Commercial Pathways and Proxy Power: How Irregular Forces Acquire Advanced Capabilities

Description

In June 2024 Italian customs officials opened shipping containers labeled â??wind turbine partsâ?• bound for Libya. Inside were disassembled components for Chinese Wing Loong II dronesâ??the same systems UN investigators had forensically linked to the January 2020 Tripoli military academy strike that killed twenty-six cadets. Four years of documentation, investigations, and enforcement actions had failed to stop the flow of deadly weapons. No supplier state faced meaningful export restrictions. No strategic partnerships were materially suspended. The components kept moving.

For irregular warfare practitioners, Libya demonstrates how proxy forces acquire advanced capabilities through commercial systems explicitly designed to preserve state deniability. This reveals something more significant than an enforcement failure. It demonstrates how commercial networks enable proxy forces to access advanced military capabilities while bypassing the state-centric arms control frameworks designed to prevent such transfers.

Department of Defense Instruction 3000.07 defines irregular warfare as â??a form of warfare where states and non-state actors campaign to assure or coerce states or other groups through indirect, non-attributable, or asymmetric activities.â?• The Libya example illustrates this definition. Commercial pathways provide the non-attributable mechanisms through which state sponsors enable proxy forces while maintaining deniability.

Understanding these pathways is operationally critical. They determine what capabilities adversary proxy forces can field, how sponsors maintain deniability, and where intelligence collection and policy interventions must focus.

Libya as an Irregular Warfare Laboratory

The Libyan conflict since 2020 epitomizes contemporary irregular warfare. The Libyan National Army (LNA) operates as a proxy force backed by the United Arab Emirates (UAE), Russia, and Egypt, while the Government of National Accord militias receive Turkish and Qatari support. While external support flowed through indirect channels, proxy force capabilities adapted qualitatively during the 2020-2024 period.

Historical examples of irregular warfare portray major powers supplying small arms, light weapons, and anti-aircraft missiles to proxy forces. These capabilities enabled resistance efforts, but maintained clear technological gaps between irregular forces and conventional militaries. Libya demonstrated a shift in capability diffusion. Proxy forces gained precision strike capabilities through Chinese Wing Loong II drones, sophisticated medium-altitude long-endurance systems capable of systematic targeting through integrated sensor-to-shooter architectures.

In the January 2020 Tripoli military academy strike, UN investigators traced supply chains through UAE networks. The international response followed established patterns with sanctions on transport intermediaries like Sigma Airlines, European Union (EU) targeted measures, and diplomatic pressure through UN Security Council statements. Yet the June 2024 customs seizure proved enforcement efforts achieved limited tactical disruptions while strategic transfer networks remained intact. For irregular warfare operations, this matters because it signals a capability proliferation pattern that doctrine and intelligence priorities havenâ??t fully incorporated. Proxy forces now access technology that narrows gaps with conventional forces while sponsors maintain deniability through commercial structures.

Commercial Integration as Strategic Architecture

Three commercial mechanisms enabled Libyan proxy forces to field advanced capabilities: joint venture production, software and services unbundling, and integration hub models.

Joint Venture Production

The Wing Loong II systems used in Libya werenâ??t simply exported from China. Production occurred through joint ventures between Chinese manufacturers and UAE entities, creating domestic production that bypassed traditional export controls. This model transforms what would trigger scrutiny as a cross-border sale into domestic manufacturing within an allied state.

EDGE Group, the UAE state defense conglomerate formed in 2019, operates joint ventures with Chinese defense contractors including China Aerospace Science and Technology Corporation (CASC). These partnerships produce unmanned aerial vehicles (UAVs) in UAE facilities rather than importing complete systems. When Wing Loong II components appear in Libya, they carry UAE, not Chinese, provenance.

For irregular warfare operations, this matters operationally. Intelligence collection focused on Chinese exports misses UAE-produced systems with identical capabilities. Moreover, arms control mechanisms

targeting Chinese sales donâ??t apply to UAE domestic production, even when the same Chinese technology enables the capability. Proxy forces gain advanced systems while sponsors maintain deniability through commercial partnership structures.

