Irregular Warfare Center

Spotlight

Amplify | Illuminate | Address Vol. 4 Ed. 7 | July 2025 Deter | Defend | Defeat

Experts Convene in Arlington to Address Aviation and Transportation Vulnerabilities in Irregular Warfare

ARLINGTON, Va. – Leading experts in national security, aviation, and transportation convened this week for a critical workshop, "Defense of the Homeland: Aviation and Transportation in Irregular Warfare." Held from July 15-16 in Arlington, Virginia, the event brought together government officials, military leaders, academics, and industry professionals to explore the evolving threats to U.S. homeland security in an era of irregular and hybrid warfare.

CLEAR's Principal, Product Manager Vladimir Stojkovski answers questions during a panel chat for Mitigating Cyber Threats to Aviation Operations during the Defense of the Homeland: Aviation and Transportation in Irregular Warfare Workshop in Arlington, Virginia, July 16, 2025.

The workshop, organized by the Irregular Warfare Center (IWC), focused on identifying vulnerabilities within the nation's aviation and transportation sectors and developing actionable strategies to enhance resilience against modern threats. Discussions highlighted the blurring lines between traditional warfare and criminal activity, the rapid proliferation of advanced technologies like drones, and the increasing sophistication of adversarial tactics. The overarching goal was to develop actionable items and define future priorities for the irregular warfare community in safeguarding the homeland.

"In my role as Director of the Homeland Defense Fellowship (HDF) Program and as a faculty member teaching Countering Irregular Warfare at CISA, this workshop offered an important opportunity to engage with a diverse group of experts. Our goal was to confront irregular challenges that pose significant threats to the security of the U.S. homeland," said Department of Homeland Security (DHS) Chair | Visiting Professor, Director, Homeland Defense Fellowship (HDF) program Mr. Antonio "T" Scurlock.

The Critical Role of Aviation and Transportation in Irregular Warfare

IWC Director Dr. Dennis Walters initiated discussions by emphasizing "the critical role of aviation, airlines, and transportation in irregular warfare." The IWC, with its mission and authorities, aims to address the complex nature of irregular warfare, which often operates below the threshold of conventional conflict. Unlike traditional homeland defense definitions, irregular warfare encompasses a broader spectrum of threats that can significantly impact national security without direct military engagement.

Participants explored the profound implications of disruptions to these vital sectors. For instance, failures in port infrastructure, with 80% of cranes manufactured in the People's Republic of China, present vulnerabilities susceptible to remote access and control. A hypothetical scenario suggested a complete halt to the maritime supply chain, leading to economic impacts comparable to the $1 billion per day loss experienced during the Port of Los Angeles shutdown due to COVID-19 and labor disputes.

"It is critically important for government personnel and agencies to discuss security challenges across sectors. Cross-domain collaboration strengthens homeland defense and enables proactive responses to emerging threats," added Shurlock.

Evolving Threat Landscape: Plausible Scenarios and Their Impacts

The workshop delved into a range of plausible, yet often overlooked, catastrophic scenarios that could be orchestrated by adversaries or exploited for strategic effect. Some of the guest panelists urged attendees to consider what a major attack on the homeland might look like today, beyond conventional military conflict.

Specific threats and their potential impacts included:

Offshore Oil Platforms: Drawing parallels to the 2010 Deepwater Horizon spill, experts discussed the cyber vulnerabilities of offshore oil platforms, which, if exploited, could trigger a major national emergency with cleanup costs potentially exceeding $65 billion.

GPS Outages: The ease of jamming and spoofing GPS signals, as seen in recent events, could lead to widespread distrust in navigation systems, causing crashes in major waterways and strategic disruptions.

Mass Migration Scenarios: Adversary-induced mass migration, potentially fueled by disinformation campaigns, could overwhelm U.S. border security resources. -*Cont. Pg. 2*

Director's Corner

Dr. Dennis Walters, IWC Director

From Defense to Deterrence: Building Pacific Resilience

Last month, I wrote to you about the dangerous culture of risk aversion within the Department of Defense and how the IWC's embrace of calculated risk-taking enables us to defend the homeland more effectively. This month, I want to share how that same innovative approach is proving essential as we turn our attention westward to the Pacific, where reestablishing deterrence against an increasingly aggressive China requires building resilience across entire societies.

