 3.

5 *Lebanon's Economic Contraction Deepens, Highlighting Critical Need for Reforms and Key Investments*, https://www.worldbank.org/en/news/press-release/2024/12/10/lebanon-s-economic-contraction-deepens-highlighting-critical-need-for-reforms-and-key-investments [access: 16.10.2025].

6 *Lebanon Humanitarian Fund Annual Report 2022*, https://www.unocha.org/publications/report/lebanon/lebanon-humanitarian-fund-annual-report-2022 [access: 16.10.2025].

minimum wage, even after the recent increase to 18 million pounds, allows meeting the nutritional needs of a family for a maximum of six months[7].

The causes of the crisis should be found, m.in, in the costs of the 15-year civil war, the taking out of international loans by successive governments, the financial burden associated with accepting more than 1.5 million refugees from Syria, and the explosion in Beirut in 2020, which destroyed a port extremely important for the economy and a silo where the state's grain resources were stored. It is worth noting here that Lebanon imports 80 percent of its food, and the port of Beirut was the main place of receiving it. The rage of the Lebanese was caused by media information blaming corrupt politicians for the Beirut explosion. Another problem in Lebanon is corruption, which concerns not so much individuals but is a way of exercising power. This practice begins at the very top of the power hierarchy: state and government positions are filled according to religious keys, which has led to the emergence of a rigid political system based on the search for compromise between political elites who use patronage networks to pursue their own interests[8]. The political and business elites of each religious group share control over ministries, institutions, and state-owned companies, treating them as their own feudal estates. Politicians fill key positions in the administration and public sector with members of their families, co-religionists, and loyalists. Ministries controlled by politicians (e.g., energy and telecommunications) are a source of huge, unclear contracts for companies associated with them. Public funds are being diverted, and services (such as electricity supplies) remain at a very low level. Simultaneously, the judicial branch was designed to be subordinate to the executive and legislative branches, which weakened judges' ability to hold corrupt officials accountable. Any attempts at reform or external audits, such as the investigation into the Beirut explosion, are effectively blocked to protect the interests behind them.

However, corruption does not only concern the highest level of state administration; it is a common practice to give bribes in healthcare, education, and enterprises (e.g., for promotion or employment). This is largely due to the sense of inefficiency of public institutions, but also to the functioning of the

7 *ESCWA warns: more than half of Lebanon's population trapped in poverty*, https://www.unescwa.org/news/lebanon-population-trapped-poverty [access: 16.10.2025].

8 S. Nowacka, *Perspektywy odbudowy Libanu*, „Biuletyn PISM" 2021, no. 97.

practice of „wasta", which is common in many Arab countries, i.e. the use of personal connections or influential relationships in order to obtain benefits, favors, and even shortcuts to bypass administrative obstacles. Transparency International's 2022 Corruption Perceptions Index ranked Lebanon 150th out of 180 countries, down from 128th place in 2012[9].

Lebanon sought help from global institutions, such as the International Monetary Fund, to overcome the economic crisis. However, the latter made support conditional on putting the political scene in order, which was impossible for a long time – the reforms demanded by the IMF required the formation of a government with full powers, which was impossible due to No head of state. Since the spring of 2022, Lebanon has been in political paralysis: parliamentary elections did not produce a majority coalition with a mandate to govern, and a few months later, President Michel Aoun's term of office ended. His successor was also unable to be chosen due to the impasse between supporters and rivals of the two main Shiite parties, Hezbollah and the Amal Movement. The state was headed by the interim government of Najib Mikati, and over the following months, the National Assembly made 13 unsuccessful attempts to elect the head of state. After the outbreak of the war in Gaza, when Hezbollah became involved in operations supporting Hamas, the process of electing a head of state was completely halted until January 2025. With a majority of 99 out of 128 votes, the deputies elected Joseph Aoun as the commander of the Lebanese Armed Forces. He appointed a prime minister within a few days, a move that was well received internationally.

The country's media landscape, dominated by non-state media, which is a political weapon, is also of considerable importance for the development of Russian disinformation in Lebanon. This is due to the fact that most of the media are owned by religious groups (e.g. the popular Al Manar station is the official TV channel of the pro-Russian Hezbollah) or by individuals or entities associated with particular political parties. Politicians are part of the boards of media institutions, which allows them to influence the content they transmit and public opinion.

9 *Our Work in Lebanon*, https://www.transparency.org/en/countries/lebanon [access: 16.10.2025].

All of this makes Lebanese society extremely susceptible to disinformation, both internal (concerning mainly refugees from Syria) and external, mainly from Moscow. Russian disinformation in Lebanon acts as a tool of influence aimed at controlling the narrative and weakening political opponents. Its aim is to undermine trust in the Western world, especially in the US and its allies, weaken NATO's position as a guarantor of security in the Middle East, and strengthen the belief that Russia is an alternative force that guarantees order and stability. In the context of the war in Ukraine, disinformation is aimed at reinforcing the view that defeating Russia is impossible, while Ukraine is a failed state, historically a part of Russia torn away by hostile Western powers, and that Ukrainians are not a nation. This is expected to lead to a reduction in support for Ukraine in this region.

The main Russian narratives in Lebanon are as follows:

1. Discrediting the US – the United States of America and its European allies are responsible for instability in the Middle East, while Russia is a counterweight to them and seeks to stabilize the situation in the region;
2. Discrediting the West, both politically and morally and ethically. Western civilization is decadent and demoralized, and therefore, it is on the verge of collapse;
3. Arousing resentment towards Ukrainians and discrediting Ukraine by presenting it as part of the morally corrupt West and a country ruled by Nazis;
4. Undermining trust in NATO and portraying the Alliance as an oppressive and hostile organization towards the Middle East;
5. Creating the image of Russia as a country victorious in the Ukraine war;
6. Presenting the world as multipolar in opposition to the Western narrative of a bipolar world, in which not two political-military blocs collide, as during the Cold War, but two opposing moral and ethical systems.

For disinformation to be effective, it must be launched on at least several levels simultaneously[10]. As in Europe, it flows in Lebanon from both traditional and social media.

10 A. Majchrzak, *W krainie kolorowych matrioszek – jak działa rosyjska dezinformacja?*, https://demagog.org.pl/analizy_i_raporty/w-krainie-kolorowych-matrioszek-jak-dziala-rosyjska-dezinformacja/ [access: 27.09.2025].

Traditional media

Television remains the most important source of information for Lebanese. A 2021 survey by Internews showed that about 58% of the 1568 respondents surveyed watch TV for at least an hour a day, and 20% watch more than two hours a day[11]. Since local stations are more popular in Lebanon than pan-Arab media, Moscow primarily cooperates with them, especially with channels that support Hezbollah, such as Al-Manar TV, which has been collecting and publishing narratives that may suit Russia's interests in the region for many years. They concern, m.in, the positioning of Russia – willing to support the Lebanese army – as a counterweight to the US, which imposes sanctions on Hezbollah. As a result, many Lebanese see Russia as an important alternative, ready to support Lebanon unconditionally[12].

The authors of the report „The Russian Propaganda Nesting Doll: How RT is Layered Into the Digital Information Environment" found as many as eight Kremlin narratives on Al-Manar and its website, according to their analysis, that come mainly, if not exclusively, from RT, Sputnik News, and the Russian news agency TASS[13]. From my observations, since Russia's full-scale invasion of Ukraine, there has been a lot of content on this television that duplicates the pro-Kremlin narrative, both from the mouths of guests and journalists of the station: these are mainly statements that Ukraine is a chess pawn in the hands of the Americans, the crisis in Ukraine was caused by the United States, Russia does not attack civilians – its attacks are directed only at military facilities, Meanwhile, the Ukrainian side uses civilians as human shields[14].

Moscow also uses its own Arabic-language media, that is, RT Arabic television (formerly known as Russia Today) and Sputnik Arabic radio station,

11 *The Architecture of Distrust: Understanding Mis & Disinformation in Lebanon*, https://static1.squarespace.com/static/61751a56593c762f6c492e6b/t/680a5738bdab466ffdbd0c2a/1745508154161/The+Architecture+of+Distrust%3A+Understanding+Mis+%26+Disinformation+in+Lebanon.pdf [access: 8.10.2025].

12 A. Segal, *Russia's Information Warfare in the Middle East*, Potsdam 2024, p. 9.

13 B. Schafer et al., *The Russian Propaganda Nesting Doll*, https://securingdemocracy.gmfus.org/wp-content/uploads/2024/05/Laundromat-Paper.pdf?utm_source=chatgpt.com [access: 16.10.2025].

14 *Megaphone*, https://x.com/megaphone_news/status/1501189639750701059?s=46 [access: 28.09.2025].

along with their social media accounts on platform X, where they are very active. As the Middle East Institute has established, RT Arabic and Sputnik Arabic produce much more content on this platform than does BBC Arabic or Al Jazeera. While RT Arabic and Sputnik Arabic have posted an average of 180 and 87 tweets per day since their inception, Al Jazeera maintains an average of 55 tweets and BBC Arabic only 32[15]. The vast majority of these posts contain Kremlin disinformation; on the one hand, they emphasize that Russia is not responsible for the war in Ukraine, and on the other, they undermine the credibility of Western countries, with the US at the forefront. Both RT Arabic and Sputnik Arabic, as well as their social media, refer to Russia's invasion of Ukraine - in the Kremlin's terminology – as a "special military operation" (العملية الخاصة-العسكرية), avoiding using terms such as "war" or "invasion".

Among the most popular tweets from RT Arabic and Sputnik Arabic are those discussing alleged secret biological laboratories run by the US in Ukraine. A tweet published on March 25, 2022, by RT Arabic stated, "Biden's son is involved in funding biological labs in Ukraine that threaten global biosecurity. Russia demands explanations from the United States! #Russia #Ukraine #BiologicalLaboratories"[16].

Importantly, Arabic-language Russian media are also trying to introduce animosity between Ukraine and the Islamic world. In the spring of 2022, RT Arabic showed a popular online video of Ukrainian soldiers eating pork lying on the Koran and then using the pages of Islam's holy book to light a fire[17]. "Attention, fake video! Russia staged a video in which unknown people pretended to be Ukrainian soldiers cutting pork on the Koran and burning its pages. They speak broken Ukrainian and use pocket knives. Russia must be condemned for insulting Islam in order to discredit Ukraine", Oleg Nikolenko, spokesman for the Ukrainian Foreign Ministry, wrote on Twitter at the time.

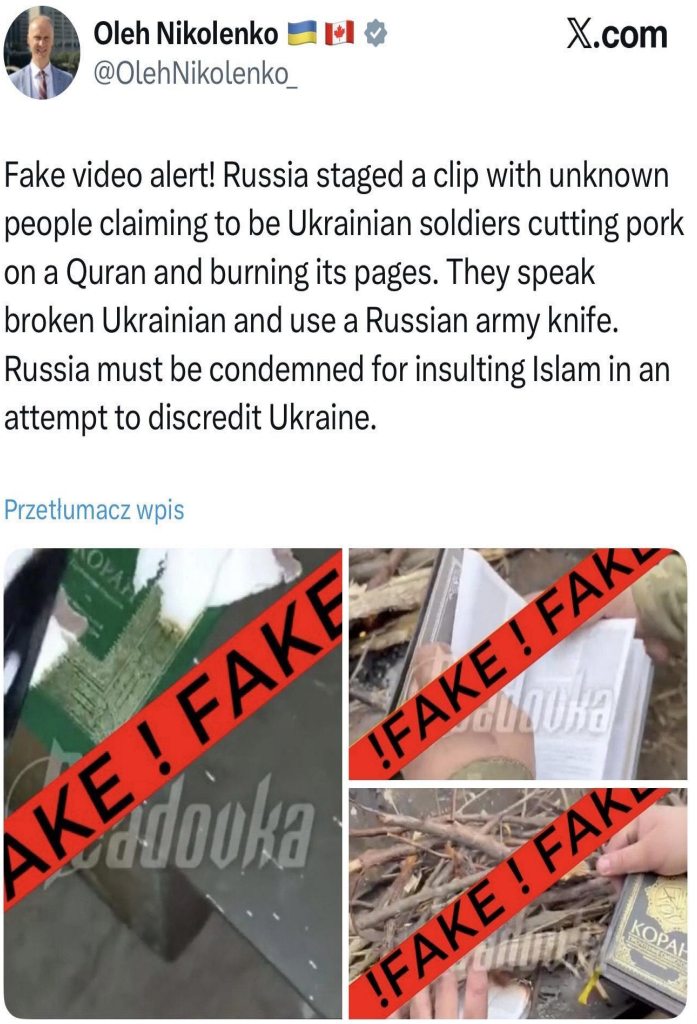
15 E. Janadze, *The digital Middle East: Another front in Russia's information war*, https://www.mei.edu/publications/digital-middle-east-another-front-russias-information-war [access: 28.09.2025].

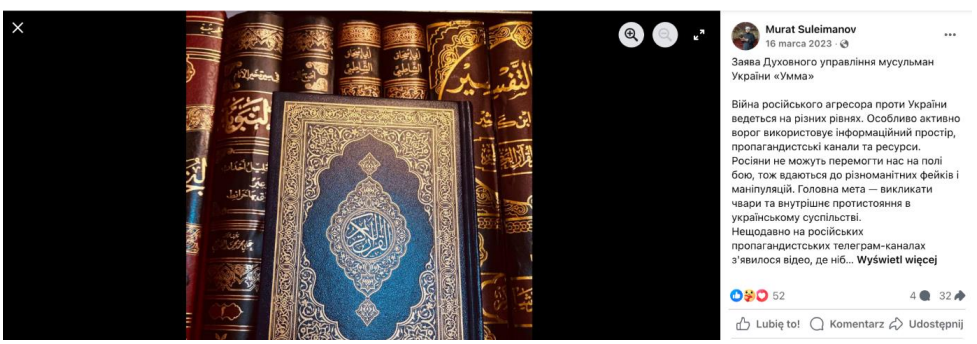
16 *Russian cyber strategy in the Middle East and North Africa (MENA): Analysing the Kremlin's disinformation efforts amid 2022 invasion of Ukraine*, https://dspace.cuni.cz/bitstream/handle/20.500.11956/178359/120427340.pdf?sequence=1&isAllowed=y [access: 28.09.2025].

17 M. Styszyński, *Arab context of the Ukraine conflict in Russia Today Arabic and Sputnik*, „Krakowskie Studia Międzynarodowe" 2023, no. 1, p. 124.

The Spiritual Administration of Muslims of Ukraine "Ummah" also referred to the matter, noting that this is another attempt by Moscow to "destabilize the situation on religious and interethnic grounds". In Ukraine, Muslims are an integral part of civil society; they enjoy all rights, can freely confess and preach their religion, and build mosques. In Russia, on the other hand, Muslims are oppressed, used as cannon fodder in an unjust war, and persecuted even for outward manifestations of religious identity, the organization said in a statement on Facebook.

Source: A. Segal, op. cit.





Source: Facebook/Murat Suleimanov [access: 16.10.2025].

A network of Arabic social media channels

The number of social media users in Lebanon has been steadily increasing, increasing by 10 percent between 2022 and 2024[18]. In January 2024, there were 4.52 million social media users in Lebanon, accounting for 85.6 percent of the total population, with Facebook and X being the most popular social media platforms[19]. In the spring of 2022, just after the full-scale Russian invasion of Ukraine, several Arabic-language channels were created on the latter platform, "pretending to be" news media channels, such as Moscow News and Russia News. Their goal is primarily to relieve Russia of responsibility for the war in Ukraine and shift it to third countries – mainly the US – to discredit Ukrainians as morally degenerate and ridicule President Volodymyr Zelensky.

Since April 2024, when Volodymyr Zelensky signed a law lowering the conscription age in Ukraine from 27 to 25, these channels have focused on the issue of military conscription. At the time, the Russian Foreign Ministry stated that Ukraine was "hunting" for men, and this narrative was taken over by Russia News and Moscow News, which portrayed rare cases of abuse of power by Ukrainian mobilization centers as common, using words such as "hunting for men" and "kidnapping". The tweet on the left states: "In the Khmelnytskyi region, a Ukrainian woman broke a window at a recruitment center after her husband was kidnapped, while the tweet on the right says: Zelensky's bandits are showing creativity in kidnapping Ukrainian citizens from their homes".

Both of these channels also try to ridicule and discredit Ukrainians morally, hitting, for example, Ukrainian women. Numerous posts talk about young Ukrainian women who left their fiancés fighting at the front to find a new love abroad. They also accuse the Ukrainian military of terrorist activities, including carrying out the Bucha massacre, although evidence collected by international organizations indicates that these were Russian units belonging to the 35th and 36th Infantry Regiments. General Army of the Eastern Military District, two airborne divisions, and units of the National Guard tortured and

18 *Lebanon media guide*, https://www.bbc.com/news/world-middle-east-14648683 [access: 8.10.2025].

19 S. Kemp, *Digital 2024: Lebanon*, https://datareportal.com/reports/digital-2024-lebanon [access: 8.10.2025].

murdered several hundred inhabitants of the city[20]. According to the pro-Kremlin propaganda present on RT Arabic and Sputnik Arabic, the order for the massacre in Bucha was given by Volodymyr Zelensky, while he himself fled to Polish.

20 M. Piechowska S. Zaręba, *Masakra w Buczy. Rosyjskie zbrodnie na Kijowszczyźnie*, https://www.pism.pl/publikacje/masakra-w-buczy-rosyjskie-zbrodnie-na-kijowszczyznie [access: 16.10.2025].

Source: X/Moscow News [access: 16.10.2025].

Source: A. Segal, op. cit.

Individual accounts allegedly run by attractive women

In this case, Moscow simply uses a psychological mechanism based on the social perception of gender. Women are typically seen as warmer, more sympathetic, and less threatening than men, who are considered prone to aggression and hostility[21]. Hence, the greater tendency (often subconscious) of Internet users to interact with a fake account pretending to be a woman. An additional advantage of such accounts is the physical attractiveness of their alleged owners. Profile pictures (often generated by artificial intelligence) show women with symmetrical face shapes, flawless complexions, full lips, prominent cheekbones, and large eyes, that is, features commonly considered attractive to men[22]. According to the results of research by the Israeli company

21 F. Wen et al., *Do We See Masculine Faces as Competent and Feminine Faces as Warm? Effects of Sexual Dimorphism on Facial Perception*, „Evolutionary Psychology" 2020, no. 4, p. 5.

22 A.L. Jones, J. Bastian. *Biological Bases of Beauty Revisited: The Effect of Symmetry, Averageness, and Sexual Dimorphism on Female Facial Attractiveness*, „Symmetry" 2019, no. 2, p. 279.

Cyabra, women's social media accounts enjoy on average more than three times more viewership than men's profiles[23].

The alleged owners of these accounts claimed to be members of the Kremlin's diplomatic or media corps. They publish on platform X in Arabic, and their posts are an example of the combination of hard and soft propaganda. The former has an overtly anti-Ukrainian and anti-American overtone, while the latter creates a positive image of Russia as a country of beautiful women who adhere to the traditional division of gender roles between men and women. According to a report by the Institute for Strategic Dialogue, „pro-Kremlin women on Arabic-language Twitter not only advertise the state but also engage in propaganda"[24]. This ad takes the form of a photo of a sexy policewoman from Moscow or a flight attendant of a Russian airline, a woman with a small child emphasizing in the description that in Russia "women are in their natural place, while in Western countries we no longer distinguish between men and women", and finally women emphasizing how much Russia loves Arab countries.

These "women" reach very large – for example, the account allegedly run by Maria Raskolniow had 11 thousand followers. The owner of the account introduced herself as an employee of the "Arab press department of the Russian sputnik_ar agency". The profile photos of these "journalists" are most often generated by artificial intelligence or stolen from other accounts; the aforementioned Maria Raskolniowa used a photograph of fashion and beauty influencer Dzana Dzzyzzle from Instagram.

23 *What Makes Fake Profiles Effective? A New Research by Cyabra*, https://cyabra.com/blog/what-makes-fake-profiles-effective-a-new-research-by-cyabra/ [access: 11.10.2025].

24 M. Ayad, *Propaganda Primping: The 'Kremlinistas' of Twitter*, https://www.isdglobal.org/digital_dispatches/propaganda-primping-the-kremlinistas-of-twitter/ [access: 8.10.2025].

Source: X/Russian_press [access: 16.10.2025].

Trolls and bots

Trolls and bots are tasked with creating and/or distributing controversial or false content. In the Lebanese media landscape, they are behind Russian propaganda, accusing Ukraine of collaborating with terrorist groups such as Hamas and Hezbollah. Platform X has seen many posts accusing Ukrainian President Volodymyr Zelensky of supplying weapons to Hamas and reporting on the presence of Ukrainian mercenaries in the Israeli army. It is likely that trolls or bots are responsible, m.in for distributing a video allegedly prepared by the BBC on social media. He argued that the international, independent collective of investigative journalists Bellingcat had confirmed Ukrainian arms deliveries to Hamas, and Bellingcat explained that the video was fabricated. According to the Center for Combating Disinformation, functioning under the National Security and Defense Council of Ukraine, it is most likely that information about the alleged wounding of the First Secretary of the Ukrainian Embassy in Lebanon, Mykola Khostko, during the Israeli action against Hezbollah in September 2024 – this was a clear suggestion that Ukraine was cooperating with Hezbollah[25].

Most likely, a video allegedly from Mosul in 2016 was also distributed on Twitter in March 2022. The United States (at the request of the Iraqi army) then attacked a hospital used as an operational center by the so-called Islamic State. Commenting on the video, Arabic-speaking Twitter users wrote in unison: „this is the so-called U.S. humanity in Iraq when the Americans bombed a hospital in Mosul with internationally banned chemical weapons. Now, the same US is talking about humanity in Ukraine". However, the video did not come from Iraq; it was filmed during a Russian airstrike on a hospital in Mariupol on March 9, 2022.

Disinformation is a tool of Russian "soft power" and an extremely important element of the information war in Lebanon. Its aim is to create an even friendlier environment for Russian interests in Lebanon, weaken Western competition, and consolidate the position of the Kremlin's allies, such as Hezbollah. It

25 *Fake Disinformation that the first secretary of the Ukrainian Embassy in Lebanon was injured as a result of the explosion in Beirut*, https://disinfo.detector.media/en/post/disinformation-that-the-first-secretary-of-the-ukrainian-embassy-in-lebanon-was-injured-as-a-result-of-the-explosion-in-beirut [access: 8.10.2025].

focuses on strengthening the Kremlin's political influence and weakening the narrative of the West, especially the US and NATO. Importantly, Moscow is making perfect use of the West's weakness: many European media outlets have withdrawn from the Middle East for economic reasons, while Russian state-owned media outlets such as Sputnik Arabic and RT Arabic continue to operate there. In January 2023, the BBC decided to close its Arabic-language radio services (including in Lebanon), which was explained by the need to cut spending and switch more to digital and TV services than to traditional FM radio[26]. The BBC and its management emphasize that such situations can be exploited by the media of other countries that expand their disinformation influence. This is what happened in Lebanon: Sputnik took over some of the frequencies on which BBC Arabic was previously broadcast.

Russian disinformation in Lebanon is based on techniques such as emotional manipulation, selective presentation of facts, duplication of conspiracy theories, and "narrative reversal" – for example, presenting Russia as a victim of Western aggression. In doing so, it takes advantage of Lebanon's complicated internal situation.

Russian disinformation in Lebanon plays an important role in shaping the perception of Moscow as an alternative to the West, especially in the context of regional conflicts (such as the war in the Gaza Strip), criticism of US imperialism, and the promotion of Russia's image as a stable and loyal partner. Thanks to the consistent use of local languages, media channels, and social tensions, Russia is effectively building its information influence, especially among societies disillusioned with Western policies, such as those in the Middle East. However, for disinformation efforts to prove effective in the long term, Russia must back them up with real actions in the field of economic or military cooperation or humanitarian support, which Lebanon desperately needs. So far, this cooperation has been quite limited: Russia and Lebanon are not connected by arms contracts, military presence, free trade agreements, or large infrastructure projects. Humanitarian support is equally limited, coming down to emergency assistance in times of crisis. For example, during the COVID-19 pandemic, Russia donated Sputnik vaccines (partly as a donation), and after the explosion in the port of Beirut, it sent rescue teams,

26 *BBC boss warns of Russian and Chinese propaganda*, https://www.bbc.com/news/articles/cj9jgmexmx4o [access: 12.10.2025].

doctors, and medical equipment. A mobile military hospital. Therefore, there is room to weaken Russia's influence in the field of information policy. Western countries must start supporting bottom-up initiatives, such as start-ups that build fact-checking platforms. An example of such a platform in Lebanon is Sawab, founded in 2022 by six journalism students and graduates. Its aim is to reduce the spread of false information in Lebanon and raise awareness of the importance of verifying information before it is published or shared. Currently, Sawab cooperates, among m.in, with WhatsApp. It also seems essential that social media platforms take action, m.in as they increase investment in moderators who are familiar with Arabic and its local dialects and provide them with appropriate training on human rights, including on freedom of expression, non-discrimination and hate speech. International cooperation on disinformation should also include international training for journalists, academia, publicists and government officials.

Bibliography

Ayad M., *Propaganda Primping: The 'Kremlinistas' of Twitter*, https://www.isdglobal.org/digitaldispatches/propaganda-primping-the-kremlinistas-of-twitter/ [access: 8.10.2025].

BBC boss warns of Russian and Chinese propaganda, https://www.bbc.com/news/articles/cj9jgmexmx4o [access: 12.10.2025].

Dezinformacja – czym jest i jak ją zweryfikować, https://cyberprofilaktyka.pl/blog/dezinformacja---czym-jest-i-jak-ja-zweryfikowac_i23.html [access: 27.09.2025].