Software and Services Unbundling

Focusing on hardware export controls alone doesnâ??t capture what makes modern military systems effective. Targeting algorithms, sensor fusion packages, and autonomous decision systems flow as software and technical services, not physical exports.

Wing Loong II drones deployed in Libya integrated Chinese AR-1 and Blue Arrow-7 missiles through targeting software packages that enabled precision strikes. These algorithmic capabilities are transferred through technical service contracts and software licensing arrangements that fall outside traditional arms control mechanisms. A drone airframe alone doesnâ??t conduct precision strikes. The integrated software package converts commercial UAV platforms into precision targeting systems.

The operational implication is that intelligence collection must track software transfers and integration services, not just hardware shipments. Traditional arms monitoring focuses on physical components crossing borders. Modern capability transfer occurs through code repositories, technical support contracts, and integration services delivered remotely.

Integration Hub Models

EDGE Groupâ??s structure illustrates how integration hubs function as capability multipliers. Rather than producing complete systems, integration hubs combine commercial components, proprietary software, and foreign military technology into operational capabilities. The model systematically evades controls designed around complete weapon systems by assembling capabilities from components that individually escape scrutiny.

EDGE operates across 25 entities spanning missiles, cyber warfare, and autonomous systems. When UN investigators documented Wing Loong II deployments in Libya, they traced components through multiple corporate entities and jurisdictions. The airframe came through one channel, targeting systems through another, and integration services through a third. No single transaction triggered export controls because the integrated capability only emerged at the hub.

For irregular warfare practitioners, this means proxy force capabilities canâ??t be assessed by counting delivered systems. Integration hubs enable capabilities by combining commercially available

components that only become military systems through integration services. Intelligence priorities must track hub capacity and integration partnerships, not just component transfers.

Why Arms Control Frameworks Fail

Traditional arms control assumes sovereign states as primary actors, bilateral or multilateral agreements as enforcement mechanisms, and sufficient political will for collective action when violations are documented. Advanced capability transfers to proxy forces operate differently.

Commercial networks involve multiple intermediaries across jurisdictions. Joint venture production occurs inside integration hubs, rendering domestic what would otherwise trigger export controls. Software and services flow through corporate structures designed to minimize regulatory oversight. Enforcement targets replaceable logistics actors. Critically, strategic value calculations by states often override arms control norms.

The UAE is another example that illustrates this dynamic clearly. Despite documented Libya embargo violations from 2020 through 2024, the UAE hosts Al Dhafra Air Base and critical Western military infrastructure. The country maintains $29.3 billion in active U.S. Foreign Military Sales cases as of early 2025, and serves as an Abraham Accords partner advancing Middle East policy objectives. When Italian customs seize shipments and the EU sanctions logistics companies, supplier states face no export restrictions, joint ventures undergo no enhanced scrutiny, and strategic partnerships remain unchanged. The end result is documentation without accountability. The strong U.S. interests in the UAE mean the commercial pathways enabling proxy force proliferation receives insufficient scrutiny.

For irregular warfare practitioners, this creates a predictable adversary playbook. Structure capability transfers through commercial pathways specifically designed to exploit these gaps. The operational question shifts from â??will adversaries attempt to arm proxy forcesâ?• to â??how will they structure transfers to avoid consequences.â?• These commercial pathways demand adjustments in intelligence priorities, force protection assumptions, and policy mechanisms.

Intelligence Collection Must Expand Beyond Traditional Targets

Tracking military exports and government procurement only captures state-to-state transfers. Commercial joint ventures, software licensing agreements, integration hub production capacity, and dual-use logistics networks should become primary collection targets.

Expanding collection beyond state military actors requires different methods and coordination across agencies that traditionally focus on government-to-government transfers rather than commercial defense ecosystems. Commercial intelligence capabilities must map corporate ownership structures and financial flows. Technology tracking systems must monitor software repositories and technical service contracts. Corporate network analysis must identify integration hub partnerships and their component supply chains.

The Libya case demonstrates the operational cost of this intelligence gap. Four years of documented UAV deployments occurred before customs officials connected supply chains to specific joint venture structures. Intelligence collection structured around traditional state exports missed capability transfers occurring through commercial networks operating in plain sight.