The challenge we face in the Indo-Pacific is unlike anything we've encountered before. China's hybrid warfare approach—blending economic coercion, influence operations, criminal networks, and information warfare—targets the very foundations of democratic societies. Traditional deterrence models focused on military capability alone miss a crucial point: a society that crumbles under the first application of pressure cannot deter anything. True deterrence in this environment requires something deeper—comprehensive resilience that spans from special operations forces to everyday citizens.

Our Functional Area Networks have proven remarkably effective in this mission precisely because they mirror the whole-of-society approach that resilience demands. When partner nations face complex challenges that span multiple domains—from countering influence campaigns to building economic resilience against coercion—our volunteer networks can rapidly mobilize expertise from across the Department, interagency partners, academia, and the private sector. This summer's engagements across the Pacific demonstrated this adaptive capacity in action.

I want to particularly recognize the Daniel K. Inouye Asia-Pacific Center for Security Studies (APCSS) for their invaluable partnership and leadership in this effort. APCSS has been instrumental in bringing together diverse stakeholders from across the region to tackle these complex challenges. Their commitment to fostering resilience through education, dialogue, and partnership perfectly complements the IWC's network-centric approach. Their collaborative workshops we've supported this summer exemplify how academic institutions, military organizations, and civil society can work together to build the kind of comprehensive resilience that effective deterrence requires.

What makes resilience-building particularly challenging—and essential—is its inherently decentralized nature. Just as Admiral Nimitz trusted his commanders to make tough decisions at Midway, building societal resilience requires trusting diverse networks of citizens, civil society organizations, and institutions to recognize threats and respond effectively. Beijing's strategy deliberately targets this trust, seeking to fragment societies by exploiting divisions and undermining confidence in democratic institutions.

Our response must be equally systematic but fundamentally different in character. Where China seeks to divide and weaken, we must connect and strengthen. This means building partnerships that span from Taiwan's National Security Council to regional civil society organizations, from academic centers to grassroots community groups. It means developing frameworks that help ordinary citizens recognize and resist influence operations while strengthening the legal, economic, and social institutions that underpin democratic resilience.

The work we've done this summer examining potential Taiwan scenarios, analyzing criminal networks, and fostering regional partnerships all serves this broader resilience mission. When we push beyond traditional military planning to examine post-conflict resistance scenarios, we're helping societies prepare for the full spectrum of hybrid threats. When we trace connections between transnational criminal organizations and state actors, we're exposing vulnerabilities that resilient societies must address.

Resilience and deterrence are inextricably linked in this environment. A resilient society—one with strong institutions, engaged citizens, and robust networks of mutual support—presents a fundamentally different proposition to potential aggressors than one that appears fragmented and vulnerable. To counter and deter PRC aggression in the Indo-Pacific requires the combined efforts of societies committed to mutual resilience and respect.

The IWC's network-centric approach offers a model for building this kind of comprehensive resilience. By embracing calculated risk-taking and empowering diverse communities of practice, we're not just defending against today's threats—we're building the societal foundations that make effective deterrence possible.

Stay tuned for more great things!
Dr. Dennis Walters, IWC Director

U.S. Army Gen. (Ret.) Stephen Lyons, former commander, U.S. Transportation Command, takes questions from IWC Deputy Director, Chief of Staff Dr. Lori Leffler, as part of a "fireside chat" panel during the Defense of the Homeland: Aviation and Transportation in Irregular Warfare Workshop at

Director, Irregular Warfare Center Dr. Dennis Walters addresses the audience during the Defense of the Homeland: Aviation and Transportation in Irregular Warfare Workshop in Arlington, Virginia, July 15, 2025.

PRISM: Call For Manuscripts

The IWC is seeking Manuscripts for an upcoming special edition of PRISM!

Submit today!

Media Highligts

"Intelligence Wars, Their Warriors, and Legal Ambiguity –Part I: Wars and Warriors"
by: Brig Gen (Ret) Ken Watkin, Lieber Institute West Point
https://lieber.westpoint.edu/intelligence-wars-their-warriors-legal-ambiguity-part-i-wars-warriors/

"Foreign Influence is Fueling the War in Sudan"
by: Charles A. Ray, Foreign Policy Research Institute
https://www.fpri.org/article/2025/07/foreign-influence-is-fueling-the-war-in-sudan/

Irregular Warfare Center

Spotlight

Amplify | Illuminate | Address

Vol. 4 Ed. 7 | July 2025

Deter | Defend | Defeat

Experts Convene in Arlington to Address Aviation and Transportation Vulnerabilities in Irregular Warfare- *Cont.*

like the 1980 Mariel boatlift and the 1994 Haitian and Cuban interdictions demonstrated the immense strain on resources, a capacity the Coast Guard noted it no longer possesses at the same scale.