ESCWA warns: more than half of Lebanon's population trapped in poverty, https://www.unescwa.org/news/lebanon-population-trapped-poverty [access: 16.10.2025].

Fake Disinformation that the first secretary of the Ukrainian Embassy in Lebanon was injured as a result of the explosion in Beirut, https://disinfo.detector.media/en/post/disinformation-that-the-first-secretary-of-the-ukrainian-embassy-in-lebanon-was-injured-as-a-result-of-the-explosion-in-beirut [access: 8.10.2025].

Harvard Kennedy School – raport: Who is afraid of fake news?, „Harvard Kennedy School Misinformation Review" 2022, vol. 3, no. 3.

Janadze E., *The digital Middle East: Another front in Russia's information war*, https://www.mei.edu/publications/digital-middle-east-another-front-russias-information-war [access: 28.09.2025].

Jones A.L., Bastian J., *Biological Bases of Beauty Revisited: The Effect of Symmetry, Averageness, and Sexual Dimorphism on Female Facial Attractiveness*, „Symmetry" 2019, no. 2.

Kaczmarek K., *Konsekwencje dezinformacji: przegląd wybranych narzędzi i technik manipulacji*, „Bezpieczeństwa Narodowe" 2024, no. 45.

Kemp S., *Digital 2024: Lebanon*, https://datareportal.com/reports/digital-2024-lebanon [access: 8.10.2025].

Lebanon Humanitarian Fund Annual Report 2022, https://www.unocha.org/publications/report/lebanon/lebanon-humanitarian-fund-annual-report-2022 [access: 16.10.2025].

Lebanon media guide, https://www.bbc.com/news/world-middle-east-14648683 [access: 8.10.2025].

Lebanon's Economic Contraction Deepens, Highlighting Critical Need for Reforms and Key Investments, https://www.worldbank.org/en/news/press-release/2024/12/10/lebanon-s-economic-contraction-deepens-highlighting-critical-need-for-reforms-and-key-investments [access: 16.10.2025].

Majchrzak A., *W krainie kolorowych matrioszek – jak działa rosyjska dezinformacja?*, https://demagog.org.pl/analizy_i_raporty/w-krainie-kolorowych-matrioszek-jak-dziala-rosyjska-dezinformacja/ [access: 27.09.2025].

Megaphone, https://x.com/megaphone_news/status/1501189639750701059?s=46 [access: 28.09.2025].

Nowacka S., *Perspektywy odbudowy Libanu*, „Biuletyn PISM" 2021, no. 97.

Our Work in Lebanon, https://www.transparency.org/en/countries/lebanon [access: 16.10.2025].

Piechowska M., Zaręba S., *Masakra w Buczy. Rosyjskie zbrodnie na Kijowszczyźnie*, https://www.pism.pl/publikacje/masakra-w-buczy-rosyjskie-zbrodnie-na-kijowszczyznie [access: 16.10.2025].

Russian cyber strategy in the Middle East and North Africa (MENA): Analysing the Kremlin's disinformation efforts amid 2022 invasion of Ukraine, https://dspace.cuni.cz/bitstream/handle/20.500.11956/178359/120427340.pdf?sequence=1&isAllowed=y [access: 28.09.2025].

Schafer B. et al., *The Russian Propaganda Nesting Doll*, https://securingdemocracy.gmfus.org/wp-content/uploads/2024/05/Laundromat-Paper.pdf?utm_source=chatgpt.com [access: 16.10.2025].

Segal A., *Russia's Information Warfare in the Middle East*, Potsdam 2024.

Styszyński M., *Arab context of the Ukraine conflict in Russia Today Arabic and Sputnik*, „Krakowskie Studia Międzynarodowe" 2023, no. 1.

The Architecture of Distrust: Understanding Mis & Disinformation in Lebanon, https://static1.squarespace.com/static/61751a56593c762f6c492e6b/t/680a5738bdab466ffdbd0c2a/1745508154161/The+Architecture+of+Distrust%3A+Understanding+Mis+%26+Disinformation+in+Lebanon.pdf [access: 8.10.2025].

Wen F. et al., *Do We See Masculine Faces as Competent and Feminine Faces as Warm? Effects of Sexual Dimorphism on Facial Perception*, „Evolutionary Psychology" 2020, no. 4.

What Makes Fake Profiles Effective? A New Research by Cyabra, https://cyabra.com/blog/what-makes-fake-profiles-effective-a-new-research-by-cyabra/ [access: 11.10.2025].

Dominika Sikorska
ORCID 0009-0009-2449-9284
sikorska.contact@gmail.com

China's Path to Technological Superpower: Made in China 2025 and Dual-Use Technologies

Abstract

The article investigates the role of China's Made in China 2025 (MIC 2025) strategy as a blueprint for China becoming a global technological superpower. The paper explores how MIC 2025 integrates civilian industrial modernization with military capability development supported by a system of Military-Civil Fusion. It also analyses how MIC 2025 has promoted dual-use technologies and innovation in ten strategic sectors, such as new generation IT, robotics, advanced rail transportation, energy saving and new energy vehicles, new materials, or biotech and pharma. Drawing on Chinese policy documents, commentaries, and academic literature, and international research and analyses, the paper evaluates MIC 2025's achievements and remaining vulnerabilities. It seeks to contribute to a more nuanced understanding of how China's industrial policy intertwines with the military and security objectives in the pursuit of technological leadership.

Key words

Made in China 2025, dual-use technologies, Military-Civil Fusion, technological superpower

Introduction

China's rise over the past four decades has been marked by extraordinary economic growth and by significant technological development. The Made in China 2025 (中国制造 2025, hereafter MIC 2025) initiative announced in 2015 by the State Council of the People's Republic of China (PRC) declares, "building an internationally competitive manufacturing industry is the

only way China can enhance its comprehensive national strength, ensure national security, and build itself into a world power"[1]. This reflects China's long-term vision for national rejuvenation, global competitiveness, and laying the foundations for realizing the Chinese Dream (中国梦). MIC 2025, a state-led strategy, is the comprehensive national plan designed to upgrade China's manufacturing base, foster innovation in different sectors, and reduce dependence on foreign technology imports. The strategy is closely intertwined with the policy of Military-Civil Fusion (军民融合, hereafter MCF)[2], which seeks to combine civilian and military technological development. MIC 2025, supported by MCF, reflects a strategic belief that strong manufacturing, progress in advanced technologies and technological self-reliance are indispensable for economic resilience, defence modernization and national security. MIC 2025 targets ten strategic sectors which include (1) new-generation information technology, (2) high-end numerically controlled machinery and robotics, (3) aviation and aerospace equipment, (4) offshore engineering equipment and high-tech ships, (5) advanced rail transportation equipment, (6) energy saving and new energy vehicles, (7) electrical equipment, (8) agricultural machinery and equipment, (9) new materials, and (10) biotech, pharma, and high-performance medical devices. The cutting-edge civilian innovations in those sectors can be simultaneously applied by the People's Liberation Army (PLA), enabling military transformation and defence modernization. The paper aims to analyse the role of MIC 2025 in accelerating China's technological rise, focusing on the development of dual-use technologies. The analysis is guided by several central research questions:

1. How has MIC 2025 contributed to advancing China's industrial capabilities and technological innovation?

2. How has MIC 2025 been integrated into military modernization goals through the framework of MCF?

1 国务院关于印发《中国制造2025》的通知 [*Notice on the Publication of "Made in China 2025"*], https://www.gov.cn/zhengce/content/2015-05/19/content_9784.htm [access: 22.08.2025].

2 习近平主持召开中央军民融合发展委员会第一次全体会议 [*Xi Jinping Presided Over the First Plenary Meeting of the Central Integrated Military and Civilian Development Commission*], https://www.gov.cn/xinwen/2017-06/20/content_5204059.htm [access: 22.08.2025].

3. What are the successes and shortcomings of the initiative after a decade of its implementation?

Methodologically, an analysis of original Chinese policy documents is combined with a review of Chinese and international academic literature, studies, and commentaries. The paper begins with the examination of the origins and objectives of MIC 2025. Next, it presents the MCF concept and its evolution, and the interconnectedness of MIC 2025 and MCF. Finally, it assesses the recent achievements and vulnerabilities of MIC 2025, identifying their dual-use potential. The paper seeks to contribute to a more nuanced understanding of how China's industrial policy intertwines with the military and security objectives in the pursuit of technological leadership.

Made in China 2025: Origins and Objectives

A decade ago, it was recognized that China's manufacturing was huge in scale but lagging technologically. Chinese leaders saw advanced manufacturing and technological innovation as essential to alter the country's state from "large but not strong" through "large but fairly strong" into "large and strong"[3]. In this context, in May 2015, the PRC State Council announced Made in China 2025 (MIC 2025), which aims to enhance the nation's manufacturing base and drive technological innovation. MIC 2025 is the first stage of a three-phase plan, which includes Made in China 2035 and Made in China 2045[4], and is to be achieved by 2049, the centennial of the People's Republic of China. The initiative is to "build our country into a manufacturing power that leads the development of the world's manufacturing industry through three decades of efforts. By the time the People's Republic of China celebrates the 100th anniversary of its founding, this will lay a solid foundation for realizing the Chinese dream

3 Q. Huang,"中国制造*2025*":成就、趋势与开放发展 *["Made in China 2025": Achievements, Trends, and Development*], „应用经济学评论" [„The Applied Economics Review"] 2025, no. 5, p. 10.

4 《中国制造*2025*》解读之：中国制造*2025*，我国制造强国建设的宏伟蓝图 [*The Interpretation of "Made in China 2025": Made in China 2025, a Grand Blueprint for Building China Into a Manufacturing Power*], „工业炉" [„Industrial Furnace"] 2025, no. 3, p. 46.

of the great rejuvenation of the Chinese nation"[5]. Drawing inspiration from Germany's Industry 4.0 development plan for smart manufacturing, MIC 2025's aims to enhance indigenous innovation, improve manufacturing quality, and reduce reliance on foreign technology. The core objectives are to be achieved by state support, which includes employing government subsidies, guiding state-owned enterprises (SOEs), research and development (R&D) funding, attracting and recruiting field experts, scientists and technological developers, and facilitating technology transfers and acquisitions[6]. MIC 2025 defines specific targets to benchmark progress by 2025. For instance, it seeks to achieve 70% self-sufficiency in core components and basic materials in key industries. What is more, it aims for full intelligentization for key areas of the manufacturing industry and achieving a globally advanced level of the green development of the manufacturing industry. Another example is that the proportion of internal expenditure on R&D expenditure of the manufacturing industry above a certain size in the main business income is to increase to 1.68%. Other targets include the development of quality and efficiency, or integrating information technology and industrialization, with broadband penetration reaching 82% by 2025[7]. The longer-term goal is to attain a leading position in global high-tech markets. MIC 2025 identifies ten strategic sectors as pillars of this transformation. These sectors include (1) new-generation information technology, (2) high-end numerically controlled machinery and robotics, (3) aviation and aerospace equipment, (4) offshore engineering equipment and high-tech ships, (5) advanced rail transportation equipment, (6) energy saving and new energy vehicles, (7) electrical equipment, (8) agricultural machinery and equipment, (9) new materials, and (10) biotech, pharma, and high-performance medical devices[8]. Developing capabilities in each of these sectors is crucial to economic and national security. Not only will it move China up the global value chain, but it will also significantly

5 国务院关于印发《中国制造*2025*》的通知 [Notice on the Publication of "Made in China 2025"]…

6 *Made in China 2025: Global Ambitions Built on Local Protections*, https://www.uschamber.com/assets/documents/final_made_in_china_2025_report_full.pdf [access: 22.08.2025].

7 国务院关于印发《中国制造*2025*》的通知 [Notice on the Publication of "Made in China 2025"]…

8 Ibidem.

reduce dependency on foreign suppliers. In sum, the overarching objectives of the MIC 2025 are to comprehensively upgrade China's industrial base and make domestic firms globally competitive in high-value sectors, and ensure greater self-reliance in critical sectors crucial to national sovereignty and economic growth. This, in turn, will lead the country through the process of vital industrial and technological reforms.

Military-Civil Fusion: Concept and Evolution

Military-Civil Fusion is a comprehensive strategy that aims to close the barriers between the civilian and military sectors. Its main objective is to enable the „military to civilian transfer, [and] civilian participation in military" („军转民"、"民参军")[9], which is to be achieved by seamless collaboration and resource exchange between these two sectors. The advancements in science, technology, and industrial capacity should be applied in military initiatives, and military efforts should be used for civilian purposes. The concept of Military-Civil Fusion can be traced back to Mao Zedong's rule. It has evolved under a variety of Chinese administrations, from Mao Zedong, Deng Xiaoping, Jiang Zemin, Hu Jintao to Xi Jinping. Each leader contributed to the concept's development, which has become one of China's future strategies. From the focus on the transfer of civilian technology to the military sector, the development of technologies with both civilian and military applications has been emphasized[10]. Xi Jinping made Military-Civil Fusion a strategic priority, which led to the establishment of the Central Military-Civil Fusion Development Commission (军民融合发展委员会) in 2017[11]. This high-level body, chaired by Xi Jinping, stresses the importance of

9 国务院办公厅关于推动国防科技工业军民融合深度发展的意见 [*Opinions of the General Office of the State Council on Promoting Closer Civil-Military Integration in the National Defence Science and Technology Industry*], https://www.gov.cn/zhengce/content/2017-12/04/content_5244373.htm [access: 25.08.2025].

10 N.S. Manhas, *China's Military-Civil Fusion from Mao to Xi: A Long Roadmap*, „Journal of Polity and Society" 2024, no. 1, p. 49.

11 中共中央政治局召开会议决定设立中央军民融合发展委员会 [*The Political Bureau of the CPC Central Committee Holds a Meeting Deciding to Establish the Central Military-Civil Fusion Development Commission*], https://www.gov.cn/xinwen/2017-01/22/content_5162263.htm [access: 25.08.2025].

MCF and enables coordination across ministries, the military, and industries. Policies under MCF include creating joint research platforms, dual-use technology incubators, or talent programs that embed military experts in civilian projects[12]. There are local MCF committees led by Party officials in nearly every province in China, which enables the alignment of regional industrial plans with military requirements. MCF emphasizes building dual-use infrastructure and supply chains that can serve peacetime commerce and defence production. It promotes the idea that there is no clear dividing line between the civilian and military sectors of development in a modern nation. Modern start-ups deploying AI algorithms, laboratories researching new materials, or factories producing high-tech goods are all part of the broader national security ecosystem. This multi-faceted strategy, covering technological, economic, industrial, and geopolitical spheres, represents a far more direct integration of civilian and defence resources than its earlier versions focusing on "military-civil integration"[13]. MCF reflects the quest for technology and military strength, which can be mutually reinforced and centrally directed from the top.

Made in China 2025 and Military-Civil Fusion

It was observed that under Xi Jinping's rule, the Military-Civil Fusion "has been part of nearly every major strategic initiative, including Made in China 2025"[14]. Many sectors targeted by MIC 2025, which aim for civilian market dominance, are those needed to build a world-class military, and the MCF strategy provides the bridge. It ensures that innovations supported by MIC 2025 can be transferred to the People's Liberation Army and the defence industry. Ten strategic sectors, which are significant for the national economy and have the potential to confer civilian and military advantages, include:

12 Y. Zhao, 新时代我国军民融合发展的战略举措探析, „现代商贸工业" [„Modern Business Trade Industry"] 2025, no. 15, p. 14–16.

13 N.S. Manhas, op. cit., p. 50.

14 *Civil-Military Fusion: The Missing Link Between China's Technological and Military Rise*, https://www.cfr.org/blog/civil-military-fusion-missing-link-between-chinas-technological-and-military-rise [access: 25.08.2025].

1. New generation IT, i.e. integrated circuits and special equipment, information communication equipment, operating systems and industrial software. These include semiconductors, 5G telecommunications, artificial intelligence and cutting-edge chips. Such technology is crucial for the development of a smart economy, and digital society, and can be used to secure communications, surveillance, and advanced military command systems.

2. High-end CNC machines and robotics, including advanced machine tools, automation systems, and industrial robots. These can enhance the development of "smart factories" and productivity, which benefits civilians. Militaries, on the other hand, benefit from the same technologies in automated production of weapons, unmanned systems, and AI-driven technologies.

3. Aviation and aerospace equipment, covering aircraft, heavy-duty helicopters, unmanned aerial vehicles (UAVs), carrier rockets, heavy-duty launch vehicles, satellites, and space platforms. This sector promotes the development of engines, space technology, manned spaceflight, and lunar and deep space exploration projects. Civilian advances in this sector can be transferred into military use to upgrade air and space power. An industrial base producing commercial jets and rockets can also produce military transport planes, missiles, and surveillance satellites.

4. Offshore engineering equipment and high-tech ships, including luxury cruise ships, liquid natural gas (LNG) tankers, deep-sea space stations, large floating structures, and the development of deep-sea exploration. Civilian shipyards build advanced ships to boost civilian trade and energy exploration. In parallel, they use similar know-how to support the construction of warships and submarines, enabling naval modernization.

5. Advanced rail transportation equipment, such as green, intelligent, high-speed trains and heavy-duty rail transit equipment systems. This sector seeks to establish a world-leading modern rail transit industry system. High-speed rail is mainly a civilian infrastructure used for economic development, but also has value in military logistics. This infrastructure enables fast redeployment of troops and equipment, enhancing national mobility and resilience.

6. Energy-saving and new energy vehicles (NEVs), focused on the development of hybrid and electric vehicles, including low-carbon, informatized, and intelligentized automobiles, as well as upgraded batteries,

drive motors, and engines. On the one hand, reduced emissions and the adoption of world-leading NEVs are civilian benefits. On the other hand, technologies, such as batteries or electric propulsion, can be applied to military vehicles and naval vessels. Strategically, NEVs advancement reduces dependence on imported oil.

7. Electrical equipment, covering the improvement of super-capacity hydropower units, nuclear power units, heavy-duty gas turbines, coal-fired power units, renewable energy and new energy equipment, and advanced energy storage devices. A modern power infrastructure is essential for the development of industry and cities. It also provides the backbone for critical defence facilities and military bases. Upgraded power electronics, grid stability, and nuclear reactor designs are crucial for national security.

8. Agricultural machinery and equipment, focusing on advanced farm machinery, agricultural technology, and smart agriculture, which accelerates production processes of grains, crops, cotton, oil, sugar, as well as breeding, planting, harvesting, transportation, and storage. Not only can these enable agricultural productivity and food security, but they also enhance stability in a protracted crisis. On the other hand, logistics systems or agricultural drones can be repurposed by the military.

9. New materials, such as high-performance structural materials, functional polymer materials, special inorganic non-metallic materials, advanced composite materials, superconducting materials, nanomaterials, and bio-based materials. New materials are essential for military and civilian use. They are used in the manufacturing of lighter, stronger industrial and consumer components, as well as aerospace-grade alloys for engines or heat-resistant materials for missiles.

10. Biotech, pharma, and high-performance medical devices, including chemical medicines, traditional Chinese medicines (TCM), biotech medicines, new vaccines, medical robots, treatment devices or 3D bioprinting. Advancements in this sector not only improve public health, but also contribute to military medicine and biodefence. A strong biotech sector can also reduce reliance on foreign pharmaceuticals[15].

15 国务院关于印发《中国制造*2025*》的通知 [Notice on the Publication of "Made in China 2025"]…

Each of these sectors exhibits a dual-use character, highlighting the MIC 2025 and MCF integration. As civilian industries transform and upgrade, the innovations can be transferred to the military. For instance, the upgrades in the information technology sphere, e.g., Artificial Intelligence, semiconductors or telecommunications, are all dual-use areas. New 5G, 6G and fibre-optic networks are developed for civilian use, and provide the PLA with high-bandwidth communications for command and control. Advances in AI, from autonomous driving algorithms to facial recognition, can have military applications such as target recognition, surveillance systems, and swarm drones. The innovations in semiconductors have been identified as having "immense commercial and military significance"[16]. In the aerospace and aviation domains, one of the MIC 2025's objectives is to develop space infrastructure and indigenous civilian aircraft, the commercial jet C919. This has yielded expertise in materials, avionics and aerodynamics, which can also benefit military aviation programs. On one hand, there has been an expansion of Chinese commercial drones possessing a dominant market share[17]. On the other hand, there have been breakthroughs in unmanned aerial vehicles (UAVs) capable of mid-air drone swarm deployment[18]. The expansion of the Chinese satellite network promoted by MIC 2025 provides the PLA with secure communications and precision navigation (the BeiDou navigation system) independent of foreign systems (GPS). Huge capacity and technical advances made in shipbuilding, another MIC 2025's pillar, have benefited the PLA Navy (PLAN), the world's largest army[19]. High-tech ships, liquid natural gas (LNG) tankers, aircraft carriers, and deep-sea exploration serve China's naval growth and modernization. Another example is the domain of energy-saving and new energy vehicles, including batteries, engines, lightweight materials, and

16 M. Rubio, *The World China Made "Made in China 2025" Nine Years Later*, https://www.americanrhetoric.com/speeches/PDFFiles/Marco-Rubio-The-World-China-Made.pdf [access: 25.08.2025].

17 M. Rubio, op. cit.

18 H. Nan, *China's Military-Civil Fusion: A Challenge to the US Military-Industrial Complex?*, https://www.thinkchina.sg/technology/chinas-military-civil-fusion-challenge-us-military-industrial-complex [access: 25.08.2025].

19 A. Palmer, *Unpacking China's Naval Buildup*, https://www.csis.org/analysis/unpacking-chinas-naval-buildup [accessed: 25.08.2025].

complete industrial systems[20]. Innovations in this sector can help the military to reduce the reliance on fuel supply lines in areas such as land vehicles, naval propulsion and aerospace. The modernization of crucial national sectors is bolstered by advanced manufacturing and robotics. Upgrades in this domain lead to faster, more accurate, and more effective manufacturing systems, which can be adopted by civilian and military industries alike. Institutionally, MIC 2025 and MCF are actively integrated by a variety of actions supported by the Chinese state. The number of private Chinese companies certified as military suppliers has increased, as barriers to entry have been reduced and incentives for technological companies have been distributed to pursue defence contracts[21]. In addition to beneficial incentives and policy support, other measures, including market expansion, participation of the private sector, and industrial cluster development, have been reinforced[22]. For instance, the Shanghai Minhang National MCF Zone, which is focused on aviation and aerospace, consists of small and medium-sized "high-tech enterprises" that serve the commercial sector and align with military needs. Such companies are rewarded financially through subsidies for contributing to defence outcomes[23]. The military gains quicker access to cutting-edge commercial technology, and civilian programs gain funding and direction by addressing national security imperatives. In sum, MIC 2025 elevates China's overall technological base in pivotal industries, while MCF mechanisms channel those civilian advances into military applications. As official strategy documents indicate, developing China into a technological superpower is not an end, but a means to "strong and rejuvenated nation" status[24], with military strength being its integral part.

20 国务院关于印发《中国制造*2025*》的通知 [Notice on the Publication of "Made in China 2025"]…

21 G. Levesque, *Commercialized Militarization: China's Military-Civil Fusion Strategy*, https://www.nbr.org/publication/commercialized-militarization-chinas-military-civil-fusion-strategy/ [access: 25.08.2025].

22 Z. Chen, L. Zhong, 新时代下军民深度融合的路径 [The Path to Deep Integration of Military and Civilian Sectors in the New Era], „中国军转民" [„Defense Industry Conversion in China"] 2025, no. 1, p. 23–24.

23 G. Levesque, op. cit.

24 国务院关于印发《中国制造*2025*》的通知 [Notice on the Publication of "Made in China 2025"]…

Made in China 2025: Progress and Dual-Use Significance

Ambitious upgrades across MIC 2025's ten strategic sectors have been actively pursued since the strategy was launched over a decade ago. China has achieved leadership in 5G networks, high-speed rail, and electric vehicles, but still faces enduring vulnerabilities in semiconductors, jet engines, and frontier pharmaceuticals. The Military-Civil Fusion strategy has been supporting the advances in dual-use technologies, which have been systematically channelled to strengthen the People's Liberation Army while also fuelling economic growth. The table below presents the examples of significant progress in each sector by 2025, highlighting their dual-use significance.

