BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Privatization of Security Revisited: the Expansion of Private Security Companies in the Age of Hybrid Conflict (2013-2025)

Andrei Alexandru BABADAC*
* Romanian agency for investment and foreign trade, Romania
e-mail: andrei@andreibabadac.org

Abstract

We are witnessing the emergence of the "distributed state" : a governance model where sovereign responsibilities are networked rather than hierarchical. This article revisits the trajectory of private security companies (PSCs) over the last decade, identifying a structural transition from neoliberal outsourcing to "distributed sovereignty". Drawing on the theoretical frameworks of Singer and McFate, the analysis reveals how the "market for force" has expanded into the cognitive and cyber domains , effectively outsourcing the definition of security itself. The article highlights the specific implications for governance, noting that private security is embedded in resilience plans at EU as well as in Romania at national level, this dependency creates new vulnerabilities regarding accountability and strategic autonomy. Ultimately, the article posits that the regulation of this distributed architecture will define the legitimacy of the twenty-first-century state.

Keywords:
Privatization of Security; Hybrid Warfare; Cyber Governance; Private Military Companies; Security Governance; Durable Disorder.

Article info
Received: 27 October 2025; Revised: 11 November 2025; Accepted: 4 December 2025; Available online: 15 January 2026

Citation: Babadac, A.A. 2025. "Privatization of security revisited: the expansion of private security companies in the age of hybrid conflict (2013–2025)". *Bulletin of "Carol I" National Defence University*, 14(4): 87-98. https://doi.org/10.53477/2284-9378-25-60

Introduction: From Liberal Peace to Strategic Disorder

When Privatization of Security was first published in 2013 (Babadac 2013), the expansion of private security companies (PSCs) appeared as a rational extension of neoliberal economic reform and state modernization. The logic of efficiency and flexibility – imported from corporate management – seemed to provide governments with a tool for maintaining global order at lower cost and higher responsiveness. That moment coincided with what many scholars then described as the "liberal peace paradigm": a belief that global governance, international institutions, and open markets could together sustain a predictable security environment.

A decade later, that world has fractured. The erosion of multilateralism, the diffusion of technology, and the hybridization of warfare have produced what McFate (2019) terms an "age of durable disorder," in which instability is not an exception but a systemic feature. The privatization of security no longer functions merely as a symptom of neoliberal outsourcing – it has become a structural mechanism for managing disorder. Private security companies, defense contractors, cyber firms, and risk consultancies now populate what Singer (2003) originally called the "market for force," but that market has since evolved from the physical battlefield to the digital, information, and psychological domains.

This transformation reveals the paradox of twenty-first-century security: while states remain the principal legal authorities in war and peace, they depend increasingly on private actors to maintain both. The wars of Iraq and Afghanistan created a foundation for private military contracting; the conflicts in Syria, Yemen, and Ukraine have normalized it. The post-2014 hybrid confrontations between Russia and the West blurred traditional distinctions between state and non-state, military and commercial, legitimate and clandestine. As Petraeus and Roberts (Petraeus and Roberts 2022) demonstrate, the "character" of warfare evolves faster than its nature: technology, information, and privatization have changed the ways states exercise power, but not the political purposes for which power is used.

At the same time, the privatization of security exposes a deeper normative tension. Kilcullen (2009, 45) observed that modern conflicts occur "among the people," where legitimacy and perception matter as much as firepower. The proliferation of private security actors within societies – guarding cities, ports, and data centers – blurs the line between citizen and client, protection and control. In this sense, privatization represents not simply a reconfiguration of military capacity but a redefinition of political authority.

By 2025, the global private security industry will encompass not only military contracting but also cyber defense, crisis logistics, satellite surveillance, and AI-based threat analysis. The phenomenon must therefore be analyzed not merely

through the lens of economics, but through the frameworks of security governance, technological acceleration, and political legitimacy. As the following sections argue, the privatization of security now constitutes a central component of what might be called the "distributed state": a system in which power is networked, responsibilities are outsourced, and security has become both a commodity and a governance function.

Theoretical Framework: Security Governance in the Market for Force

The privatization of security erodes the Weberian concept of the state's monopoly on legitimate violence, replacing it with polycentric governance networks. These networks merge state institutions, corporate entities, and non-state actors into complex systems of contractual control. As Avant (2016) argues, private security markets embody neoliberal governance itself: authority becomes distributed, and accountability becomes transactional.

