The Battlefield Is Everywhere:

Irregular Warfare, the Gray Zone, and the Imperative of Signature Reduction in the Age of Artificial Intelligence

Celia D. Hanley

The United States faces adversaries who have dispensed with the distinction between war and peace. Russia's hybrid warfare doctrine and China's doctrine of Unrestricted Warfare operate continuously, below the threshold of kinetic conflict, exploiting every domain, economic, informational, cyber, and human, to achieve strategic objectives without triggering conventional military response. Ubiquitous technical surveillance (UTS), the operationalized manifestation of these doctrines, has collapsed traditional assumptions about clandestine access, attribution, and operational initiative.

This article examines how these adversary frameworks operate in current practice, drawing on documented cases including Russia's Center 795 assassination directorate, the Skripal and Navalny poisonings identified by Bellingcat (an independent investigative journalism organization specializing in open-source intelligence) and investigative partners, and Russia's outsourced sabotage campaign against European defense infrastructure. It then addresses how artificial intelligence (AI) is transforming irregular warfare, accelerating adversary capabilities while creating new vulnerabilities, and argues that the U.S. must urgently adopt signature reduction doctrine as the foundational counteroffensive gray zone capability, supported by whole-of-government institutional reform. The survival of U.S. clandestine operatives, the protection of U.S. Special Operations Forces (SOF), and the integrity of U.S. interagency operations in denied and semi-permissive environments depend on closing the gap between doctrine and practice in this domain.

The End of the Peacetime Assumption

The most consequential sentence written about modern warfare was not authored by a military strategist. It was written by two senior People's Liberation Army (PLA) Air Force colonels, Qiao

Celia D. Hanley is the founder and president of Catalina Intelligent Solutions, LLC (CatalinaIQ), an intelligence-led risk management and mitigation consulting firm. She served as a senior operations officer with the Central Intelligence Agency, as a supervisory program manager and chief of the Western Hemisphere Division at the Defense Intelligence Agency, and as associate director, International Security, at Raytheon Company (RTX), where she directed counterintelligence, executive protection, evacuation planning, and insider threat programs across 58 countries.

Liang and Wang Xiangsui, in their 1999 treatise *Unrestricted Warfare*:

> [Unrestricted warfare] means that all means will be in readiness, that information will be omnipresent, and the battlefield will be everywhere. It means that all weapons and technology can be superimposed at will… the boundaries lying between the two worlds of war and non-war of military and non-military, will be totally destroyed.[1]

That declaration has been dismissed, debated, and periodically rediscovered in U.S. national security discourse for a quarter century. It has not been answered. The U.S. continues to organize its military, intelligence, and interagency architecture around a Westphalian binary, peace or war, military or civilian, foreign or domestic, that its principal adversaries have systemically abandoned. The cost of this mismatch is not theoretical. It is measured in compromised operations, exposed officers, and strategic objectives undermined before the first uniformed Soldier crossed a line of departure.

…the interagency community must reframe irregular warfare not as a niche SOF mission set but as the primary mode of strategic competition in the current environment…

This article argues that the interagency community must reframe irregular warfare not as a niche SOF mission set but as the primary mode of strategic competition in the current environment; and that the institutional, doctrinal, and training reforms required to compete effectively in irregular warfare must be treated with the same urgency accorded to conventional force modernization. At the operational heart of this argument is a specific and under-resourced capability: signature reduction, the doctrine of actively managing physical and digital patterns-of-life to preserve operational initiative under ubiquitous surveillance conditions.

The Doctrinal Landscape: Two Adversary Models, One Gray Zone

Russia and China pursue gray zone competition through distinct but structurally similar doctrines that exploit the same fundamental vulnerability in U.S. strategic culture: the assumption that competition has rules, that violence has thresholds, and that the state retains a monopoly on the instruments of coercion.

Russia's approach is rooted in what Timothy Thomas has termed "reflexive control," which is a strategy of shaping adversary decision-making by controlling the information environment in which decisions are made.[2] The Russian military theorist Valery Gerasimov articulated an updated version of this in his now-famous 2013 article in the *Military-Industrial Courier*, observing that "the role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness."[3] Russia does not seek to defeat the U.S. militarily. It seeks to fragment U.S.-led coalitions, corrode public trust in democratic institutions, and create conditions in which effective Western response to Russian aggression is impossible, not because the West lacks capability, but because it lacks consensus.

The RAND Corporation has documented Moscow's specific hybrid toolkit: propaganda and social media manipulation; cyber intrusions and sabotage; economic coercion through energy leverage; political influence operations and support for preferred candidates; support for separatist proxies and unmarked special forces; and the implicit backstop of nuclear and conventional military force.[4] These instruments, employed below the threshold of overt armed conflict, are calibrated to achieve strategic

objectives while denying NATO the clear legal and political justification required to invoke collective defense mechanisms.

A useful theoretical lens for understanding where hybrid warfare is most likely to succeed comes from Alexander Lanoszka's analysis in *International Affairs*: a belligerent is most likely to employ hybrid tactics when it has local escalation dominance but not global dominance, seeks to revise the status quo, and targets societies with exploitable ethnic or political cleavages, particularly where it enjoys informational advantages over outside actors.[5] This framework explains why Russia deploys hybrid warfare most aggressively in the former Soviet space and why, facing mass expulsions of intelligence officers from Europe following 2022, it has increasingly relied on criminal proxies and disinformation as its human intelligence (HUMINT) infrastructure atrophies. Lanoszka also identifies hybrid warfare's inherent paradox: by resorting to irregular methods, the belligerent appears averse to escalation while simultaneously leveraging the threat of escalation to deter a strong response.