New Pandemics: The deliberate manufacturing and spread of a new pandemic by an adversary was considered, highlighting the potential for widespread societal and economic disruption.

Manufactured Wildfires/Natural Disasters: The low-cost potential for adversaries to use drones with incendiary payloads in vulnerable areas to ignite wildfires, causing billions in damage as seen in California, was also discussed.

Asymmetric Attacks: The possibility of a terrorist group releasing a Weapon of Mass Destruction (WMD) or deploying an underwater unmanned vehicle while the U.S. is distracted by other conflicts was identified as a significant asymmetric threat.

Panelists further elaborated on future homeland threats, including armed water drones, armed ground robot vehicles, static-firearm sniper rifles, weaponized smart safe houses, and coordinated human and drone attacks. These threats, he noted, are often not adequately considered at state, local, or federal levels.

Resilience and Preparedness: A Call for Introspection and Action

A major focus of the workshop was on the urgent need to improve national resilience, capacity, and response awareness within the homeland. Discussions centered on whether existing authorities are sufficient to act decisively in such scenarios and what maritime domain awareness truly entails in a contested environment. The question of personnel capacity, drawing parallels to the 500% increase in the Coast Guard during WWII, highlighted the need for expanded training centers and rapid force generation.

A core message resonated throughout: the homeland is no longer a sanctuary. Participants reflected on Abraham Lincoln's 1838 quote, suggesting that physical presence is no longer required to inflict distress on the homeland, emphasizing the need for offensive thinking and the potential to use similar indirect tools against adversaries.

Counter-Unmanned Aircraft Systems (CUAS): Addressing the Proliferation

The proliferation of Unmanned Aircraft Systems (UAS) and the challenges of effectively countering them in the homeland context were extensively debated. Insights from conflicts in Ukraine and Azerbaijan highlighted the rapid pace of UAS/CUAS development and the incorporation of AI for swarming and "mind hiving" tactics.

The symposium noted a significant demand signal for industry to build CUAS capabilities but also recognized the need to optimize counter-drone operations within high-level strategic competition. A critical assumption challenged was the lack of public approval for using technology that might cause property damage or collateral effects in the homeland; studies suggest high public support for CUAS, especially at military installations, provided senior leaders explain the necessity.

The TSA Federal Air Marshal Service shared insights on the challenges of training and funding for CUAS, noting that counter-UAS is often an "extra" duty. They highlighted the importance of partnering with state and local first responders, providing them with low-cost or no-cost tools and training, such as a three-day course for police officers on identifying nefarious drone activity. A significant concern raised was the sheer volume of drone sightings at airports (500,000 per day), with many operators being "clueless and careless" rather than intentionally malicious, underscoring the need for public education on impacts and laws.

Supply Chain Vulnerabilities and Hybrid Threats to Agriculture

The fragility of global supply chains was a critical discussion point, particularly concerning agriculture. The 2022 fertilizer shortage, exacerbated by geopolitical events, demonstrated how a two-week slowdown could lead to a 30% decrease in yields, highlighting agriculture's designation as critical infrastructure often overlooked in national security planning.

The "PRC Hybrid Playbook" was discussed, detailing strategic pressure on U.S. agriculture through supply chain dominance, industrial espionage, and intellectual property theft. Examples included the acquisition of Syngenta, seed stealing, and the refusal to approve fourth-generation biotech until China gains an advantage. The meat industry, heavily impacted by COVID-19 plant shutdowns, and the control over agricultural technology (Agtech) drones and software (e.g., John Deere's control over farming equipment) were cited as systemic vulnerabilities.

This "bio-cyber-economic hybrid threat nexus" was described as an integrated strategy, not random events, requiring a deliberate posture to safeguard U.S. agriculture. The current U.S. response was characterized as siloed and reactive, underscoring the need for wargames and public-private response tests to identify weak links and policy gaps.