Singer's model (Singer 2003) of the market for force remains instructive. It describes a world where private firms compete to offer military expertise, logistics, and technology in the same way global corporations offer financial or transport services. However, the 2020s have extended this logic far beyond physical combat: private actors now guard data, algorithms, and infrastructure as much as territory or personnel.

McFate's notion of "durable disorder" (McFate 2019) usefully frames the coexistence of permanent instability and commercialized security. Yet, it must now be understood alongside a resurgence of great-power competition. Petraeus and Roberts show how modern conflict spans from high-intensity mechanized warfare to irregular insurgencies and digital campaigns (Petraeus and Roberts 2022). Ryan identifies this as the fusion battlefield – a multidimensional environment in which conventional, cyber, and informational operations intertwine (Ryan 2022, 58).

Within this system, privatization represents a form of strategic adaptation. States increasingly rely on private partners for flexibility, deniability, and innovation. As Brose warns, reliance on slow, state-owned defense bureaucracies has rendered Western militaries vulnerable to faster, cheaper, and decentralized technologies-precisely the space in which private companies excel (Brose 2020).

The Transformation of Warfare and the New Drivers of Privatization

The hybridization of warfare – where conventional, irregular, information, and economic instruments converge – has elevated the private sector from subcontractor to co-producer of power. The Russian Federation's use of private military companies

such as the Wagner Group exemplifies this evolution. Wagner's operations across Ukraine, Syria, Libya, and several African states revealed how private entities could extend state influence while maintaining plausible deniability. Wagner combined mercenary tactics with corporate organization, functioning simultaneously as a geopolitical instrument and a commercial venture securing mining, logistics, and infrastructure contracts (Sukhankin 2019).

In liberal democracies, the logic differs, but the effect converges. The United States and its allies increasingly rely on private partners not only for logistics and protection, but for intelligence, cyber operations, and weapons systems integration. Companies like Constellis and Aegis manage complex security portfolios; Palantir Technologies, meanwhile, provides real-time battlefield analytics and AI-driven targeting support that underpin modern command architectures. The war in Ukraine has demonstrated the indispensability of private data, satellite, and software providers to contemporary defense. Starlink's communications systems and Maxar's satellite imagery illustrate how private assets have become operational components of state warfighting capacity.

Singer's (2003) early observation – that corporations would one day rival states as military providers – has materialized. Today, the boundaries between defense contractors, information firms, and military actors are fluid. What Kilcullen described as "wars among the people" now occur through networks managed as much by engineers and coders as by soldiers (Kilcullen 2009).

The cyber domain has become the most dynamic arena of privatized security. Since 2013, the explosion of ransomware, espionage, and hybrid cyber-operations has pushed states to outsource both defensive and offensive capabilities to private entities. Firms such as CrowdStrike, FireEye, and Palo Alto Networks have evolved into quasi-sovereign defenders of national infrastructure. Their operations – attributing attacks, restoring compromised systems, or neutralizing malware – represent functions traditionally associated with intelligence and defense agencies (Deibert 2020).

This digital privatization introduces profound strategic implications. Brose emphasizes that the future of warfare will hinge not on superior firepower, but on control of the "kill chain" – the integration of sensors, data, and decisions across distributed networks (Brose 2020). Private technology companies now dominate this chain. Their algorithms determine how states perceive threats, allocate responses, and manage escalation. The speed at which data flows through these networks gives private actors a form of temporal power: the ability to shape not only the way conflicts are fought, but also when and why they occur.

Furthermore, the cybersecurity industry functions as a market of deterrence. Corporations sell "resilience" as a subscription service – protecting critical

infrastructure, financial systems, and even democratic processes. This model transforms security from a collective good into a privatized commodity. The same firms that defend against cyber threats often conduct post-incident consultancy, risk assessment, and narrative control, blurring lines between defense, information management, and reputation protection.

Ryan (2022) and Petraeus & Roberts (2022) both argue that the next decade of conflict will be defined by the integration of artificial intelligence and autonomous systems into every level of warfare. The private sector leads this transformation. Companies like Anduril, Shield AI, and Helsing in Europe develop autonomous reconnaissance and targeting platforms for both commercial and military clients. The result is a new military-industrial ecology, in which innovation cycles are driven by venture capital and dual-use technology rather than state procurement.