China's doctrine is broader in ambition. *Unrestricted Warfare* posits that the boundaries between military and civilian affairs, between domestic and foreign, and between war and non-war have been permanently abolished by the conditions of the modern world. Beijing's Military-Civil Fusion strategy operationalizes this at the institutional level: every Chinese citizen, every Chinese company, and every Chinese research institution is, under Article 7 of China's 2017 National Intelligence Law, obligated to "support, assist and cooperate with state intelligence work."[6] This creates a legally mandated intelligence apparatus of extraordinary scale that operates continuously across every domain in which Chinese entities are present, which is to say, everywhere.

RAND's systematic analysis of Chinese gray zone operations across U.S. allies and partners reveals a consistent pattern of multi-domain layering: maritime militia and coast guard vessels to assert physical presence, lawfare and administrative measures to solidify legal claims, economic coercion to isolate target governments diplomatically, cyberattacks to degrade defensive awareness, and disinformation to shape the narrative environment.[7] This reflects a coherent doctrine of graduated coercion designed to advance strategic objectives while keeping any individual action below the threshold that would trigger a decisive military response.

...the gray zone is not a temporary condition between peace and war. It is the permanent operational environment.

Both doctrines converge on a single operational reality the U.S. interagency community must internalize, which is that the gray zone is not a temporary condition between peace and war. It is the permanent operational environment. Critically, as Captain John Chambers' West Point Modern War Institute analysis established, adversaries deliberately target Phase 0—the "Shape" phase of U.S. military operations—precisely because this is where American bureaucracy is most fragmented and reaction time is slowest.[8] The adversary has already chosen its theater. The question is whether the United States will compete in it.

UTS as the Operational Manifestation of Gray Zone Warfare

Ubiquitous technical surveillance is not a metaphor for a concerning trend. It is the specific, operationalized infrastructure through which adversaries conduct gray zone warfare at scale. As Christopher Moede has argued in the *Small Wars Journal*, UTS is "the operationalized manifestation of Chinese unrestricted warfare

in contemporary strategic competition"—a condition that "collapses normative assumptions of access, attribution, and initiative."[9]

CIA Director William Burns has described UTS as an "existential threat" to clandestine operations, a characterization underscored by Craig Gruber and colleagues in their peer-reviewed analysis of how pervasive commercial data collection has fundamentally altered the clandestine operating environment.[10] The threat operates across five data domains identified by the FBI and the Center for Internet Security's National Working Group on Countering UTS: travel, visual/physical surveillance, online activity, electronic signals, and financial transactions.[11] Each domain, individually, provides limited insight. Aggregated across time and correlated by AI-powered analytical systems, they constitute a pattern-of-life portrait sufficiently detailed to identify, track, expose, and exploit any individual, including clandestine operatives, who uses commercial services without deliberate countersurveillance discipline.

CIA Director William Burns has described UTS as an "existential threat" to clandestine operations...

The DoD's own analysis, published by the West Point Army Cyber Institute, documented that commercial data can be used to identify the home addresses of service members, map their movement patterns, infer their assignments, and predict their behavior, all without penetrating a single classified system.[12] Research published in *Science* demonstrates that as few as four spatiotemporal data points are sufficient to uniquely identify ninety percent of individuals in a large anonymized mobility dataset, illustrating how the aggregation of ordinary commercial activity produces operational exposure that no individual data stream reveals alone.[13] When the battlefield is everywhere, and ordinary behavior is persistently analyzable and exploitable, the traditional security model, protect the classified, manage the unclassified, fails at its foundation.

Russia's Hybrid Warfare in Practice: Three Case Studies

The doctrinal frameworks described above are not theoretical constructs. They are operational realities with documented case histories. Three cases illustrate the evolution of Russian hybrid warfare and the operational security failures that open-source investigation has exposed.

The Skripal Poisoning: GRU Unit 29155 and the Novichok Infrastructure

On March 4, 2018, former Russian military intelligence officer Sergei Skripal and his daughter Yulia were found unconscious on a park bench in Salisbury, England, having been poisoned with a Novichok-class nerve agent. UK authorities identified two suspects who had traveled to Salisbury under false identities, later identified by Bellingcat, the independent open-source investigative team, in partnership with The Insider, as Colonel Anatoliy Chepiga and Dr. Alexander Mishkin, both officers of the GRU's clandestine Unit 29155.[14]

Kevin Riehle's comprehensive analysis of Russian intelligence architecture establishes the institutional context: Unit 29155 is a standing covert action unit, organizationally distinct from and often uncoordinated with the GRU's intelligence collection directorates. The unit dispatches officers abroad to conduct physical actions—assassinations, political interference, and infrastructure sabotage. Its European footprint, coordinated through a Switzerland-based forward headquarters, has been implicated in operations spanning the Skripal poisoning, a coup attempt against the pro-NATO government of Montenegro, and sabotage operations in Czechia and Bulgaria.[15] Understanding Unit

29155 as a standing institutional capability, not an ad hoc response, is essential to grasping the systemic character of Russia's covert warfare program.

The Bellingcat investigation that unraveled the Skripal operation is a foundational case study in what open-source intelligence (OSINT) can achieve against operatives who underestimate the aggregation risk of commercial data. Using commercially available Russian databases accessible through Telegram bots for approximately ten euros, Bellingcat researchers retrieved Chepiga's date of birth, passport number, court records, license plate number, vehicle identification number, previous vehicle ownership history, traffic violations, and frequent parking locations in Moscow.[16] The cover identities held by the GRU officers could not survive cross-reference against the commercial data exhaust they had generated over years.

A subsequent Bellingcat investigation, conducted jointly with The Insider and *Der Spiegel*, identified the chemical weapons infrastructure behind the Skripal poisoning. Telecommunications metadata revealed close coordination between GRU Unit 29155 and the St. Petersburg State Institute for Experimental Military Medicine. Sergey Chepur, the institute's chairman, communicated with GRU commander Major General Andrey Averyanov at least sixty-five times in the period from November 2017 through early March 2018.[17] The investigation demonstrated that Russia had maintained an active Novichok development and weaponization program years beyond its officially announced closure date, and that this program was operationally integrated with clandestine assassination missions.

