

Assembling the A-Team: Creating an Interagency Office to Counter Irregular Warfare

Description

When a new American president takes office on January 20th, they will confront a dangerous national security environment shaped by Irregular Warfare (IW) challenges. From cyber warfare and gray zone conflicts to terrorism and insurgency, these challenges demand immediate, actionable solutions. In September, the Irregular Warfare Initiative invited our readers to contribute fresh, pragmatic, and non-partisan policy recommendations to help shape the next administration's approach to these threats. In our second article, Erik Ackroyd argues for a new interagency office working on irregular warfare.

Irregular warfare is a nebulous term that very much resembles the polycephalic hydra of Greek mythology. The [manipulation of international law](#) and norms to secure regional hegemony, [use of unmarked soldiers and equipment](#) to occupy the territory of another nation, highly violent [transnational militia and terror networks](#), [recurring cyberattacks](#), [threats to critical infrastructure](#), and everything in between fall within the domain of irregular warfare. Ultimately, what binds this near-infinite array of actors is a wish to fight with *just* enough plausible deniability built into their respective deeds to forestall the escalation of a conflict to the level of traditional conventional or nuclear war, typically involving the use of soldiers, tanks, ships, planes, and nuclear arms to occupy territory or otherwise impose political and material defeat upon an enemy. In essence, irregular warfare consists of just about everything under the sun since it works both separately and in tandem with conventional warfare to achieve desired outcomes. However, separating irregular warfare from conventional warfare perhaps occludes more than it clarifies. The goal of securing influence over other actors's [assur\[ing\] or coerc\[ing\]](#) states or other groups, as in [the words](#) of the Congressional Research Service can be seen as the goal of both conventional *and* irregular warfare as traditional alliance networks and wars are meant to defend friends and repel enemies through any means necessary. For instance, surreptitious cyberattacks aimed at key banks or commercial actors are not much different than the use of formal naval blocks used to curtail a nation's economic activity. Therefore, it is of great importance to recognize that warfare—whether conventional or irregular—is [a continuum](#) requiring management from whole-of-society inputs.

Consequently, the United States government should consider the implementation of a new interagency office to coordinate these various inputs while bringing irregular threats into strategic focus. Such a body would not seek to duplicate the efforts of the Office of the Director of National Intelligence (ODNI) or other such entities focused solely on collecting and disseminating governmental intelligence. Rather, this new entity should resemble a more informal version of the [National Defense Advisory Commission \(NDAC\)](#), which was established in 1940 by Franklin Roosevelt's administration to marry the leadership of governmental agencies (e.g. the Departments of War, Labor, and Agriculture) with that of commercial heavyweights (e.g. the Ford Motor Company or Higgins Industries) to concentrate defense production, stabilize consumer prices, and promote broad innovation.

Indeed, as the Second World War effectively demonstrated, everything the American people could muster was necessary for expelling the forces of fascism from both the Atlantic and Pacific. This meant not only recruiting millions of men to fight in uniform, but also recruiting men and women at home [to create effective propaganda](#), [to coordinate the production of materiel](#) to support those fighting abroad, to bolster deception, and to generate revenue through things like war bonds to ensure the United States and its allies had the treasure to prosecute a war against tyrants. In other words, there was little distinction between means and ends, warfighter and civilian, as the whole heft of the United States had to be mobilized to ensure victory in two theaters.

Likewise, the numerous domains of irregular warfare today require many of the same public-private inputs as those used to fight in the Second World War. Cyber threats require [both government bodies and private businesses to protect](#) the data and infrastructure of the American people. The United States Navy must use its advanced warships and munitions to not only compete against other navies, but to [protect vital shipping lanes like the Red Sea](#) from disruptions. The American foreign policy apparatus must take staunch positions in forums like the United Nations to ensure strategic competitors like the People's Republic of China (PRC) [cannot amend or abuse elements like international maritime law](#) to become the suzerain of a whole region. In this way, there is little distinction between irregular and conventional threats, with many of the same tools used across the board.

With that in mind, it's time to muster a new A-team to assess and respond to irregular threats in a holistic, far-seeing manner. The Department of Defense (DoD) veered close to this idea in miniature when it [consolidated several military intelligence elements to form](#) the Defense Clandestine Service (DCS). The formation of the DCS signaled a desire to overcome a degree of myopia imposed by the Global War on Terrorism. Rather than focusing solely on highly localized [battlefield intelligence](#) as it had during the start of the post-9/11 wars in Iraq in Afghanistan, the DCS would gather information relevant to the broader military capabilities of near-peer competitors and revisionist powers like the

PRC and Iran. In doing so, other intelligence organizations like the overburdened Central Intelligence Agency (CIA) could redirect resources away from military intelligence to securing information on the social, economic, and political aspects of a given target. This symbiotic approach allows one agency to tap into the resources and expertise of the other to create a larger, complementary vision of the world and the various threats to American interests. An upscaled version of this arrangement could help the executive office dampen the impact of irregular warfare as well. That is, creating a unified operational command center shared by various agencies could not only align means with ends, but also save costs on redundancies while enhancing the strengths of each constituent organization.