Table 1. Made in China 2025: Progress, Military-Civil Fusion Relatedness and Dual-Use Implications

Sector	**MIC 2025: Progress**
New generation and IT industry	World's largest 5G deployment (>4m base stations by 2024)[a-1] Global leadership in AI research output[a-2] Strong companies like Huawei or SenseTime[a-3] Chip self-sufficiency below 25%, being below the 70% target;[a-4] yet, Chinese chips accounting for nearly 40% of global chip output value[a-5] Limited ability to manufacture ultraviolet (EUV) lithography machines; semiconductors remaining a choke point[a-6]
	Dual-Use and MCF Implications
	5G networks as the digital backbone for PLA communications[a-7] AI applied to surveillance, drones, and "intelligentized" warfare[a-8]
Sector	**MIC 2025: Progress**
High-end numerically controlled machinery and robotics High-end CNC machines and robots	A sharp rise in robot density (470 units per 10,000 employees in 2023[a-9] Expansion of domestic robot firms; yet, high-precision CNC and advanced robotic systems sourced abroada[a-10]
	Dual-Use and MCF Implications
	Defence production strengthened by automation capacity and rapid scaling of weapons manufacturing
Sector	**MIC 2025: Progress**
Aviation and aerospace equipment [a-11]	The introduction of a commercial aircraft C919 by COMAC; yet 90% of its key component being provided by foreign suppliers Homegrown helicopters still in early stages Global leadership in unmanned drones; controlling 80% of the global drone market; DJI as a world-leading company in this domain Beidou, Chinese alternative to GPS, being adopted by BRI

	membership and across Eurasia, and gaining recognition as a universal satellite navigation system for commercial flights The completion of Tiangong space station, and aiming for large-scale multidisciplinary space science research and technology experiments[a-12]
	Dual-Use and MCF Implications
	Know-how for military aviation built by civil aircraft programmes. Drones, with extensive civilian uses, having military applications Beidou as a military-driven technology, driving the industry's technology
Sector	**MIC 2025: Progress**
Offshore engineering equipment and high-tech ships	China as a world leader in the shipbuilding industry[a-13] Accounting for 55% of global demand in 2024, with total sales reaching more than $110 billion[a-14] The launch of China's self-built, large-scale cruise ship[a-15] The construction of LNG carriers, offshore rigs, and aircraft carriers[a-16]
	Dual-Use and MCF Implications
	Civil shipyards supporting naval modernization Investment, infrastructure, and intellectual property from the commercial sector acquired by the military Offshore engineering expertise overlapping with military logistics, undersea surveillance, and sea lane control[a-17]
Sector	**MIC 2025: Progress**
Advanced rail transportation equipment Offshore engineering equipment and high-tech ships Advanced rail transportation equipment	The largest high-speed rail network in the world, covering 46,000 km, with indigenous trainset and signalling technologies[a-18] A high degree of self-reliance in high-speed rail technology, yet lacking the full self-sufficiency[a-19] Rail projects exported and built with foreign countries; "a diplomatic tool" and an important component of the Belt and Road Initiative[a-20]
	Dual-Use and MCF Implications
	High-speed rail networks as an efficient supply chain for the military, enabling the rapid deployment of military personnel and equipment, enhanced coordination of military operations, and improved security of strategic mobility[a-21] High-speed rail exports as a means to shape geopolitical influence
Sector	**MIC 2025: Progress**
Energy saving and new energy vehicles (NEVs) Electrical equipment Agricultural machinery and equipment	The number of NEVs in China reaching 31.4 million in 2024[a-22] From January to August 2025, NEV production and sales exceeding 8.2 million vehicles; the increase of market penetration to 45%[a-23] 45% of automotive market demand met by NEVs[a-24] (MIC 2025's target for 2025: 20%[a-25]) 90% of the market share held by domestic NEV manufacturers[a-26] China's dominant position in battery production, covering ca. 75% of global capacity[a-27]

	Dual-Use and MCF Implications
	Reduced oil import reliance due to the electrification technology Military vehicles and submarines supported by battery innovations
Sector	MIC 2025: Progress
Electrical equipment Biotech, pharma, and high-performance medical devices	More than 80% share of the global solar panel market, and a 60% share of the global wind turbine market; a high degree of self-reliance[a-28] A technology leader in nuclear power, aiming to build "Nuclear Belt and Road"; yet, this sector is to be enhanced[a-29] The development of the indigenous Hualong One nuclear reactor[a-30] The rapid deployment of ultra-high-voltage (UHV) grid optimizing cross-regional resource allocation[a-31]
	Dual-Use and MCF Implications
	Reliable domestic energy infrastructure as a core element of national security Power electronics applicable to naval propulsion and high-energy weapons
Sector	**MIC 2025: Progress**
Agricultural machinery and equipment	Crop cultivation and harvesting mechanization rate exceeding 75%[a-32] BeiDou Navigation Satellite System applied by "intelligent agriculture"[a-33] The wide application of agricultural drones, with China's annual agricultural drone operations exceeding 2.6 billion mu (approximately 166 acres) annually[a-34]
	Dual-Use and MCF Implications
	Agricultural modernization as a core factor enhancing food security Drone technologies transferable to military reconnaissance and logistics
Sector	**MIC 2025: Progress**
New materials	China's global dominance in the rare earth sector: ca. 60% of global rare earth elements (REE) production, 90% of REE processing, 99% of global heavy rare earth elements (HREE) processing[a-35] A vast R&D base for new materials Incremental progress in key materials, such as advanced carbon fibre, as well as in composites and alloys; yet, existing quality gaps in advanced carbon fibre (T-1000 carbon fibre)[a-36]
	Dual-Use and MCF Implications
	Rare earths as a critical component for munitions and radars Aerospace and naval hardware enhanced by advanced composites
Sector	**MIC 2025: Progress**
Biotech, pharma, and high - performance medical devices	Significant investments in biotech R&D[a-37] China as a global powerhouse in biotech research[a-38] Domestic COVID-19 vaccines, including a homegrown mRNA Covid vaccine, developed since 2020[a-39]

	China leading in the field of genomics, but still lagging in high-end devices[a-40]
	Dual-Use and MCF Implications
	Domestic vaccine production as a source of resilience Biomedical research as a support for military health and bio-defence applications

[a-1] *2024* 年通信业统计公报 [*Statistical Bulletin on Telecommunications Development in 2024*], https://www.gov.cn/lianbo/bumen/202501/content_7003010.htm [access: 28.08.2025].

[a-2] W. Chang, R. Arcesati, A. Hmaidi, *China's Drive Towards Self-Reliance in Artificial Intelligence: From Chips to Large Language Models*, https://merics.org/sites/default/files/2025-07/MERICS%20Report-AI_Stack_final.pdf [access: 28.08.2025].

[a-3] Ibidem.

[a-4] *Taiwan and the Global Semiconductor Supply Chain – China's Pursuit of Semiconductor Self-Sufficiency*, https://www.roctaiwan.org/uploads/sites/86/2025/04/250401_April_May_Issue_final.pdf [access: 28.08.2025].

[a-5] Q. Huang, op. cit.

[a-6] *Made in China 2025: The Cost of Technology Leadership*, https://www.europeanchamber.com.cn/en/publications-archive/1274 [access: 28.08.2025].

[a-7] S. Palve, *China's 5G-Powered Unmanned Army! PLA Bets On 1st Mobile 5G Station To Power Its Robots & UAVs In Warzone*, https://www.eurasiantimes.com/chinas-5g-powered-unmanned-army-pla-bets-on-1st-mobile-5g-station-to-power-its-robots-uavs-in-warzone/ [access: 28.08.2025].

[a-8] *China's National Defense in the New Era*, https://english.www.gov.cn/archive/whitepaper/201907/24/content_WS5d3941ddc6d08408f502283d.html [access: 28.08.2025].

[a-9] *China Emerges as Global Frontrunner in Industrial Robot Density: Report*, https://english.www.gov.cn/news/202411/21/content_WS673e6b34c6d0868f4e8ed447.html [access:28.08.2025].

[a-10] *Made in China 2025: The Cost of Technology Leadership*…

[a-11] Ibidem.

[a-12] Y. Zhao et. al., *On-Orbit Space Technology Experiment and Verification Project Outlook of China's Tiangong Space Station*, „Space Sci Technol" 2023, no. 3, p. 61.

[a-13] *China Dominates the Shipbuilding Industry*, https://www.csis.org/analysis/china-dominates-shipbuilding-industry [access: 28.08.2028].

[a-14] Q. Huang, op. cit.

[a-15] *Made in China 2025: The Cost of Technology Leadership*…

[a-16] M. Rubio, op. cit.

[a-17] Ibidem.

[a-18] Q. Huang, op. cit.

[a-19] *Made in China 2025: The Cost of Technology Leadership…*

[a-20] M. Rubio, op. cit.

[a-21] R. Uppal, *High-Speed Rail (HSR) in Military Logistics: China Leads the Way*, https://idstch.com/geopolitics/high-speed-rail-hsr-in-military-logistics-china-leads-the-way/ [access:29.08.2025].

[a-22] 图表：决胜"十四五"打好收官战 | 我国新能源汽车产业加速提质向新 [*Chart: Winning the Final Battle of the 14th Five-Year Plan|China's New Energy Vehicle*

Industry Accelerates Quality Improvement and Moves Towards a New Era], https://www.gov.cn/zhengce/jiedu/tujie/202508/content_7036224.htm [access: 29.08.2025].

[a-23] Ibidem.

[a-24] Ibidem.

[a-25] *Made in China 2025: The Cost of Technology Leadership*…

[a-26] Ibidem.

[a-27] *The Battery Industry Has Entered a New Phase*, https://www.iea.org/commentaries/the-battery-industry-has-entered-a-new-phase [access: 29.08.2025].

[a-28] *Made in China 2025: The Cost of Technology Leadership*…

[a-29] M. Rubio, op. cit.

[a-30] *World's First Hualong One Reactor Put Into Commercial Operation*, https://www.caea.gov.cn/english/n6759361/n6759362/c6811183/content.html [access: 29.08.2025].

[a-31] 十四五”国家电网发展成效③：供电保障坚强可靠 [*Development Achievements of the State Grid in the 14th Five-Year Plan ③: Strong and Reliable Power Supply*], http://www.nw.sgcc.com.cn/info/1013/23258.htm [access: 29.08.2025].

[a-32] 农业农村部召开全国农业机械化工作推进会议 [*The Ministry of Agriculture and Rural Affairs Held a National Meeting to Promote Agricultural Mechanization*], https://www.gov.cn/lianbo/bumen/202504/content_7020519.htm [access: 29.08.2025].

[a-33] *BeiDou Navigation Satellite System*, http://en.beidou.gov.cn/APPLICATIONS/Agriculture/ [access: 29.08.2025].

[a-34] 大疆农业联合农民日报发布《农业无人机行业白皮书（2024/2025）》[*DJI Agriculture and Farmers' Daily Released the "Agricultural Drone Industry White Paper (2024/2025)"*], https://ag.dji.com/cn/newsroom/ag-cn-news-white-paper-2025 [access: 29.08.2025].

[a-35] G. Baskaran, M. Schwartz, *Developing Rare Earth Processing Hubs: An Analytical Approach*, https://www.csis.org/analysis/developing-rare-earth-processing-hubs-analytical-approach [access: 29.08.2025].

[a-36] M. Rubio, op. cit.

[a-37] A. Brown, J. Groenewegen-Lau, *Lab Leader, Market Ascender: China's Rise In Biotechnology*, https://merics.org/en/report/lab-leader-market-ascender-chinas-rise-biotechnology [access: 29.08.2025].

[a-38] Ibidem.

[a-39] *Made in China 2025: The Cost of Technology Leadership*…

[a-40] M. Rubio, op. cit.

By 2025, Made in China 2025 has fostered an industrial-technological base substantially. In areas such as telecommunications, transport or green technologies, state-driven scale and incentives have helped close gaps quickly, which has created both civilian benefits and military dividends. However, the sectors requiring long-term fundamental innovation, like semiconductors, jet engines, and pharmaceuticals, still need more time to meet ambitious targets fully. From a Military-Civil Fusion perspective, dual-use synergies have emerged. 5G, 6G, and AI-enabled systems support PLA command networks, domestic energy technologies secure military bases, and automated factories

scale arms production. MIC 2025, along with accompanying strategies such as MCF, has laid the foundation for China's long-term techno-military rise.

Conclusions

China's pursuit of becoming a technological superpower has been supported by initiatives such as Made in China 2025 and Military-Civil Fusion, which have reshaped China's industrial and technological landscape over the past decade. MIC 2025 can be seen as neither an unqualified triumph nor a failure. It is the first step of a long-term strategy that has impacted the civil and military domains. On one hand, it has contributed to significant achievements or overachievements in core sectors by focusing national resources and providing financial and policy support. This has led to notable successes in 5G and 6G telecommunications, renewable energy, high-speed rail, shipbuilding, or electric vehicles. On the other hand, it has exposed the areas with room for improvement, where complete self-sufficiency has not been achieved yet, and China needs more time, sustained research, and other indispensable sources to accomplish the ambitious targets. Even though some domains, such as semiconductors, certain high-end components, or commercial aircraft, have not achieved MIC 2025 goals, the overall achievements have contributed to the broader vision of a global "great power" (大国) with solid foundations for realizing the Chinese Dream (中国梦) of the great rejuvenation of the Chinese nation[25]. The status of "great power" cannot be achieved without a complete and independent industrial system, and a modernized national security system. Hence, the advancements under MIC2025 have been gradually transferred into the military, blurring the lines between civilian economic progress and defence capacity. MCF has enabled the integration of MIC 2025 targets with military goals. MIC 2025 sectors targeted for civilian development have had parallel military applications and benefits for the PLA. The integration of the long-term policies supports China's transition from "large but not strong" through "large but fairly strong" into a "large and strong" nation[26]. This paper

25 国务院关于印发《中国制造*2025*》的通知 [*Notice on the Publication of "Made in China 2025"*]…

26 Q. Huang, op. cit.

has some limitations. It may not capture every facet, as it primarily relied on open-source data and analyses. Classified military benefits of MCF or the most recent Chinese internal assessments would provide a more detailed perspective on the dual-use interrelation between industrial and military policies. The evaluation of MIC 2025 progress is an overall picture of 2025 and recent years. China's progress in the core sectors is evolving rapidly. Further research could delve into specific case studies to provide deeper insights. It could also analyse global reactions and responses in the time of technological competition. As MIC 2025 is the first stage of the greater strategy, understanding the successes and limitations of MIC 2025 and accompanying policies, such as MCF, will be crucial for analysts and policymakers alike. China's path to technological superpower status has been a long journey. The first decade under MIC 2025 has moved China closer to that status. A decade ago, China was largely seen as the world's low-cost factory. Now, it has become a competitor in several advanced industries and has laid the groundwork for future breakthroughs. Yet, this is a continuous journey, meaning China must address internal weaknesses and external challenges. What can be seen on China's path to technological superpower is that Made in China 2025's legacy will be visible for years to come: both in the civilian and military sectors, both in China and globally.

Bibliography

Baskaran G., Schwartz M., *Developing Rare Earth Processing Hubs: An Analytical Approach*, https://www.csis.org/analysis/developing-rare-earth-processing-hubs-analytical-approach [access: 29.08.2025].

Brown A., Groenewegen-Lau J., *Lab Leader, Market Ascender: China's Rise In Biotechnology*, https://merics.org/en/report/lab-leader-market-ascender-chinas-rise-biotechnology [access: 29.08.2025].

Chang W., Arcesati R., Hmaidi A., *China's Drive Towards Self-Reliance in Artificial Intelligence: From Chips to Large Language Models*, https://merics.org/sites/default/files/2025-07/MERICS%20Report-AI_Stack_final.pdf [access: 28.08.2025].

Chen Z., Zhong L., 新时代下军民深度融合的路径 [*The Path to Deep Integration of Military and Civilian Sectors in the New Era*], „中国军转民" [„Defense Industry Conversion in China"] 2025, no. 1.

Huang Q.,"中国制造*2025*":成就、趋势与开放发展 [„*Made in China 2025": Achievements, Trends, and Development*], „应用经济学评论" [„The Applied Economics Review"] 2025, no. 5.

Levesque G., *Commercialized Militarization: China's Military-Civil Fusion Strategy*, https://www.nbr.org/publication/commercialized-militarization-chinas-military-civil-fusion-strategy/ [access: 25.08.2025].

Manhas N.S., *China's Military-Civil Fusion from Mao to Xi: A Long Roadmap*, „Journal of Polity and Society" 2024, no. 1.

Nan H., *China's Military-Civil Fusion: A Challenge to the US Military-Industrial Complex?*, https://www.thinkchina.sg/technology/chinas-military-civil-fusion-challenge-us-military-industrial-complex [access: 25.08.2025].

Palmer A., *Unpacking China's Naval Buildup*, https://www.csis.org/analysis/unpacking-chinas-naval-buildup [access: 25.08.2025].

Palve S., *China's 5G-Powered Unmanned Army! PLA Bets On 1st Mobile 5G Station To Power Its Robots* &

Rubio M., *The World China Made "Made in China 2025" Nine Years Later*, https://www.americanrhetoric.com/speeches/PDFFiles/Marco-Rubio-The-World-China-Made.pdf [access: 25.08.2025].

UAVs In Warzone, https://www.eurasiantimes.com/chinas-5g-powered-unmanned-army-pla-bets-on-1st-mobile-5g-station-to-power-its-robots-uavs-in-warzone/ [access: 28.08.2025].

Uppal R., *High-Speed Rail (HSR) in Military Logistics: China Leads the Way*, https://idstch.com/geopolitics/high-speed-rail-hsr-in-military-logistics-china-leads-the-way/ [access: 29.08.2025].

White Paper on China's Industrial Development Trends for the Next 50 Years, https://img.frostchina.com/attachment/17560512/3dotWjbdTCLfXgWYp5mcSp.pdf [access: 28.08.2025].

Zhao Y. et al., *On-Orbit Space Technology Experiment and Verification Project Outlook of China's Tiangong Space Station*, „Space Sci Technol" 2023, no. 3.

Zhao Y., 新时代我国军民融合发展的战略举措探析, „现代商贸工业" [„Modern Business Trade Industry"] 2025, no. 15.

Julia Czajka
Academic Center For Strategic Analysis
ORCID: 0009-0000-6596-7069
j.czajka@akademia.mil.pl

Computer crime in the information society

Abstract

The development of new forms of communication and information exchange which use electronic and digital devices makes the problem of computer crime grow in importance. The advances in technology and electronics have made devices like computers, cellular phones, and the Internet available to the population. Although ICT (information communication technology) devices make everyday life easier, their operation generates a number of risks.

This paper focuses on computer crime in the face of the development of the information society. The main objective of the study discussed here was to determine the impact of computer crime on the information society. The classification and forms of computer crime, the methods used as a tool to prevent computer crime, and the strategies used to combat computer crime at international level were among the issues identified for the problem under study.

Key words

computer crime, information society, cyber threats, cybercrime, data protection and security

Introduction

The development of social and economic life depends on the ability to communicate and exchange information[1]. The second half of the twentieth

1 J. Radzimirski, *Społeczeństwo informacyjne*, [in:] *Informatyka ekonomiczna: podręcznik akademicki,* eds. S. Wrycza, Warszawa 2010, p. 470.

century saw the rise of importance of computer devices as communication media. They brought about a qualitative change as a new type of society emerged: a society based on information, where information is among the most valuable commodities; it affects economies and is decisive to their competitiveness. This new society based on information and its exchange is called the information society. Coined after the 1950s, the concept of information society identifies the advances in engineering, especially electronics and information communication technologies as key development drivers of the information society[2]. The first theoretical works from the USA and Japan concerning the information society were written in the 1960s and 1970s; the first ones from Europe, including Poland, appeared in the 1990s.

The official term "information society" was adopted at the 2005 World Summit on the Information Society (WSIS) in Tunis. According to the definition of information society, it has been established that it is a type of society in which everyone is allowed free access to create, receive, share and use information and knowledge, which contributes to economic, social, political and cultural development[3]. The foundation which the information society needs to function on are modern telecommunication networks, which should reach all citizens and be publicly available.

The development and sophistication of ICT is accompanied by a wide range of potential vulnerabilities that may imply security breaches of data or IT systems and infrastructure. One of the risks to users of ICT devices and systems is *computer crime*, which the International Criminal Police Organisation "INTERPOL" defines as "[...] criminal acts against computer systems and criminal acts committed using computers as crime tools"[4]. In turn, some researchers define „computer crime" as „any criminal activity in which the computer is either a tool or an object of attack"[5] or „a phenomenon of forensic science involving any criminal behaviour relevant to the functioning

2 Ibidem, p. 473.
3 Ibidem, p. 471.
4 *Charakterystyka przestępczości komputerowej*, http://przestepstwo-komputerowe.eprace.edu.pl/1081,Charakterystyka_przestepczosci_komputerowej.html#google_vignette [access: 26.12.2024].
5 K.J. Jakubski, *Przestępczość komputerowa – podział i definicja,* „Przegląd Kryminalistyki" 1997, no. 2, p. 31.

of electronic data processing, which directly harms the processed information, its carrier and circulation in computers and entire computer connection systems, as well as the computer hardware itself and the right to computer programs"[6]. Approaches to computer crime equally include a narrow and broad range of understanding; all of the definitions cited above apply to and include criminal acts using a computer as a tool or object of attack. When considering the problem of computer crime, it is worth mentioning its purpose, which is "the theft of data, unauthorised disclosure of information, sabotage of an IT system or other legally prohibited actions against the IT infrastructure of an organisation, company, individual, institution or an entire state"[7]. Note that it is not only individuals who can fall victim to computer crime; the victims can be groups, such as commercial companies, which can pose a threat to the national economy.

Research methods

The problem outlined above was decisive to this author's undertaking the research aimed to identify the key determinants of computer crime in the information society. The main problem was formulated as the following research question: 'How does computer crime affect the functioning of the information society?' Specific problems were formulated as the following questions to address the main problem:

1. What is the classification and forms of computer crime?
2. What are the methods of computer crime prevention?
3. What strategies exist to combat computer crime at the international level?

The subject of computer crime is important and worth addressing for several reasons. Firstly, the fundamental problem concerns the correlation between computer crime and the information society. In an age of evolving information and communication technologies, society is increasingly reliant on digital infrastructures in various spheres of daily functioning, both private and professional. This phenomenon provides benefits while generating

6 Ibidem, s. 31.

7 D. Filipek, *Co to jest przestępczość komputerowa?*, https://itcenter.pl/2023/10/31/co-to-jest-przestepczosc-komputerowa/ [access: 26.12.2024].

new risks related to computer crime. Awareness and understanding of this phenomenon and its consequences is essential to safe functioning in cyberspace. Secondly, computer crime is a serious threat to state security. Attacks on critical infrastructure, including financial and energy systems, can paralyse the entire state and stir public chaos. These arguments are the basis for justifying the high importance of the problem being addressed. It remains relevant in this day and essential to understand and counter one of the greatest modern challenges. Investigating computer crime in today's information society can contribute to structuring knowledge on the subject being addressed here. It can also raise awareness of the risks involved in the use of electronic or digital devices, as well as promote ethical and safe use of the latest technologies.

The research objective was achieved by applying a research method such as content analysis. This method builds on existing material that is the body of knowledge on a given issue, reflecting existing beliefs and opinions. Publications, scientific papers and content from selected websites and web portals were used in this paper.

Discussion and findings

Classification and forms of computer crime

Computer crime is a type of crime which the Polish criminal law qualifies as a typical economic crime[8]. As A. Adamski points out, "[...] being one of the latest types of criminal activity, it [computer crime] challenges the traditional criminal law system"[9]. The official website of the Podlaskie Province Police Command details the classification and types of computer crime (fraud) committed online (on the Internet), which are specified in the Polish Criminal Code of 1997[10]:

8 A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, p. 115.
9 Ibidem, s. 115.
10 Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, Dz. U. 1997, no. 88, ited 553, art. 267, 268, 268a, 269, 269a, 269b, 286, 287.

– illegal acquisition of information (hacking);
– covert computer monitoring and data capturing (sniffing);
– computer sabotage;
– computer espionage;
– malicious software (malware) distribution and software cracking;
– hacking tools;
– phishing[11].

Illegal acquisition of information, known as *hacking*, is the use of remote techniques and tools to gain unauthorised access to computer systems, networks or data. The activity means hacking into someone else's computer or mobile device (a phone or tablet) to steal data. Its fixture is to include manipulation or exploitation of gaps in systems to steal data, interrupt services, or initiate other actions. The most often motivation behind hacking is financial, political, social or educational. Its consequences include the possibility of corrupting or deleting information stored in the memory of a device or making it difficult for authorised personnel to access the data[12].

Covert computer monitoring and data capturing (sniffing) is defined as "illegal monitoring and data capturing by means of technical facilities, monitoring of networks with the intent of stealing data, spying on network activity and collecting information about users"[13]. Initially, sniffing was a tool used by network administrators to diagnose and analyse online link performance issues, but hackers quickly recognised the potential of this technique and began using it for illegal ends[14]. This type of activity uses special computer software to capture and analyse data. The objective of criminals committing sniffing is to extract confidential data for a financial gain or, by

11 *Rodzaje i kwalifikacja przestępstw komputerowych*, https://podlaska.policja.gov.pl/pod/policja-podlas/dzialania/przestepczosc-gospodar/struktura-wydzialu/zespol-iii/rodzaje-i-kwalifikacja/28410,Rodzaje-i-kwalifikacja-przestepstw-komputerowych.html [access: 26.12.2024].

12 *Hacking*, https://www.comcert.pl/slownik/hacking/ [access: 26.12.2024]; *Czym jest hacking?*, https://conselion.pl/czym-jest-hacking-komputerowy/ [access: 26.12.2024].

13 *Kształtowanie się cyberprzestępczości*, https://gazeta.policja.pl/997/numery-specjalne/specjalne-gazeta-policy/gazeta-policyjna-nr-2-s/212264,Ksztaltowanie-sie-cyberprzestepczosci.html [access: 26.12.2024].

14 *Podsłuch komputerowy*, https://cyberprzestepczosc.info/podsluch-komputerowy/ [access: 26.12.2024].

tracking a user's online activity, to act against individuals, violating the human right to privacy.

Computer sabotage is an action with the objective of disrupting or blocking the operation of a computer system. The main subject of protection in this criminal act is IT data of major importance for state defence; it can be, for example, operational data of the Armed Forces, information concerning critical infrastructure, or data concerning citizens, like personal data. Computer sabotage consists of modifying data without authorization, violating the integrity of the attacked system, destroying, corrupting, deleting or altering computer data of major importance to national defence, communication security, or the functioning of the government, another state agency or a central or local government institution. The methods most often used by criminals carrying out computer sabotage include: computer viruses, worms, logic bombs, denial of service attacks, unauthorised modification of information, scanning of information or unauthorised access to or use of information[15].