The Navalny Poisoning: FSB Pattern-of-Life and Digital Exposure

The August 2020 poisoning of Russian opposition figure Alexei Navalny with Novichok revealed a second layer of Russia's assassination infrastructure: a clandestine unit within the Federal Security Service (FSB) specializing in chemical weapons deployment. A joint investigation by Bellingcat, The Insider, *Der Spiegel*, and CNN identified a team of FSB operatives who had shadowed Navalny during more than thirty overlapping flights across Russia from 2017 onward.[18]

The investigative methodology used in the Navalny case demonstrates the extent to which commercial data has become the decisive intelligence terrain.

The investigative methodology used in the Navalny case demonstrates the extent to which commercial data has become the decisive intelligence terrain. Bellingcat's Christo Grozev described the key tools: reverse phone-search Telegram bots; vehicle registration databases containing passport numbers, addresses, and license plates; passenger manifests obtained from Russian data brokers; and facial recognition platforms that matched operatives' cover identities to their authentic social media presence.[19] One particularly illustrative identification was a facial recognition platform that matched an FSB operative's cover identity to an image his wife had posted on social media. The documentation that sustained a clandestine cover identity could not survive the aggregation of years of authentic digital behavior.

The investigative conclusion extended beyond individual operatives. Bellingcat and its partners identified evidence that the FSB had maintained an active Novichok development capability through a network of state-run institutes disguised as civilian research entities—demonstrating that Russia's gray zone operations combine assassination, chemical weapons development, and institutional deception as integrated components of a single strategic

program.[20]

Center 795 (Military Unit 75127): The Outsourced Assassination Directorate

The Center 795 case, which emerged from reporting by The Insider, Meduza, Charter97, and other investigative outlets in March 2026, documents a newer and more structurally significant development in Russian hybrid warfare: the systematic outsourcing of clandestine operations to criminal proxies, disposable agents, and criminal networks recruited through encrypted applications.[21]

The operational failure that exposed Alimov was systematic rather than incidental.

Center 795, formally designated Military Unit 75127 and established by Russian General Staff order in December 2022, was built in direct response to the institutional damage inflicted on Unit 29155 by the Skripal exposure. Its architecture reflected lessons learned from that failure: structural separation from compromised predecessor units; unprecedented compensation (handlers earning approximately $7,800 per month; the unit commander assessed at approximately $500,000 per year); and operational isolation from the GRU's formal hierarchy.[22] The unit was, by design, meant to be impossible to detect.

The exposure came not from a classified intelligence penetration but from a commercial data failure of striking banality. Denis Alimov, 42, a decorated FSB Alfa Group veteran serving as a senior Center 795 operative, arrived at Bogotá's El Dorado International Airport on February 24, 2026, presenting the unremarkable profile of a Russian tourist. He was met by an Interpol Red Notice (an international alert issued by Interpol requesting law enforcement worldwide to locate and provisionally arrest an individual pending extradition—see the Glossary at the end of this article), activated at the request of federal prosecutors in the Southern District of New York.[23] Alimov stood accused of orchestrating the attempted assassination of two prominent Chechen dissidents residing in Europe, having offered a $1.5 million bounty per target—payable whether the individual arrived in Russia dead or, in the operational vocabulary of Russian intelligence, "legally deported."

The operational failure that exposed Alimov was systematic rather than incidental. Because Alimov spoke only Russian and his recruited proxy—Darko Durovic, a Serbian national—spoke only Serbo-Croatian, the two communicated through Google Translate to mediate between their encrypted messaging exchanges. This was not a spontaneous lapse. It was their standing operational procedure. Every message passed through Google's servers. Google operates under U.S. legal jurisdiction. The FBI secured a court order and read the murder plot, surveillance logs, target profiles, and searches for weapons, in real time.[24] Alimov had also used his operational phone number to participate in public Telegram fitness groups, creating a linkage between his clandestine identity and his authentic digital pattern-of-life that Western counterintelligence then exploited to map the entire network.

The Center 795 case illustrates two equally important lessons. First, as Abram Shulsky and Gary Schmitt observe in their foundational analysis of counterintelligence methodology, a series of operational failures, rather than isolated incidents, should alert an intelligence service to the possibility of systemic compromise.[25] In the Center 795 case, the systemic problem was not penetration but institutional degradation: the mass expulsion of Russian intelligence officers from European embassies following 2022 gutted Russia's HUMINT infrastructure, forcing reliance on criminal proxies with no clandestine training and commercial platforms with no

operational security.[26] Second, the commercial data ecosystem that exposes U.S. clandestine operators is equally capable of unraveling adversary operations. The information environment is an indifferent terrain. Operational discipline, or its absence, determines who gets read and who does the reading.

AI and the Future of Irregular Warfare

AI is not approaching irregular warfare. It has arrived, and its impact is already asymmetric in ways that favor adversaries who have fewer constraints on its application. On the offensive side, AI has dramatically accelerated the capabilities that make gray zone competition effective. AI-powered social media analysis allows adversaries to identify, target, and cultivate at-risk individuals—cleared personnel, government employees, researchers, and executives—with precision and at a scale no human intelligence operation could replicate. The 2026 Annual Threat Assessment of the U.S. Intelligence Community documents that Chinese operators used AI agents "to an unprecedented degree" to execute cyberattacks and drive information operations in 2025.[27] Generative AI creates synthetic media including deepfakes, fabricated documents, AI-authored influence content, indistinguishable from authentic material without specific authentication infrastructure. Russia deploys AI for information operations at scale, generating disinformation campaigns that would require thousands of human operators to produce by manual means.[28]

In the physical domain, AI enables pattern-of-life surveillance at resolutions and scales that were impossible five years ago. AI-powered correlation of data from commercial sources which include location services, biometric databases, loyalty programs, real-time bidding networks, and social media exhaust, can identify, track, and expose clandestine operatives without the deployment of a single human intelligence asset on the ground. Reporting in August 2025 documented that adversaries had used AI to unmask undercover law enforcement officers from commercially available data, illustrating the operational urgency of this threat for all categories of U.S. government personnel operating under cover.[29]

AI is not approaching irregular warfare. It has arrived...

