Excerpt from InterAgency Journal 16-1
©2026 - Simons Center

Disclaimer: The articles published in the IAJ represent the opinions of the authors and do not reflect the official views of any United States government agency, the Department of War, the Department of the Army, the U.S. Army Command and General Staff College, the Command and General Staff College Foundation and Alumni Association, the Simons Center, or any other non-government, private, public or international organization.

Speed and Risk:
Lessons from Ukraine in Accelerated Adaptation

by Paul Schwennesen, Kerry Halferty Hardy and Benjamin Remler

In a cluttered workshop in central Ukraine, a technician handed over what appeared to be an ordinary fiber-optic spool used for a tethered First-Person-View (FPV) drone. The technician pointed to the hollow plastic core at its center: "That," he said, tapping the cavity, "is now useful space. We use it for avionics hardware while the Russians fill it with explosives."

Fiber-optic-controlled drones have emerged as an important response to the intense electronic warfare environment of the Russia-Ukraine war. Because the drones are physically tethered to the operator by fiber cable, they are immune to radio-frequency jamming. One of the unanticipated aspects of this development is that the spool's core has now become valuable design space. This small design choice reflects a broader divergence in how each side approaches adaptation.

Russian and Ukrainian engineers exploit the space in different ways: Russian technicians opt for explosives, even if the fiber windings dampen fragmentation effectiveness. Ukrainian engineers,

Paul Schwennesen, Ph.D., is a director at Global Strategy Decisions Group. His firsthand battlefield observations of emerging military technologies from Ukraine, particularly those in unmanned systems and electronic warfare, has been highlighted in European thinktanks, the U.S. Department of Defense, and the U.S. Congress. In 2023 he was awarded the Verkhovna Rada medal for "Merit to the Ukrainian people." His work examines the intersection of civilian technological ecosystems and modern battlefield adaptation. He conducts analysis for H.S.H. Prince Michael of Liechtenstein at Geopolitical Intelligence Services.

Kerry Halferty Hardy is a consultant and advisor focused on global networks, institutions, and strategy. She has over two decades of international experience building coalitions across public, private, and civil society sectors in areas including healthcare, technology, and development. Since 2022, she has conducted multiple field visits to Ukraine, observing frontline innovation and facilitating engagement between the Ukrainian military, political stakeholders, international partners. She lectures in a masters program in international business and diplomacy at ESCP Business School.

Benjamin Remler is an independent researcher working on the evolution of the electromagnetic and unmanned warfare landscape in the Russo-Ukrainian war. A recent graduate of Oxford's Russian and Eastern European Studies program, he has researched communication infrastructure projects in post-Soviet states and advises research units and private sector clients in various NATO countries on radiofrequency hardware and evolving tactics, techniques, and procedures of the Russo-Ukrainian warfare. His work has been published in the Ukrainian Review, Armada International, with a publication forthcoming with the Foreign Policy Research Institute.

by contrast, use it to transport carefully tuned avionics modules. "The Russians don't especially care," one Ukrainian engineer said with a shrug. "They will just send ten more drones to finish the job. We have to be more calculating." The exchange captures a broader technological dynamic emerging in the conflict: Ukrainian innovation tends toward precision and rapid iterative refinement, sharpening, as it were, technological "scalpels." Russian forces, meanwhile, typically rely on scale and industrial capacity, mobilizing a heavier "sledgehammer" approach to technical innovation.

The war in Ukraine has thus become a real-time laboratory for observing military adaptation. It offers a vivid example of what the United States (U.S.) Army terms *transforming in contact*, that is, the rapid integration of new technologies, tactics, and organizational practices while actively engaged with a capable adversary. Ukraine's experience also demonstrates that such transformation extends beyond military institutions alone. The country's innovation ecosystem integrates civilian engineers, volunteer organizations, private technology firms, and government agencies into a distributed national defense effort. The result is remarkably rapid battlefield innovations and an almost complete societal mobilization of technical expertise, a 21st-century *levée en masse*.

This dynamic ecosystem offers important lessons for interagency cooperation, defense modernization, and the ethical governance of emerging military technologies. The developments noted in Ukraine raise operational questions that introduce legal and governance challenges, particularly as innovation moves closer to the point of use.

Distributed Innovation Under Fire

In January, our team visited a drone assembly workshop operated by an elite Ukrainian military strike unit directorate. The visit confirmed a pattern that has emerged over the course of the war: Ukraine's reliance on domestic technical innovation is accelerating and diminishing the role of foreign assistance.