Computer espionage is a form of intelligence operations that is based on the acquisition of confidential data and its transmission to a specific intelligence service via computer networks. This presupposes, first and foremost, that computer espionage is an action in favour of another country[16]. Computer espionage is similar to traditional espionage in many ways. It is characterised by the secrecy of the operation (masking the spy as effectively and for as long as possible), operating in conspiracy (under the pretext of legitimate activity), acquisition of classified information and transmitting it in various forms through computer networks.

Distribution of malware (malicious software) and cracking are crimes which consist in breaching or defeating security features of the exploited software. There is distinction between network cracking (defeating the security features of computer systems) and software cracking (bypassing or removing exploited software-based barriers)[17]. When a device is infected with malware,

15 A. Warchoł, *Sabotaż komputerowy*, https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/2020/03/12/sabotaz-komputerowy/ [access: 26.12.2024].

16 *Szpiegostwo komputerowe*, http://pandf.wex.pl/szpiegostwo.html [access: 26.12.2024].

17 *Przestępstwa komputerowe*, https://informaticalegis.com/uslugi/przestepstwa-komputerowe/ [access: 26.12.2024].

unauthorised access, data attacks or device freezing are possible. The intent of criminals who commit cracking is to profit from acquired credentials, for example by cracking banking services, to collect personal data for sale or to extort money.

Delving into computer crime, the typical hacking tools used by cyber criminals are worth mentioning. They help to exploit security gaps in systems and networks. These tools include Nmap (for network mapping), Wireshark, Metasploit, John the Ripper, Burp Suite, Aircrack-ng or Kali Linux[18]. While they can be used by criminals, they are common and ethical tools of security professionals, for example, to close security gaps in their own systems.

The final category of computer crime is phishing, a type of attack based on email or cellular text messages (SMS). The latest data from a report by NASK's CSIRT (Cyber-Security Incident Response Team) reveals that the organisation received nearly 96,000 reports of phishing on Polish networks during 2023[19]. The perpetrators of phishing attacks usually want to deceive the victim or cause the victim to take action as the criminals intended. The most common way this happens is by impersonating parcel couriers, government agencies, telecom operators or even friends in an attempt to phish for login details, social media credentials or even bank account credentials. As pointed out on the Polish government's official website, gov.pl, fraudsters have been increasingly operating via instant messaging and social networks, where an example is the "BLIK scam"[20]. Phishing messages are characterised by a high degree of authenticity. Cyber criminals are careful to prepare such messages with precision, so that they appear to be as real as possible, while they are actually fake and pose a high risk (through infected links they can feature, for example).

An increasingly popular type of computer crime is spoofing[21]. This is a type of attack in which a criminal can impersonate a bank, a government agency

18 *Najpopularniejsze narzędzia hakerskie*, https://akademiawywiadu.pl/najpopularniejsze-narzedzia-hakerskie/ [access: 26.12.2024].

19 *Raport roczny z działalności CERT Polska 2023*, https://cert.pl/uploads/docs/Raport_CP_2023.pdf#page=87 [access: 26.12.2024].

20 *Czym jest PHISHING i jak nie dać się nabrać na podejrzane wiadomości e-mail oraz SMS-y?*, https://www.gov.pl/web/baza-wiedzy/czym-jest-phishing-i-jak-nie-dac-sie-nabrac-na-podejrzane-widomosci-e-mail-oraz-sms-y [access: 26.12.2024].

21 *Czym jest spoofing? Jak go rozpoznać i nie dać się nabrać?*, https://www.gov.pl/web/baza-wiedzy/czym-jest-spoofing-jak-go-rozpoznac-i-nie-dac-sie-nabrac [access: 26.12.2024].

or official, or even another individual, in order to obtain the victim's data or money by deception. Fraudsters can impersonate not only an email address or phone number, but also an IP address (the address of the device connected to a computer network).

The catalogue of risks discussed here refers to attacks with the intent of stealing data; these activities are often financially motivated. Computer crimes also include attacks on infrastructure and cyberspace. These include cryptojacking (the unauthorised use of another person's computer to mine cryptocurrencies), hybrid attacks (particularly dangerous attacks that target state security and involve threats to critical infrastructure, public agencies or economic institutions), or DoS (Denial of Service) and DDoS. (Distributed Denial of Service) attacks that overload a system, network or website by generating large volumes of network traffic, which make the attacked systems or services unavailable to users.

Computer crime, due to its dynamic evolution and multifaceted nature, represents a significant challenge for modern users, entire states and systems. The classification discussed here includes hacking, sniffing, computer sabotage and espionage, cracking, phishing, and spoofing. Although each of the listed crimes is characterised by different methods of action, they share the same overall goal, which is to steal data and gain unauthorised access to information. The increase in the number of attacks, such as phishing and spoofing, suggests a growing threat to data security and privacy, especially in the context of the increasingly popular use of new technologies and instant messaging. Computer crime requires continuous prevention and the application of systemic solutions adapted to the changing realities of the digital world.

Methods of computer crime prevention

Digital attacks are on the rise and can affect any computer user. According to projections by the Council of the European Union, as many as 41 billion devices worldwide will be connected to the Internet of Things in 2025 and, as a consequence, cyber attacks and cybercrime will become more frequent

– and more sophisticated[22]. It is likely that the scale of the problem will grow, which is why awareness of the risks, possible prevention and vigilance, as well as knowledge of methods to prevent computer crime, is so important.

According to a model proposed by cybercrime prevention specialists, methods to prevent digital attacks include four stages:

1) prevention;
2) preparation;
3) response;
4) recovery[23].

The first two stages (prevention and preparation) mean preparing the IT infrastructure in such a way as to make a potential attack as difficult as possible. They include the secure connection of users' computers, including the use of anti-virus software and dedicated platforms that counter potential threats in real time. Response means decisions made in the face of an actual attack, including the victim's response to e.g. the issue of ransom. The last stage (recovery) is a kind of test for the performance of backup solutions and the recovery of the systems' infrastructure to a state of continued operability[24].

The main axis of protection against cybercriminal activity proposed by some experts is the development and implementation of IT security policies and procedures for information system management. An effective solution to prevent loss of access to information is to make regular backups (they are data backups)[25]. Continued education and awareness-raising of users on IT security also remains important.

Concerning individual methods of protection against computer crime, some sources stress the importance of cyber maturity[26]. Cyber maturity is about extreme caution and vigilance during use of digital devices and the Internet. It is recommended to avoid suspicious websites that can intercept

22 *Cyberbezpieczeństwo: jak UE radzi sobie z cyberzagrożeniami*, https://www.consilium.europa.eu/pl/policies/cybersecurity/ [access: 26.12.2024].
23 A. Kostrzewa, *Zapobieganie cyberprzestępczości*, https://mitsmr.pl/b/zapobieganie-cyberprzestepczosci/PLZjzYpX3 [access: 26.12.2024].
24 Ibidem.
25 D. Filipek, op. cit.
26 A. Kostrzewa, op. cit.

data, to secure accounts with strong passwords or use additional (multi-factor) verification methods, and to use anti-virus and firewall software[27].

Strategies of combating computer crime at the international level

As mentioned, cybercrime, including computer crime, is a growing problem in an increasingly digital world. In addition to improving self-awareness about the risks of cybercrime, states and international institutions like the European Union are constantly working at national and international levels to increase the safety on the Internet and of computer use. Processes are underway at European level to strengthen EU-wide resilience to illegal cyber operations. European cybersecurity measures implemented by the European Union Cyber-Security Agency and CERT-EU (Computer Emergency Response Team for EU institutions, offices and agencies) include tracking malicious activities and ensuring education and awareness among citizens and businesses about computer threats and incidents[28]. The institutions of the European Union financially support efforts to ensure and enhance online security, given the important role of the security of networked systems and services in society.

In addition to the measures taken at the European level, regulations and papers on cybercrime exist on the international tier that have been adopted by members of the United Nations. They include the UN Convention against Transnational Organised Crime (UNTOC) of 15 November 2000, the pages of which specify standards for combating organised crime, including criminal acts committed using computer and telecommunications networks[29]. The UNTOC and other UN resolutions on cybercrime are legal instruments in the international system that can help fighting computer crime and foster a coherent approach among the UN member states.

27 M. Budka, C*zym jest cyberprzestępczość i jak się przed nią bronić?*, https://www.money.pl/gospodarka/czym-jest-cyberprzestepczosc-i-jak-sie-przed-nia-bronic-6743245515295296a.html [access: 26.12.2024].

28 *Jak chronić się przed cyberprzestępczością*, https://www.europarl.europa.eu/topics/pl/article/20200327STO76003/jak-chronic-sie-przed-cyberprzestepczoscia [access: 26.12.2024].

29 J. Wrona, *Cyberprzestrzeń a prawo międzynarodowe: status quo i perspektywy*, Białystok 2017, p. 159–160.

Conclusion

A review of publications and sources on computer crime reveals that it represents one of the most serious challenges of the information society and has a significant impact on it. With humans operating in an environment based on modern information communication technologies and systems, the catalogue of risks entailed by their use is obviously expanding. The evolution of increasingly sophisticated forms of online attacks spurs a growing awareness of the landscape of cyber risks and the opportunities to prevent and combat them. As indicated in this work, computer attacks such as hacking, phishing or sniffing share the common goal of gaining unauthorised access to data or information resources, which can lead to financial losses, breach of privacy and even threats to the critical infrastructure of entire countries. Methods of computer crime prevention from the standpoint of the individual user were indicated, stressing the role of education, public awareness and systemic solutions in the fight against cyber threats; European strategies to combat computer crime were identified. The conclusions of this work can contribute to raising awareness of the risks and promoting responsible and ethical use of technology.

Bibliography

Adamski A., *Prawo karne komputerowe*, Warszawa 2000.

Budka M., C*zym jest cyberprzestępczość i jak się przed nią bronić?*, https://www.money.pl/gospodarka/czym-jest-cyberprzestepczosc-i-jak-sie-przed-nia-bronic-6743245515295296a.html [access: 26.12.2024].

Charakterystyka przestępczości komputerowej, http://przestepstwo-komputerowe.eprace.edu.pl/1081,Charakterystyka_przestepczosci_komputerowej.html#google_vignette [access: 26.12.2024].

Cyberbezpieczeństwo: jak UE radzi sobie z cyberzagrożeniami, https://www.consilium.europa.eu/pl/policies/cybersecurity/ [access: 26.12.2024].

Cyberbezpieczeństwo: jak UE radzi sobie z cyberzagrożeniami, https://www.consilium.europa.eu/pl/policies/cybersecurity/ [access: 26.12.2024].

Czym jest hacking?, https://conselion.pl/czym-jest-hacking-komputerowy/ [access: 26.12.2024].

Czym jest PHISHING i jak nie dać się nabrać na podejrzane wiadomości e-mail oraz SMS-y?, https://www.gov.pl/web/baza-wiedzy/czym-jest-phishing-i-jak-nie-dac-sie-nabrac-na-podejrzane-widomosci-e-mail-oraz-sms-y [access: 26.12.2024].

Czym jest spoofing? Jak go rozpoznać i nie dać się nabrać?, https://www.gov.pl/web/baza-wiedzy/czym-jest-spoofing-jak-go-rozpoznac-i-nie-dac-sie-nabrac [access: 26.12.2024].

Filipek D., *Co to jest przestępczość komputerowa?*, https://itcenter.pl/2023/10/31/co-to-jest-przestepczosc-komputerowa/ [access: 26.12.2024].

Hacking, https://www.comcert.pl/slownik/hacking/ [access: 26.12.2024].

Jak chronić się przed cyberprzestępczością, https://www.europarl.europa.eu/topics/pl/article/20200327STO76003/jak-chronic-sie-przed-cyberprzestepczoscia [access: 26.12.2024].

Jakubski K.J., *Przestępczość komputerowa – podział i definicja,* „Przegląd Kryminalistyki" 1997, no. 2.

Kostrzewa A., *Zapobieganie cyberprzestępczości*, https://mitsmr.pl/b/zapobieganie-cyberprzestepczosci/PLZjzYpX3 [access: 26.12.2024].

Kształtowanie się cyberprzestępczości, https://gazeta.policja.pl/997/numery-specjalne/specjalne-gazeta-policy/gazeta-policyjna-nr-2-s/212264,Ksztaltowanie-sie-cyberprzestepczosci.html [access: 26.12.2024].

Najpopularniejsze narzędzia hakerskie, https://akademiawywiadu.pl/najpopularniejsze-narzedzia-hakerskie/ [access: 26.12.2024].

Podsłuch komputerowy, https://cyberprzestepczosc.info/podsluch-komputerowy/ [access: 26.12.2024].

Przestępstwa komputerowe, https://informaticalegis.com/uslugi/przestepstwa-komputerowe/ [access: 26.12.2024].

Radzimirski J., *Społeczeństwo informacyjne*, [in:] *Informatyka ekonomiczna: podręcznik akademicki*, eds. S. Wrycza, Warszawa 2010.

Raport roczny z działalności CERT Polska 2023, https://cert.pl/uploads/docs/Raport_CP_2023.pdf#page=87 [access: 26.12.2024].

Rodzaje i kwalifikacja przestępstw komputerowych, https://podlaska.policja.gov.pl/pod/policja-podlas/dzialania/przestepczosc-gospodar/struktura-wydzialu/zespol-iii/rodzaje-i-kwalifikacja/28410,Rodzaje-i-kwalifikacja-przestepstw-komputerowych.html [access: 26.12.2024].

Szpiegostwo komputerowe, http://pandf.wex.pl/szpiegostwo.html [access: 26.12.2024].

Warchoł A., *Sabotaż komputerowy*, https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/2020/03/12/sabotaz-komputerowy/ [access: 26.12.2024].

Wrona J., *Cyberprzestrzeń a prawo międzynarodowe: status quo i perspektywy*, Białystok 2017.

Lech Majewski
Academic Centre for Strategic Analysis
War Studies University, Warsaw
l.majewski@akademia.mil.pl

The Air Defence System of the Republic of Poland in the Era of Armed Forces Transformation

Abstract

The article analyses the evolving Air Defence System of the Republic of Poland as an integrated ecosystem of forces, assets, command structures and procedures designed to ensure the inviolability of national airspace and to protect the population, the Armed Forces and critical infrastructure from the full spectrum of airborne threats. Polish modernisation efforts are situated within a deteriorating European security environment and in light of recent conflicts – above all the war in Ukraine – which have demonstrated the operational salience of ballistic and cruise missiles, long-range stand-off weapons and the mass employment of unmanned systems. Against this background, the article examines the layered architecture of PL ADS, including the Wisła, Narew and Pilica/Pilica+ programmes, very-short-range systems (Grom, Piorun, Poprad) and an emerging reconnaissance and strike layer based on drones, all integrated through the network-centric Integrated Battle Command System (IBCS) and an expanded radar and radiotechnical component.

Particular attention is devoted to ensuring interoperability with NATO's Integrated Air and Missile Defence (IAMD) posture and to European initiatives such as the emerging missile shield and associated financial instruments (EIB loans, EU funds, SAFE). The author highlights the strategic importance of integrating fifth-generation F-35 aircraft with ground-based air and missile defence, as well as the parallel development of air-to-air refuelling

capability, airborne early warning platforms and a national satellite programme to secure information superiority. On the basis of current procurement decisions, the state of implementation of key programmes and operational lessons from Ukraine, the article identifies major shortfalls: an insufficient scale of C-UAS capabilities, delays in integrating Wisła and Narew, legacy systems that are technologically obsolete, limited interoperability at the operational level and an underexploited potential for industrial participation and technology transfer.

The article concludes that the transformation of Poland's air defence is a long-term, capital-intensive process whose success will depend on coherent sequencing: building a genuinely multi-layered architecture, prioritising missile defence and C-UAS, investing in space and AI-enabled network-centric C2, and deepening European defence cooperation. Full readiness and effective interoperability of PL ADS – understood as a credible pillar of deterrence and defence on NATO's eastern flank – appear attainable only in the early 2030s, provided that high levels of investment are sustained and the identified gaps are systematically addressed.

Key words

air defence system, air and missile defence, Republic of Poland, Narew programme, F-35 integration, unmanned aerial systems (UAS), counter-UAS (C-UAS), network-centric command and control (C2/IBCS), NATO Integrated Air and Missile Defence (IAMD), European missile shield

Introduction

The Air Defence System of the Republic of Poland (PL ADS) is understood here as the integrated set of forces, assets, command arrangements and procedures organised to assure the inviolability of national airspace and to safeguard the population, the Armed Forces and critical functions of the state from the full spectrum of airborne threats. In practical terms, this encompasses early warning and air surveillance, battle management, command, control, and communications; kinetic and non-kinetic effectors; and supporting logistics, training, and infrastructure. Its immediate tasks are to provide persistent coverage for key political-administrative centres, military installations, defence-industrial nodes and critical infrastructure; to deny or disrupt hostile airborne reconnaissance and strike; and, when ordered, to contribute to the attainment of air superiority at the operational and - where feasible - strategic levels. In joint and combined operations, PL ADS must deliver responsive air

cover and fire support to other branches of the Armed Forces and, by shaping the air environment, facilitate the isolation of designated areas of operations.

A deteriorated European security environment and the demonstrated salience of air and missile threats in recent conflicts define the strategic context for Poland's air defence. Adversary capabilities now span legacy manned aviation, increasingly precise ground-launched ballistic and cruise missiles, long-range air-launched stand-off weapons, as well as a rapidly proliferating ecosystem of uncrewed systems – from massed, expendable first-person-view (FPV) drones to larger reusable platforms. These developments compress warning timelines, complicate attribution and saturate traditional point-defence architectures. Accordingly, the Polish approach emphasises a multi-layered, network-centric design that combines medium-range area defence, short-range and very-short-range components, and a growing counter-UAS portfolio, all fused by modern battle-management systems and underpinned by resilient communications and electromagnetic spectrum discipline.

Institutionally, PL ADS forms a critical component of the state defence system and is designed to be interoperable with NATO's Integrated Air and Missile Defence posture. In peacetime, round-the-clock duty provides continuous surveillance, identification and air policing, with defined transitions to heightened readiness or wartime rules of engagement. Responsibilities are apportioned between the Operational Commander (assuring day-to-day functioning and operational control) and the General Commander (force generation, preparation and allocation of forces and assets). This dual structure is codified in ministerial decisions and implementing instructions. It is complemented by legal and procedural arrangements governing cooperation with allied forces operating in or above Polish territory.

From a capability perspective, the system under construction is explicitly layered. At the upper tier, medium-range effectors (e.g., the Wisła segment) provide area defence against ballistic and aerodynamic threats. At the lower tiers, the Narew and Pilica/Pilica+ segments deliver short- and very-short-range defence of manoeuvre forces and key points, while indigenous MANPADS and mobile launchers extend coverage and mobility at the tactical edge. Equally decisive are the enablers: modern 3D surveillance radars, passive location systems, height-finding sensors, airborne early warning contributions, and a battle management/command system capable of sensor-to-shooter

pairing across services and, where mandated, across allied formations. The introduction of fifth-generation combat aircraft will further expand the sensor and shooter portfolio, provided that air-to-air refuelling, hardened basing and secure datalinks mature apace.

This article proceeds from the premise that air defence is an ecosystem, not a single programme. It examines (I) the governance and legal framework that anchors PL ADS, (II) the current and planned composition of its layered architecture, (III) the sensor and command-and-control backbone required for genuine network-centric operations, (IV) the international setting – NATO interoperability and European initiatives – together with financing instruments, (V) the integration of fifth-generation air power with ground-based defence, and (VI) the implications of emerging technologies and recent operational lessons, particularly in the counter-UAS domain. It concludes by identifying priority gaps and recommending sequencing choices that would accelerate the transition from disparate acquisitions to a coherent, resilient and sustainable Air and Missile Defence posture fit for the next decade.

Architecture and Governance

The Air Defence System of the Republic of Poland constitutes a crucial component of the state's defence system and should be compatible with NATO's air defence architecture. In peacetime, round-the-clock combat duty is maintained within the system. Responsibility for ensuring the system's functioning lies with the Operational Commander of the Branches of the Armed Forces. Responsibility for the preparation and allocation of forces and assets to carry out tasks rests with the General Commander of the Branches of the Armed Forces. The detailed rules governing the organisation and performance of combat duty within Poland's air defence system are set out in decisions of the Ministry of National Defence and in the „Instruction on the Organisation and Performance of Combat Duty in the Air Defence System".

Capability Layers and Effectors

In cooperation with the United States, the United Kingdom and the European Union, Poland is building a multi-layered air defence system. It has been undergoing systematic modernisation for many years, and this process has accelerated markedly since the outbreak of the war in Ukraine. Contracts have been signed for the procurement of the Patriot system and of the Narew system. 360-degree radars – an innovation – will be introduced. We are implementing the Integrated Battle Command System (IBCS), the world's most advanced command and control system, which provides network-centric capabilities. The Patriots will be integrated into a single network together with the Narew system's i-Launchers. In addition, artillery rocket launchers will be connected to this network. The 37th Air Defence Missile Squadron achieved Initial Operational Capability (IOC) in December 2024. In September 2025, the first live missile firing from a Polish Patriot battery was conducted at the Ustka training range—an essential step towards Full Operational Capability (FOC) of the system. Live-fire exercises have also been conducted with the "Small Narew". The first Patriot batteries are already operational, and the system is being expanded. The introduction of a multi-channel system into the air-defence troops can already be described as a revolution. We have completed tests of the Pilica+ system at the Ustka range, where its capabilities were verified. These tests were conducted against real targets simulating airborne means of attack. At the current stage, the functionality of Pilica+ is promising. The first validated and tested Pilica+ batteries are scheduled for delivery next year. It must, however, be remembered that building an integrated air and missile defence system – including its financing – is a highly demanding, long-term and costly process. At present, funding is provided from the Ministry of National Defence budget, the Armed Forces Support Fund, including foreign financial instruments (e.g., Foreign Military Financing – FMF), as well as resources obtained from the European Union.

In the near future, the F-35 aircraft will also operate within the Air Defence System. Polish pilots are currently training on them in the United States, and in 2026, both the aircraft and the trained pilots will be redeployed to Poland.

The air defence system being developed in Poland is designed to protect three tiers. The first – Wisła – comprises Patriot missile launchers with

a range of up to 100 kilometres. The second – batteries under the Narew programme – are equipped, inter alia, with CAMM-ER missiles with a range of 45 kilometres. The third – lowest tier is the Pilica programme, under which Poland will purchase over 20 batteries equipped with CAMM missiles with a 25-kilometre range. We also possess Polish short-range man-portable air defence systems (MANPADS) of the Grom and Piorun types (which occupy the lowest level of this architecture), launched from shoulder-fired launchers. Mesko S.A., a company within the Polish Armaments Group, had delivered approximately 3,000 missiles by February 2025. This system is in active use in Ukraine. Another element in this architecture is the self-propelled Poprad surface-to-air missile system from PIT-Radwar. The system is mobile and equipped with a turret comprising four launchers and two cameras – daylight and night – along with a rangefinder. Poprad can perform tasks in two modes. The first entails integrating the vehicle within the broader air defence system, from which the crew receives orders and target designations. The second is autonomous operation, in which the crew independently selects the sector of the sky. It employs Grom and Piorun missiles. The contract was signed in 2015. A total of 79 systems have been delivered to the Polish Armed Forces, including to the 8th Koszalin Air Defence Regiment and the 12th and 17th Mechanised Brigades.

Poland has also ordered MQ-9 Reaper military uncrewed aerial vehicles produced by the American company General Atomics. The procurement documentation was signed on December 12, 2024, with a value of approximately USD 310 million. Deliveries to Poland are scheduled for the first quarter of 2027. We possess a Coastal Missile Unit (two missile squadrons). Contracts have been signed for the manufacture and delivery of two additional CMUs. In 2016 and 2019, the CMU conducted live-fire exercises at a range in Norway. We are building a Polish satellite programme and will also form part of the European missile shield.

Another crucial element of the Air Defence System is the radiotechnical troops, whose core is the 3rd Radiotechnical Brigade (3rd Radiotechnical Brigade, 3BRt). Among the most modern radar stations in service with the Brigade's units – forming the equipment of radar posts – are the NUR-12M and RAT-31DL sets, the mobile three-coordinate medium-range radar stations NUR-15 and NUR-15M, and the mobile radar altimeters NUR-41. Orders

have been placed for Bystra radars (for Pilica batteries), P-18PL early-warning radars, and the Passive Location System. Awaiting execution contracts are the long-range RDL-45 Warta radar and the Sajna multifunction fire-control radar. Warta can detect objects at distances of up to 470 km. Sajna is a precision radar station used to guide surface-to-air missiles. Their acquisition will fill the remaining critical gaps in Poland's multi-layered air and missile defence.

Maritime defence will be served by the Miecznik programme, which is still in its early stages. Every effort should be made to bring this programme to a successful conclusion. This is feasible, but it requires continuous financing. Under the programme, three frigates are to be constructed – one prototype and two serial-production vessels – equipped with CAMM missile launchers.

Sensors and Command-and-Control: International Context and Financing

Another crucial element of the Air Defence System is the radiotechnical troops, whose core is the 3rd Radiotechnical Brigade (3rd Radiotechnical Brigade, 3BRt). Among the most modern radar stations in service with the Brigade's units – forming the equipment of radar posts – are the NUR-12M and RAT-31DL sets, the mobile three-coordinate medium-range radar stations NUR-15 and NUR-15M, and the mobile radar altimeters NUR-41. Orders have been placed for Bystra radars (for Pilica batteries), P-18PL early-warning radars, and the Passive Location System. Awaiting execution contracts are the long-range RDL-45 Warta radar and the Sajna multifunction fire-control radar. Warta can detect objects at distances of up to 470 km. Sajna is a precision radar station used to guide surface-to-air missiles. Their acquisition will fill the remaining critical gaps in Poland's multi-layered air and missile defence.