Information Operations: Preparing Populations for Hybrid Threats

The psychological impact of attacks and the role of disinformation and misinformation campaigns in hybrid warfare were extensively examined. The Colonial Pipeline incident, where a ransomware attack led to mass panic and a declared state of emergency, was cited as an example of a hybrid threat where the population's response became part of the attack.

Hybrid threats operating below the threshold of full-scale war, are difficult to detect and attribute, often combining to create compounding effects that undermine trust in government, institutions, and society. Critical infrastructure, with its interconnectedness and reliance on public-private cooperation, is a key vulnerability, as disruptions rarely stop at borders.

The European experience in preparing populations for hybrid threats offered valuable lessons. Countries like Sweden, through its "Total Defense" strategy and mailed guidebooks, and the UK, with its cyber strategy and Resilience Academy, have actively worked to inform and train their citizens. Romania's Euro-Atlantic Resiliency Centre, established in 2021, embodies a whole-of-government and society approach to building resilience. Key takeaways included the need for clear strategies, policies, and agencies, and the importance of apolitical organizations in preparing populations, especially in politically divided societies.

Strategic Integration, Special Operations, and Future Directions

Discussions on strategic integration highlighted the importance of setting conditions for success in irregular warfare. Adversaries are actively engaged in "Operational Preparation of the Environment (OPE)," establishing economic, social, and political conditions to destabilize their targets. Examples included the increasing number of Chinese nationals crossing the southern border, illicit drugs operations funding fentanyl precursors, and Chinese businesses acquiring land near sensitive national security infrastructure. The challenge lies in detecting these disparate actions and understanding their cumulative effect.

The workshop also touched upon the critical need for interagency cooperation, noting that while individual agencies may excel in their "stovepipes of excellence," a unified understanding and response to complex threats are often lacking. The concept of "unity of effort" rather than strict "unity of command" was proposed as a more realistic approach in a multi-stakeholder environment.

Irregular Warfare Center Director Dr. Dennis Walters discusses irregular challenges and collaboration opportunities aviation, transportation and homeland security with the Special Advisor for Homeland Security and Defense to the U.S. Vice President Mr. Tom Opelak.

Mitigating Cyber Threats to Aviation Operations

Cybersecurity experts from TSA, 7 Viking Security, and CLEAR discussed the evolving nature of cyber threats to aviation. The shift from traditional vulnerabilities to AI-based and insider threat access points was highlighted, with concerns about deepfake and voice spoofing for social engineering. The convergence of IT and operational technology (OT) means that systems like baggage handling and HVAC are now potential targets.

The biggest problem identified was overconfidence in security measures. Experts stressed the need for robust vendor management, contingency plans, and regular tabletop exercises (TTXs) that blend different organizations to identify faults before they occur. The increasing sophistication of fakes necessitates higher fidelity identity verification, potentially leveraging advanced biometrics while ensuring consent and control of data. The promise of AI and machine learning in quickly identifying anomalous behavior was acknowledged, but so were the risks of agentic AI being used offensively and the challenges of integrating new technologies with antiquated legacy systems.

Industry-Government Collaboration on Mobility and Resilience

The critical reliance on commercial airlift for national defense was a key topic. TRANSCOM moves 90% of personnel and 40% of bulk cargo for the Department of Defense via commercial carriers, amounting to billions annually. The State Department also relies heavily on commercial aviation for its personnel and cargo movement.

Maintaining this capacity between crises is a challenge, especially for small-wing and rotary aircraft internationally. The need to foster capabilities through the State Department to ensure American carriers maintain experience in various areas of responsibility was emphasized. Pilot readiness and availability were identified as primary concerns, with companies facing challenges in qualifying pilots for operations in warzones. The importance of deep and ongoing relationships with industry was underscored, with examples like FedEx offering free flights during the Kabul evacuation.

"All of the sessions, "Information Operations in Defense of the Homeland," "Emerging Technology and Defense of the Homeland," and "Threat Finance and Economic Levers in Defense of the Homeland", were outstanding," said Shurlock. "Each panel provided valuable insights and constructive challenges to prevailing ideas, all within the framework of the Chatham House Rule. I found the case study on hybrid threats targeting U.S. agriculture and agribusiness particularly enlightening."