Resource constraints and industrial limitations have forced Ukrainians to pursue rapid iteration over mass production as an operating defense schema. Owing partly to the extraordinarily broad cross-section of society called to frontline defense, there is vast opportunity for sharing novel and cross-pollinating expertise. Operational units collaborate directly with civilian developers through informal (often family-based) contact networks to refine drone systems in a near real time response to battlefield conditions. Engineers and operators are increasingly one-and-the-same, or at minimum tightly integrated in a rapid, horizontal information-sharing ecosystem.

The war in Ukraine has thus become a real-time laboratory for observing military adaptation.

The workshop we visited represents only the endpoint of a widely distributed innovation chain. Across Ukraine, volunteer groups, small technology startups, and independent engineers experiment with drone components, communication systems, and navigation solutions in a remarkably fluid, highly decentralized structure. Rheinmetall's CEO Armin Papperger dismissed this ecosystem in a March 2026 interview with *The Atlantic* as the work of "Ukrainian housewives with 3D printers in their kitchens," adding that Ukraine's drone development amounted to "playing with Legos."[1] The response from Ukrainian industry was immediate and pointed. Oleksandr Yakovenko, founder of TAF Industries, one of Ukraine's leading drone manufacturers, noted that his company alone produces up to 100,000 FPV

drones per month, that Ukrainian drones in 2025 accounted for ninety percent of all confirmed combat losses of the Russian army, and that Ukrainian firms iterate on a weekly cycle while European defense counterparts require three to five years and hundreds of millions of euros to certify even minor upgrades. The contrast sharpened further when German media reported the same week that Rheinmetall's own flagship counter-drone system for the Bundeswehr was running at least sixteen months behind schedule. The exchange is instructive not because it settles a debate about production volumes, but because it illustrates the gap in understanding between legacy defense institutions and the distributed model Ukraine has built under fire, and the growing cost of that misunderstanding for Western defense planning.

Designs that fail the acid test of combat operations are flagged as irrelevant.

Promising designs "succeed" in the evolutionary sense: they move toward operational units, where technicians assemble final systems, integrate explosive payloads, iterate on the fly, and provide feedback to design clusters up and down the complex web of procurement. Designs that fail the acid test of combat operations are flagged as irrelevant. Frontline units we visited at Kramatorsk told us bluntly that the Switchblade loitering munition was "not up to the job." A similar narrative unfolded around GPS-guided munitions such as Excalibur, Ground Multiple Launch Rocket System (GMLRS), and other Western technologies: the electronic thicket of the Ukrainian frontlines was simply more than these systems could handle.

The individuals performing this work might be described as "fighting technicians." Their role extends well beyond design, maintenance, or repair. Indeed, they function as de facto translators between the battlefield and the engineering community, rapidly converting operational feedback into design improvements. This innovation loop has now compressed to an astonishingly fast six-month cycle on average.[2] The unit we observed demonstrated broad technical competence across the drone ecosystem, including radio-frequency control systems, fiber-optic guidance, relay networking, and customized firmware development.

This model also has implications for force design. The line between operator and engineer is permanently blurred. The systems these personnel operate demand critical understanding as well as proficiency. This innovation architecture bears little resemblance to traditional centralized defense procurement systems. Instead, it reflects a distributed model of co-development between civilian and military actors. This structure accelerates adaptation; however, it also bypasses many of the institutional processes through which systems are typically reviewed and validated.

Russia's approach diverges significantly, although not entirely, from a structural standpoint. Captured hardware and intercepted communications suggest that Russian innovation cycles are markedly slower, yet once systems prove effective, Russian industrial capacity enables production at far greater scale. The resulting contrast is not merely technological but strategic: Ukraine prioritizes speed and adaptability, while Russia relies on mass and industrial depth.

As the technology case-studies assessed below show, the dynamic battlefield innovation space that Ukraine has pioneered holds major implications for transformation initiatives in U.S. interagency and whole-of-government operations. This in turn has consequences for U.S. procurement systems and the larger culture around military technology, including how ethics and education are integrated into its use.