In October 2022, during the NATO Defence Ministers' Summit, fifteen states signed a letter of intent in Brussels concerning the construction of the European Sky Shield Initiative - Poland was not among them. Germany launched the coalition of states wishing to strengthen Europe's air defence in autumn 2022 and now comprises over twenty countries. However, in April 2024, Prime Minister Donald Tusk announced that Poland would join the European initiative to create a missile shield: "A missile shield, to be built not only on our own but within a European initiative, is a cornerstone of Poland's

deterrence and defence plan," the Prime Minister stated. Subsequently, in June 2024, he added: "A safe sky over Europe, a safe sky over Poland, is becoming before our eyes a priority for the entire EU. We have grounds for moderate but real satisfaction for now. I am very pleased". The point is to ensure that what we introduce is compatible with what the Germans, Czechs and Slovaks possess. Only then can we interoperate – for example, using the same missiles across different types of launchers. On our own, we are not able to secure ourselves against an attack by airborne means from the Russian Federation – there would be too many of them. Hence, both resources and forces must be mobilised to repel such an attack, and this can be achieved only collectively.

The Polish government has signed an agreement with the European Investment Bank under which it will receive a loan of €300 million. The funds will be allocated to the development of Poland's satellite programme, which forms part of the European missile shield.

In March 2025, the President of the European Commission, Ursula von der Leyen, announced a plan to rearm Europe, intended to mobilise up to €800 billion for defence. The plan includes a loan package of €150 billion, among other things, for air defence. Meanwhile, on June 9, 2025, in London, NATO Secretary General Mark Rutte called on Allied countries to quadruple their spending on air defence, AFP reported. He emphasised that the danger would not disappear even once the war in Ukraine ends: "[We] must have more forces and capabilities in order to implement our defence plans fully. We see how Russia strikes Ukraine from the air. Therefore, we will reinforce the shield that protects our skies".

Poland will be the largest beneficiary of European funds for defence and security. Of the €150 billion earmarked for this purpose under the new programme, Poland will receive €43.7 billion (September 2025). This is the most considerable amount allocated to a member state, the European Commission announced. Nineteen member states submitted applications to the Commission. "This decision is a great success for Poland and a guarantee of continued investment in our security and the development of our defence industry. We aim to utilise the funds from this fund to enhance the key capabilities of the Polish Armed Forces, including air and missile defence, artillery systems, ammunition procurement, drones, and counter-drone systems. It will also support strategic capabilities, the protection of critical

infrastructure, military mobility and cyberspace", said Deputy Prime Minister Władysław Kosiniak-Kamysz.

F-35 Integration: Roles, Enablers, Gaps

In March 2025, at the 3rd Air Defence Missile Brigade in Sochaczew, a Polish-American intergovernmental agreement was signed for the implementation of Phase II of the Wisła programme, valued at almost USD 2 billion. The agreement provides for the further development of air-defence systems, logistics systems and training equipment for the Patriot batteries already in service. This represents a further step toward building a multi-layered missile defence system and strengthening the strategic alliance with the United States. Deliveries of two additional batteries are scheduled to take place at the turn of 2026 and 2027, with completion of the deliveries planned for 2029. Despite the many important decisions taken – especially recently – regarding the Wisła and Narew programmes, the modernisation of the air-defence forces is still ongoing and remains unfinished. Current plans for the modernisation of air and missile defence envisage, above all, the acquisition of eight medium-range Wisła batteries and twenty-three short-range Narew batteries. According to this plan, two medium-range Patriot batteries have been acquired to date, which will only partially satisfy the Armed Forces' needs for short- and medium-range systems. In 2018, Poland purchased two Patriot batteries for USD 4.75 billion. The price – which differs substantially from the figure cited in some Western media (around USD 1 billion) – reflects the fact that these were not baseline sets. Each battery includes not one but two AN/MPQ-65 radars, eight M903 launchers (the standard is six), and we also purchased 208 of the most advanced PAC-3 MSE missiles. The transaction additionally covered integration of the systems with the Integrated Air and Missile Defence Battle Command System (IBCS).

Unfortunately, the implementation of Phase II of Wisła, which was to include the delivery of six further batteries, was postponed in 2019. It was only in 2023, at the defence fair in Kielce, that another contract was signed for the purchase of six systems. The package includes forty-eight M903 launchers, twelve GhostEye radars and PAC-3 MSE missiles. The price is USD 9.3 billion. Including the purchase of technology enabling domestic production of

components for the Patriot system (e.g., M903 launchers), Poland has so far invested USD 17.3 billion in American systems. These will constitute the main component of the Wisła programme within the modernisation of medium-range air defence to counter airborne means of attack such as medium-range ballistic missiles, guided missiles, aircraft and uncrewed aerial vehicles.

Under the Wisła programme, an American Patriot battery in its basic configuration costs around USD 1 billion and requires a crew of ninety. The set comprises an AN/MPQ-65 radar capable of detecting targets at distances exceeding 150 km, which can simultaneously track many targets and guide missiles towards them. The system's maximum range depends on the missile variant used. The PAC-3 MSE missile provides a fantastic range of 160 km, with a maximum altitude of 30 km.

For many years, Poland's ground-based air defence has still included obsolete surface-to-air missile (SAM) systems:

1. Short-range (up to 25 km) S-125 systems – modernised S-125 Newa sets purchased in 1974–86 and in service with air-defence units.

2. Short-range (up to 24 km) Kub SAM systems acquired in the mid-1970s, forming the core equipment of the Land Forces' air-defence regiments.

3. Self-propelled Osa SAM systems with a range of up to 10.5 km, purchased in 1984–1990 and likewise in service with the Land Forces' air-defence regiments.

These systems are based on Soviet technological solutions from the 1960s and 1970s and were partially modernised by the Polish defence industry. Technologically, they are now outdated and cannot counter all potential threats. Owing to their age and combat capabilities, they will have to be completely withdrawn from service in the near future.

The construction of the Armed Forces' Air Defence System should guarantee the acquisition of new technologies for Poland's industry. Access to maintenance and repair facilities, as well as the restoration of combat potential, should be critical, while also creating opportunities for potential export. The purchase price of new equipment – such as a launcher, tank, howitzer, aircraft, or missile – accounts for only a third of the total expenditure. The remaining two-thirds must be allocated to sustainment, modernisation, overhauls, adaptation of infrastructure to equipment operation and the creation of a support system for at least three, and even four, decades of service life. For

this reason, purchases of new armaments – worth hundreds of billions – must be judicious, transparent and intelligible.

For example, in January 2020, Poland signed a contract for the purchase of thirty-two F-35 aircraft for USD 4.6 billion. The first were to be handed over to Poland in 2024 (we received them in 2025 for the training of Polish pilots in the United States). They will achieve operational readiness four years later. They will replace the obsolete MiG-29 and Su-22 aircraft, which have been practically withdrawn from service.

The F-35 is indeed the latest – and, one may confidently say, the best – fifth-generation multirole aircraft available on the Western market. It was developed in collaboration with scientists from seven countries. Currently, over 1,230 F-35s are in service in twelve countries, and the type has accumulated over one million flight hours. The first F-35 took to the air in 2006, but its first basing in operational units occurred only in 2019 – at a US base in the United Arab Emirates. Two weeks later, the F-35 was used in its first combat mission, bombing ISIS tunnels. Outside the United States, the F-35 is in service with the air forces of the United Kingdom, Australia, Israel, Italy, Japan, the Netherlands, Canada, Belgium and Norway.

Polish F-35s are expected to achieve full operational capability by 2030. The aircraft will be able to perform a broad spectrum of tasks – not only air-to-air and air-to-surface/sea missions, but also reconnaissance, including radar (AESA), electronic, and electro-optical missions, utilising organic passive systems and all-aspect reconnaissance suites. While retaining low-observability features in a ground-attack configuration, the aircraft can alternatively carry two AARGM-ER anti-radiation missiles, the same number of JDAM bombs, or eight Small Diameter Bombs (SDB-I or SDB-II), together with two AIM-120 AMRAAMs for self-defence. The F-35 itself will engage only the most difficult and most important targets; other aircraft or branches of the armed forces will prosecute other targets. Therefore, the aircraft should be integrated into Poland's ground-based air and missile defence system. To this end, the IBCS battle-management system, introduced within Wisła and planned for Narew in the near future, is designed to cooperate with the F-35, even to the extent of enabling these fighters to serve as a "flying radar" for the air-defence system. Thanks to this, ground-based air-defence systems will be able to see further and select means of countering aerial targets more rationally.

Synchronising command systems will be a significant challenge for Polish and American forces and will undoubtedly require additional procurements.

The Armed Forces of the Republic of Poland are not yet fully prepared to operate in conjunction with the F-35. A key problem is the lack of air-to-air refuelling capability. This results from the decision taken by the United Right government in 2016 to withdraw Poland from the European MRTT programme. Analyses are currently underway in this area – no decision has been made. Prime Minister Donald Tusk publicly criticised the withdrawal from the programme. No new policy decision – either to return to the MRTT programme or to build national capabilities – has yet been taken. Air-to-air refuelling capabilities are considered by NATO to be in very short supply and should be developed, including in quantitative terms, to be fully usable in a crisis or conflict. Without air-to-air refuelling, the operational employment of F-35s and F-16s will be severely constrained.

Another area of concern regarding cooperation with the F-35 is the command system for Land Forces units. Information transmitted by the aircraft can support even the actions of a tank company or mechanised sub-units on the battlefield. Modernisation of communications within the Land Forces is currently far less advanced, and there is a need to take further appropriate decisions – for example, to standardise communications systems at the tactical level and to build a unified battle-management system.

Based on the available materials, it can be stated that the comprehensive logistical support for the aircraft and equipment provided by the contractor under the global support system, which is only scheduled to last until 2030, is too short, as it will end when the last aircraft is handed over to Poland. This conclusion is based on experience with operating the F-16.

The signed contract likewise does not provide for the construction of the infrastructure necessary for operating the aircraft. There is very little time to prepare and modernise the air bases. Depending on location, the costs of these works may, according to Ministry of National Defence estimates, amount to nearly PLN 2 billion.

For the revolution associated with introducing the F-35 into the Armed Forces' armament to materialise truly, a tremendous amount of work and further investment will be required, including in areas such as communications,

logistics, and the protection and defence of own forces. A separate issue is the training system and the procurement of armaments.

The Air Force requires two further squadrons of combat aircraft, and the F-35 – alongside air-superiority aircraft such as the Eurofighter and the F-15EX – may be among the leading candidates.

Irrespective of the above, doubts also concern the manner in which negotiations with the American side were conducted and, plainly speaking, what we managed to "win" during the purchase of the F-35 aircraft. Decisions on the acquisition of military equipment of such high value should be made based on a national consensus, as their effects will be long-term and will influence the decisions of subsequent governments. They were taken very quickly, and the entire procedure was completed in under a year, while foregoing a competitive tender and offset requirements – even though Lockheed Martin offered opportunities for technology transfer. When executing an order both so costly and so important, it is crucial to conduct an analysis addressing issues such as acquisition and operating costs, life-cycle costs, verification of requirements defined by the end-users, logistical and training needs, the need to build the requisite infrastructure, and, for example, risks that may arise at the delivery or operational stages.

Western states that purchase the F-35 do so via competitive tenders. For instance, Finland, Germany and Switzerland conducted comparative evaluations of multiple aircraft from different manufacturers. Based on such tenders, they additionally secured substantial investments in their economies and in new technologies. For example, Switzerland will pay CHF 6 billion for the F-35 aircraft, but the Americans are to invest CHF 2 billion in the country under offset arrangements. A similar situation exists in Germany.

In our case, it is unclear what compensation will be received for such enormous expenditure, or whether any will be received at all. Technology transfer, production in Poland, or the issue of long-term sustainment were, at the time of purchase, secondary matters. Real success can only be guaranteed by tangible technology transfer, the ability to leverage existing Polish solutions, the production of components in Poland, and securing the rights to develop the acquired equipment further. Moreover, a US government report dated September 23, 2023, states that the aircraft can perform missions in only just over half of cases. It is also expensive to produce and maintain. According to

US government estimates, by 2040, the costs of sustaining the F-35 fleet will be 79 per cent higher than those of its older-generation predecessors, the F-16 and F/A-18. From the outset, the F-35 has been relatively failure-prone and requires sophisticated maintenance, which has led to criticism. This does not, however, prevent the US government from planning to spend USD 1.7 trillion on the purchase, sustainment and repair of nearly 2,500 of these aircraft. The US government relies heavily on subcontractors, some of whom are located outside the country, thus limiting its decision-making latitude. There is also a shortage of spare parts and support equipment, causing repair delays. The report likewise identified delays in establishing workshops for conducting complex repairs. It should also be emphasised that the procurement process for the F-35 was not conducted transparently, which, given an order valued at over PLN 20 billion and operating costs that, over 40 years, may be estimated at a further c. PLN 50 billion – must be assessed particularly critically. The classification of the F-35 procurement and the abandonment of a competitive purchase significantly reduced the chances of obtaining a favourable offset offer.

To fully leverage the capabilities of the F-35, the Polish Air Force will need to undergo a profound transformation, including integration into the global logistics support system. This will represent a generational leap relative to the F-16 – not only technologically and operationally, but also financially.

Of course, the purchase of F-35 aircraft is an important step towards strengthening the Armed Forces' capabilities; however, without continued modernisation of ground-based air defence under the Wisła, Narew and Pilica programmes, it will not be possible to ensure the security of the air bases from which these aircraft will operate.

At the same time, it should be noted that the F-35 will not replace dedicated reconnaissance aircraft or operational- and tactical-class unmanned aerial systems, the acquisition of which has been planned under the Płomykówka, Zefir, and Gryf programmes, respectively.

Poland needs at least 160 multirole combat aircraft. At present, we have 47 F-16 fighters and 12 of the 48 ordered FA-50s (practically without armament). The FA-50's combat capabilities are minimal. Even supplementing these purchases with the 32 fifth-generation F-35s bought in 2020 will not deliver the required capability. We must decide to procure additional fighters.

Three proposals are under consideration: further F-35s (which would allow fleet unification), as well as aircraft intended for achieving air superiority – the F-15EX from the United States or the Eurofighter Typhoon from Europe.

Given the rules of the SAFE programme, it will not be easy to opt for American designs. Poland could, for example, acquire Eurofighters. These aircraft enable the attainment of air dominance. An advantage of the Eurofighter is the substantial technology transfer proposed by its manufacturer. Approximately 50 per cent of the costs associated with investing in Eurofighters could remain in Poland. This is an opportunity to enhance the capabilities of our aerospace industry.

To increase air defence capability, it is also necessary to acquire air-to-air refuelling aircraft, which are also produced in Europe. Poland could avail itself of Airbus's offer and purchase, for instance, A330 MRTT aircraft. Continuous control of the airspace should be provided by early-warning aircraft. Poland operates two Saab 340 AEW aircraft, which are considered outdated. This is a bridging solution, and further aircraft must be ordered. The Swedish Saab GlobalEye may be an attractive option. For both tanker aircraft and early-warning platforms – and given the critical nature of airborne threats – it would be prudent to purchase three to four such aircraft. Currently, we can rely on NATO-owned AWACS; however, possessing at least partial autonomy in this area would be highly valuable.

To fully exploit the capabilities of the F-35, it is also necessary to build an integrated system of air defence, reconnaissance, electronic warfare and air-to-surface strike, supported by modern network-centric command-and-control systems.

Moreover, the decision to purchase F-35 aircraft should not result in postponing other modernisation programmes such as Wisła, Narew, Płomykówka, the Zefir and Gryf UAV programmes, or those related to the acquisition of reconnaissance satellites, new electronic warfare (EW) assets, and further multirole combat aircraft geared towards achieving air superiority – all of which together will create a system enabling the full exploitation of the F-35's capabilities. Without building a modern air-defence system, fully leveraging the F-35 will be difficult, if not impossible. Consequently, the task of constructing a modern air-defence system should receive the highest priority in the modernisation process. Lacking such a system, in the event of

a conflict, the F-35s would be at risk of destruction while still on the ground, and the Air Force would be forced to redeploy them beyond the range of the potential adversary's aviation and rocket artillery, which in practice would mean relocating the aircraft to air bases outside the territory of Poland.

Another vital factor affecting the full utilisation of the air-defence system is the necessity of building a national space-based reconnaissance system. It should be a raison d'ětat for Poland to develop indigenous national satellite competencies. Space competencies ought to be among the key elements of air defence. Satellite information is becoming the foundation of the contemporary battlespace. Situational awareness on the battlefield is the condition that determines the effective use of the latest technologies and the combat potential of the Polish Armed Forces.

Within the Air Defence System, satellites provide early warning against missile attacks. Systems such as the American SBIRS (Space-Based Infrared System) detect ballistic-missile launches and track their trajectories. They also enable the coordination of defensive actions and the transmission of data to missile-defence systems. Poland should invest in satellite systems for detecting ballistic missiles and other threats originating in outer space. Such technologies are crucial for missile-defence systems and for rapid response to potential attacks. Systems like SBIRS (Space-Based Infrared System) could be integrated into Poland's air defence system. Poland should invest in satellite systems for detecting ballistic missiles and other space-based threats.

A notable example of foreign acquisition of space technologies is Israel, which, along with Italy, is developing the OPSAT-3000 satellite system. It will operate in conjunction with Italy's COSMO-SkyMed and utilise the combined use of radar and optical data. Further examples of the latest modernisation decisions in some countries include Israel again, which will become the first state in the world to employ laser weapons in air defence to counter aerial threats (artillery, rocket projectiles and UAVs). The Iron Beam system complements traditional air-defence systems. A good example is also the United Kingdom's DragonFire, Ukraine's Trident (Trójząb), and the US DEM-SHORAD.

In January 2021, work began in the United States on a pod enabling laser communications between various types of aircraft and geostationary satellites. Unlike traditional radio-frequency communications, this technology will operate more effectively in environments with electromagnetic interference.

The US is building a constellation of 150 communications satellites that will interconnect using laser beams. The Americans are already putting into practice the following principles of armed forces modernisation:

1. A networked (network-centric) command-and-control system, the idea of which is to connect everything with everything. The Air Force is, of course, the testbed.

2. Autonomous systems that cooperate with humans are being implemented at scale across all branches of the armed forces.

3. Artificial intelligence - which today is the key to data, and data is now the battlespace.

There is decreasing talk of tanks, aircraft, missiles, warships, or even satellites; rather, the focus is on networks, communications, data, and the potential of technology (artificial intelligence) that automates processes, anticipates future events, estimates risks, and proposes preventive actions. Nevertheless, do we all appreciate that this is the path to the future – that the true potential lies here, not merely in tanks or missiles; that no materiel, however cutting-edge on the modern battlefield, matters at all if it is not plugged into a highly resilient, high-throughput information network? The rapid development of information technologies has driven their application to operations in cyberspace, particularly to damage critical infrastructure (banks, energy, industrial facilities, or military infrastructure systems). All this increases the importance of non-contact operations, in which belligerents are beyond the reach of direct observation. In the short term, robotisation will lead to the complete autonomy of task execution by most combat systems.

A question thus arises: are the selected examples outlined above feasible, given our state's current economic potential, assuming we intend to meet the rapidly changing new requirements of the contemporary battlespace? One must bear in mind that we live in a period of revolutionary technological change – the Fourth Industrial Revolution – which, before our eyes, is transforming the world and our lives, and which also has a profound influence on the development of new weapons systems. One cannot prepare for the next war and achieve success by repeating established, previously employed patterns. Examples include lost wars by France, Egypt, Iran, Armenia, and, most recently – and all indications suggest – Russia.

In 2022, President Emmanuel Macron, speaking at a defence exhibition in Paris, stated that spending large sums to buy elsewhere is not a good idea – calling the defence industry a "sector of the future". In March 2021, UK Prime Minister Boris Johnson assessed that "cyber power is revolutionising the way we live and fight wars, much as air power did a hundred years ago". Michèle Flournoy, President Joe Biden's nominee for Secretary of Defence, said in her Congressional hearing the memorable words "megabits instead of megatons" (she was, of course, not selected). The Americans place digital technologies, autonomous and unmanned systems – working with crewed aircraft or manned vessels – and artificial intelligence at the top of their priorities. The Pentagon anticipates that in the coming decade, autonomous robots will become a primary instrument of warfare.

In Poland, there is a noticeable absence of joint projects with EU states akin to those pursued by Germany, Italy or France. Poland is arming as if it belonged to no alliance. Furthermore, the procurement process under our predecessors was not transparent. We have inherited a substantial debt that needs to be repaid. We bought the latest armaments [F-35s, HIMARS, Abrams tanks, Patriots (2014)], satellite imagery (France – electro-optical satellites), FA-50 aircraft, Korean tanks and self-propelled howitzers in the manner of Arab states, which can afford it and have vast billions they do not know how to spend.

For us, unless we produce it ourselves or participate in production, it will be unaffordable. Moreover, buying off-the-shelf armaments is very costly. The "spike" in armaments means that over PLN 100 billion could initially flow to Washington, and even more to Korea. The so-called "off-the-shelf purchases" have raised – and continue to raise – controversy, particularly when conducted without a tender allowing comparison of the merits of the weapons procured, without meaningful offset, and without opportunities for localisation and modernisation by the domestic industry.

Drones in the Air Defence System – the example of Ukraine

The war in Ukraine has become a war of drones – to such an extent that the United States, despite possessing the world's most advanced military and defence-industrial complex, has found itself lagging and unprepared to

produce rapidly large quantities of small, inexpensive drone systems. Although missiles, artillery and anti-tank munitions are indispensable, roughly 80 per cent of Kyiv's success in destroying targets derives from drones. The goal on the modern battlefield is for soldiers to treat drones as if they were their personal weapon, radio, night-vision goggles or grenade – simply part of their standard kit. Drones are now successfully replacing the forward observer who identifies targets for artillery fire or air support. Drones and new technologies provide a critical advantage to troops in harm's way. With the proliferation of drones on both sides, the battlefield has become paralysed. The area within a 15-mile radius of the front line is now considered a closed zone, because most drones can reach it and are capable of destroying even small groups of soldiers, halting vehicle movement, and preventing resupply or force rotation.

Ukraine's plan for 2025, according to President Zelensky, envisages producing almost five million drones of various types – twice as many as in 2024. Drones will undoubtedly provide valuable support, but they will not furnish full capabilities to defeat the adversary. In this context, NATO (including Poland) must ensure the development of its own counter-UAS means, while also maintaining the growth of classic instruments of warfare such as artillery and aviation, as well as space and electronic-warfare systems. Western states possess a military and technological advantage over Russia that Moscow cannot overcome. Although Russia has largely learned to defend itself against drones, it has not managed to develop methods for effectively countering guided cruise missiles, artillery munitions or bombs, or even GMLRS and ATACMS rockets.

As reported by The Times, the British Army is introducing a new military strategy, known as "20-40-40," aimed at reducing casualties among soldiers. This strategy, part of the periodically conducted Strategic Defence Review, focuses on integrating modern technologies with traditional heavy military equipment. Robots and drones are to complement heavy platforms. Under the "20-40-40" approach, units equipped with Challenger 3 tanks will employ loitering munitions ("kamikaze drones") and long-range missiles carried by robots – for example, THeMIS – in the initial phase of battle. In this scheme, inexpensive expendable drones and missiles are to constitute 40 per cent of the means of combat, while a further 40 per cent will be reusable drones, such as the MQ-9 Reaper, which are more costly and durable. Heavy equipment

can then enter terrain that has been prepared by fire. According to a source at the UK Ministry of Defence, the objective is to integrate heavy platforms with modern technologies to enhance the Army's effectiveness. Heavy equipment, such as tanks, will account for around 20 per cent of combat capability and will remain in the rear until the final stage of the battle - this is a sound example for our planners at the General Staff of the Polish Armed Forces.

In Poland, lessons from Ukraine are being analysed at a NATO institution established on February 17, 2025, in Bydgoszcz: the NATO-Ukraine Joint Analysis, Training and Education Centre (JATEC). "JATEC's task is to enhance the Ukrainian Armed Forces' ability to defend and deter, to strengthen NATO-Ukraine cooperation, and to analyse lessons from the war in Ukraine that will be factored into allied strategies". By contrast, Alex Wang – a 28-year-old American entrepreneur regarded in the AI sector as a visionary, a "prodigy," and a guru of artificial intelligence, who founded Scale AI at the age of 19, quickly becoming one of the world's youngest billionaires, and who is not an engineer and has not engaged in (and still does not engage in) the development of AI algorithms – goes further still and characterises the war of the future as follows.

It will not be mass – understood as the number of soldiers or combat platforms that determines success, but rather "agility," variability and tempo of action, even if our forces are smaller than the adversary's. "Thanks to AI agents" Wang writes, "battle plans will be formulated and adjusted in real time to exploit enemy weaknesses – from the first strike to decisive victory – before technologically inferior forces even realise that the game has begun".

What are AI Agents, to which Wang ascribes such significance? They are specialised programmes that automate and render autonomous the capacity to undertake independent actions in digital environments. In this case, we are dealing with solutions far more advanced than traditional chatbots that merely answer posed questions. AI agents are capable of perceiving their environment, processing information, making decisions, and executing tasks autonomously. Moreover, they communicate with one another and act proactively on behalf of their user. Because they operate based on machine learning, they can take and implement decisions without constant human supervision. They can function in complex environments owing to both their ability to learn from experience and to integrate information from diverse

sources. They also exhibit the ability to cooperate with other agents and IT systems, as well as respond rapidly to changing conditions. "You can define an AI Agent in one word: proactivity", said Enver Cetin, an AI expert at the global firm Experience Engineering Ciklum. "It refers to AI systems and models that can act autonomously to achieve goals without the need for constant human direction. An agentic AI system understands the user's goal or vision and the context of the problem it is trying to solve".