AI also creates new defensive capabilities and the U.S. must invest in both dimensions simultaneously. AI-enabled anomaly detection can identify adversary operatives whose digital patterns diverge from claimed identities. AI-powered analysis can surface coordinated inauthentic behavior in information operations before it reaches effective scale. AI-assisted counterintelligence can identify at-risk personnel through behavioral signals that human analysts would miss. The critical variable is whether U.S. institutions invest in these capabilities before the adversary's offensive AI advantage becomes decisive—and whether the organizational architecture exists to deploy them at the required speed.

Signature Reduction: The Doctrinal Answer to UTS in Irregular Warfare

The doctrinal response to UTS in the irregular warfare context has a name: signature reduction. It is the active, deliberate management of physical and digital patterns-of-life to reduce adversary collection opportunities and preserve operational initiative. As Moede articulates, signature reduction is "the gray zone counteroffensive to the operational condition of UTS in unrestricted warfare"—a scalable doctrine that restores freedom of maneuver within an environment of pervasive surveillance.[30]

Signature reduction rests on a principle that

is counterintuitive but operationally validated: the goal is not to disappear. An individual who suddenly goes dark, stops using loyalty programs, deletes social media, stops generating expected data exhaust, triggers adversary AI anomaly detection as reliably as anomalous presence does. The algorithm is looking for what does not fit the baseline. Absence is a form of presence.

The goal of signature reduction is to blend...

The goal of signature reduction is to blend: to generate patterns-of-life so consistent with the authentic baseline for a legitimate professional in a given role that adversary pattern-of-life analysis cannot resolve a target worth pursuing. This requires judgment—continuous, cross-domain, adversary-calibrated judgment about which patterns to maintain, which to modulate, and which to eliminate. It is not a one-time remediation. It is a sustained operational discipline.

Signature reduction doctrine integrates two complementary domains. In the physical domain: force protection route selection and ambiguous movement patterns; environmental attribution management (appearance, attitude, approach, and adaptation to local norms); and physical signature reduction fundamentals. In the digital domain: digital signature management; attribution management; personal and operational cybersecurity hygiene; secure and private communications discipline; and emerging technology vector awareness, including AI-enabled surveillance, biometric aggregation, and real-time bidding network exposure.[31]

What the Center 795 case, the Skripal investigation, and the Navalny poisoning collectively demonstrate is that signature reduction discipline, applied by either side, is often the decisive operational variable. Center 795 failed because its operatives used commercial services without the discipline that signature reduction requires. The FSB operatives who followed Navalny were exposed because their travel patterns, phone metadata, and financial data created an aggregated portrait that open-source investigators could reconstruct using commercially available tools. The GRU officers who poisoned the Skripals left a data trail that Telegram bots could traverse for ten euros.

What Signature Reduction Is Not: Clearing Common Misconceptions

Before addressing institutional implications, it is important to address what signature reduction is not, because misconceptions about the doctrine undermine its adoption and effectiveness.

Signature reduction is not primarily a technology solution. It is a human discipline supported by technology. The operative who uses an encrypted communications application but generates identifiable travel patterns, loyalty card records, and social media exhaust has not achieved signature reduction; they have secured one pipe in a surveillance architecture that has dozens. The Center 795 case is the clearest illustration: Alimov used encrypted messaging applications he believed to be secure. He was read in real time because he routed those messages through a commercial translation service operating on U.S. servers.

Signature reduction is not operational security (OPSEC) as traditionally understood. Traditional OPSEC focuses on protecting specific information from specific disclosure risks. Signature reduction addresses the more fundamental challenge of the aggregated digital existence; the fact that the sum of many individually innocuous data points constitutes a portrait that can expose identity, role, purpose, and network. As Shulsky and Schmitt's analysis of counterintelligence methodology establishes,

the adversary's ability to correlate apparently unrelated data points, rather than any single disclosure, is often what reveals compromise.[32] This is a different problem requiring a different solution.

Signature reduction is not a mission-specific activity. It is a persistent condition. The Navalny case is instructive: FSB operatives who maintained rigorous discipline during active surveillance operations were exposed by the metadata patterns generated during their non-operational activities—phone calls, travel records, and coordination patterns accumulated over three years. The exposure happened not when they were executing an operation but when they were being ordinary government employees with phones.

Finally, signature reduction is not primarily an individual capability. It is an organizational one. An institution can train individual operatives in signature reduction discipline. But the program fails if even one node in a communication chain—a handler, a coordinator, a logistics contact—does not maintain equivalent discipline. The Center 795 case illustrates this precisely: a network built with exceptional institutional architecture was exposed through the individual failure of a single operative to maintain discipline in his non-operational digital life.

Institutional Implications: How the U.S. Must Posture for Irregular Warfare

The doctrinal and operational analysis above has clear institutional implications for how the United States must organize, train, and equip for irregular warfare competition in the current environment. Five areas require urgent attention.

First: Establish Signature Reduction as a Doctrinal Standard, Not a SOF Specialty

The Irregular Warfare Center (IWC), as the DoD Instruction 3000.07-appointed doctrinal steward for irregular warfare, has a foundational role to play in establishing signature reduction training standards across the force.[33] But the application of signature reduction doctrine cannot be limited to SOF. Every U.S. government employee operating in a denied or semi-permissive environment, such as intelligence officers under diplomatic cover, interagency personnel in conflict zones, law enforcement agents conducting international operations, faces the UTS threat.