Electronic Warfare and Radio Links

Ukrainian developers, engineers, and technicians have repeatedly demonstrated their acumen in leveraging commercial hardware and open-source programs to develop highly effective systems and subsystems. Such efforts overcome a great number of crippling technical and operational bottlenecks, leading the way in militarizing civilian drone technologies. Military Express Long Range System (MILELRS), an adaptation or 'fork' of the civilian Express Long Range System for radio control and 'Military BETA,' an adaptation of the civilian BetaFlight flight control protocol (MILBETA) provide a striking example of successful Ukrainian innovation in the face of Russian countermeasures. MILERLS and MILBETA are custom systems, with which the Ukrainians 'flash' (configure) the drone's radio receiver and flight controller, respectively. Prior to 2024, control link jamming by man-portable and trench electronic warfare platforms enabled the Russians to jettison large numbers of Ukrainian FPV drones.[3] The math was in their favor: drone/unmanned aerial system (UAS) links all derive from Semtech's LoRa (short for Long Range) modulation technology and are by design extremely weak and vulnerable to higher-power interfering signals, especially when a drone is closer to the jammer than its operator.

When the Ukrainians developed and scaled the use of MILELRS and MILBETA in spring 2024, the Russians reacted with panic – Ukrainian drones were no longer falling out of the sky. They were compelled to entirely upend their tactics and switched to video transmission jamming as their primary vector for electronic attack. Protocols such as MILELRS and MILBETA were game-changers. The earliest iterations enabled AES-128 encryption, dynamic frequency reconfiguration, redundant receiver chains, multi-receiver integration, and automatic and manual channel switching. Recent iterations of MILELRS and MILBETA provide more sophisticated features, such as live electronic interference statistics, equipping Ukrainian operators to evade or hone in on Russian jammers.

Ukrainian developers, engineers, and technicians have repeatedly demonstrated their acumen in leveraging commercial hardware and open-source programs to develop highly effective systems and subsystems.

Small and nimble teams of Ukrainian firmware engineers and programmers developed both systems to be readily configurable onto the very same civilian-sourced electronic components which soldiers had grown used to, and to enable Ukrainian tinkerers to further experiment with and iterate on commercial hardware front-ends. As of this year, MILELRS and MILBETA are workhorses for drone radio control for a great many Ukrainian drone teams. These protocols are so popular that the Russians have recovered the underlying firmware and put great effort into understanding and harnessing it for their own use.

Neither of these twinned systems has the bearings of the military specification-chasing development process which characterize U.S. Government prototyping and procurement cycles. Ukrainian engineers have the agency to work with open-source systems and commercial hardware and seized the chance to see their systems implemented and experimented on by eager Ukrainian units. What their experience unequivocally demonstrates is that, if there is a will, pools of engineering and tinkering talent will find a way to leverage commercial technologies and equipment into purpose-fit military tools, with outstanding records on the battlefield.

There is nothing inevitable about this success. The Russian Armed Forces' own experience demonstrates this, to their own detriment. Russia does not suffer from lack of engineering talent. In 2023, Russian developers such as Aleksandr Barashkov of Gagaring Laboratories had already identified the need for encrypted radio transmission protocols analogous to MILELRS, before Ukraine had set the precedent of scaling its own custom solutions. Barashkov and Gagaring developed an encrypted radio protocol, Kuznechik ('Grasshopper'). By Barashkov's own admission and to the Ukrainians' delight, Kuznechik – admittedly an effective system, with a strong record during the Kursk campaign – was first met with derision by the Russian military's procurement authorities.[4] Instead of welcoming the contributions of boutique developers, the Russian military kept relying on mass-produced drones with off-the-shelf and inadequately configured civilian transceivers. The Ukrainians capitalized on this by configuring their own jammers to spoof and disarm the Russian drones.[5]

While Russia's level of technical sophistication has evolved at an alarming rate... Russian servicemembers lack the variety of cost-effective solutions and products their Ukrainian counterparts can rely on...

And so it goes for much of the Russian military's approach to innovation and procurement cycles. While Russia's level of technical sophistication has evolved at an alarming rate and kept its military in the fight, Russian servicemembers lack the variety of cost-effective solutions and products their Ukrainian counterparts can rely on to address any number of minute operational and technical challenges. This is the consequence of a dysfunctional organizational philosophy, not of lack of resources or technological acumen.

The Ukrainians, in the meantime, are applying the MILELRS/MILBETA playbook to an astounding variety of electromagnetic challenges. This is true, for instance, of navigation capabilities. Satellite navigation denial has become a routine feature of the battlefield, to such an extent that Ukrainian frontline drone operators assume constant Global Navigation Satellite System (GNSS) denial and predominantly rely on familiarity of the terrain. Numerous Ukrainian developers are pursuing the use of terrestrial beacon systems, which leverage angle-of-arrival and time-of-arrival estimates of position relative to base stations to secure navigation capabilities. The result is not precision, but sufficient reliability under degraded conditions. Ukrainian defense industry leader Sine Engineering has successfully commercialized integrated beacon-enabled navigation with other command-and-control subsystems, and other Ukrainian developers have had the opportunity to test similar solutions.