The foregoing examples clearly indicate the direction of further development of the modern battlespace - and the particular role within it of the Air Defence system, and within that, AI. They are important in the context of the accusations levelled at the Ministry of National Defence regarding the alleged disregard for Ukrainian lessons on the use of drones, and for the preparation of a Strategic Defence Review, which is already overdue. We do not intend to fight as in Ukraine; instead, by drawing appropriate conclusions from what has been achieved thus far, we are systematically preparing for the new technological challenges of the theatre of operations.

Current Shortfalls and Priority Actions

In sum, the most important problems affecting the functioning of the air-defence system include the following issues:

– Insufficient quantity of counter-UAS systems at an appropriate scale – the Polish Armed Forces do not yet possess effective systems to defeat drones, nor adequate protection of tanks against drone attacks, which poses a significant risk in the event of potential strikes. Delays in the development and training of drone forces, along with a lack of appropriate structures and specialists to operate modern technologies, weaken the ability to counter contemporary airborne threats;

– Imperfect air-defence architecture – despite the purchase of modern systems (e.g., Patriot under the Wisła programme), the system remains insufficiently integrated. It requires supplementation with early-warning assets, such as airborne early-warning aircraft and radar aerostats;

– Ongoing modernisation and integration of additional elements within air defence – Poland is fielding short- and medium-range systems (Pilica+, Mała Narew, Narew, Wisła), yet operational readiness is still being attained and

further investment is required, especially in the integration of communications and command;

– Procedural and tactical issues – effectiveness is constrained by peacetime rules and procedures that impede immediate response to threats such as low-flying cruise missiles. The risks associated with intercepting a missile over built-up areas lead to caution and delays in decision-making;

– Obsolescent anti-missile equipment and lack of area-defence capability – at present, Polish air-defence units operate predominantly in a point-defence mode, and full area defence remains a challenge for the future.

Poland is systematically modernising its air-defence system, but it still struggles with gaps in defence against drones and modern threats, a shortage of advanced early-warning systems, and procedural and integration problems that limit overall effectiveness.

Moreover:

The principal challenge in integrating Wisła and Narew is the lack of full financing, delays in signing and executing subsequent contracts, misalignment of command systems at the operational level, and the technical complexity of integrating diverse components with differing functions and technologies. There is insufficient funding and contract slippage – particularly for deliveries of IBCS command cabins, mobile communications nodes and support vehicles. Without a rapid contract signature, the integration and operation of the systems could be delayed by years;

Insufficient development of the operational-level command system – the current Dunaj system does not meet modern battlefield requirements and must be replaced or thoroughly modernised. A new operational-level air-defence management system is not yet in place;

Difficulties arise in integrating heterogeneous components and exchanging information across air-defence tiers – protocols such as Link 11B and Link 16 are in use. However, their level of integration is inadequate for the comprehensive employment of Wisła and Narew as a single, coherent system;

Delays in the delivery of key elements, such as fire-control radars (e.g., the Sajna radar for Narew), counter-UAS components (CUAS), and the development and fielding of new missiles (CAMM-MR and FCM);

Personnel and organisational challenges within the military and defence industry that affect the pace of implementation and the effectiveness of integration.

Coordination of Wisła and Narew within the IBCS framework aims to ensure their cooperation as a unified network. However, we are still far from achieving operational readiness.

As I have already emphasised, drones are playing an ever greater role on today's battlefield. Detecting and neutralising them requires entirely different means and tactics. In recent years, Poland has purchased air-defence equipment worth close to PLN 200 billion. In this way, we are preparing above all for full-scale war and for countering ballistic and cruise missiles. The challenge, however, may lie with much less sophisticated drones.

Funds made available to Poland under SAFE could be used to purchase additional counter-UAS systems. Requirements include, among other things, a nationwide system for detecting such threats. What is needed are not only detection systems but also defeat systems - these should be deployed at the border, at critical infrastructure sites, defence industry plants, airports, military units, and other important institutions. For years, there has also been discussion of the SONA programme, under which the Polish Armed Forces would acquire mobile air defence capable of providing cover for manoeuvring troops.

It is necessary to acquire air-to-air refuelling aircraft, which are also produced in Europe. Poland could consider Airbus's offer and purchase, for example, the A330 MRTT aircraft.

Continuous control of the airspace should be ensured by airborne early-warning aircraft. Poland has purchased two Saab 340 AEW aircraft; these are used and obsolete. This is a bridging solution, and further aircraft must be ordered. The Swedish Saab GlobalEye may be an attractive option. For both tanker and early-warning aircraft – and given their critical importance – it would be prudent to consider procuring three to four such platforms.

In a future war, the winner will be the one who updates technology the fastest. This will be a technological shift that, at this point, is irreversible. As the war in Ukraine has demonstrated, Poland should invest particularly heavily in a modern Air Defence system. Building a multi-layered Air Defence architecture is a complex and long-term process that must be continuous

and systematically adapted to rapidly changing technologies and the requirements of the contemporary theatre of operations. Poland's air defence is transforming. To meet modern battlefield demands, our standard should be international cooperation grounded in the exchange of knowledge and the latest technologies. Full readiness and effective interoperability of the entire Air Defence system is expected only at the beginning of the next decade. As the war in Ukraine shows, without modern air-defence systems, there can be no question of effectively defeating an adversary.

Bibliography

Cielma M., *System obrony powietrznej Polski*, „Nowa Technika Wojskowa" 2022, no. 1.

Ditrich R., *Czy nasza obrona przeciwlotnicza jest gotowa? Ekspert nie zostawia suchej nitki*, https://forsal.pl/kraj/bezpieczenstwo/artykuly/9830349,czy-nasza-obrona-przeciwlotnicza-jest-gotowa-ekspert-nie-zostawia-suc.html [access: 20.10.2025].

Dura M., *Polska obrona przeciwlotnicza w 2024 roku. Więcej do zrobienia niż zrobiono w trakcie*, https://defence24.pl/sily-zbrojne/polska-obrona-przeciwlotnicza-w-2024-roku-wiecej-do-zrobienia-niz-zrobiono-w-trakcie [access: 21.10.2025].

Juraszek P., *Wyciągnęli wnioski z Ukrainy. Kraj NATO zmienia koncepcję wojny*, https://tech.wp.pl/wyciagneli-wnioski-z-ukrainy-kraj-nato-zmienia-koncepcje-wojny,7161525847968480a [access: 23.10.2025].

Kaleta K., *Powietrzna Tarcza Polski – co już mamy i dlaczego wciąż jest tak dużo do zrobienia?*, https://sektorobronny.pl/powietrzna-tarcza-polski-co-juz-mamy-i-dlaczego-wciaz-jest-tak-duzo-do-zrobienia/ [access: 23.10.2025].

Kaleta W., *Kupujemy jeden z najlepszych systemów obrony. Koszty idą w miliardy, a to dopiero początek*, https://www.wnp.pl/bezpieczenstwo/co-z-wisla-narwia-i-pilica-obronny-parasol-polski-napedza-- krociowe-wydatki,903274.html [access: 23.10.2025].

Kulik T., *Uwarunkowania bezpieczeństwa powietrznego państwa w aspekcie militarnych zagrożeń powietrznych*, „Kwartalnik Bellona" 2020, no. 2.

Michalik Ł., *Wnioski z wojny w Ukrainie. W Polsce powstaje centrum analityczne NATO*, https://tech.wp.pl/wnioski-z-wojny-w-ukrainie-w-polsce-powstaje-jatec-centrum-analityczne-nato,7126280513645376a [access: 23.10.2025].

Palanowski J., *Polskie F-35: rewolucja, którą trzeba wykorzystać*, https://defence24.pl/sily-zbrojne/polskie-f-35-rewolucja-ktora-trzeba-wykorzystac [access: 23.10.2025].

Przestroga dla NATO. Błędne wnioski z wojny w Ukrainie, https://tech.wp.pl/przestroga-dla-nato-bledne-wnioski-z-wojny-w-ukrainie,7192696374401792a [access: 23.10.2025].

Radomyski A., *Pożądane kierunki rozwoju zdolności Sił Zbrojnych RP w zakresie obrony powietrznej*, [in:] *Przyszłość Sił Powietrznych i jednostek obrony powietrznej w Siłach Zbrojnych RP*, Warszawa 2015.

Wyzwania i rozwój obrony powietrznej Rzeczypospolitej Polskiej, eds. Radomyski A., Malinowski P., Michalski D., Warszawa 2025.

Magdalena El Ghamari
University College of Professional Education
Centre for State Security Threat Studies
Academic Centre for Strategic Analysis
ORCID: 0000-0001-5798-7545
m.el-ghamari@akademia.mil.pl

Captagon, Conflict and the Sudan-Libya Border Triangle

Abstract

The article discusses how the synthetic stimulant Captagon has become integrated into the war and shadow economies of the Sudan–Libya–Sahel borderlands, turning a historically marginal drug into a crucial revenue source for armed groups and political-military entrepreneurs. Using a case-study design, the study triangulates open-source reporting, international datasets, and grey literature to map production nodes, trafficking corridors, and the institutional and territorial vacuums that enable them. It argues that the Sudan–Libya border triangle – anchored in western Sudan, Fezzan in southern Libya, and adjoining Sahelian interfaces – operates as a logistical hinge connecting Levantine industrial production with Gulf consumer markets and emerging European transit points. Captagon's political economy sustains militias through taxation and direct participation in smuggling, inances arms procurement, and consolidates parallel governance, thereby entrenching conflict fragmentation and undermining stabilisation efforts. The article further shows how Captagon functions as a tool of hybrid warfare: revenues fuel coercive capacity while battlefield consumption exacerbates fviolence, erodes community resilience, and burdens already fragile health systems. Building on debates about illicit economies and conflict, the analysis cautions against mono-causal explanations: Captagon profits amplify violence primarily where they intersect with state failure, fragmented sovereignty, and cross-border criminality. Policy implications include a shift from

enforcement-only approaches toward integrated strategies that combine precursor control, targeted financial disruption, maritime and desert interdiction, and border-area development with demand-reduction and treatment services. Regionally, enhanced intelligence-sharing across the Red Sea and Sahara corridors, along with calibrated engagement with de facto authorities, is necessary to address operational realities without legitimising predation. For Europe, including Poland, the growing use of North African and Eastern Mediterranean routes underscores Captagon as a convergent security, governance, and public health challenge. The article contributes an empirically grounded framework for analysing narcotics-driven conflicts in fragile borderlands and offers a multi-level agenda for mitigation.

Key words Captagon, Sudan–Libya border triangle, Fezzan, RSF, war economy, hybrid warfare, illicit economies, transnational organised crime, smuggling routes, precursor control, border governance, MENA security, Sahel, public health and addiction, European security

Introduction

The Middle East and North Africa (MENA) region has long grappled with deep-seated political instability, protracted armed conflicts, and structural socio-economic crises. Over the past decade, scholarly and policy attention has increasingly shifted toward the role of illicit economies in exacerbating these dynamics. Among them, the rise of the synthetic stimulant Captagon has emerged as a particularly concerning phenomenon. Once a marginal drug, Captagon evolved into both a widely consumed narcotic and a strategic financial resource for armed groups, militias, and political actors across several states in the region. A particularly alarming nexus has developed in the border triangle linking Sudan, Libya, and the Sahel, where weak state structures, porous borders, and fragmented authority have created fertile ground for the production, trafficking, and militarization of Captagon[1]. This fragile zone – already destabilized by ethnic tensions, militia rivalries, and foreign interventions – has become a strategic corridor for smuggling operations that connect local conflicts to wider regional and transnational criminal networks.

1 *Two Years On, Sudan's War is Spreading*, https://www.crisisgroup.org/africa/horn-africa/sudan/two-years-sudans-war-spreading [access: 29.08.2025].

Captagon, chemically a combination of amphetamine and theophylline, has gained traction not only as a recreational or performance-enhancing substance within local populations but also, and more critically, as a trade commodity embedded in war economies. Its production and smuggling networks generate substantial revenues that sustain militia operations, finance arms procurement, and perpetuate cycles of violence. In particular, clandestine narcotics factories operating in parts of Sudan and Libya have been identified as central nodes in this illicit economy, with revenues directly linked to the prolongation and intensification of ongoing conflicts[2].

The purpose of this article is to analyze the impact of Captagon production and trade on conflicts and political crises in the Sudan–Libya border triangle, while situating the phenomenon within the broader geopolitical and security context of the MENA region. Through a case study approach, the article seeks to capture the multidimensional nature of the Captagon economy, illustrating how narcotics trafficking serves both as a mechanism of conflict financing and as a driver of social degradation. Particular attention is given to the intersection of illicit markets, governance vacuums, and hybrid warfare strategies, as well as the consequences for local communities who bear the brunt of addiction, violence, and institutional erosion. Against this backdrop, the study is guided by the following research questions:

1. What are the main mechanisms of Captagon production and trafficking in the Sudan–Libya border triangle?
2. How does the Captagon trade sustain armed conflicts and exacerbate political and social instability in the MENA region?
3. What strategies – at the national, regional, and international levels – offer the greatest potential for mitigating the Captagon trade and its destabilizing effects?

By linking empirical evidence with theoretical debates on illicit economies and conflict, this study contributes to wider discussions on the role of transnational criminal markets in sustaining insecurity. It underscores the urgent need for interdisciplinary research and international cooperation in

2 *Syria has become a narco-state*, https://www.economist.com/middle-east-and-africa/2021/07/19/syria-has-become-a-narco-state?utm_campaign=shared_article [access: 29.08.2025].

addressing narcotics-driven conflicts, highlighting the Sudan–Libya–Sahel borderlands as a microcosm of broader destabilizing dynamics that continue to shape the MENA region.

The Geopolitical and Socio-Economic Context of the Sudan–Libya Border Triangle

The border triangle linking Sudan, Libya, and parts of the Sahel represents one of the most volatile and insecure zones in North Africa and the broader Middle East. Weak state presence, porous borders, and the proliferation of armed groups, militias, and transnational criminal networks characterise it. The geopolitical complexity of the region stems from the convergence of multiple dynamics: fragile governance, unresolved civil wars, ethnic tensions, and economic collapse. These conditions foster a permissive environment for illicit activities ranging from arms trafficking and human smuggling to the production and circulation of narcotics, notably Captagon.

Sudan has been experiencing a decade of compounded crises, marked by the ousting of President Omar al-Bashir in 2019, the fragility of subsequent transitional arrangements, and the eruption of a new civil war in April 2023. These developments have fostered state fragmentation and deepened the country's economic implosion[3]. Rival factions – the Sudanese Armed Forces (SAF) and the Rapid Support Forces (RSF) – control vast territories, often outsourcing governance to local militias or tribal coalitions. This power vacuum has transformed Sudan's western peripheries into lawless corridors where trafficking networks intersect with political violence[4].

Libya's trajectory in the aftermath of the 2011 collapse of Muammar Gaddafi's regime has been marked by profound and persistent destabilisation, reflecting both the internal disintegration of state institutions and the entrenchment of competing centers of power supported by shifting coalitions

3 H. Abazid, *Drug Abuse in the Middle East: A Focus on Syria*, [in:] *Handbook of Substance Misuse and Addictions: From Biology to Public Health*, ed. V. Preedy, Cham 2021, p. 1–20.

4 *Two Years On, Sudan's War is Spreading*, https://www.crisisgroup.org/africa/horn-africa/sudan/two-years-sudans-war-spreading [access: 29.08.2025].

of militias and external actors. Since 2011, the country has been fractured between competing governments in Tripoli and Benghazi, each relying on a constellation of militias and foreign sponsors. The collapse of centralised authority enabled Libya to become a critical hub for smuggling routes across the Sahara. The southern region of Fezzan, bordering Niger, Chad, and Sudan, is particularly significant: it functions as a gateway for trans-Saharan flows of migrants, arms, and narcotics[5]. The Libya–Sudan border triangle, largely unmonitored, thus serves both as a staging point for smuggling operations and as a refuge for militias who tax or directly manage these illicit flows.

Any comprehensive analysis must also account for Syria, which has emerged as the pivotal hub of industrial-scale Captagon production, shaping both regional illicit economies and transnational trafficking networks[6]. Over the past decade, the Syrian conflict has transformed the country into the epicentre of the global Captagon trade. Production facilities – allegedly linked to the Syrian regime and Hezbollah – have industrialised the process, flooding the Middle Eastern market with billions of pills annually[7]. While much of the trade is directed toward Gulf states, trafficking routes increasingly extend through North Africa, with Libya and Sudan serving as secondary transit corridors toward Europe and the Sahel. The logistical infrastructure developed for weapons and human smuggling is now exploited to move narcotics, reinforcing hybrid economies of war.

The emergence of clandestine Captagon factories within the Sudan–Libya borderlands illustrate how local instability connects to broader geopolitical economies of conflict. Revenues from narcotics trafficking provide vital financial streams to militias, insurgent groups, and political entrepreneurs, thereby fueling protracted wars and undermining peace efforts. The phenomenon exemplifies how narcotics have been weaponised in hybrid conflicts: they not only generate income but also produce social devastation

5 W. Lacher, *Libya's Fragmentation: Structure and Process in Violent Conflict*, London–New York 2020.

6 C. Rose, *Border Traffic: How Syria Uses Captagon to Gain Leverage over Saudi Arabia*, https://carnegieendowment.org/research/2024/07/border-traffic-how-syria-uses-captagon-to-gain-leverage-over-saudi-arabia?lang=en [access: 29.08.2025].

7 J. Ababsa, *The al-Assad Regime's Captagon Trade*, https://carnegieendowment.org/sada/2022/10/the-al-assad-regimes-captagon-trade?lang=en [access: 29.08.2025].

through addiction, violence, and the erosion of community resilience. In this light, the Sudan–Libya border triangle operates as a microcosm of broader MENA security dynamics. It demonstrates how narcotics economies, insurgency, and geopolitical rivalries intersect in fragile borderlands. A comprehensive understanding of Captagon's role in these contexts is therefore indispensable for analysing the hybrid warfare strategies employed across the region and developing effective counter-narcotics, counterterrorism, and stabilisation policies.

Discussion

The role of Captagon in fueling conflicts and destabilizing the MENA region, particularly in the Sudan-Libya border triangle, invites critical engagement with existing scholarship and reports. Several authors, such as Al-Imam et al.[8] and Steenkamp[9], emphasize Captagon as both a cause and consequence of regional instability, highlighting how its trade finances armed groups and prolongs conflicts. This view aligns with journalistic investigations documenting clandestine factories in Sudan and Libya actively supporting militia operations. However, it is important to critically assess the extent to which Captagon production itself drives conflict dynamics versus serving as one element within a broader constellation of economic and political factors. Abazid underlines that state failure and weak governance underpin many regional crises, suggesting that drug trafficking may be more symptomatic of deeper institutional collapse than an independent conflict driver. Thus, the causal link between Captagon and conflict may be intertwined with structural governance failures, limiting simplistic attributions of conflict causality to the drug trade.

Moreover, while numerous authors acknowledge the health and social harms caused by Captagon consumption, such as addiction and societal disruption, there remains debate over how effectively these issues are prioritized

8 A. Al-Imam et al., *Captagon: use and trade in the Middle East*, „Human Psychopharmacology: Clinical and Experimental" 2017, no. 3, p. 2548.

9 C. Steenkamp, *Captagon and conflict: Drugs and war on the border between Jordan and Syria*, „Mediterranean Politics" 2025, no. 3, p. 478–502.

compared to the overarching security concerns. The predominance of security-focused responses risks overshadowing public health strategies necessary for sustainable resolution. As noted in health system analyses, integrating drug prevention and treatment programs alongside security measures is crucial, yet often insufficiently implemented.

International interventions, documented in reports by bodies like the UNODC and Interpol, advocate stronger border controls and international cooperation. Yet, critiques exist regarding the practical effectiveness of such approaches amid entrenched local militias and porous borders. Interventionist strategies may, at times, exacerbate local grievances or fail when disconnected from conflict resolution and political stabilization efforts. This tension is well articulated by authors[10] who argue that no regime or force alone can address these complex dynamics without holistic political solutions.

In summary, while literature broadly agrees on Captagon's significance in destabilizing the region, there is a need for more nuanced understanding that situates drug trafficking within wider governance, political, and socio-economic contexts. Addressing Captagon's impact necessitates multidisciplinary approaches that balance security imperatives with public health, social development, and political stability. Future research should thus focus on these intersections to identify more effective and sustainable strategies.

Mechanisms of Captagon Production and Trafficking in the Sudan–Libya Border Triangle

The production and trafficking of Captagon in the Sudan–Libya borderlands represent one of the most pressing security and governance challenges in the broader MENA region. Captagon, a synthetic amphetamine derivative, has transformed from a marginal psychostimulant into a strategic commodity that fuels both the black-market economy and the war economies of multiple armed groups. Its significance is twofold: on the one hand, it functions as a performance-enhancing substance widely consumed by combatants and

10 A. Al-Imam et al., *Risk Factors of Suicidal Ideation in Iraqi Crystal Methamphetamine Users*, „Brain Sciences" 2023, vol. 13, no. 9, p. 1279.

youth populations; on the other, it has become a principal source of revenue for militias, insurgent movements, and hybrid political-military actors.

The Sudan–Libya–Sahel border triangle has emerged as a critical logistical node for Captagon production and redistribution. Semi-legal and clandestine laboratories, often concealed in remote desert areas or within territories controlled by militias, constitute the backbone of local production. These facilities benefit from ineffective state control, fragmented sovereignty, and limited law-enforcement capacity. Tribal networks and transnational criminal syndicates provide protection and facilitate access to precursor chemicals. These chemicals are often diverted from legitimate pharmaceutical markets or trafficked through existing smuggling routes used for arms, gold, and fuel.

The technical process of Captagon production is relatively straightforward, requiring rudimentary laboratory equipment and access to chemical precursors such as amphetamine base and theophylline. However, the scalability of production depends on steady supplies of these precursors, which are smuggled across borders through the same clandestine networks that historically managed weapons trafficking during the Libyan civil war and the Darfur conflict in Sudan. These overlapping flows highlight the structural entanglement between narcotics production and broader illicit economies in fragile borderlands.

Once produced, Captagon tablets are transported along complex, multi-layered trafficking routes. The Sudan–Libya corridor acts as a staging ground from which shipments are routed north toward the Mediterranean coast for onward transport to Southern Europe, eastward through Egypt into the Levant, and westward into the Sahel and West Africa. Smugglers employ diverse methods: desert convoys across Fezzan, clandestine crossings along poorly monitored border points, and maritime shipments via Libyan ports such as Misrata or Benghazi. Increasingly, traffickers rely on containerised cargo to conceal narcotics shipments, complicating interdiction efforts through European Monitoring Centre for Drugs and Drug Addiction[11].

Syrian and Lebanese networks also intersect with these routes. Syria has become the epicentre of industrial-scale Captagon production, while

11 *Captagon Trafficking and Consumption in the Middle East*, file:///C:/Users/melghamari/Downloads/captagon-report_7september2023_final.pdf [access: 29.08.2025].

Hezbollah and regime-linked actors are reported to play central roles in global distribution[12]. The Sudan–Libya triangle is thus not an isolated production site but part of a transnational web linking Levantine producers, Gulf consumer markets, and European transit points.

The revenues from Captagon trafficking constitute a vital financial stream for militias and insurgent groups operating across Sudan, Libya, and beyond. These profits are channeled into arms procurement, payment of fighters, and the consolidation of parallel governance structures. In Sudan, both the Rapid Support Forces (RSF) and smaller tribal militias have been accused of taxing smuggling routes and benefiting from narcotics flows. In Libya, factions within Fezzan leverage drug revenues to maintain autonomy from the central authorities in Tripoli and Benghazi[13]. This dynamic entrenches fragmentation and undermines international stabilisation initiatives. Moreover, Captagon has become a weapon of war. Combatants in Libya, Syria, and Sudan reportedly consume the drug on the battlefield, as its stimulant properties enhance endurance, suppress fatigue, and increase aggression. While this temporarily boosts combat effectiveness, it also intensifies the brutality of armed clashes and exacerbates patterns of violence against civilians. Captagon consumption among fighters reinforces cycles of addiction, dependency, and militarized violence, further eroding prospects for conflict resolution.

The spread of Captagon extends beyond the military domain, exerting devastating effects on local societies. Communities in the Sudan–Libya–Sahel borderlands face rising addiction rates, health crises, and the collapse of traditional social structures. Families experience disintegration as addiction spreads among youth, while public health systems –already weakened by conflict – cannot provide adequate treatment. The growth of narco-economies has also entrenched corruption within fragile governance systems, as state officials often collude with traffickers in exchange for revenue. This dynamic deepens the crisis of legitimacy facing central governments in both Sudan and Libya. The interplay of narcotics trafficking, militia financing, and social collapse creates a reinforcing feedback loop: illicit revenues empower armed

12 *The Assad Regime's Narco-State*, https://carnegieendowment.org/sada/2022/10/the-al-assad-regimes-captagon-trade?lang=en [access: 29.08.2025].

13 W. Lacher, op. cit.

groups, which in turn destabilase governance, enabling further expansion of criminal markets. The resulting spiral of violence, corruption, and humanitarian deterioration threatens not only border communities but also regional stability.