A new interagency effort might consist of a small office filled with one or two senior officials from many of the major federal departments and agencies who are responsible for American defense or foreign policy (e.g. the Departments of State and Defense). While not quite at the secretary or undersecretary levels, these officials should be of significant enough rank to understand the complexities of their respective organizations, the internal and external constraints they face, and be endowed with enough authority to share these complexities with others. In many ways, this new interagency office would be like the Cabinet of the United States; however, the key difference is that this new body would be focused on the warfare continuum rather than concerning themselves with maintaining the good graces of the American voter. In essence, domestic policy as it is traditionally envisioned would be eschewed by this new office in the interest of staying focused on adversaries from both within and without. Thus, the themes of terrorism (both domestic and foreign), cyberwarfare, supply chain security, and more would all fall within the purview of this office without having to redirect attention to domestic distractions like offsetting America's carbon footprint or lowering interest rates and gas prices for consumers during pivotal election seasons.

The goal of gathering so many senior minds from disparate departments would be for each organization to regularly brief the others on the worldviews, ambitions, fears, and key projects unique to each of them. For instance, the representative(s) of the National Security Agency (NSA) could note that there has been a rise in the use of cyberattacks by [Iran](#), [the PRC](#), and/or [North Korea](#) against the physical infrastructure, personal records, and intellectual property of the American people. The Department of Defense could chime in to confirm this account while the Department of Commerce shares how such cyber intrusions could lead to a [loss of confidence in e-commerce](#) if left unabated. In turn, this candid sharing of information and perspectives creates a combined sense of urgency within the new counter-IW agency to curtail any shrinking of America's economic and technological edge.

With this new cross-departmental understanding of a common threat, an operational game plan could be quickly sketched out and passed along to the relevant authorities within and between each organization. For instance, the Department of Commerce could use its connections with the civilian

tech sector to create new security protocols and reporting mechanisms to better home in on cyber threats. Likewise, the NSA could work in conjunction with the DoD to launch tailored, retaliatory cyberattacks to let adversaries know that cyberweapons cut both ways. Moreover, select technology companies could help to enhance the counter-IW efforts of the federal government by [enabling agencies to use things like generative artificial intelligence](#) to create allied botnets, targeted disinformation campaigns, and other smokescreens to slow enemy operations in the cyber domain and beyond. Even the Departments of Education and Labor could be brought into the mix by offering tuition assistance, grants, and stronger wage standards to incentivize young Americans to seek degrees and jobs in cybersecurity, creating a long-term commitment to the cause.

Again, the goal would be to create a more effective division of labor while bringing in voices that are typically not heard by the conventional intelligence community under the NSC, ODNI, and other such organizations. By allowing the Cabinet to deliberate and determine the *strategic* interests of the United States, the interagency counter-IW consortium could freely haggle amongst itself and brainstorm how to actualize those interests and create desired effects at the *operational* level. With a truly interagency picture in mind, not just broad departmental directives from the President and Cabinet, each agency within the federal government could then use its respective strengths and resources to create a whole-of-government, if not whole-of-society, response to pertinent threats.

Of course, this assumes that each organization within the counter-IW office does not view the others as competitors. Indeed, agencies may fear that too much collaboration could blur the [mandates or prohibitions](#) that distinguish one agency from another, leading to legal trouble, exacerbating battles for funding, or creating internal dysfunction within each agency. For example, the CIA's [restrictions on collecting information on U.S. persons](#) could be compromised by too eagerly participating in an interagency crackdown on [domestic violent extremists](#) hypothetically being radicalized and funded, at least in part, by [foreign adversaries such as Russia](#). Thus, with only one or two folks to represent the CIA at such a juncture, [decision overload](#) may lead to self-restrictive behavior, effectively promoting or maintaining the very bureaucratic siloing the counter-IW office is meant to resolve. Nevertheless, it is important to create some sort of vehicle that actually mobilizes interagency cooperation rather than merely gesturing at the concept.

To reiterate, there is considerable overlap between the means and ends of conventional and irregular warfare. Both modes of conflict seek to influence an adversary, whether through overt fighting, use of proxies to harass or undermine allied institutions, or the clandestine battle for hearts and minds in cyberspace and beyond. Indeed, we now find ourselves in a space where [conflict is a continuum](#) rather than a stark dichotomy constituted by peace on one end and war on the other. Even when the United States is not involved in kinetic combat with adversaries like the PRC on land, at sea, or in the skies,

both parties (and many others) seek to shape the political, social, and economic environments to favor their forces if conventional or nuclear war does erupt. Thus, competition in the 21st century has once again become a whole-of-society effort as highly sophisticated polities seek to defeat each other in a multitude of ways before shots are ever fired. Recognizing this, a dedicated office to mobilize the whole might of the United States as was done during the Second World War is essential to maintain an edge or, at the very least, mitigate the harm done from nonstop competition below the threshold of conventional warfare. The A-team would channel the creative and destructive energies of the American republic—though perhaps under a different name to escape copyright infringement.

Erik Ackroyd is an independent researcher interested in grand strategy and post-conflict reconstruction and rehabilitation. He holds an MA in Diplomacy from Norwich University.

Image generated by OpenAI's DALL·E, customized for this article

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

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

Date Created

2025/01/16