Signature reduction is not a mission-specific activity. It is a persistent condition.

The institutional posture problem is also a bureaucratic organization problem. As Chambers' analysis demonstrates, the Department of Defense is frequently not the lead agency operating in Phase 0—where adversaries concentrate their gray zone effort. The multiagency coordination processes that substitute for unified authority in this phase are precisely the seams that adversaries exploit.[34] Signature reduction doctrine must therefore be embedded in the organizational culture of the intelligence community, law enforcement, and interagency coordinating bodies, not simply within DoD.

Formal training standards and doctrinal development are necessary but insufficient without the cultural shift that makes individual operatives treat signature reduction as a daily discipline rather than a pre-deployment checklist. That cultural shift requires leadership emphasis, institutional incentives, and frank acknowledgment that the threat has materially changed since the cover models and tradecraft standards that currently govern U.S. clandestine operations were developed.

Second: Adopt a Whole-of-Society Counterintelligence Model

Russia and China do not conduct espionage as a government-only enterprise. They operate whole-of-society espionage ecosystems that deploy state intelligence agencies, nominally private firms, talent recruitment programs, and criminal proxies simultaneously. The U.S. counterintelligence enterprise, built on a government-centric model that compartmentalizes the private sector and academia as receivers of threat information rather than active participants in the national security ecosystem, is structurally mismatched to this threat.

Russia and China do not conduct espionage as a government-only enterprise.

Riehle's analysis of Russian intelligence architecture documents the asymmetry: the Foreign Intelligence Service (SVR), FSB, GRU, and their associated commercial fronts operate as overlapping, sometimes competing but collectively comprehensive intelligence ecosystems.[35] RAND's analysis of Chinese gray zone operations similarly documents how Beijing leverages Communist Party institutional linkages, extending from senior leadership down to provincial and people-to-people exchanges, to build influence networks invisible to a counterintelligence architecture designed to track government-to-government operations.[36]

Between eighty and ninety percent of the innovation that adversaries most actively target resides in the commercial and academic sectors.[37] The counterintelligence community cannot protect this innovation without the active participation of the institutions that generate it. Legislative reforms that enable meaningful information sharing, create structured public-private counterintelligence partnerships, and establish academic pipeline visibility programs, particularly to identify PRC talent recruitment operations targeting doctoral candidates and post-doctoral researchers before they enter the cleared workforce, are necessary complements to the doctrinal reforms described above.

Third: Redevelop the Cover Model for the UTS Environment

The cover model built over seven decades of Cold War clandestine operations, which is sustained by documentation, backstory, and institutional discipline, is insufficient in an environment where adversaries run commercial data analytics against anyone who travels to certain locations, makes certain purchases, and exhibits certain behavioral patterns. The tradecraft model must be rebuilt from the ground up to account for the aggregated digital existence.

Cover development that does not include longitudinal digital pattern-of-life management is cover development that adversaries can collapse with commercially available tools. Shulsky and Schmitt's observation that intelligence services are often compromised not by dramatic failures but by the patient accumulation of individually minor lapses applies with redoubled force in an environment where those lapses are automatically aggregated and analytically correlated by AI systems the adversary runs continuously.[38]

Fourth: Integrate Strategic Intelligence Disclosure as Offensive Counterintelligence

The most effective offensive counterintelligence tool against Russian hybrid warfare and the doctrine of Reflexive Control is Strategic Intelligence Disclosure (SID)—the selective, preemptive declassification of intelligence to establish credible counter-narratives before adversary disinformation takes root. The U.S. application of SID prior to Russia's 2022 invasion of Ukraine, selectively

declassifying intelligence on Russian invasion timelines, false-flag preparations, and proxy narratives, preempted Moscow's Reflexive Control strategy and denied it narrative surprise.[39]

Bellingcat's investigations of the Skripal and Navalny poisonings demonstrate a complementary model: open-source investigators, using commercially available tools and unclassified data, produced attribution findings more credible to international audiences precisely because they were demonstrably independent. Following the 2018 Skripal attack, Russian state media advanced no fewer than 138 separate and contradictory narratives to deflect attribution.[40] Bellingcat's independently verifiable, publicly documented findings were not susceptible to the same deflection campaigns because their sources were observable by anyone willing to examine them.

The interagency community should develop doctrine for coordinating classified intelligence collection with open-source investigative capacity, not by directing or controlling independent investigators, but by ensuring that U.S. government declaratory posture is calibrated to how declassified intelligence and open-source findings can be mutually reinforcing.

Fifth: Develop AI-Specific Capabilities for Both Offensive and Defensive Irregular Warfare

The AI dimension of irregular warfare requires capabilities development that does not fit neatly into existing acquisition or organizational categories. On the defensive side: AI-enabled anomaly detection for signature reduction monitoring; AI-powered counterintelligence analysis for at-risk personnel identification; and AI-assisted counter-influence capabilities for detecting coordinated inauthentic behavior in the information domain before it reaches effective scale.

On the offensive side, the United States has imposed constraints on its own information operations capabilities that adversaries do not observe. A calibrated development of U.S. AI capabilities in the information domain, within the legal and policy frameworks established by law and executive authority, is a necessary component of effective gray zone competition. An adversary that can deploy synthetic media, AI-generated influence content, and disinformation at scale while facing no equivalent capability has a structural advantage in the information environment that no amount of defensive investment will overcome.

SOF, specifically, should be positioned as forward counterintelligence nodes—operating persistently in denied and semi-permissive environments to detect adversary proxy networks, map hybrid infrastructure, and generate the deep-attribution intelligence necessary to disrupt adversary decision-making cycles. When integrated with AI-enabled analytical capability and structured interagency counterintelligence sharing, SOF-generated human intelligence can provide the ground-truth context that technology-centric analysis cannot.