The same can be said of video transmission systems, for which the Ukrainians have created and scaled an impressive number of remedial platforms. The impetus for these solutions has been Russia's successful use of video jamming to suppress Ukrainian drone teams, a problem which endures to this day but which the Ukrainians have partly mitigated. Anti-video jamming solutions include frequency transverters that conceal readily recognizable National Television Standard Committee/Phase Alternating Line analog signals in the X and Ku bands (10-12 GHz), which are largely populated by low-earth orbit satellite signals. Ukraine's Brave1 market even includes a large selection of aerial drone relays, which do degrade video quality but spare operators' control stations from high-power Russian video link jamming signals. Some Ukrainian firms such as Scream Industries also produce their own high-frequency

video transmission systems, an impressive feat that the Russians have echoed only by drawing from Chinese manufacturers. It should be noted that while these systems enhance the flexibility and adaptability of Ukrainian troops to Russian countermeasures, they also increase the burden of configuration and integration on the edge.

This continuous technical challenge has driven a fluid information-sharing culture, where operators, engineers, and technicians increasingly turn to online communities and AI language tools to resolve configuration and integration problems in the field. Operators and technicians alike frequently coordinate via closed group chats on Discord, Signal, or Telegram.

Individually, these products and the operational challenges they respond to matter less than the technological and institutional facts which underlie them. These are that global markets for commercial electronics behave like military supply chains, and that nimble teams with resources and decision-making subsidiarity can transform civilian hardware and open-source software into cost-effective military systems. These are the structural conditions that now define unmanned warfare, and any institution seeking to field and adapt these systems must reckon with them.

Ethical Governance of Rapid Military Innovation

Ukraine's experience provides an early view of where military innovation is heading: faster cycles, more actors, and decisions closer to the edge. These shifts clearly affect how systems are built, but also impact the exercise of judgment, assignment of responsibility, and risk management.

The ethical challenges that follow are not hypothetical. They are already visible in the use and adaptation of systems in the field and will only sharpen as the pace of adaptation increases.

Human Judgment Under Time Compression

At the unit level, operators are no longer working from raw information alone. Systems filter, prioritize, and present options in a software-mediated environment that compresses the time available for deliberation. The risk is not that humans are removed from decisions, but that their role becomes merely confirmatory. We observed this pressure directly: the speed at which targeting decisions are made in a fiber-optic FPV environment leaves little room for hesitation, and the systems themselves are designed to minimize it. Preserving real judgment under these conditions depends less on additional technology than on training and command culture. Operators must be expected, but also empowered, to question system outputs even under time pressure.

Ukraine's experience provides an early view of where military innovation is heading: faster cycles, more actors, and decisions closer to the edge.

There is a temptation to treat AI-enabled decision support as a categorically distinct moral problem, one that requires new ethical frameworks rather than rigorous application of existing ones. The operators we spoke with were less convinced. One framed it directly: There is not much distinction between entering an AI targeting command and firing a missile. Collateral damage and mistakes happen either way. What changes is not the moral weight of the outcome but the architecture of command-and-control and the risk is that more complex architectures may result in the dilution of responsibility. The moral burden does not disappear when a system intermediates a decision. It relocates, often to places where it is harder to see and harder to assign. That relocation is precisely what governance frameworks need

to track and what training and command culture need to counteract by insisting that individuals, not systems, bear responsibility for outcomes.

The same structure that allows rapid adaptation also complicates accountability.

Distributed Innovation and Diffused Responsibility

The same structure that allows rapid adaptation also complicates accountability. Systems are developed and modified across a mix of civilian volunteers, private firms, and operational units, usually without clear boundaries between them. Changes may occur in the field, sometimes immediately prior to use, in ways that alter a system's characteristics from those reviewed at any earlier stage. Traditional models of command responsibility assume clearer lines between development, approval, and employment than this environment provides. When something goes wrong, the question of who is responsible, whether the designer, the modifier, the operator, or the commander, may not have a clear answer. That ambiguity is not incidental; it is a structural feature of distributed innovation and requires structural rather than individual responses.

