The Concept of an Economic Warfare Operations Capability (EWOC)

Tim Welter, PhD in collaboration with staff members of the Potomac Institute for Policy Studies

STEPS: SCIENCE, TECHNOLOGY, ENGINEERING, AND POLICY STUDIES

ISSUE 8, 2023

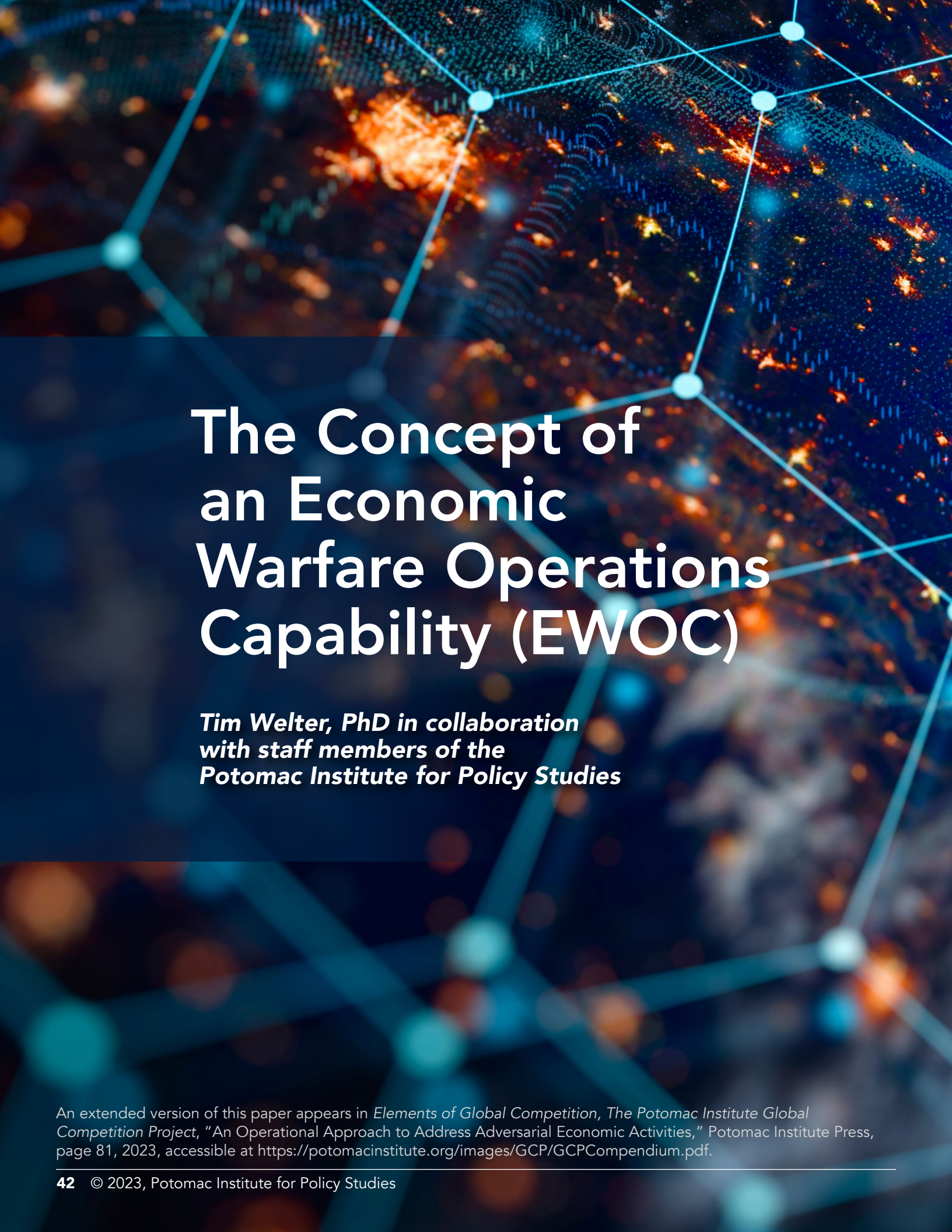
STEPS (Print) ISSN 2158-3854
STEPS (Online) ISSN 2153-3679

Tim Welter and Potomac Institute for Policy Studies Staff. "The Concept of an Economic Warfare Operations Capability (EWOC)" *STEPS* 8 (2023): 42-55.