Addressing Captagon production and trafficking requires comprehensive, multi-level interventions. Traditional supply-side approaches – such as border enforcement or interdiction – are insufficient in fragmented sovereignty and ongoing war contexts. Instead, effective strategies must combine legal, military, economic, and public health dimensions. At the local level, investment in community resilience, alternative livelihoods, and social services can reduce dependency on illicit economies. Regionally, coordinated frameworks for intelligence sharing and precursor chemical monitoring are critical. At the global level, cooperation between MENA states, the EU, and international organisations such as UNODC is essential to disrupt trafficking networks that span continents.

Captagon is no longer merely a narcotics problem; it has evolved into a strategic driver of hybrid warfare and state fragmentation in the MENA region. The Sudan–Libya border triangle illustrates how illicit economies intertwine with armed conflict, shaping the trajectories of local wars and the geopolitical security environment of the wider region.

Reactions of States and the International Community to the Captagon Problem in the MENA Region

The growing impact of Captagon on the security and stability of the Middle East and North Africa has prompted a wide range of responses from national governments and international organisations. Captagon is no longer perceived solely as a narcotics issue but as a multidimensional threat that cuts across the domains of security, governance, public health, and regional stability. However, efforts to curb its production, trafficking, and consumption face formidable obstacles stemming from political instability, fragile institutions, fragmented sovereignty, and the complexity of armed conflicts in the region.

In the border triangle of Sudan and Libya, state-led counternarcotics measures are severely constrained by weak or absent central authority. In Sudan, the collapse of governance following successive political crises and

the ongoing conflict between the Sudanese Armed Forces (SAF) and the Rapid Support Forces (RSF) has left large areas beyond effective state control. Attempts to dismantle Captagon production networks have been piecemeal and largely ineffective, as armed groups continue to dominate territories where clandestine factories operate. These groups protect production and integrate trade into broader war economies, making enforcement efforts highly risky and often counterproductive.

Libya faces a similar, though distinct, challenge. Since the fall of Muammar Gaddafi in 2011, the country has been fragmented between rival governments and a multiplicity of militias that control different parts of the territory. In this environment, counter-narcotics operations suffer from a lack of coordination, contested jurisdiction, and widespread corruption. Smuggling networks have exploited the power vacuum in the southern region of Fezzan, turning the area into a hub for the transit of Captagon and other illicit commodities. The inability of Libyan authorities to secure borders or establish unified command structures has allowed trafficking networks to flourish, linking domestic militias with transnational organised crime groups.

Recognising the transnational nature of the Captagon trade, the international community has taken steps to support affected states. The United Nations Office on Drugs and Crime (UNODC)[14], Interpol, and regional security organisations such as the Arab Interior Ministers Council have launched initiatives to strengthen border management, enhance intelligence-sharing, and provide technical assistance. Programs include training customs and law-enforcement personnel, deploying advanced scanning technologies at border points, and building regional platforms for exchanging information on trafficking patterns. Interpol has also coordinated international operations targeting Captagon shipments, some resulting in record seizures in the Mediterranean and the Gulf[15]. Nevertheless, enforcement alone is insufficient

14 *World Drug Report 2023*, https://www.unodc.org/unodc/data-and-analysis/world-drug-report-2023.html [access: 29.08.2025]; *World Drug Report 2024*, https://www.unodc.org/unodc/data-and-analysis/world-drug-report-2024.html [access: 29.08.2025].

15 D. Hilton, M. Amin, *Inside the Drugs Factory: How Captagon is Fuelling the War in Sudan*, „Middle East Eye", https://www.middleeasteye.net/news/inside-drugs-factory-how-captagon-fuelling-war-sudan [access: 29.08.2025].

to address the problem. Scholars and practitioners emphasise that sustainable counter-Captagon strategies must go beyond repression to incorporate legal, social, and economic dimensions. Legal reforms are needed to harmonise anti-narcotics laws across MENA states and close loopholes that traffickers exploit. Socially, public health initiatives are essential to reduce demand, particularly among youth populations vulnerable to addiction and exploitation by armed groups. Economic interventions, including alternative livelihood programs, are necessary in border communities where smuggling has become a survival strategy without state investment and employment opportunities.

The responses of Gulf states also highlight the broader regional dimension of the Captagon trade. Countries such as Saudi Arabia and the United Arab Emirates, which are major consumer markets, have intensified customs inspections, invested in rehabilitation facilities, and tightened penalties for trafficking. Their concerns have also led to diplomatic pressure on Syria and Lebanon, accused of being the primary sources of Captagon production and export. This illustrates how the Captagon problem, while rooted in fragile states like Sudan and Libya, reverberates across the MENA region and beyond, shaping security agendas and diplomatic relations.

At the same time, international cooperation remains uneven and constrained by geopolitical rivalry. Disagreements between external actors over approaches to Syria, Libya, and Sudan often undermine collective action. For instance, while some international partners advocate engagement with de facto authorities to enable pragmatic cooperation against trafficking, others oppose such moves for fear of legitimising militias or authoritarian regimes. These tensions reflect the difficulty of mounting coordinated responses to transnational challenges in conflict-affected environments.

In sum, despite multiple national, regional, and global initiatives, the Captagon problem continues to pose a formidable challenge. The persistence of armed conflict, weak governance, and high demand ensures the trade remains lucrative and resilient. Effective responses will therefore require not only the reinforcement of law enforcement but also integrated, interdisciplinary strategies that combine security, governance, public health, and socio-economic measures. Only through such comprehensive approaches, grounded in both local realities and international cooperation, can the destructive impact of Captagon on the MENA region be mitigated.

Conclusion

Captagon has evolved into one of the central destabilising forces in contemporary Middle East and North Africa, reshaping both the dynamics of armed conflicts and the illicit political economy of fragile states. Syria and Lebanon were considered the epicentres of Captagon production and export for many years, but recent political and military transformations have altered this geography. The fall of Bashar al-Assad's regime and the dismantling of large-scale laboratories in Syria created a vacuum in the narcotics economy. As the new authorities in Damascus initiated counternarcotics measures, criminal networks were forced to search for alternative production hubs. Within this shifting landscape, Sudan has rapidly emerged as a key center of the evolving Captagon economy.

Investigations by international institutes and journalists confirm that Sudan, once primarily a transit corridor, has transformed into a locus of industrial-scale production. Since the outbreak of Sudan's civil war in April 2023, authorities have discovered several major laboratories, marking a sharp escalation in scale and sophistication. One site in the Blue Nile region could produce 7,200 pills per hour; another in Khartoum held approximately 10 million pills in stock; and the most striking discovery came in February 2025 in al-Jaili, where machinery was uncovered with the capacity to produce 100,000 pills per hour, the country's largest seizure to date. This rapid progression from small-scale operations to mechanised mass production underscores the growing attractiveness of Sudan as a manufacturing hub and the increasing sophistication of local networks.

The rise of Sudan as a Captagon center is not accidental but rather the outcome of structural conditions that echo those once observed in Syria. Protracted conflict, fragmented sovereignty, weak law enforcement, endemic corruption, and proximity to lucrative Gulf markets together create an environment conducive to narcotics economies. The confrontation between the Sudanese Armed Forces (SAF) and the Rapid Support Forces (RSF) has fractured state authority and opened zones of impunity. The RSF appears to play a central role: both major laboratory seizures in Khartoum took place in areas under their control, strongly suggesting complicity or direct involvement. Given the RSF's record of exploiting illicit economies—from gold smuggling

and livestock trade to looting, Captagon production seems to be a logical extension of its wartime financing strategies. With the SAF regaining parts of Khartoum, production will likely relocate westward into Darfur, where RSF strongholds overlap with established trafficking routes leading into Libya and Chad.

The ramifications of this transformation are considerable, as revenues derived from the Captagon trade constitute a stable and renewable financial base for armed actors, thereby institutionalising the war economy and contributing to the protraction of Sudan's civil conflict. The presence of industrial-scale facilities tied to transnational networks further demonstrates that trafficking increasingly connects Northeast Africa with the Gulf and Europe, primarily through the Red Sea and Mediterranean corridors. Port Sudan has already become a focal point for seizures, highlighting the vulnerability of maritime routes and the potential for systemic corruption among customs and security services. At the same time, the domestic spread of Captagon compounds Sudan's humanitarian crisis. Local authorities report a surge in consumption since the outbreak of war, as the drug is used to suppress hunger, dull trauma, and sustain productivity. In this way, addiction is embedding itself in fragile communities, aggravating social breakdowns alongside political and military instability.

Although geographically distant, these developments directly affect Poland and the wider European Union. As an EU member, Poland is exposed to the spillover of illicit narcotics flows into European markets. Smuggling routes increasingly link North Africa and the Middle East to Europe. Shipments cross the Mediterranean via Libyan ports such as Benghazi and Misrata toward Southern Italy and Malta; others are routed from Syria and Lebanon through Turkey into Greece and the Balkans; while new corridors have opened through the Red Sea, with consignments leaving Port Sudan and moving via the Suez Canal into European ports under the cover of commercial cargo. The Syrian route remains one of the most established, with shipments directed to Greece, Cyprus, or major Mediterranean ports before being distributed through the Balkans into Central Europe. At the same time, Sudan has become an emerging departure point, with overland consignments moving across Darfur into Libya and re-exported across the Mediterranean.

The reality of these routes has been confirmed by European law enforcement agencies, which have intercepted massive shipments in Italy (Naples and Salerno), Greece (Piraeus), and Germany in recent years. These cases illustrate that Captagon is no longer confined to the Middle Eastern market but has already entered Europe. Such trafficking channels overlap with existing migration and arms smuggling routes, creating the risk that narcotics flows converge with irregular migration corridors. For Poland, this convergence is particularly significant: it represents not only a law enforcement and public health challenge but also a strategic concern, as narcotics-driven conflicts in MENA can exacerbate migration pressures, heighten terrorism risks, and undermine wider European security.

These dynamics demand a recalibration of international responses. Counter-Captagon strategies that historically concentrated on Syria and Lebanon are now outdated. The emergence of Sudan – alongside secondary hubs in Iraq, Türkiye, and Kuwait – demonstrates the need for a geographically broader approach. The United States and its partners must expand their interagency strategies to include Sudan, with careful monitoring of RSF-controlled territories and scrutiny of vulnerabilities within SAF-controlled ports and border posts. At the same time, cooperation across the Red Sea corridor – particularly with Egypt, Saudi Arabia, and the Horn of Africa – will be essential to addressing maritime smuggling and the flow of precursor chemicals. However, enforcement measures alone will not be sufficient. A holistic strategy is required, combining interdiction with political stabilisation, peacebuilding, and creating economic alternatives for vulnerable communities. As long as Sudan's civil war continues and Libya remains fragmented, Captagon production and trafficking will remain highly attractive to militias in search of financial autonomy. Equally pressing are public health responses: addiction among Sudanese youth and combatants highlights the urgent need for prevention and treatment programmes, which are currently absent in most of the region. Ultimately, Captagon exemplifies how synthetic drug economies migrate, adapt, and entrench themselves in fragile states where conflict and impunity provide fertile ground. The Sudanese case demonstrates that the collapse of one hub – in this instance, Syria – does not eliminate the threat but redistributes it into new environments shaped by similar vulnerabilities. This shift underscores the need to understand

Captagon as a transnational and adaptive phenomenon requiring equally adaptive and cooperative strategies. For policymakers and researchers alike, Sudan's emergence as a Captagon hub highlights the necessity of placing narcotics economies at the center of analyses of conflict financing, hybrid warfare, and regional security. Without sustained international attention, the drug's entrenchment in Sudan threatens not only to prolong the civil war and erode governance but also to export instability far beyond the region's borders.

Bibliography

Ababsa J., *The al-Assad Regime's Captagon Trade*, https://carnegieendowment.org/sada/2022/10/the-al-assad-regimes-captagon-trade?lang=en [access: 29.08.2025].

Abazid H., *Drug Abuse in the Middle East: A Focus on Syria*, [in:] *Handbook of Substance Misuse and Addictions: From Biology to Public Health*, ed. V. Preedy, Cham 2021.

Al-Imam A. et al., *Risk Factors of Suicidal Ideation in Iraqi Crystal Methamphetamine Users*, „Brain Sciences" 2023, vol. 13, no. 9.

Al-Imam A. et al., *Captagon: use and trade in the Middle East*, „Human Psychopharmacology: Clinical and Experimental" 2017, no. 3.

Hilton D., M. Amin, *Inside the Drugs Factory: How Captagon is Fuelling the War in Sudan*, „Middle East Eye", https://www.middleeasteye.net/news/inside-drugs-factory-how-captagon-fuelling-war-sudan [access: 29.08.2025].

Lacher W., *Libya's Fragmentation: Structure and Process in Violent Conflict*, London–New York 2020.

Rose C., *Border Traffic: How Syria Uses Captagon to Gain Leverage over Saudi Arabia*, https://carnegieendowment.org/research/2024/07/border-traffic-how-syria-uses-captagon-to-gain-leverage-over-saudi-arabia?lang=en [access: 29.08.2025].

Steenkamp C., *Captagon and conflict: Drugs and war on the border between Jordan and Syria*, „Mediterranean Politics" 2025, no. 3.

Syria has become a narco-state, https://www.economist.com/middle-east-and-africa/2021/07/19/syria-has-become-a-narco-state?utm_campaign=shared_article [access: 29.08.2025].

The Assad Regime's Narco-State, https://carnegieendowment.org/sada/2022/10/the-al-assad-regimes-captagon-trade?lang=en [access: 29.08.2025].

Two Years On, Sudan's War is Spreading, https://www.crisisgroup.org/africa/horn-africa/sudan/two-years-sudans-war-spreading [access: 29.08.2025].

World Drug Report 2023, https://www.unodc.org/unodc/data-and-analysis/world-drug-report-2023.html [access: 29.08.2025].

World Drug Report 2024, https://www.unodc.org/unodc/data-and-analysis/world-drug-report-2024.html [access: 29.08.2025].

Marek Rohr-Garztecki
ORCID Nr 0000-0001-9676-2891
marek.garztecki@gmail.com

Strengthening of the EU's Common Security Policy as a source of possible conflict in Transatlantic relations

Abstract

The idea of a common EU security policy, originating from the so-called Pleven Plan announced in October 1950, has experienced many ups and downs. Never fully realized, it is now subject to two opposing impulses. The first was the dramatic deterioration of the European security environment caused by Russia's aggression against Ukraine; the second, President Trump's announcement that the American "security umbrella" over European NATO members would be conditional on their radical increase in defence spending. Analysing the United States' attitude toward its European allies, the article points out that throughout nearly the entire existence of NATO, this attitude has also been subject to significant fluctuations. This attitude results from the interplay of two conflicting needs: maintaining an adequate level of the United States' own military equipment resources and retaining the ability to influence the decisions of its allies. The strength of this influence, apart from the level of the threat environment and the state of American resources, is also conditioned by the allies' capacity to acquire military equipment. The current international situation has made most European NATO states realize that their armed forces are unable to fulfil their primary task – defending their own territory – and that domestic defence industries cannot rapidly supply the necessary equipment for this purpose. At present, the United States provides 64% of the armaments of European NATO countries, which in 2024 accounted for 35% of American arms exports. This places Europe in

the position of the largest American client, while at the same time giving it a strong bargaining position. Moreover, many products of the American defence industry could not function without components manufactured in Europe. In conclusion, the article proposes measures which, by strengthening in the short term both the EU's security policy and the material means to secure it, will help maintain mutually beneficial cooperation with the United States.

Key words EU, NATO, security policy, burden sharing

Introduction

The Russian invasion of Ukraine in February 2022 permanently transformed the European security environment. While Russia's earlier military interventions in Georgia in 2008 and Ukraine in 2014 were regarded by most West European countries as local conflicts, this time they were perceived as a direct threat to their own security. By the end of 2024, this perception was further reinforced by the newly elected U.S. president, Donald Trump, who announced that the American "security umbrella" over European members of the North Atlantic Treaty Organization (NATO) would be conditional on their radically increasing in their defence spending[1].

Faced with mounting challenges, the European NATO states recognized that their armed forces were unable to fulfil their primary mission – defending their own territories – and that domestic defence industries could not quickly provide the necessary equipment.

Poland's front-line position makes it particularly vulnerable to potential Russian hostilities. As a member of the European Union (EU), it benefits from various forms of economic cooperation among member states, and as a member of NATO, it enjoys the "security umbrella" provided by the Alliance. This protection primarily takes the form of American troops stationed on its territory, the implicit guarantee of combat support in the event of enemy aggression (the so-called Article 5 assurances), and the access to advanced US-manufactured military equipment. Therefore, preserving strategic cohesion

1 Z. Gwadera, *US allies question extended deterrence guarantees, but have few options*, https://www.iiss.org/online-analysis/military-balance/2025/03/us-allies-question-extended-deterrence-guarantees-but-have-few-options/ [access: 20.03.2025].

between NATO members that belong to the EU and those that do not, such as the United States, is of vital importance to Poland.

The aim of this article is to examine whether and how efforts to strengthen the EU's Common Security and Defence Policy (CSDP) may influence its relations with non-European members of NATO, primarily the United States. Based on this analysis the objective is to propose measures, that will enable Poland to sustain strategic cooperation with the United States while simultaneously contributing to the development of the EU's security policy. To achieve this, it is necessary to outline the main events that led to the creation of the CSDP, the key factors shaping transatlantic relations, and the changes in the international security environment that have affected NATO's internal dynamics.

Literature review

A substantial body of scholarship on transatlantic relations – encompassing both academic articles and monographs – has emerged over the decades, with a significant portion of these works analysing tensions and conflicts among the member states of the Atlantic Alliance. As Hallams[2] observes, crises and periods of strain have been recurring features of the transatlantic relationship, and there is little reason to expect that such frictions will cease in the future. At the end of the Second World War, approximately three million American military personnel were stationed in Europe. According to Koivula[3], the United States initially intended to delegate responsibility for post-war security arrangements to the United Nations – a vision reflected in the naming of the organisation's principal executive body as the "Security Council". What would later evolve into NATO was at first conceived as a temporary arrangement for the continued stationing of American forces in Europe. Their presence was expected to last only until a stable peace had been secured on the continent[4].

2 E. Hallams, *The United States and NATO since 9/11: The Transatlantic Alliance renewed*, New York 2010, p. 129.

3 T. Koivula, H. Ossa, *NATO's Burden-sharing disputes: Past, Present and Future Prospects*, Cham 2022, p. 36.

4 Ibidem, p. 40.

However, increasing Soviet assertiveness and the growing influence of domestic communist movements created new security concerns that necessitated a revision of these assumptions. The founding of the North Atlantic Treaty Organization (NATO) in April 1949 thus gave permanent institutional form to the American military presence in Europe.

The first major political rift in transatlantic relations following the Second World War occurred in November 1956, when the United States condemned the joint Israeli–British–French invasion of Egypt[5]. Although not the principal cause, this episode was one of the factors that influenced France's 1966 decision to withdraw from NATO's integrated military command structure and to expel all non-French Alliance forces from its territory. A subsequent and equally significant conflict unfolded in the lead-up to the Second Gulf War in 2002–2003, when several long-standing West European NATO members, led by France and Germany, refused to support the United States in its bid to overthrow Saddam Hussein's regime in Iraq[6].The support that Washington received from newly admitted and aspiring NATO members was met with open derision by the French president[7]. As Longhurst and Zaborowski note[8], the ensuing diplomatic friction between the administration of U.S. President George W. Bush and key European allies became a hallmark of the transatlantic relationship during that period.

One of the most enduring and recurrent sources of tension within NATO, Koivula argues[9], concerns the issue of burden-sharing. This dispute, he explains, stems from the continual need to determine how the Alliance's costs and responsibilities should be apportioned among its members. Deni[10.] similarly observes that burden-sharing disagreements have troubled NATO

5 E. Hallams, op. cit., p. 14.
6 T. Lansford, B. Tashev, *Old Europe, new Europe and the US: Renegotiating Transatlantic Security in the post 9/11 era*, Burlington 2005, p. 7.
7 T. Lansford, B. Tashev, op. cit., p. XXII.
8 K. Longhurst, M. Zaborowski, *Old Europe, new Europe and the transatlantic security agenda*, New York 2005, p. 193.
9 T. Koivula, H. Ossa, op. cit., p. 1.
10 J. Deni, *NATO and Article 5: The Transatlantic Alliance and the twenty-first-century challenges of collective defense*, Lanham 2017, p. 77.

for decades, while Haglund characterises[11] them as a long-standing and inherent feature of the Alliance. Blankenship[12] notes that as early as the Kennedy administration, the United States had threatened to withdraw its troops from West Germany unless it received compensation for the costs associated with their deployment. Although much of the literature on burden-sharing has focused on disputes between the United States and its European partners, Haglund[13] demonstrates that similar tensions have also arisen among European members themselves, notably between France and Germany.

NATO is financed through both direct and indirect contributions. Direct funding levels are determined in proportion to each member's Gross National Income and are channelled into the Alliance's civilian and military budgets. Indirect contributions – comprising the maintenance of national armed forces – represent a substantially larger share of overall NATO-related expenditure[14]. The question of fairness in these contributions has been conceptualised in various ways, the most prominent being the notion of "common" or "collective goods". Such goods possess two defining characteristics: they are universally available, and their use by one actor does not diminish their availability to others[15]. Koivula identifies[16] NATO-provided security as such a collective good. Those who benefit from it without offering equivalent contributions are labelled "free riders". Lansford contends[17] that the possibility of free-riding and the pursuit of self-interest make NATO particularly appealing to new entrants – a perspective that contrasts sharply with the prevailing view among constructivist scholars, who, according to Hallams[18] emphasise shared ideological values as the principal source of cohesion within the Alliance.

11 D.G. Haglund, *Alliance within alliance? Franco-German military cooperation and the European pilar of defense*, New York 2018, p. 153.
12 B.D. Blankenship, *The burden-sharing dilemma: Coercive diplomacy in US alliance politics*, London 2023, p. 45.
13 D.G. Haglund, op. cit., p. 154.
14 T. Koivula, H. op. cit., p. 15.
15 D.G. Haglund, op. cit., p. 155.
16 T. Koivula, H. Ossa, op. cit., p. 6.
17 T. Lansford, B. Tashev, op. cit., p. 299.
18 E. Hallams, op. cit., p. 106.

Koivula identifies[19] four primary factors shaping the dynamics of NATO's burden-sharing disputes: geopolitical shifts related to Russia, changes in American foreign policy, the degree of European strategic activism, and the conduct of out-of-area operations. He employs a two-axis framework to analyse these variables: a horizontal axis representing NATO's internal unity and solidarity, and a vertical axis capturing the scope and integrity of the future burden-sharing agenda. The intersection of these axes produces four potential scenarios for the Alliance's evolution into the early 2020s, which Koivula labels[20] "incapacitated NATO", "self-interested member countries", "transatlantic bargaining", and "transatlantic solidarity".

In contrast to Koivula's structural approach, Blankenship[21] advances the concept of "alliance control theory". This framework posits that patron states – such as the United States – adjust their burden-sharing pressures on allies according to three key variables: the ally's latent military potential, the external threat environment, and the patron's own resource constraints. Whereas Koivula's typology delineates hypothetical scenarios, Blankenship's theory offers a more predictive analytical tool capable of anticipating concrete outcomes in burden-sharing disputes.

Methodology

This article is primarily descriptive in nature. Its sources consist mainly of primary materials, including official EU and NATO documents, published interviews and statements by key figures, as well as assessments produced by leading analytical organisations such as the Atlantic Council, Chatham House, and the IISS. It also engages with recent scholarship on burden-sharing in the context of military alliances.

The article adopts a hybrid methodological approach that integrates a constructivist theoretical framework with systems analysis. Constructivism, as a theoretical approach in international relations, emphasises the social construction of international reality – particularly the roles of identity, norms,

19 T. Koivula, H. Ossa, op. cit., p. 11.
20 Ibidem, p. 184.
21 B.D. Blankenship, op. cit., p. 5.

and discourse in shaping state behaviour[22]. Systems analysis, on the other hand, treats the European security order as a dynamic and interdependent system composed of states, institutions, and strategic interactions. This perspective facilitates the examination of structural change, feedback loops, and interdependencies – especially in response to the systemic shock produced by Russian aggression.

Case description

An examination of post-Second World War military alliances reveals striking similarities across contexts, regardless of their geographical scope or membership composition. Such alliances are inherently asymmetrical in power: one member – the patron – constitutes a clearly dominant military force, while the others – the allies – rely on the patron's capabilities to deter potential aggressors that they could not withstand alone. The principal benefit derived by the patron from its allies lies in the ability to project power across a much broader geographical area than its own territory would permit.

Friction within alliances typically manifests in two recurring forms. The first arises from the patron's perception that the costs of maintaining troops abroad are excessive. The second emerges from the allies' perception that the presence of foreign forces on their territory diminishes their sovereignty.

Another consequence of the Second World War was the destruction of much of Western Europe's defence-industrial capacity. Moreover, the war accelerated technological innovation, most of which occurred in the United States – whose territory remained largely untouched by the conflict. Following the collapse of the Soviet Union, most Western European states, convinced of the permanence of peace in Europe and reassured by the American "security umbrella", drastically reduced their defence expenditures. This led to the closure of numerous production lines and, in some cases, entire military manufacturing facilities[23]. The United States, by contrast, engaged in military operations across the globe – from Afghanistan to the Middle East – and

22 A. Wendt, *Social theory of international politics*, Cambridge 1999, p. 1–2.

23 K. Giles, *Who will defend Europe? An awakened Russia and a sleeping continent*, London 2024, p. 110.

expanded its arms production accordingly. As a result, Europe became doubly dependent on United States' "outsourcing": not only for security guarantees but also for the material means of ensuring them.