Information Operations and Cognitive Effects

Information operations present a distinct ethical category, one where consequences extend well beyond the immediate battlefield and where the line between tactical communication and strategic narrative is increasingly difficult to hold. Commercial platforms such as Telegram and TikTok that enable rapid horizontal coordination within Ukraine's innovation ecosystem also extend the reach of battlefield footage far beyond its intended audience. Content produced to demonstrate tactical effectiveness to a unit commander can quickly start shaping political perceptions among domestic populations, allied governments, and adversary information environments simultaneously.

The distortion runs in both directions, and its consequences are concrete. Ukraine's deep strike drone campaign has generated dramatic footage that circulates widely, projecting an impression of strategic effectiveness unsupported by operational data.[6] RUSI's December 2025 assessment found that fewer than ten percent of Ukrainian strike munitions reached their targets, and fewer still delivered meaningful effect, a gap between appearance and reality that is difficult to communicate once the footage has circulated.

The policy stakes of that gap became visible in early 2026, when reporting on Ukrainian drone operators' success against a NATO formation during Exercise Hedgehog 2025 in Estonia, circulated widely and began shaping Western military thinking about drone warfare. Analysts at the Modern War Institute cautioned that the exercise results were being drawn out of context, that drone saturation during the exercise was far below what Ukrainian operators encounter on actual battlefields, and that the policy conclusions being derived from the coverage were therefore unreliable.[7] The ethical challenge is not simply one of operational security. It is that tactically sound and legally permissible actions can produce unintended and unanticipated political and social consequences, which no current governance framework adequately addresses.

Failure Modes in Rapid Adaptation

These risks compound in contested electronic environments. Sensor inputs are frequently degraded or contradictory, increasing the likelihood of misidentification at precisely the moments when decisions must be made fastest. Semi-autonomous systems behave inconsistently under interference or when pushed beyond their expected parameters, and locally improvised

electronic warfare measures, frequency shifts, ad hoc jamming, and relay disruptions can affect friendly systems operating in the same space as readily as adversary ones. What our team observed was not a clean division between systems working and systems failing, but a continuous gradient of degraded performance that operators were managing in real time, often without full visibility into the reasons behind a system's behavior. One example was instructive: operators managing "REB" ('Radio-Electronic Warfare,' the Russian and Ukrainian acronym for Electronic Warfare and colloquialism for EW equipment) devices at the unit level noted that turning off their own jammers to facilitate friendly drone operations by other units, simultaneously exposed themselves to greater risk of Russian attack. An increasingly common response is that units now invest in video transmission intercept technology. Knowing what the enemy's drones are observing provides better situational awareness than broadcast jamming. Any governance framework will have to account for how systems actually behave under these conditions, not how they performed in testing.

Governance Under Conditions of Speed

These conditions do not reduce the need for oversight. They merely change where and how it must operate. Governance that relies on centralized review processes designed for slower development cycles will always lag behind the systems it is meant to oversee. It should travel with innovation rather than preceding it, which means building oversight capacity into operational units rather than locating it exclusively at institutional levels removed from the point of use.

That requires clarity about authority at each level of the system. At the tactical level, units are already adapting and employing systems in ways that constitute de facto procurement and development decisions. At the operational level, those adaptations need to be integrated, assessed, and either validated or corrected across formations. At the strategic level, policy, legal oversight, and interagency coordination set the boundaries within which adaptation occurs. The problem in Ukraine, and the risk for any institution seeking to replicate its model, is that tactical-level adaptation is moving faster than operational and strategic oversight can follow.

The problem in Ukraine, and the risk for any institution seeking to replicate its model, is that tactical-level adaptation is moving faster than operational and strategic oversight can follow.

Control has to be understood as a continuous function rather than a gate. Pre-deployment validation remains necessary, but it cannot be the only point at which systems are assessed. Operators need the demonstrated ability to override or abort system actions in real time, and that ability needs to be tested, not assumed. After-action review, at both the technical and command level, is the mechanism through which performance is understood and responsibility is assigned. It is currently underdeveloped relative to the pace of adaptation it is meant to assess.

Risk in this environment is not uniform and should not be treated as such. Decisions involving lethal effects carry the highest burden of scrutiny and the least tolerance for ambiguity in authority or control. Enabling systems, electronic warfare, communications, and Intelligence, Surveillance, and Reconnaissance (ISR), carry different but still significant risks, particularly where their effects interact with civilian infrastructure or allied systems operating in the same space. Information effects, as discussed, constitute a distinct category where consequences may

extend far beyond the battlefield and persist long after the tactical moment has passed. Risk cannot be eliminated. This framework instead clarifies where risk is located and who is responsible for managing it.