Force Protection Assumptions Require Revision

When proxy forces access precision strike and persistent surveillance through commercial pathways, the technological sophistication gap that historically characterized irregular warfare narrows. Doctrine and tactics designed around low-tech adversaries become inadequate when proxies field integrated targeting systems.

While not an irregular conflict, Ukraineâ??s 3rd Separate Assault Brigadeâ??s July 2025 operation near Borova illustrates this capability diffusion. First-person view (FPV) drones and unmanned ground vehicles alone dismantled Russian defenses. Defenders surrendered to machines via white cloths in what analysts termed a â??ghost operation,â?• capturing positions that resisted prior assaults. This demonstrates how advanced capabilities enable tactical objectives previously requiring conventional force projection.

For irregular warfare operations, this means force protection planning must account for proxy forces fielding capabilities traditionally associated with conventional militaries. Counter-UAV systems, electronic warfare capabilities, and dispersed operations become necessary against adversaries previously considered low-tech threats. The doctrinal assumption that irregular forces lack persistent surveillance and precision strike no longer holds when commercial pathways enable these capabilities.

Policy Responses Need Friction Mechanisms

Preventing all proliferation through commercial networks is unrealistic given their scale and adaptability. But three interventions could increase costs enough to affect some calculations.

First, treat mission-critical software as controlled items equivalent to hardware. Targeting algorithms, sensor fusion packages, and autonomous decision systems should require explicit export licensing. Integration services combining components into military systems should face the same scrutiny as hardware exports. This addresses regulatory arbitrage where capabilities bypass hardware-focused controls.

Second, impose end-use monitoring-like requirements on defense joint ventures. Commercial partnership structures shouldnâ??t exempt participants from accountability. Companies forming integration hub partnerships should face mandatory reporting on system deployments and automatic license suspension for documented diversions to embargoed parties. The EDGE-CASC partnerships enabling Wing Loong II production should carry the same oversight burden as direct Chinese exports.

Third, leverage market access. Members of North Atlantic Treaty Organization (NATO) are forecasted to spend $2.9 trillion per year for defense by 2035. Companies enabling proliferation to proxy forces through commercial pathways should face exclusion from coalition procurement. This creates economic consequences where political enforcement fails. If firms choosing to operate integration hubs that arm proxy forces face exclusion from Western defense markets, some will calculate differently.

The goal isnâ??t proliferation prevention but sufficient friction that commercial pathways carry reputational, economic, and market access costs. If capability transfer through these mechanisms isnâ??t cost-free, some actors will calculate differently.

The Irregular Warfare Adaptation

The commercial pathways presented here in which proxy forces obtain advanced capabilities represent irregular warfare evolution, not arms control failure. Proxy forces gaining advanced capabilities through networks that bypass state-centric controls is the continuation of irregular warfareâ??s defining characteristic by achieving strategic effects through indirect means that complicate attribution and response.

The adaptation challenge for Western forces mirrors what Ukraine faced deploying autonomous systems with institutional resistance, doctrinal revision requirements, and the time lag between recognizing patterns and adjusting operations. By the time Libyaâ??s 2020-2024 experience fully informs doctrine and intelligence priorities, commercial pathways will have evolved further.

For irregular warfare practitioners, the operational imperative is immediate. Map commercial networks as primary capability transfer mechanisms, adjust force protection for technologically sophisticated proxies, and recognize that arms control documentation without enforcement creates adversary

confidence rather than deterrence. The June 2024 customs seizure proved what enforcement couldnâ??t stop. The question is whether Western doctrine will adapt to what commercial networks now enable.

Branko Ruzic is a defense analyst specializing in irregular warfare, technology proliferation, and strategic competition. His research focuses on how commercial networks enable proxy force capabilities and the implications for Western security policy.

Image from WikiCommons user Mztourist. Licensed under Attribution-ShareAlike 4.0 International. Photo cleaned up to remove background.

The views expressed are those of the author and do not reflect the official position of the Irregular Warfare Initiative, Princeton Universityâ??s Empirical Studies of Conflict Project, the Modern War Institute at West Point, or the United States Government.

If you value reading the Irregular Warfare Initiative, please consider supporting our work. And for the best gear, check out the IWI store for mugs, coasters, apparel, and other items.

Date Created
2026/04/03