This ecology erodes the traditional separation between public defense and private enterprise. As Ryan notes, the "fusion battlefield" combines physical and digital domains through continuous data exchange. The private sector's dominance in AI and machine learning ensures that states must either collaborate or risk obsolescence. The privatization of autonomy extends beyond hardware into the algorithms that prioritize threats and allocate force – effectively delegating elements of command to code.

Privatization also reflects economic adaptation. Global defense spending has increasingly flowed through private channels; by 2025, private security and defense firms will constitute one of the fastest-growing sectors in transnational capital markets. This growth corresponds to what McFate calls the "endless demand for security" in a world of enduring instability (McFate 2019). Yet it also reinforces structural dependency: states outsource risk but not responsibility, while corporations acquire influence without accountability.

Petraeus and Roberts stress that even in Ukraine – a conflict marked by traditional attrition – private actors play decisive roles in logistics, information, and precision support (Petraeus and Roberts 2022). The trend suggests a return not to total war but to total mobilization, in which the entire society, including its private sector, becomes a participant in conflict. In this environment, privatization is not a deviation from the state's function but a constitutive element of its resilience strategy.

Political Economy, Law, and Ethics of Privatized Security

Privatization of security must be situated within a broader political-economic and legal framework. It is not simply an operational convenience but an expression of neoliberal governance – the extension of market rationality into domains once reserved for sovereign authority. As Avant (2016) and Krahmann (2017) note, private security embodies a shift from hierarchy to network, from rule-based administration to contract-based management.

Economically, this transformation creates powerful incentives for perpetual insecurity. Security becomes a growth industry. McFate cautions that in a world of durable disorder, peace may no longer be profitable (Avant 2016). When stability threatens revenue, actors – whether corporations or states – may prefer managed instability. This dynamic mirrors what Kilcullen observed in counterinsurgency: the presence of external contractors often sustains the conflict ecosystems they claim to resolve (Kilcullen 2009).

Legally, privatization challenges the foundations of accountability. International humanitarian law presupposes clear chains of command and state responsibility. Yet private entities operate in contractual rather than hierarchical relationships, complicating liability for violations. The Montreux Document and the International Code of Conduct for Private Security Providers represent attempts to regulate the industry, but both remain voluntary. As Petraeus and Roberts remark, "war has outpaced law". (Petraeus and Roberts 2022)

Ethically, the privatization of security raises fundamental questions of legitimacy. Who authorizes the use of force when private actors are both providers and beneficiaries of insecurity? Can a corporation claim moral neutrality while shaping the conditions of conflict? Brose (2020) and Deibert (2020) highlight parallel dilemmas in the digital sphere: algorithmic decision-making and data monopolies concentrate enormous coercive power in non-state hands.

The privatized security sector thus occupies an ambiguous moral terrain. It enables states to act more efficiently, yet undermines the collective control that defines legitimate authority. Its normalization – across military, cyber, and information domains – represents the quiet privatization of sovereignty itself.

The European and Romanian Context: Integration, Regulation, and Strategic Autonomy

The European experience provides an illuminating case of how privatization, once treated as a pragmatic response to shrinking defense budgets, has matured into a pillar of continental resilience. Within the European Union (EU), the evolution of private security has been shaped not only by market forces but also by normative frameworks that embed private actors in hybrid governance.

Following the 2015 migration crisis, a series of terrorist attacks, and the acceleration of Russian hybrid operations, the EU has pursued a comprehensive strategy of resilience. The EU Security Union Strategy 2020-2025 formalized what was already occurring in practice: the outsourcing of critical security functions to private entities operating under EU-wide standards. Private firms now manage cybersecurity for financial systems, surveillance of transport nodes, and logistics for humanitarian operations. The European Defence Fund and Permanent Structured Cooperation

(PESCO) have also opened the defense innovation ecosystem to private consortia, aligning commercial innovation with collective defense objectives.

This institutionalization of privatized security has altered the balance between regulation and competition. The International Code of Conduct Association (ICoCA) and ISO 18788:2015 standards have established operational benchmarks, but enforcement remains fragmented across national jurisdictions. Some member states – such as France, the Netherlands, and Romania – maintain rigorous licensing regimes, while others adopt a lighter regulatory touch to encourage competitiveness. The result is a semi-harmonized market in which private actors operate under a patchwork of overlapping but non-binding rules.