Legal Constraints Under Accelerated Development

Under the Law of Armed Conflict, the principles of distinction, proportionality, and feasible precautions shape how authority, control, and risk must be managed, and each becomes complicated under the conditions observed in Ukraine. There, rapid iteration and field-level modifications make it both harder and easier to ensure that targets are correctly identified and that effects remain limited as required. Pervasive surveillance means better battlefield situational awareness, yet sensor inputs are often degraded or contradictory, and systems are adapted in real time, sometimes immediately prior to use. Proportionality assessments are similarly affected when system performance changes under interference or environmental conditions, making outcomes harder to predict in practice.

The Law of Armed Conflict does not require perfection; it requires what is feasible given the circumstances confronting a commander.

Systems are often employed before formal review processes are complete, or after they have been modified in ways that alter their original characteristics. Distributed development further complicates this by fragmenting the authority and technical basis typically required for such reviews, making it harder to determine who is responsible for ensuring compliance.

In this environment, compliance depends both on system design and how systems are adapted and used in practice. Existing legal frameworks remain applicable, and managing risk within those constraints becomes simultaneously easier and more difficult under these rapidly changing conditions. It is a lesson worth noting.

It is also worth stating plainly what the legal analysis above does not capture: Ukraine is fighting under conditions of existential threat, and that context shapes what 'feasible precautions' means in practice. The Law of Armed Conflict does not require perfection; it requires what is feasible given the circumstances confronting a commander.

Those circumstances in Ukraine – the scale of the threat, the pace of operations, the absence of the institutional infrastructure that peacetime review processes assume – are not the circumstances facing U.S. agencies or partner militaries operating under different mandates and with different strategic stakes. Therefore, the lesson for U.S. and allied institutions is not that Ukraine's risk tolerance is a model to replicate. Rather, it is that the relationship between speed, accountability, and legal compliance will look different depending on what is at stake, and that any governance framework has to be honest about that difference rather than papering over it.

Implications for U.S. and Partner Organizations

Ukraine's experience offers something rarer than a case study – it provides a real-time precedent for distributed, civilian-integrated military innovation under sustained pressure. Extracting lessons from that experience requires discipline. However, not everything that works under conditions of existential threat will translate directly to institutions operating under peacetime legal authorities, procurement constraints, and civil-military boundaries. The task is to separate what is structurally replicable from what depends on irreproducible conditions.

A central lesson is that, in key domains, defense institutions are no longer the sole

drivers of innovation. Ukraine's ecosystem integrates universities, volunteer organizations, small firms, and independent engineers into a distributed development chain that formal procurement systems were never designed to accommodate. For U.S. and partner organizations, the implication goes beyond simply consulting civilian actors. The feedback architecture linking operational experience to technical development must be redesigned to operate around shorter cycles and through more direct, bidirectional communication. The six-month iteration loop observed in Ukraine did not result from a top-down policy directive. Instead, it emerged bottom-up, from necessity and from closer, organic coordination and collaboration between users and producers.

Much of the innovation seen on both sides of the conflict depends on commercial components, often sourced globally. This creates exposure to supply chain disruption and manipulation. Ukraine experienced this challenge head-on. By 2024, ninety-six percent of the FPV drones procured by Ukraine's defense ministry came from Ukrainian manufacturers and suppliers, reflecting a robust domestic production base in final assembly and integration. A much smaller share of the underlying components, however, are Ukrainian-made.

According to a December 2025 industry assessment by the Snake Island Institute and IRON cluster, frames and casing components were roughly eighty-five percent localized, while flight controllers, motors, and thermal imagers remained only twenty-five percent localized. Ukraine remained heavily dependent on imports for digital video links and specialized electronic modules. These chokeholds have reverberations at the unit level. Two years ago, operators we spoke with reported significant failure rates in 3D-printed components used to substitute for parts that could no longer be sourced reliably, a direct workaround for import gaps that in turn introduced new problems. Conditions have improved with more stable sourcing and maturing domestic production, but it illustrates well how supply chain shortfalls translate into battlefield performance, and how quickly the innovation ecosystem can occasionally self-correct when it must.

The current state is best described as hybrid. Domestic design and assembly are expanding, while reliance on imported high-end optics and commercial multicopters continues. Ukraine has built a fallback path, not a full replacement of existing supply chains. DJI-class multicopters remain in frontline procurement even as domestic alternatives are developed and tested.