POTOMAC INSTITUTE PRESS

STEPS: Science, Technology, Engineering, and Policy Studies
is published by Potomac Institute Press of the
Potomac Institute for Policy Studies.

Access to *STEPS* is available free online at:
www.potomacinstitute.org/steps.



The Concept of an Economic Warfare Operations Capability (EWOC)

Tim Welter, PhD in collaboration with staff members of the Potomac Institute for Policy Studies

An extended version of this paper appears in *Elements of Global Competition, The Potomac Institute Global Competition Project*, "An Operational Approach to Address Adversarial Economic Activities," Potomac Institute Press, page 81, 2023, accessible at https://potomacinstitute.org/images/GCP/GCPCompendium.pdf.

Introduction

The US enjoyed the benefits of a relatively unmatched monopolar position on the global stage in the immediate aftermath of the Cold War. That position has been challenged in recent years by rivals, such as China and Russia, working to shift the geopolitical and global economic environment in their favor.[1] To do so, both nations have employed asymmetric "gray zone" tactics, actions below the threshold of war, but which still vitally threaten the economic and security interests of the US and others.[2]

Gray zone operations include propaganda, media misinformation and disinformation, deliberate supply chain disruptions, and economic manipulation and coercion, along with other more traditional military equipping activities.[3] Economic warfare activities are the most concerning, as such activities are focused on destabilizing and diminishing the vitality of the US economy[4] and interfere directly with the United States' ability to acquire, secure, and field capabilities required to defend the nation.

The industry and supply chains that the US government relies upon for weapons, technology, infrastructure support, and other factors of vital importance are at risk—highlighted recently by the PPE and other shortages experienced during the early days of the COVID-19 pandemic.[5] Subsequently, factors limiting US access (deliberate or not) to critical technologies and other products and commodities vital to a healthy population and economy have become a growing concern for national leaders.

An emphasis of the 2022 National Security Strategy (NSS) was to invest in and partner with the commercial sector to strengthen the US national security posture—a societal-level approach to addressing the threats and realities of a dynamic global competitive environment. The approach carries over from the 2017 NSS and 2018 National Defense Strategy (NDS). Both emphasized the need for a strong, resilient defense industrial base as an integral part of national security, as the 2017 NSS stated, "…a vibrant domestic manufacturing sector, a solid defense industrial base, and resilient supply chains [are] a national priority."[6] The policy guidance across two administrations is encouraging, but there is still much to be acted upon.

Prior to the COVID-19 pandemic, US government efforts to combat asymmetric "gray zone" attacks were more reactive, fragmented, and siloed. The pandemic inspired US government agencies to re-evaluate how to identify, support, and maintain industrial base elements vital for US national security. However, the nation still lacks the strategy (2022 NSS aside), workforce skillsets, and business operations to properly address the scope of the challenge at hand.

The US government's approach to countering the infusion of adverse capital and other asymmetric economic activities that directly impact DOD missions has also been limited and disparate. While policymakers have acted,[7] the remaining challenge demands a fundamental shift in statecraft. Remedies will likely be constrained by the inertia of long-established institutional processes, cultures, and norms inside and outside the government. An evolution in thought and approaches to new threats come historically with a debate over the balance between liberty and security (e.g., post 9/11). Change, if effective, drives uncomfortable organizational and cultural shifts away from the status quo. In this case, a shift from 20-plus-years of the big "M" military as America's primary lever of national power toward others in the "DIME"—diplomacy, information, military, and economy—is necessary.