The paradox for the EU is evident. On the one hand, privatization advances efficiency and innovation; on the other, it complicates accountability and coherence. The emergence of strategic autonomy as an EU goal reinforces this duality: autonomy requires both technological independence and regulatory unity. Yet, the EU's reliance on private cyber-defense and logistics contractors means that strategic autonomy itself now depends on the coordination of public and private capabilities rather than on purely state capacity.

Within NATO, privatization has become structurally embedded. The Alliance's Defence Innovation Accelerator for the North Atlantic (DIANA) and NATO Innovation Fund explicitly link private firms with military innovation pipelines. Cyber resilience, satellite surveillance, and unmanned systems development increasingly occur through public-private ecosystems. While this collaboration enhances adaptability, it also produces dependence: the defense of critical digital infrastructure, for instance, now rests on contracts with corporations headquartered in a handful of Western economies.

Petraeus and Roberts argue that modern warfare's tempo leaves no alternative; state bureaucracies cannot innovate at market speed (Petraeus and Roberts 2022). Yet this logic raises questions about sovereignty and interoperability. If deterrence is underwritten by private code and cloud services, who ensures its continuity in a crisis? The Article 5 guarantee, traditionally grounded in state capacity, now requires the participation of firms that are neither bound by alliance treaties nor accountable to electorates.

Romania's security sector illustrates how a national market can evolve from reactive service provision to strategic partnership. In the early 2000s, private security primarily addressed domestic protection of banks, malls, and critical facilities. By the 2020s, the industry had diversified into cyber defense, energy-infrastructure security, and intelligence consultancy. Successive amendments to Law 333/2003 modernized licensing and oversight, while EU accession facilitated integration into continental standards.

Romania's geopolitical position – bordering Ukraine and the Black Sea – has made it a frontline state in the European hybrid-threat landscape. Private Romanian firms now participate in NATO logistics, maritime security, and EU cyber-resilience initiatives. Several companies provide AI-based surveillance and maritime situational awareness for the Danube–Black Sea corridor, supported by EU funding mechanisms. The private sector's involvement in critical-infrastructure protection and civil-military preparedness demonstrates how privatization, properly integrated, can enhance state resilience rather than undermine it.

Yet, vulnerabilities persist. Oversight mechanisms remain under-resourced, and coordination between ministries and corporate actors is inconsistent. Romania's experience thus mirrors the continental challenge: privatization strengthens operational capacity, but demands equally robust governance to safeguard legitimacy.

Accountability, Ethics, and the Human Security Dilemma

The growing entanglement of private actors in security functions raises enduring normative questions about accountability, transparency, and human rights. The diffusion of coercive authority across contracts and algorithms erodes traditional notions of public responsibility.

International law still assumes clear chains of command. The Geneva Conventions and their Additional Protocols were drafted for state militaries, not corporate contractors. The Montreux Document remains the principal soft-law instrument, emphasizing state obligations to regulate PMSCs (International Committee of the Red Cross and Swiss Government 2008). Yet, its voluntary nature limits its reach. ICoCA has created a framework for compliance and grievance mechanisms, but its jurisdiction is neither global nor binding.

This gap is compounded in cyberspace. Private cybersecurity firms operate transnationally, frequently crossing legal boundaries to investigate or counter intrusions. Attribution – the act of identifying a culprit – has strategic implications: when a private company publicly attributes a cyberattack to a foreign state, it can escalate diplomatic tensions. Deibert notes that such "narrative authority" constitutes a new form of soft power exercised by corporate actors. Thus, privatization extends beyond security delivery to security definition – deciding who is a threat and what constitutes aggression (Deibert 2020).

The ethical dilemma centers on motive. In the classical social contract, protection was a public duty; in the privatized model, it is a service sold under profit motives. McFate warns that in a marketized security order, peace becomes unprofitable. The economic incentives driving private actors may diverge from the humanitarian imperatives of stability (McFate 2019).

Brose's account of U.S. defense procurement illustrates how entrenched interests resist disruption even when innovation is vital. Similarly, in the global security

market, large firms thrive on continual demand (Brose 2020). This structural dependency risks transforming security into an endless commodity cycle: threat inflation feeds contract renewal, and crisis becomes a business model.