Much of the innovation seen on both sides of the conflict depends on commercial components, often sourced globally. This creates exposure to supply chain disruption and manipulation.

The drivers behind substitution efforts are a combination of industrial policy and a recognition of strategic risk. Chinese manufacturers dominate critical inputs including flight controllers, motors, and permanent magnets. Tighter export restrictions have made that dependence an operational vulnerability in its own right. For any nation seeking to replicate Ukraine's model, the lesson is that fielding-speed and supply chain sovereignty are not the same. Mistaking the two constitutes a strategic risk itself.

It is worth noting here that Ukraine's production base is neither purely domestic nor fully globally sourced. Joint ventures with European partners, including French and German firms, link design, production, and operational feedback across borders. When several states share these functions, authority over technology transfer, export licensing, and system modification is divided across

governments with different legal frameworks and different risk tolerances. As systems are modified in use, it becomes less clear which authority is responsible for governing those changes. The U.S. has largely remained outside these arrangements, and therefore outside the feedback loops they generate. That is as much a loss of visibility as it is an industrial gap.

The feedback loop between operational experience and technical development is the Ukrainian model's strength and where U.S. and partner procurement systems face the most exposure. Non-modular systems that cannot be modified, updated, or replaced within the timeframe of a tactical problem are uncompetitive in the environment Ukraine has pioneered. The reliability issues we observed in 3D-printed components and their subsequent mitigation provide the clearest illustration of what compressed iteration looks like in practice.

The feedback loop between operational experience and technical development is the Ukrainian model's strength and where U.S. and partner procurement systems face the most exposure.

Compression of the feedback loop cannot come at the cost of governance, however. Speedy oversight mechanisms at the point of use must accompany rapid innovation, thus preserving legal compliance and civilian control without becoming a brake on adaptation. In practice, this means embedding legal and technical review closer to operational units, maintaining short validation loops as systems are modified, and ensuring that real-time oversight follows systems into the field rather than holding them up at initial deployment. Modular systems that are modified in theater must be assessed in context. Doing so requires closer integration between operators, legal advisors, and technical specialists. It also requires feedback mechanisms that capture systems' performance during use and integrate that knowledge back into subsequent adaptation.

These challenges are amplified in a whole-of-government context, and the amplification is not uniform. The Department of Defense operates under procurement authorities and risk tolerances that, while slow by Ukrainian standards, are designed for the acquisition of military systems. The State Department's authorities over foreign military financing and partner capacity-building create a separate set of constraints that directly slow U.S. ability to assist allies in adopting and adapting new capabilities. The Commerce Department, whose export control authorities govern the flow of the dual-use components this paper has been discussing, sits at the center of the supply chain vulnerability argument without a clear mechanism for coordinating with operational users in real time. Each institution has a role, yet none of them was designed to play that role at the speed entailed by Ukraine's experience. The challenge becomes even more complex when these same processes extend across allied partners.

At a Franco-Ukrainian forum on dual-use production, we learned the extent to which joint ventures are now structured across borders rather than within a single national system. French policy and financing are actively supporting some of these arrangements, but the pattern is broader. Design, production, and operational feedback are increasingly shared across partners rather than contained within one chain of authority. That shift carries practical consequences. Decisions on technology transfer, export licensing, and the handling of operational feedback now pass through multiple governments with different legal constraints and different tolerances for risk. The result is not simply a more complex supply picture, but a coordination problem that introduces delay at points where adaptation is otherwise rapid.

Regulatory friction is not hypothetical. A recent firsthand experience involving export approval for a simple polymer-resin shotgun speed loader required weeks of preparation and significant specialist expense simply to determine whether jurisdiction lay with the State Department or the Commerce Department. International Traffic in Arms Regulations (ITAR) requirements and associated penalty risks disproportionately affect small businesses, which represent a major reservoir of the kind of innovation this paper describes.

The underlying problem across all three institutions is identical to what the Ukraine experience evokes at the unit level: Speed redistributes risk rather than eliminating it. In Ukraine, this redistribution has already occurred. Risk has migrated toward the edge– the field configuration and the operator making a targeting judgment in seconds. Both U.S. and partner institutions face an analogous shift whenever they accelerate acquisition, expand the circle of innovation actors, or introduce AI-enabled decision support. In fact, risk tends to move where institutional frameworks are thinnest and does so faster than coordination mechanisms are currently designed to follow. Recognizing where risk relocates under conditions of speed is the precondition for governing it. For interagency practitioners, that means locating the risks of acquiring a capability quickly and ensuring that institutions responsible for governing risk are positioned to see it.