Conclusion: The Decisive Terrain Is Operational Initiative

The adversary has already chosen the battlefield. It is everywhere. It is commercial, informational, financial, digital, and human—and it operates continuously, without the declaration of war that would trigger the institutional machinery the U.S. has built to defend itself. Russia's hybrid warfare doctrine and China's Unrestricted Warfare framework are not exotic academic constructs. They are operational realities, documented in prosecuted cases, open-source investigations, and the Annual Threat Assessments of seventeen U.S. intelligence agencies.

The response cannot be primarily technological. Technology is a necessary component of effective irregular warfare

competition, AI-enabled surveillance, AI-enabled analysis, AI-enabled influence operations; but technology cannot substitute for the human judgment that signature reduction doctrine places at the center of clandestine operations in the UTS environment. As Moede has argued, the decisive terrain in this competition is not technical alone—it is operational initiative generated by and through human judgment amidst the pressures of the operational environment.[41]

The U.S. interagency community has the human capital, the institutional knowledge, and, if the political will to fund it can be sustained, the financial resources to compete effectively in the gray zone. What it has not yet done is make the doctrinal and organizational investments that this competition requires: signature reduction as a foundational training standard across the force; whole-of-society counterintelligence that integrates the private sector and academia as active participants; a cover model rebuilt for the UTS environment; Strategic Intelligence Disclosure as offensive counterintelligence doctrine; and AI-specific capabilities that address both the offensive and defensive dimensions of irregular warfare.

The Center 795 case, the Skripal investigation, and the Navalny poisoning are not merely historical case studies. They are operational templates that adversaries are refining and deploying right now—against U.S. personnel, U.S. allies, and U.S. interests. The question is not whether the U.S. will face irregular warfare in the gray zone. It is already there. The question is whether it will organize itself to compete. ***IAJ***

Glossary of Key Terms and Organizations

The following definitions are provided to assist readers unfamiliar with the specialized terminology, organizations, and intelligence concepts referenced throughout this article. Terms are listed alphabetically.

Term / Organization	Definition
Bellingcat	An independent investigative journalism organization founded in 2014 by British journalist Eliot Higgins. Bellingcat specializes in open-source intelligence (OSINT) investigations, using commercially available data, social media analysis, satellite imagery, and geolocation techniques to investigate state-sponsored violence, disinformation, and covert operations. Its investigations of the Skripal and Navalny poisonings—identifying GRU and FSB operatives through passport databases, facial recognition, and telecom metadata—have become landmark case studies in what open-source analysis can achieve against state intelligence services. Website: www.bellingcat.com.
Center 795 (Military Unit 75127)	As reported by The Insider, Meduza, and Charter97 (March 2026), Center 795 is an alleged Russian General Staff covert action unit reportedly established in December 2022 following exposure of GRU Unit 29155 by the Skripal investigation. According to that reporting, Center 795 was designed with structural separation from compromised predecessor units and a reliance on criminal proxies and disposable agents recruited through encrypted applications—a deliberate adaptation to post-Skripal counterintelligence pressure. These allegations remain subject to ongoing U.S. federal proceedings.
Deepfake	Synthetic audio, video, or image content generated by artificial intelligence—typically deep learning models—that realistically depicts individuals saying or doing things they did not say or do. Deepfakes are weaponized in information operations to fabricate evidence, impersonate officials, and generate disinformation at scale. Authentication infrastructure capable of distinguishing deepfakes from authentic media remains a critical and under-resourced defensive gap.
GRU Unit 29155	A clandestine covert action unit of Russia's General Staff Main Intelligence Directorate (GRU), organizationally distinct from the GRU's intelligence collection directorates. Unit 29155 is a standing capability for physical operations abroad, including assassinations, political interference, and infrastructure sabotage. Its European footprint—coordinated through a Switzerland-based forward headquarters—has been implicated in the 2018 Skripal poisoning in the UK, a coup attempt in Montenegro (2016), and sabotage operations in Czechia and Bulgaria.
Gray Zone	The contested space between routine statecraft and open armed conflict, in which state and non-state actors pursue strategic objectives through ambiguous, deniable, and often non-kinetic means. Gray zone operations are designed to achieve effects below the threshold that would trigger a conventional military response or invoke collective defense mechanisms such as NATO Article 5. Activities include information operations, cyber intrusions, economic coercion, proxy violence, and political influence campaigns.

Term / Organization	Definition
Hybrid Warfare	A model of conflict that blends conventional military force, irregular tactics, information operations, economic coercion, cyber capabilities, and proxy actors to achieve strategic objectives while maintaining plausible deniability. Russia's hybrid warfare doctrine, as articulated by theorists including Valery Gerasimov, integrates these instruments as components of a unified operational art rather than as discrete activities. The term is also applied, with structural differences, to China's Unrestricted Warfare framework.
Interpol Red Notice	An international alert issued by Interpol (the International Criminal Police Organization) at the request of a member country, requesting law enforcement worldwide to locate and provisionally arrest an individual pending extradition, surrender, or similar legal action. A Red Notice is not an international arrest warrant—it does not compel arrest—but it alerts border control and law enforcement agencies in Interpol's 196 member countries to detain the subject if located. In the Center 795 case described in this article, a Red Notice activated at Bogotá's El Dorado International Airport upon Denis Alimov's arrival led to his apprehension. Red Notices are publicly searchable on Interpol's website (www.interpol.int).
HUMINT (Human Intelligence)	Intelligence derived from human sources—informants, agents, liaison contacts, and clandestine operatives—as opposed to signals intelligence (SIGINT), imagery intelligence (IMINT), or open-source intelligence (OSINT). HUMINT operations require cover, access, and tradecraft. The mass expulsion of Russian intelligence officers from European embassies following Russia's 2022 invasion of Ukraine significantly contracted Russia's HUMINT infrastructure, generating pressure to rely on criminal proxies as substitutes.
Military-Civil Fusion (MCF)	China's national strategy to eliminate barriers between civilian and military sectors in research, industry, technology, and human capital. Under Article 7 of China's 2017 National Intelligence Law, every Chinese citizen, company, and research institution is legally obligated to support state intelligence work when requested. MCF creates a legally mandated intelligence and technology acquisition apparatus of extraordinary scale that operates across every domain in which Chinese entities are present—commercial, academic, and governmental.
Novichok	A class of highly lethal nerve agents developed by the Soviet Union (and continued by Russia) under the classified 'Foliant' program. Novichok agents inhibit acetylcholinesterase, causing potentially fatal disruption of the nervous system. They are classified as chemical weapons prohibited under the Chemical Weapons Convention. Novichok agents were used in the 2018 poisoning of Sergei and Yulia Skripal in Salisbury, UK, and in the 2020 poisoning of Alexei Navalny. Bellingcat's investigations revealed that Russia maintained an active Novichok development and weaponization program through a network of state-run institutes presented as civilian research entities.