Human-security advocates argue that this commodification undermines universality. When protection depends on the ability to pay, inequalities deepen. The privatization of border control, for instance, often results in harsh enforcement practices outsourced to companies shielded from public scrutiny. Likewise, private surveillance networks in urban environments generate data asymmetries that reinforce social stratification.

To reconcile efficiency with ethics, governance must evolve. Three principles are essential:

1. Transparency – public disclosure of contracts, operational mandates, and risk assessments.
2. Accountability – legal mechanisms that attach responsibility for misconduct both to firms and to the states that employ them.
3. Human-centric design – embedding human rights due diligence into technological and operational planning.

These principles resonate with Ryan's vision of a "values-based adaptation" in future warfare: states and corporations must integrate ethical foresight into innovation cycles (Ryan 2022). Only through such integration can privatization serve collective security rather than narrow interest.

Privatization, Technology

The decade ahead promises an even deeper convergence of technology, markets, and security. Petraeus and Roberts foresee an era of simultaneous competition across land, sea, space, and cyberspace – a "multi-domain continuum" (Petraeus and Roberts 2022). Privatization will be central to that continuum, not peripheral.

Autonomous systems – drones, sensors, and robotic platforms – are increasingly produced by private firms. The integration of AI into command systems will extend the delegation of decision-making from humans to algorithms. Ryan predicts that the next revolution in military affairs will be cognitive, defined by the struggle to shape perception and information flows. Private tech companies, social-media platforms, and data-analytics firms already play decisive roles in that domain (Ryan 2022).

The implication is profound: control of cognition becomes control of conflict. When algorithmic systems determine threat priorities or disseminate narratives, they effectively wield strategic influence. Unless constrained by transparent governance, this cognitive privatization may distort democratic decision-making and blur truth itself as a weapon.

Global defense-technology markets link security to financialization. Venture-capital investment in dual-use technologies – from autonomous drones to quantum encryption -creates a transnational web of dependency. States compete for innovation while relying on globalized supply chains vulnerable to disruption. The line between strategic partner and commercial supplier becomes indistinct.

McFate's concept of "durable disorder" applies here: the security economy thrives on volatility (McFate 2019). Yet, as Brose observes, technological disruption can also empower smaller states and non-state actors, democratizing power but amplifying instability (Brose 2020). The challenge for governance lies in balancing innovation's benefits against its centrifugal effects on authority.

A gradual counter-trend is emerging: states and international bodies are revisiting regulation. Proposals for an updated Montreux 2.0 framework and the EU's Artificial Intelligence Act aim to extend accountability into algorithmic security. The goal is not to reverse privatization, but to civilize it – to create what might be termed ethical sovereignty, where private capability operates under public norms.

Such efforts will face resistance from both corporate lobbies and great-power rivalry. Nevertheless, they mark an acknowledgment that the future of security cannot rest solely on efficiency; legitimacy must anchor capability.

Governing the New Security Order

Privatization of security has matured into one of the defining structural transformations of the early twenty-first century. The process that began as fiscal outsourcing has evolved into a system of distributed sovereignty, where public and private actors co-produce security, intelligence, and deterrence. This new order reflects both continuity and rupture: continuity with the state's enduring need to monopolize organized violence, and rupture in the means through which that monopoly is exercised.

The preceding analysis suggests that privatization has moved through three overlapping phases. The first, identified by Singer, was the corporate phase-the rise of private military companies performing tactical tasks for states (Singer 2003). The second, corresponding roughly to 2010–2020, was the technological phase, in which cybersecurity, information warfare, and AI-driven analytics became privatized. The third, emerging today, may be termed the governance phase: private actors now participate directly in shaping strategic environments and global norms.

This trajectory has profound implications for statehood and international order. As McFate argues, the traditional distinction between war and peace has dissolved into a continuum of durable disorder (McFate 2019). Yet, this disorder is not chaotic; it is organized through contracts, algorithms, and economic interdependence.

Privatization provides structure to instability – it commercializes uncertainty and institutionalizes flexibility.

At the same time, thinkers such as Petraeus and Roberts remind us that warfare remains fundamentally political. States cannot delegate legitimacy, even when they outsource capability (Petraeus and Roberts 2022). The challenge, therefore, is not to resist privatization, but to regulate it – embedding ethical and legal standards into the architecture of hybrid governance.