This is particularly acute in the context of artificial intelligence and autonomous systems, where the governance stakes are highest and the institutional frameworks are least developed. AI-enabled decision support (e.g.. pixel-lock targeting) does not remove human judgment from the loop so much as it reshapes the loop, transforming compressed deliberation and recommendation into irritants to human initiative. The risk is making human decision-making confirmative, rather than deliberative. Managing that risk requires a clearer command culture and more deliberate training, since these are institutional problems that no technology or procurement system can solve on their own.

In sum, Ukraine's model reflects conditions that are not exportable: existential threat, societal mobilization at scale, and a regulatory flexibility that wartime necessity produces and peacetime institutions cannot replicate. What is exportable is the underlying logic. Shorten the feedback loop and eliminate institutional distance between operators and engineers. Build governance mechanisms that travel *with* systems rather than preceding them. Treat supply chain sovereignty as a strategic question, not a procurement one. None of these require adopting Ukraine's risk tolerance. They do require honesty about the shortcomings of current institutions in dealing with the demands of modern conflict.

Conclusion

Ukraine's wartime experience suggests that modern military effectiveness increasingly depends on the pace of systems adaptation in contact, and on the effectiveness and availability of technical expertise beyond formal institutions. It provides a practical reference point for what "transforming in contact" looks like under sustained combat conditions.

For the U.S. and its partners, the challenge is not simply to accelerate innovation, but to do so within the constraints of law, accountability, and civilian control. The central issue is not a tradeoff between speed and ethics: speed, after all, merely redistributes risk. Rapid adaptation shifts risk from development to deployment while distributed innovation shifts it from hierarchy to networks. Effective governance, rather than serving as a brake on transformation in contact, must become the means by which these shifts in risk are made visible, managed, and bounded. ***IAJ***

Notes

1 A. Papperger, interview with Simon Shuster, *The Atlantic*, published March 27, 2026. Papperger's remarks are confirmed verbatim in the AFP report carried by France24, March 29, 2026, available at https://www.france24.com/en/live-news/20260329-rheinmetall-addresses-row-over-ceos-ukraine-housewives-comment; and Defense News, April 1, 2026, available at https://www.defensenews.com/global/europe/2026/04/01/ukrainian-housewives-and-skyranger-delays-german-defense-poster-child-rheinmetall-is-in-hot-water/. Rheinmetall subsequently issued a statement on its X account expressing 'utmost respect' for Ukraine's defense sector but did not retract the CEO's remarks. For Yakovenko's full response, see *The Print*, March 31, 2026, available at https://theprint.in/defence/more-hits-than-rheinmetall-ever-ukraine-drone-manufacturer-claps-back-at-ceos-housewives-remark/2893156/. The sixteen-month delay in Rheinmetall's Bundeswehr counter-drone program is reported in Defense News, ibid.

2 Per the general director of a Ukrainian Unmanned Underwater and Surface System manufacturer, March 2025.

3 M. Zaborodskyi, J. Watling, O.V. Danylyuk, and N. Reynolds, 'Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February-July 2022,' Royal United Services Institute Special Report (11/2022), pp. 2 & 37. https://www.rusi.org/explore-our-research/publications/special-resources/preliminary-lessons-conventional-warfighting-russias-invasion-ukraine-february-july-2022.

4 C. Serhii 'Flash' Beskrestnov, September 2024, https://t.me/serhii_flash/3964; "Gagaring: Electronics Laboratory,' September 2024, https://t.me/my_el_lab/850.

5 'UAV Developer,' March 2025, , https://t.me/UAVDEV/8039.

6 The sample bias problem in Ukraine drone footage was identified early by Michael Kofman, senior fellow at the Carnegie Endowment for International Peace, who observed that units posting strike footage tend to share their most successful engagements, generating a systematically distorted picture of overall effectiveness. See Kofman, remarks at Army Application Laboratory VERTEX event, reported in Defense One, July 23, 2024, available at https://www.defenseone.com/threats/2024/07/us-risks-learning-wrong-lessons-about-ukraines-drones-expert-says/398242/

7 MWI, March 2026: https://mwi.westpoint.edu/the-menace-of-misunderstanding-learning-the-wrong-lessons-from-ukraines-drone-saturated-battlefields/