Ultimately, a US government entity must be designated to "own the supply chain and industrial base problem," responsible to orchestrate the development and employment of a suite of options to protect and defend the US industrial base from asymmetric economic attack. The Office of Economic Warfare and Competition (OEWC), as proposed by David Rader* is a tenable conception of such an entity, as is the Economic Warfare Operations Capability, a more operationally focused approach outlined in this article.[8]

Vulnerabilities resulting from conflict escalation, kinetic or otherwise, will be more manageable if there is a government entity with the authority and tools to identify, orchestrate, and address fundamental risks to the industrial base and supply chains. This would require strengthened

* Former Deputy Director of the Office of Foreign Investment Review at the DOD.

partnerships between the US government and the private sector to expose and examine threats to domestic and foreign companies. Moreover, it would require an exchange of information on risks, potential responses, and drivers—both political and economic—and their interdependencies with supply chains and national security. Ultimately, gray zone economic assaults must be addressed by the US government in collaboration with the private sector and partners and allies.

Until the problem is addressed, the US government's ability to carry out its core duties to "insure domestic tranquility, provide for the common defense, promote the general Welfare, and secure the Blessings of Liberty," is at risk. This paper provides a proposed solution to that end: The Economic Warfare Operations Capability (EWOC).

Background

Understanding the Problem

The US government is not well organized for societal-level competition against adversaries. The 2023 Select Committee on the *Strategic Competition Between the United States and the Chinese Communist Party* in the US House of Representatives has the opportunity to address these issues. "Gray zone" tactics, employed by China but also by Russia and others, operate below the threshold of open kinetic warfare but still threaten US national security. This is a reality of the character of competition and conflict in the 21st century. America is just starting to awaken to this reality and challenge traditional conceptions of the spectrum of war. Remedies will require a societal-level response that actively fuse operational savvy with economic and business acumen. They will also require authorities to swiftly decide and act on, or elevate threats and vulnerabilities for action, at appropriate levels across the US government and industry.

According to *Special Warfare*:[9]

> "Gray zone security challenges, which are competitive interactions among and within state and non-state actors that fall between the traditional war and peace duality, are characterized by the ambiguity about the nature of the conflict, opacity of the parties involved, or uncertainty about the relevant policy and legal frameworks."

Gray zone warfare is thus a way to weaken a rival nation's position outside the realm of conventional armed conflict and can be used to allow a competitor nation to achieve its

political goals. The ancient Chinese military philosophy of Sun Tzu articulated its practices and tactics. The People's Republic of China uses gray zone tactics to pursue the geopolitical goals of the Chinese Communist Party (CCP). Russia is also well-practiced in gray zone tactics.[10]

Gray zone tactics are delineated in China's People's Liberation Army (PLA) doctrine of "Unrestricted Warfare." The PLA emphasize combining all elements of national power to achieve national objectives, with tactics that reportedly include: "military intimidation, paramilitary activities [maritime militia and maritime law enforcement over disputed territories breaking norms of good seamanship], co-opting of state-affiliated businesses, manipulation of borders… lawfare and diplomacy, and economic coercion, and strategic investments in, and venture capital funding of, cutting-edge technology companies."[11] Gray zone economic activities are also referred to as predatory or asymmetric economics, adversarial investment, or as adversarial economics. They are designated in this paper as "economic warfare."

Ultimately, China and Russia have each been openly accused of destabilizing and diminishing the vitality of the US economy by using gray zone operations. Both have sought influence and advantage using adversarial economics. The defense industrial base has been a consistent target, through IP theft, infiltration of supply chains, and other gray zone activities.[12]

To ensure America's security and continued prosperity, the US government needs a coherent operational framework to identify, monitor, prioritize, and coordinate (across US government and DOD entities) the mitigation of vulnerabilities to the industrial base. To accomplish this, trust and agility must be central to working relationships between the public and private sectors. Concurrently, the government's acquisition vehicles and practices must evolve to address contemporary competitive challenges at a relevant pace.