The idea of institutionalised collective defence among Western European states actually predates the establishment of NATO by more than two years and was initially conceived with a different purpose. In March 1947, Great Britain and France signed in Dunkirk a treaty of mutual defence in the event of renewed German aggression or threatening behaviour[24]. Known as the Franco-British Alliance or the Treaty of Dunkirk, it was subsumed a year later into the Treaty of Brussels. The latter established the Western Union, which also included Belgium, the Netherlands, and Luxembourg, in addition to France and Great Britain. Beyond addressing the perceived danger of German militarism, the Treaty of Brussels explicitly sought to counter the growing threat posed by the Soviet Union[25].

The Soviet-sponsored communist coup d'état in Czechoslovakia in February 1948 and the Soviet blockade of West Berlin from June 1948 to May 1949 finally convinced France that the Soviet Union – rather than Germany – constituted the primary threat to Western Europe. In October 1950, French Prime Minister René Pleven proposed a plan[26] to create a supranational army composed of contingents from multiple member states under a unified military command, with a common budget and joint procurement. This force, the so-called European Army, was to form part of the European Defence Community (EDC), established in 1952 under the Treaty of Paris. Its signatories included Belgium, Luxembourg, the Netherlands, France, Italy, and West Germany. By 1954, however, only four of the six signatories had ratified the treaty, as the French National Assembly indefinitely postponed its own ratification[27].

The concept of a collective European security framework was revived with the adoption of the Maastricht Treaty in 1992, which established the Common Foreign and Security Policy (CFSP) as one of the three pillars of the newly created European Union. Subsequently, the Treaty of Lisbon, signed in

24 S. Rynning, *NATO: From cold war to Ukraine, a history of the world's most powerful alliance*, London 2024, p. 45.
25 Ibidem, p. 45.
26 T. Koivula, H. Ossa, op. cit., p. 56.
27 Ibidem, p. 57.

2009, formally created the Common Security and Defence Policy (CSDP) as the institutional framework for the EU's civilian and military activities in the field of security and defence[28]. The CSDP also encompasses the work of the European Defence Agency (EDA), established to support EU member states in acquiring, developing, and operating military capabilities.

Findings

Until the full-scale Russian invasion of Ukraine in February 2022, the CSDP remained primarily a foreign policy and crisis management forum[29] without significant influence on EU members' arms acquisition. The invasion exposed Europe's vulnerability to Russian aggression and its inability to mount a coordinated response. Despite numerous meetings of EU institutions, by the end of October 2025, no agreement had been reached on a joint procurement framework covering all member states. On 27 May 2025, the Council of the European Union adopted the Security Action for Europe (SAFE) instrument[30] and on 27 June 2023, the European Parliament adopted the European Defence Industry Reinforcement through Common Procurement Act (EDIRPA), while the European Defence Industry Programme (EDIP)[31], in the autumn of 2025, was still awaiting adoption. All three instruments, however, remain frameworks enabling joint acquisition rather than concrete procurement contracts.

The SAFE loan instrument, projected at €150 billion, constitutes one of three mechanisms – alongside the planned expansion of the European Investment Bank's role in financing defence projects and the invocation of the "escape clause" in the Stability and Growth Pact to allow member states to increase their own defence spending – designed to raise the €800 billion envisaged under the ReArm Europe Plan[32]. Launched in March 2025 and also known as "Readiness 2030", this plan's core objectives include increasing European

28 Ibidem, p. 95.
29 L. Ratti, *NATO and the CSDP after the Ukraine war: the end of European strategic autonomy?*, „Canadian Journal of European and Russian Studies" 2023, no. 2, p. 79.
30 S. Clapp et al., *ReArm Europe Plan/Readiness 2023*, „EPRS Briefing" 2025, no. 4, p. 3.
31 Ibidem, p. 7.
32 Ibidem, p. 3.

defence spending, addressing critical procurement gaps, and revitalising the defence industrial base.

Several technical agreements and memoranda of understanding (MoUs) have recently been signed among European partners, though they remain predominantly bilateral or multilateral in nature. These include a Polish–Ukrainian MoU between PGZ and the Ukrainian Defence Industry covering ammunition, armoured vehicles, artillery, and air defence; another between Poland's WITU Institute and South Korea's Hanwha Aerospace concerning cooperation on 155 mm ammunition, modular charge systems, joint testing, and R&D; as well as four agreements, primarily among Scandinavian countries. Most of these arrangements concern matériel such as ammunition, drones, and heavy combat vehicles – areas in which the war in Ukraine has revealed acute shortages. They do not, however, address key strategic deficiencies that could critically affect the conduct of future conflicts. A recent assessment by the IISS[33] highlights five principal areas of concern.

Europe's NATO members face severe hardware shortfalls, including:

a) intelligence, surveillance, and reconnaissance (ISR) aircraft;
b) space launch capacity;
c) long-range conventional land-strike systems;
d) naval long-range strike and air-defence capabilities.

For example, European NATO members currently depend on eight American ISR platforms, and according to IISS estimates, developing domestic replacements would cost up to USD 4.8 billion. They also lack land-attack capabilities beyond 1,000 kilometres.

These deficiencies are compounded by software limitations. Europe lacks sovereign hyperscale cloud-computing capacity, leaving its armed forces dependent on major U.S. commercial providers. While Europe does possess a number of companies capable of delivering edge cloud-computing services and maintains a well-developed command-and-control software sector, interoperability problems persist due to the absence of common frameworks and standards.

33 *Progress and shortfalls in Europe's defence, an assessment, An IISS strategic dossier*, London 2025, p. 1–102.

Europe also lacks adequate Integrated Air and Missile Defence (IAMD) across nearly the entire threat spectrum. Although it possesses a solid technological base for guided weapons, national priorities risk duplication of effort in several areas. European terminal-phase missile-defence capabilities rely heavily on U.S. systems – either American-made systems operated by national militaries or U.S. systems deployed in Europe, most notably the Patriot system.

Although European countries are reforming their procurement processes and, as IISS research indicates, the total value of signed defence contracts nearly doubled between February 2022 and July 2025, European defence procurement remains primarily determined by national political priorities. Leading states continue to pursue sovereign industrial capabilities, perpetuating a fragmented industrial landscape.

The IISS assessment notes a major increase in European defence expenditure – 55% higher in nominal terms in 2025 than in 2022 – alongside a surge in venture capital investment in defence start-ups. However, it cautions that success is far from assured, as defence industries require long-term strategies, multiannual funding commitments, and firm contractual assurances to invest confidently.

While the exponential growth of European NATO members' armaments is broadly welcomed on both sides of the Atlantic, certain aspects of its implementation have proved controversial in Washington. As an EPRS brief notes, the SAFE regulation includes a clause stipulating that the infrastructure, facilities, and resources of contractors and subcontractors benefiting from this facility must be located in an EU or EFTA/EEA member state[34]. This reflects a long-standing European complaint that increased NATO military spending disproportionately benefits American defence manufacturers – a sentiment famously expressed by French President Emmanuel Macron, who objected to European states raising their defence budgets merely to buy American equipment[35]. While such views were once motivated by opposition to U.S. political dominance, they have since been reinforced by concerns

34 S. Clapp et al., op. cit., p. 6.

35 D.M. Herszenhorn, *Macron wants Europe to buy its own military hardware*, https://www.politico.eu/article/macron-wants-europe-to-build-its-own-military-hardware/ [access: 5.03.2025].

– particularly since the first Trump presidency – about the reliability and timeliness of American arms deliveries. Analysts from the Bruegel think tank warned[36] that if a future U.S. administration recalibrates defence exports to prioritise domestic stockpiles or Asian allies, Europe could face acute shortages. IISS experts have gone further, advising European leaders[37] to focus on building indigenous defence capacity rather than devising strategies to placate Washington. Foreign Affairs similarly cautioned[38] that purchasing more U.S. systems might please Washington but represents an inefficient – and potentially imprudent – way to strengthen European security, especially given the U.S. defence industry's substantial backlogs. For instance, the lead time for a new Patriot missile-defence system currently stands at seven years, while, according to Bruegel[39] 91% of F-35 aircraft ordered in 2023 were delivered late.

According to SIPRI[40] European NATO members are the largest clients of American arms producers, accounting for 35% of U.S. arms exports during 2020–2024, which represented 64% of their total military acquisitions in that period – up from 52% during 2015–2019[41]. This growing dependence nevertheless affords Europe considerable leverage, both as a buyer and as a supplier of components for U.S. military systems. CEPA reports[42] that European manufacturers already produce key parts of the F-35's fuselage (soon to be made in Germany) and components of the Patriot PAC-3 MSE

36 A. Burilkov, J. Mejino-Lopez, G.B. Wolff, *The US defence industrial base can no longer reliably supply Europe*, https://www.bruegel.org/analysis/us-defence-industrial-base-can-no-longer-reliably-supply-europe [access: 5.03.2025].

37 *Without US it's all about us in European defence*, https://www.iiss.org/online-analysis/online-analysis/2025/03/without-the-us-its-all-about-us-in-european-defence/ [access: 5.03.2025].

38 D. Rohac, E. Castellet Nogues, *Funding Europe's firepower: how the EU can funnel Its wealth into its defence*, Foreign Affairs 19.09.2025, https://www.aei.org/op-eds/fixing-europes-firepower-how-the-eu-can-funnel-its-wealth-into-its-defense/ [access: 5.03.2025].

39 A. Burilkov, J. Mejino-Lopez, G.B. Wolff, op. cit., p. 4.

40 K. Djokic, *Are the European NATO states moving towards self-reliance in arms procurement?*, https://www.sipri.org/commentary/topical-backgrounder/2025/are-european-nato-states-moving-towards-self-reliance-arms-procurement-qa-katarina-djokic [access: 19.03.2025].

41 Ibidem.

42 C. Badhwar, *Europe needs to keep buying American*, https://cepa.org/article/europe-needs-to-keep-buying-american/ [access: 18.02.2025].

system (manufactured in Spain and Poland). Poland, notably, is currently the world's largest producer of TNT.

Aware of Europe's determination to develop its own manufacturing base and reduce dependency on American suppliers, U.S. officials – according to Reuters[43] – have sent mixed signals. A State Department spokesperson stated that President Trump "welcomes recent efforts from European allies to strengthen their defence capabilities and take responsibility for their own security", while simultaneously warning against the creation of new barriers that would exclude U.S. companies from European defence projects.

The uneven sharing of defence costs within NATO has long been a source of U.S. dissatisfaction. Washington's response to what it perceives as European "free-riding" has typically taken the form of threats to withdraw U.S. troops from Europe or demands that host nations cover the cost of stationing American personnel. Since the Vietnam War era[44] Congress has occasionally linked funding for U.S. forces in Europe to increased allied spending, while also encouraging European states to purchase American military equipment. This dynamic reflects a persistent dilemma in U.S. alliance policy: applying enough pressure to boost sales of U.S.-made weapons without driving allies to seek alternatives.

While complete European autarky in defence procurement would sharply limit U.S. leverage, such a scenario remains unrealistic in the short-to-medium term. As Djokic notes[45], the European and U.S. arms industries are deeply intertwined through supply chains, joint ventures, and licensed production arrangements. Messmer adds[46] that the procurement challenge is "incredibly complex", and poor decisions will constrain the German armed forces – and by extension NATO – for decades. CEPA further highlights[47] Europe's limited production capacity for strike missiles and numerous other categories

43 G. Slattery, J. Irish, D. Psaledakis, *US officials object to European push to buy weapons locally*, https://www.reuters.com/world/us-officials-object-european-push-buy-weapons-locally-2025-04-02/ [access: 12.11.2025].

44 J. Deni, op. cit., p. 9.

45 K. Djokic, op. cit.

46 M. Messmer, *Will Germany rearm quickly enough?*, Chatham House Expert Comment, 26.07.2025, https://www.chathamhouse.org/2025/08/will-germany-rearm-quickly-enough [access: 15.04.2025].

47 C. Badhwar, op. cit.

of military equipment, noting that many systems are not manufactured by European firms at all. One reason is the fragmented nature of the European defence-industrial base: governments still tend to view defence investment primarily as a tool for stimulating local economies, which leads to duplication of effort. Messmer warns that this tendency risks creating rival national systems within NATO, citing competing projects such as the GCAP and SCAF next-generation fighter programmes and the ELSA and updated Storm Shadow long-range strike initiatives[48]. CEPA cautions[49] that if Europe wishes to develop sovereign defence capabilities, it must avoid vanity projects that yield inferior systems at higher cost compared to American alternatives – such as France's proposed replacement for the M270 MLRS.

This problem of fragmented European procurement is not new. As early as 1987, a Western European Union study found[50] that the lack of cooperation in weapons production cost European states approximately USD 35 billion annually – roughly 27% of their total defence spending that year. More than three decades later, Ratti observes[51] that little has changed, despite the 2016 and 2018 EU–NATO Declarations acknowledging that European defence mechanisms remained inadequate for addressing emerging security challenges. Consequently, if the strengthening of the CSDP is to meaningfully influence relations between European NATO members and the United States, rhetorical commitments – particularly from France – about achieving procurement self-sufficiency must match reality first.

Discussion

As previously noted, much of the literature on the subject identifies the cost of maintaining the American security umbrella over Europe as the main source of potential conflict in transatlantic relations. It also anticipates several future scenarios resulting from the patron's pressure on its allies to increase burden-

48 Ibidem.
49 Ibidem.
50 D.G. Haglund, op. cit., p. 168.
51 L. Ratti, op. cit., p. 74.

sharing – ranging from an incapacitated NATO to transatlantic solidarity[52] – while observing[53] – that such pressure is conditioned by two competing priorities of the patron: the need to conserve its own resources and the desire to preserve its influence within the alliance. My findings indicate that allies' susceptibility to this pressure depends largely on their own capacity to replace the patron's security guarantees with their own defence capabilities. This, in turn, varies according to each country's perception of its role and place within both NATO and the CSDP.

There is a sharp contrast between France's strategic identity, shaped by its Gaullist legacy, and that of Poland. As Longhurst and Zaborowski point out, like most Central and Eastern European states, Poland was subjected to the direct hegemony of its neighbours and deprived of sovereignty and statehood for much of its modern history[54]. From this perspective, the United States – as a distant, non-colonial liberal democracy – appears a far more attractive patron than the Franco-German axis that the development of the CSDP might lead to[55] Therefore, as the results of my research suggest, when Poland's transatlantic strategic identity comes into conflict with a European or CSDP-oriented one, the transatlantic orientation will prevail. This preference is likely to be shared by most of the so-called "new" NATO members – particularly the former involuntary members of the Soviet bloc.

As also noted earlier, the relationship between a patron and its allies is influenced by the strategic advantages that the patron derives from the alliance. This is particularly evident in U.S. alliance policy. At the height of the Vietnam War – when American military engagement in East Asia was at its peak – there were 66,531 U.S. troops stationed in South Korea and roughly 60,000 in Japan[56]. In 2025, South Korea, which faces an immediate threat from

52 T. Koivula, H. Ossa, op. cit., p. 11.
53 B.D. Blankenship, op. cit.,, p. 14.
54 K. Longhurst, M. Zaborowski, op. cit., p. 23.
55 Ibidem, p. 124.
56 B.D. Blankenship, op. cit., p. 98; T. Inoguchi, J. Ikenberry, Y. Sato *The U.S.–Japan Security Alliance*, Cham 2011; M. Priebe et al., *Balancing Act – How Allies Have responded to limited U.S. Retrenchment*, https://www.rand.org/pubs/research_briefs/RBA739-3.html [access: 30.10.2025].

its northern neighbour, hosts about 28,500 American troops. Japan, facing no comparable threat, still hosts around 55,000 U.S. military personnel[57].

This difference in treatment of allies can be reasonably explained by geopolitical considerations. The geographical spread of Japan's islands across the Pacific provides the United States with an incomparably larger area for strategic power projection than South Korea could ever offer. Thus, when assessing the potential consequences of a U.S. troop withdrawal from Europe, it must be recognised that the inability to project power on the European continent would significantly diminish the United States' role as a global power.

Conclusions

The findings of this study demonstrate that the United States derives both economic and strategic benefits from its membership in NATO. Whether these benefits outweigh the costs depends on two factors: first, the shifting geopolitical environment, and second – and perhaps more importantly – the perception of these benefits by American policymakers. Given that the current U.S. administration treats unpredictability as a deliberate instrument of political and economic strategy, threats to leave or downgrade NATO should not be dismissed outright. My assessment of efforts to create a common European security and defence policy reveals several weaknesses. Despite repeated attempts to launch joint EU-wide armament projects, very few have succeeded. For most European countries, these projects serve not only military purposes but also domestic economic ones. As a result, production is fragmented – not only across countries but often across multiple sites within a single country. Consequently, to date, attempts to implement the CSDP have failed to produce either pooled resources or economies of scale.

57 L. Shane, *US Forces Korea commander defends troop levels amid talk of cuts. Military Times*, https://www.militarytimes.com/news/pentagon-congress/2025/04/10/us-forces-korea-commander-defends-troop-levels-amid-talk-of-cuts/ [access: 30.10.2025]; *U.S. Forces Japan. About USFJ*, https://www.usfj.mil/About-USFJ/ [access: 30.10.2025].

It must also be noted that France, which possesses the largest military manufacturing base in Europe, is the world's third-largest arms exporter (accounting for 9.6% of global exports), a position that significantly benefits its balance of payments. France's prioritising of national interests in joint defence initiatives has contributed some times to their failure. Conversely, several bi- and multilateral armament projects – particularly among the Scandinavian countries – demonstrate that successful cooperation is possible when mutual interests align.

The main conclusion of this study is that, owing to its current limitations, the strengthening of the CSDP does not yet represent a serious challenge to American arms production and therefore is unlikely, for now, to become a major source of conflict in transatlantic relations. However, this conclusion should be qualified by several recommendations.

a) European politicians should refrain from making statements that antagonise the United States about "going solo" in defence procurement, particularly in areas or products that Europe will be unable to supply independently for some time;

b) Europe should avoid developing indigenous alternatives to American systems in fields such as multi-role strike aircraft, where U.S. products remain demonstrably superior;

c) European legislators should avoid introducing measures – such as the "Europeanisation clause" in the SAFE instrument – that effectively bar U.S. firms from participating in European defence markets;

d) Europe should instead seek to expand transatlantic cooperation in new armament projects on both sides of the Atlantic.

For Poland, the current situation presents both opportunities and challenges. Accordingly, in addition to the above, the following Poland-specific recommendations are proposed:

1. Participate in joint European armament projects only when clear national interests dictate it;

2. When given a choice between competing multilateral European armament projects of comparable value, prioritise cooperation with Scandinavian countries;

3. Take an active role in all discussions concerning the future development of the CSDP to ensure that Polish interests are reflected in the resulting provisions;

4. Develop much stronger and more comprehensive cooperation with Great Britain, particularly in the areas of air defence and complex weapons procurement, taking into account that such cooperation is also envisaged in the recent British Strategic Defence Review[58];

5. Closely monitor U.S. developments in military R&D and production – potentially through a dedicated defence attaché in Washington – and seek to offer U.S. companies cooperative opportunities or facilities in Poland, where feasible;

6. Maintain strong relationships with the U.S. Congress, remembering that it is Congress that approves appropriation bills.

We are living in an era of particularly fluid security dynamics. New and unforeseen developments may alter some of the findings and recommendations presented here. It is therefore essential that the issues examined in this study be continuously monitored and re-evaluated in light of changing circumstances.

Bibliography

Badhwar C., *Europe needs to keep buying American*, https://cepa.org/article/europe-needs-to-keep-buying-american/ [access: 18.02.2025].

Blankenship B.D., *The burden-sharing dilemma: Coercive diplomacy in US alliance politics*, London 2023.

Burilkov A., Mejino-Lopez J., Wolff G.B., *The US defence industrial base can no longer reliably supply Europe*, https://www.bruegel.org/analysis/us-defence-industrial-base-can-no-longer-reliably-supply-europe [access: 5.03.2025].

Clapp S. et al., *ReArm Europe Plan/Readiness 2023*, „EPRS Briefing" 2025, no. 4.

Deni J., *NATO and Article 5: The Transatlantic Alliance and the twenty-first-century challenges of collective defense*, Lanham 2017.

Djokic K., *Are the European NATO states moving towards self-reliance in arms procurement?*, https://www.sipri.org/commentary/topical-backgrounder/2025/are-european-nato-states-moving-towards-self-reliance-arms-procurement-qa-katarina-djokic [access: 19.03.2025].

58 *Strategic Defence Review. Making Britain Safer: secure at home, and strong abroad,* Ministry of Defence, London 2025, p. 74.

Giles K., *Who will defend Europe? An awakened Russia and a sleeping continent*, London 2024.

Gwadera Z., *US allies question extended deterrence guarantees, but have few options*, https://www.iiss.org/online-analysis/military-balance/2025/03/us-allies-question--extended-deterrence-guarantees-but-have-few-options/ [access: 20.03.2025].

Haglund D.G., *Alliance within alliance? Franco-German military cooperation and the European pilar of defense*, New York 2018.

Hallams E., *The United States and NATO since 9/11: The Transatlantic Alliance renewed*, New York 2010.

Herszenhorn D.M., *Macron wants Europe to buy its own military hardware*, https://www.politico.eu/article/macron-wants-europe-to-build-its-own-military-hardware/ [access: 5.03.2025].

Inoguchi T., Ikenberry J., Sato Y., The U.S.–Japan Security Alliance, Cham 2011.

Koivula T., Ossa H., *NATO's Burden-sharing disputes: Past, Present and Future Prospects*, Cham 2022.

Lansford T., Tashev B., *Old Europe, new Europe and the US: Renegotiating Transatlantic Security in the post 9/11 era*, Burlington 2005.

Longhurst K., Zaborowski M., *Old Europe, new Europe and the transatlantic security agenda*, New York 2005.

Messmer M., *Will Germany rearm quickly enough?*, Chatham House Expert Comment, 26.07.2025, https://www.chathamhouse.org/2025/08/will-germany-rearm-quickly-enough [access: 15.04.2025].

Priebe M., et al., *Balancing Act – How Allies Have responded to limited U.S. Retrenchment*, https://www.rand.org/pubs/research_briefs/RBA739-3.html [access: 30.10.2025].

Progress and shortfalls in Europe's defence, an assessment, An IISS strategic dossier, London 2025.

Ratti L., *NATO and the CSDP after the Ukraine war: the end of European strategic autonomy?*, „Canadian Journal of European and Russian Studies" 2023, no. 2.

Rohac D., Castellet Nogues E., *Funding Europe's firepower: how the EU can funnel Its wealth into its defence*, Foreign Affairs 19.09.2025, https://www.aei.org/op-eds/fixing-europes-firepower-how-the-eu-can-funnel-its-wealth-into-its-defense/ [access: 5.03.2025].

Rynning S., *NATO: From cold war to Ukraine, a history of the world's most powerful alliance*, London 2024.

Shane L., *US Forces Korea commander defends troop levels amid talk of cuts.* Military Times, https://www.militarytimes.com/news/pentagon-congress/2025/04/10/us-forces-korea-commander-defends-troop-levels-amid-talk-of-cuts/ [access: 30.10.2025].

Slattery G., Irish J., Psaledakis D., *US officials object to European push to buy weapons locally,* https://www.reuters.com/world/us-officials-object-european-push-buy-weapons-locally-2025-04-02/ [access: 12.11.2025].

Strategic Defence Review. Making Britain Safer: secure at home, and strong abroad, Ministry of Defence, London 2025, p. 74

U.S. Forces Japan. About USFJ, https://www.usfj.mil/About-USFJ/ [access: 30.10.2025].

Wendt A., *Social theory of international politics*, Cambridge 1999.

Without US it's all about us in European defence, https://www.iiss.org/online-analysis/online-analysis/2025/03/without-the-us-its-all-about-us-in-european-defence/ [access: 5.03.2025].

Closing Note

This special issue advances a genuinely system-level account of contemporary security by tracing the linkages among grey-zone statecraft, dual-use technological acceleration, integrated air-and-missile-defence architectures, criminalised and conflict-embedded economies, and – crucially – Europe's defence integration under the CSDP and its implications for transatlantic cohesion. Read together, the contributions contend that today's security dilemmas are not discrete problems but interacting subsystems in which legal frameworks, market incentives, technological standards, and organisational routines co-evolve under strategic pressure. In the European theatre, this co-evolution must reconcile industrial policy ambitions with alliance management, standardisation, and pragmatic co-production.

I hope these studies inform both scholarly debate and policy design wherever evidence, doctrine, and operational practice must be aligned at speed – whether in counter-disinformation efforts, capability integration and procurement (including EDIP/EDIRPA/SAFE trajectories), or in building resilient supply-chain and export-control regimes that support NATO interoperability. I am grateful to our authors for their intellectual discipline and empirical care, to our anonymous reviewers for their field-shaping critiques, delivered with generosity, and to the editorial team for the meticulous, often invisible work that enables coherence under tight timelines.

Looking ahead, we invite submissions that extend this agenda. We seek comparative research that links theatres and sectors. We welcome mixed-method evaluations that can adjudicate causal claims in data-poor settings. We also encourage policy experiments that stress-test resilience, build regulatory capacity – standards, audits, red-teaming – and strengthen alliance interoperability at the technical, legal, and organisational levels.

We particularly welcome pieces that translate theoretical clarity into implementable roadmaps for public authorities, private providers, and civil society operating in contested information spaces and fragile institutional contexts.

Dr Magdalena El Ghamari, Issue Editor
Centre for State Security Threat Studies
Academic Centre for Strategic Analysis (ACAS)
University College of Professional Education, WSKZ
ORCID: 0000-0001-5798-7545
Contact: m.el-ghamari@akademia.mil.pl