Term / Organization	Definition
OSINT (Open-Source Intelligence)	Intelligence derived from publicly available sources—including news media, social media, satellite imagery, commercial databases, government records, and academic publications—as opposed to classified collection. OSINT has become a decisive intelligence domain as the volume of commercially available data has expanded dramatically. The Bellingcat investigations of the Skripal and Navalny poisonings demonstrated that OSINT investigators using commercially accessible Russian databases (accessible via Telegram bots for approximately €10) could reconstruct the identities, movements, and organizational affiliations of GRU and FSB operatives who had maintained cover for years.
Pattern-of-Life Analysis	An intelligence methodology that aggregates data points about an individual's routine behaviors—travel, communications, financial transactions, social associations, online activity—to build a predictive behavioral profile. AI-powered pattern-of-life analysis can identify, track, and expose clandestine operatives without penetrating any classified system, because the aggregation of many individually innocuous commercial data points produces an operationally decisive portrait. As few as four spatiotemporal data points are sufficient to uniquely identify 90 percent of individuals in large anonymized datasets.
Reflexive Control	A Russian strategic concept, documented by analyst Timothy Thomas, describing the deliberate shaping of an adversary's decision-making by controlling the information environment in which those decisions are made. Rather than defeating an adversary militarily, Reflexive Control seeks to manipulate the adversary's perception of reality so that it makes decisions favorable to Russian strategic objectives—voluntarily, without awareness of the manipulation. Strategic Intelligence Disclosure (preemptive declassification of intelligence) is identified in this article as the primary U.S. countermeasure against Reflexive Control.
Signature Reduction	The active, deliberate management of physical and digital patterns-of-life to reduce adversary collection opportunities and preserve operational initiative under conditions of ubiquitous technical surveillance. Signature reduction is not the elimination of a digital or physical presence—sudden absence triggers anomaly detection as reliably as anomalous presence. The goal is to generate patterns consistent with a legitimate cover baseline so that adversary pattern-of-life analysis cannot resolve a target worth pursuing. This article argues that signature reduction should be established as a doctrinal standard across all U.S. government personnel operating in denied or semi-permissive environments, not solely within Special Operations Forces.
SOF (Special Operations Forces)	Military units trained and equipped for unconventional warfare, direct action, special reconnaissance, foreign internal defense, civil affairs, psychological operations, and counterterrorism missions. U.S. SOF components include Army Special Forces ('Green Berets'), Rangers, Delta Force, Navy SEALs, and Marine Raiders, among others. This article argues that SOF should be positioned as forward counterintelligence nodes in gray zone competition—operating persistently in denied and semi-permissive environments to detect adversary proxy networks and generate deep-attribution intelligence.

Term / Organization	Definition
Strategic Intelligence Disclosure (SID)	The selective, preemptive declassification of intelligence to establish credible counter-narratives before adversary disinformation achieves operational effect. SID is identified in this article as an offensive counterintelligence tool against Russia's doctrine of Reflexive Control. The U.S. application of SID prior to Russia's February 2022 invasion of Ukraine—declassifying intelligence on Russian invasion timelines, false-flag preparations, and proxy narratives before Russia could deploy them—is cited as a documented example of effective SID employment.
Ubiquitous Technical Surveillance (UTS)	The operationalized infrastructure of pervasive commercial and state surveillance through which adversaries conduct gray zone warfare at scale. UTS aggregates data from five domains identified by the FBI and the Center for Internet Security: travel, visual/physical surveillance, online activity, electronic signals, and financial transactions. CIA Director William Burns described UTS as an 'existential threat' to clandestine operations. UTS does not require penetrating classified systems—the aggregation of ordinary commercial data activity produces operational exposure sufficient to identify, track, and expose clandestine operatives.
Unrestricted Warfare	A strategic doctrine articulated by PLA Air Force colonels Qiao Liang and Wang Xiangsui in their 1999 treatise of the same name. Unrestricted Warfare posits that the boundaries between military and civilian affairs, between war and non-war, and between foreign and domestic have been permanently dissolved by modernity, and that all instruments—economic, cyber, informational, financial, legal, and military—must be combined to achieve strategic objectives without restriction. China's Military-Civil Fusion strategy operationalizes this doctrine at the institutional level.

Note on Sources: Definitions above draw on authoritative open sources including U.S. government publications, Interpol's official website (www.interpol.int), Bellingcat's published investigative methodology documentation (www.bellingcat.com), and peer-reviewed academic literature cited in the endnotes of this article. All definitions are based on unclassified, publicly available information.

Notes

1 Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999), 5–6. English translation published by the CIA's Foreign Broadcast Information Service.

2 Timothy L. Thomas, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies* 17, no. 2 (2004): 237;56.

3 Valery Gerasimov, "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," *Military-Industrial Courier*, February 27, 2013. Translated and published in *Military Review* (January–February 2016).