A Call for Coherent Action

Throughout the symposium, a clear message emerged: the U.S. homeland faces an array of complex, interconnected, and rapidly evolving irregular and hybrid threats that demand a "whole of nation" approach. The discussions highlighted the urgent need for increased awareness, proactive prioritization of threats and resources, and robust collaboration across government, private industry, and civil society.

Mr. Shurlock added that one the major take aways from this workshop the "techniques for building resilience in social and digital information environments; insights into dual-use technologies and anticipating adversary applications; frameworks for disrupting illicit finance networks, including cartel-linked funding streams; and a deeper understanding of the epochal shifts in social and political organization."

The experts concluded that while the U.S. has significant capabilities, institutional barriers and a lack of a pervasive "defensive mindset" have created vulnerabilities. The symposium served as a critical forum to illuminate these challenges and to begin charting a path forward, emphasizing the importance of continuous education, policy adjustments, and a unified effort to build a more resilient and prepared homeland against the threats of irregular warfare.

Cyber Experts from various partners answer questions during a panel chat for Mitigating Cyber Threats to Aviation Operations during the Defense of the Homeland: Aviation and Transportation in Irregular Warfare Workshop in Arlington, Virginia, July 16, 2025.

Irregular Warfare Center

SPOTLIGHT

Amplify | Illuminate | Address

Vol. 4 Ed. 7 | July 2025

Deter | Defend | Defeat

National Resistance Applications Seminar Concludes, Emphasizing Modern Irregular Warfare

The Irregular Warfare Center (IWC) recently concluded its National Resistance Applications Seminar at Camp Dawson, West Virginia, from July 14-17, 2025. This critical seminar, part of the larger Ridge Runner Exercise Academics, gathered approximately 200 international and U.S. special operations forces, including representatives from the UK's 2nd Ranger Battalion, the Qatari military, and U.S. Army Special Forces. The diverse attendance highlighted the global relevance of resistance strategies in today's security landscape.

The four-day curriculum aimed to equip participants with the knowledge to establish and sustain effective resistance capabilities, particularly in scenarios of foreign advisory roles or direct invasion. The seminar provided vital historical context and practical methods, drawing lessons from past conflicts to help participants develop comprehensive strategies for resisting an invading power. Collaborative sessions fostered cross-cultural understanding and problem-solving among attendees.

A significant focus of the seminar was on the integration of unmanned aerial systems (UAS) and counter-unmanned aerial systems (CUAS) in irregular warfare. IWC Contractor Nolan Peterson shared insights from Ukraine, illustrating how drones are being utilized by resistance forces and how counter-UAS measures are being developed. This module provided cutting-edge understanding of drone warfare's implications for resistance movements. Other topics included communication security, intelligence gathering, resource management, and maintaining morale within occupied territories.

The IWC's National Resistance Applications Seminar marks a significant advance in international cooperation, enhancing allied forces' preparedness for modern security threats by integrating traditional resistance principles with contemporary technological advancements. The knowledge shared at Camp Dawson is expected to bolster the resilience and national security planning of all participating nations.

IWC in the UAE

Between July 29 and August 2, Irregular Warfare Center (IWC) Chief of Operations Erik Herr, Senior Analyst for NORTHCOM, SOUTHCOM, CENTCOM, IWC Contractor Brittany Carroll, and Dr. Tom Searle, Deputy Regional Advisor for U.S. Central Command and U.S. Southern Command, collaborated with key representatives from the United Arab Emirates (UAE) and Rabdan University to lay the groundwork for the upcoming UAE Irregular Warfare (IW) Conference. The event is slated to take place in Abu Dhabi, UAE, from November 24 through 25, 2025. The conference is anticipated to bring together a substantial number of participants, with attendees from the UAE from the U.S., fostering a significant exchange of ideas and expertise.

During these planning sessions, a key focus was to refine the conference's agenda. The agenda aims to provide a clear understanding of what IW is, share valuable lessons learned from the U.S.experience, and explore practical ways to operationalize these concepts. The conference will be structured over two days: the first will focus on strategic and ministerial-level discussions, while the second will dive into the operational aspects of IW.

Irregular Warfare Center Advances Counter-PRC Strategies Through July Engagements

The Irregular Warfare Center (IWC) significantly advanced its understanding of the People's Republic of China's (PRC) hybrid warfare tactics and strengthened international partnerships in July, directly supporting Department of Defense priorities for strategic competition in the Indo-Pacific region.