The implications extend beyond conflict. The privatization of cyber and AI security signifies a deeper societal shift toward algorithmic authority. Decisions about surveillance, risk assessment, and even deterrence are increasingly automated and corporatized. As Brose (2020) and Deibert (2020) warn, such concentration of digital power risks undermining democratic accountability. The emerging frontier of "defense tech capitalism" fuses national security with venture investment, creating a geopolitical economy in which code becomes a strategic asset and sovereignty is expressed through data ownership.

Ultimately, the evolution of privatized security represents a reconfiguration of the social contract. In classical political thought, citizens granted the state the right to use force in exchange for protection. In the privatized order, that exchange becomes transactional: protection is purchased, not guaranteed. This commodification of safety alters the moral foundation of governance. The question is no longer merely who controls the means of violence but who controls the platforms that define security itself.

Looking toward 2035, three outcomes appear plausible. First, a pragmatic consolidation: states will integrate private partners through licensing, joint command systems, and data-sharing frameworks – what might be called "regulated hybridity." Second, a normative backlash: demands for transparency and human rights accountability will generate new global standards akin to a Montreux 2.0. Third, a dystopian drift: if left unchecked, privatization could entrench inequality, where protection is stratified by wealth and access to technology.

The choice among these futures will depend on governance. As Singer warned two decades ago, the privatization of force is irreversible once institutionalized. The task before policymakers and scholars is therefore to ensure that private power operates within democratic bounds, not beyond them. The next frontier of security governance will not be defined by the weapons we wield but by the contracts, codes, and ethical commitments that determine who wields them, for whom, and at what cost.

The privatization of security has evolved from post-Cold War outsourcing into a defining feature of twenty-first-century warfare and governance. This article revisits and expands the 2013 analysis of private security companies in light of

the transformations brought by hybrid warfare, digitalization, and geopolitical realignment. Drawing on contemporary perspectives from Singer, McFate, Petraeus, Ryan, and others, it situates private security within a broader framework of security governance and durable disorder. The study examines how private actors now operate across kinetic, cyber, and cognitive domains – reshaping sovereignty, accountability, and the political economy of conflict. It argues that privatization no longer supplements state power, but constitutes one of its structural components, demanding new ethical and regulatory approaches. The article concludes that effective governance of privatized security will determine whether it strengthens collective resilience or deepens global inequality.

References

Avant, Deborah D. 2016. *Markets, Hierarchies, and Networks in Private Security Governance*. *Security Dialogue* 47 (4): 293–310.

Babadac, Andrei Alexandru. 2013. "Privatization of Security: Fundamental Factors in the Expansion of Private Security Companies." *International Scientific Conference Strategies XXI:* 314-320. https://cssas.unap.ro/en/pdf_books/conference_2013.pdf.

Brose, Christian. 2020. *The Kill Chain: Defending America in the Future of High-Tech Warfare*. New York: Hachette Books.

Deibert, Ronald. 2020. *Reset: Reclaiming the Internet for Civil Society*. Toronto: House of Anansi Press.

International Committee of the Red Cross and Swiss Government. 2008. *The Montreux Document on Pertinent International Legal Obligations and Good Practices for States Related to the Operations of Private Military and Security Companies during Armed Conflict*. Montreux, Switzerland: International Committee of the Red Cross and Swiss Government.

Kilcullen, David. 2009. *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One*. New York: Oxford University Press.

Krahmann, Elke. 2017. *The Transformation of Security Governance: Beyond the State and the Market*. London: Routledge.

McFate, Sean. 2019. *The New Rules of War: Victory in the Age of Durable Disorder*. New York: William Morrow.

Petraeus, David, and Andrew Roberts. 2022. *Conflict: The Evolution of Warfare from 1945 to Ukraine*. New York: Harper.

Ryan, Mick. 2022. *War Transformed: The Future of Twenty-First-Century Great Power Competition and Conflict*. Annapolis, MD: Naval Institute Press.

Singer, P.W. 2003. *Corporate Warriors: The Rise of the Privatized Military Industry*. Ithaca, NY: Cornell University Press.

Sukhankin, Sergey. 2019. *Russian PMCs in the Gray Zone: The Case of Wagner Group*. Washington, DC: Jamestown Foundation.