4 Christopher S. Chivvis, *Understanding Russian 'Hybrid Warfare' and What Can Be Done About It*, testimony before the House Committee on Armed Services, RAND Corporation (CT-468), March 22, 2017.

5 Alexander Lanoszka, "Russian Hybrid Warfare and Extended Deterrence in Eastern Europe," *International Affairs* 92, no. 1 (2016): 175–195.

6 People's Republic of China, National Intelligence Law of the People's Republic of China, Article 7 (2017).

7 Lyle J. Morris et al., *Gaining Competitive Advantage in the Gray Zone* (Santa Monica: RAND Corporation, RR-2942-OSD, 2019). See also RAND Corporation, *China's Gray Zone Warfare Against U.S. Allies and Partners*, RRA594-1 (2021).

8 John Chambers, *Countering Gray-Zone Hybrid Threats: An Analysis of Russia's 'New Generation Warfare' and Implications for the U.S. Army* (West Point: Modern War Institute, October 18, 2016)

9 Christopher Moede, "Ubiquitous Technical Surveillance and the Renewal of Irregular Warfare," *Small Wars Journal*, February 13, 2026.

10 William J. Burns, "The Role of Intelligence at a Transformational Moment," speech, Georgia Institute of Technology, April 14, 2022. See also Craig W. Gruber et al., "Ubiquitous Technical Surveillance: A Ubiquitous Intelligence Community Issue," in *Fostering Innovation in the Intelligence Community*, Annals of Theoretical Psychology, vol. 19 (Cham: Springer, 2023).

11 Center for Internet Security / National Working Group on Countering UTS, "Countering Ubiquitous Technical Surveillance: Facts, Findings, and Recommendations for U.S. Law Enforcement" (November 2025).

12 Jaclyn Fox et al., *Death by a Thousand Cuts: Commercial Data Risks to the Army* (West Point: Army Cyber Institute, 2023).

13 Yves-Alexandre de Montjoye et al., "Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata," *Science* 347, no. 6221 (January 30, 2015): 536-539.

14 Bellingcat Investigation Team, "Skripal Suspect 'Boshirov' Identified as Colonel Anatoliy Chepiga," Bellingcat, September 26, 2018; Bellingcat Investigation Team, "The Doctor's Alibi," Bellingcat, October 9, 2018.

15 Kevin P. Riehle, *Russian Intelligence: A Case-Based Study of Russian Services and Missions Past and Present* (Washington, D.C.: National Intelligence Press, 2022), chapter 7. See also press investigations identifying Unit 29155's Switzerland-based forward headquarters and operational footprint across Europe.

16 Bellingcat Investigation Team, "Hunting the Hunters: How We Identified Navalny's FSB Stalkers," Bellingcat, December 14, 2020.

17 Bellingcat Investigation Team and The Insider, "Russia's Clandestine Chemical Weapons Programme and the GRU's Unit 29155," Bellingcat, October 23, 2020.

18 Bellingcat Investigation Team, The Insider, *Der Spiegel*, and CNN, "FSB Team of Chemical Weapon Experts Implicated in Alexey Navalny Novichok Poisoning," Bellingcat, December 14, 2020.

19 Christo Grozev, quoted in Mick Krever, "How Reporters Exposed the Spies Implicated in the Navalny Poisoning," Global Investigative Journalism Network (2021).

20 Bellingcat Investigation Team and The Insider, "Russia's Clandestine Chemical Weapons Programme and the GRU's Unit 29155," October 23, 2020.

21 C. Grozev, R. Dobrokhotov, M.Weiss et al., "Lost in Translation: How Russia's New Elite Hit Squad Was Compromised by an Idiotic Lapse in Tradecraft," *The Insider*, March 13, 2026. See also Meduza, March 14, 2026; Charter 97, "Investigation: Center 795—Russia's New Autonomous Structure for Political Assassinations Abroad," March 2026.

22 Grozev et al., "Lost in Translation."

23 Grozev et al., "Lost in Translation"; Southern District of New York, *USA v. Denis Alimov*, indictment filed February 2026.

24 Grozev et al., "Lost in Translation."

25 Abram N. Shulsky and Gary J. Schmitt, *Silent Warfare: Understanding the World of Intelligence*, 3rd ed. (Washington, D.C.: Brassey's, 2002), 126-127.

26 Riehle, *Russian Intelligence*, 72-75; Center for Strategic and International Studies, *Analysis of Russia's Hybrid Warfare Posture Post-2022*.

27 Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community*, March 2026, Cyber Section.

28 Michael C. Horowitz, "How 2026 Could Decide the Future of Artificial Intelligence," Council on Foreign Relations, January 12, 2026.

29 Politico, "AI Unmasking ICE Officers," August 29, 2025.

30 Moede, "Ubiquitous Technical Surveillance and the Renewal of Irregular Warfare."

31 Institute for Signature Reduction, *Signature Reduction Doctrine Framework* (2026).

32 Shulsky and Schmitt, *Silent Warfare*, 120-128.

33 Department of Defense Instruction 3000.07, Irregular Warfare (IW) (2023).

34 Chambers, Countering Gray-Zone Hybrid Threats.

35 Riehle, Russian Intelligence, 62-86.

36 RAND Corporation, *China's Gray Zone Warfare*, 2021, 97–110.

37 Michael W. Parrott, "Reforming U.S. Counterintelligence for Strategic Competition: Building a Complex Adaptive National Immune System," Joint Special Operations University Call for Papers (2026).

38 Shulsky and Schmitt, *Silent Warfare*, 126-127.

39 Parrott, "Reforming U.S. Counterintelligence for Strategic Competition."

40 Royal United Services Institute, "Russia's Clandestine Chemical Weapons Programme: The Bellingcat Exposure," December 3, 2020.

41 Moede, "Ubiquitous Technical Surveillance and the Renewal of Irregular Warfare."