A key initiative was the "China: Hybrid Threats Workshop, Young Leaders' Forum," held from July 6-12 in Ottawa, Canada. This groundbreaking event, a collaborative effort between Asia-Pacific Center for Security Studies, the William J. Perry Center for Hemispheric Studies, and the IWC, brought together participants from 15 nations across the Americas, Asia-Pacific, and Europe. Deputy Regional Advisor Joshua Hastey, IWC contractor, presented compelling case studies, examining the PRC's economic coercion against small states like Palau and Lithuania. His presentations highlighted how Beijing weaponizes economic interdependence to punish nations that challenge its political objectives, fostering critical discussions and valuable international connections.

Later in July, from July 22-24, the IWC hosted a pivotal Taiwan Occupation Foresight Workshop in Washington, District of Columbia. This innovative workshop explored an under-examined but crucial domain: post-invasion occupation planning and resistance forecasting in Taiwan. Unlike most strategic analyses that conclude with military conflict, this workshop focused on the political, social, and psychological consolidation efforts that would follow a potential PRC seizure of the island. The workshop's outputs will directly support the design of a multi-scenario, matrix-style wargame for use by the IWC and international partners. Experts analyzed historical PRC occupation strategies in Tibet, Xinjiang, and Hong Kong to identify patterns that could inform Taiwan's resistance planning and allied support strategies. Key themes included the PRC's use of legal formalism, demographic engineering, and the strategic manipulation of PRC vulnerabilities.

Complementing these engagements, the IWC published two significant analytical pieces. The first, "Blueprint to Counter China's Criminal State Actions: Leveling the Playing Field for Strategic Competition," examined how the PRC leverages transnational criminal networks to gain asymmetric advantages against the United States, proposing counter-threat networks (CTNs) as a response. The second, "Today's Opium Wars: The Unrestricted Warfare Playbook in the U.S. Illicit Drug Market," revealed how Beijing weaponizes drug trafficking, particularly fentanyl and marijuana, as a form of irregular warfare against the United States, advocating for a whole-of-society approach.

These July initiatives demonstrate the IWC's evolving role in countering PRC hybrid warfare strategies. By combining international partnerships, innovative wargaming methodologies, and rigorous analysis of criminal networks, the Center is building a comprehensive framework for strategic competition, positioning itself at the forefront of irregular warfare innovation in the Indo-Pacific.

Current Initiatives, Upcoming Events & IW Educational Offerings

Don't forget to check out The Department of Defense's Irregular Warfare Center (IWC) ***PRISM: The Journal of Complex Operations*** **follow the link for the latest issue!**

Spotlight Team

IWC Director Dr. Dennis Walters
IWC Chief of Staff, Deputy Director Dr. Lori Leffler
IWC Contractor, Public Affairs Officer/Editor Pedro A. Rodriguez

Contributors

IWC Contractor, Deputy Regional Advisor, INDOPACOM Dr. Joshua Hastey
IWC Contractor Senior Analyst, NORTHCOM, SOUTHCOM, CENTCOM Brittany Carroll

This Month in Irregular Warfare History

-July 28, 1914: The assassination of Archduke Franz Ferdinand in July 1914 by Serbian nationalists belonging to the Black Hand group, an act of irregular warfare, triggered the July Crisis and ultimately led to the outbreak of World War I.

-July 26, 1953: A failed attack on the Moncada Barracks in Cuba, led by Fidel Castro and his 26th of July Movement, marked a key early event in the Cuban Revolution which successfully used irregular warfare tactics to overthrow the Batista regime.

-July 7, 2005: Terrorists attacked London's transit system during rush hour, detonating bombs in three subways and one bus, killing 56 people and injuring 700. This attack, attributed to al-Qaeda, highlights the devastating impact of terrorism as a form of irregular warfare.

-July 2024: A joint international operation successfully disrupted a large-scale Russian cybercrime network, NoName057(16), which engaged in distributed denial-of-service (DDoS) attacks against countries allied with NATO. This demonstrates the use of cyberattacks as a modern form of irregular warfare.

Connect With Us

Irregular Warfare Center (IWC)

Irregular Warfare Center (IWC)

@IrregularWarCtr

IWC Homepage

IWC Contact Info

For general inquiries, please contact us at info@irregularwarfarecenter.org

For media-related inquiries, please contact us at media@irregularwarfarecenter.org