Economic Warfare

Beginning in 1953, China has used a series of "Five-Year Plans" to set strategic goals, focus government work, and guide the activities of market and non-market entities in China.[13] In 2021, China started on its fourteenth Five-Year-Plan, which set an ambitious agenda to "promote high-quality development in all aspects, including the economy, environment, and people's livelihood and well-being, and realize the rise of China's economy in the global industrial chain and value chain."[14] To that end, the CCP has employed adversarial economic activities to undermine US economic and technological advantages to pursue its own strategic objectives on the global stage.[15]

China's grand strategy of economic warfare is enhanced by state ownership of industries and businesses. State-owned enterprises (SOEs) receive significant investments from their owners (the Chinese government), allowing them to invest with less risk than that which investors in private commercial companies experience. In contrast, US businesses rarely receive government subsidies in the way and extent that Chinese SOEs receive government funding.[16]

China also uses their own venture capital[17] funding to access innovative technologies in free-market economies. The Chinese government gains access to technologies (especially by investing in small and medium size Western enterprises) and then shares those technologies with their SOEs. China's venture capitalists have been monitoring innovation hubs like Silicon Valley for investment opportunities in early-stage startups in fields deemed essential to its future military dominance (AI, Fintech, etc.).[18]

Coercive loss of intellectual property (IP) can occur when a US company "partners" with a foreign company for "mutual benefit" in a joint venture or major stock purchase.[19] China, for example, can require a partnership for access to its market.[20] IP-intensive industries account for over 45 million US jobs and the loss of IP erodes US technological supremacy, the cornerstone of its economic prosperity and miliary hegemony since World War II.

Intellectual property theft by China is said to cost the US between $225 billion and $600 billion annually.[21] Malintended foreign direct investment and the use of cyber espionage to steal IP from US companies has resulted in the proliferation of technologies and capabilities once exclusive to the US military.[22] Chinese IP theft has allowed the PLA to fill gaps in its research programs, shortening R&D timelines for fielding advanced military platforms and identifying vulnerabilities in US systems to develop countermeasures.[23,24] It also allows China to bolster its own economy, cornering advantage in competition with the US.

Current Efforts to Combat Asymmetric Economic Activities?

While the US has laws to protect companies from predatory foreign direct investment (FDI), loopholes always exist in a proper free-market economy. The Committee on Foreign Investment in the United States (CFIUS) is supposed to prevent threats to national security from FDI in US businesses. The Foreign Investment Risk Review Modernization Act (FIRRMA), passed in 2018, attempted to provide more authority, scope, and latitude to CFIUS. However, CFIUS reported to Congress in 2022 that it only reviewed a "small percentage of the total number of… foreign direct investment flows into the United States"[25] Given the scale and adaptability of investments throughout the US economy, the challenge to CFIUS is simply too great.

To counter asymmetric economic threats, including threats to national security, a different approach is needed. The 2022 NSS talks of an "integrated defense," calling for the use of all instruments of national power to address subversive gray zone activities and other contemporary threats.[26]

The CHIPS and Science Act in August 2022 represents an effort to combat economic threats in the microelectronics and high technology fields. The law allots tens of billions of taxpayer dollars to invest across industry, government, and academia for R&D, manufacturing, and workforce development critical to gaining (or recovering) an economic and security posture for the United States, in particular in semiconductor manufacturing.[27]

The Office of Strategic Capital (OSC) was established in December 2022 within DOD's Office of the Undersecretary for Research and Engineering. The OSC is a turning point for DOD in publicly recognizing the need to counter the gray zone economic threats. Their mission is to "develop, integrate, and implement proven partnered capital strategies to shape and scale investment in critical technologies." Criticality, here, would refer to military needs.

At least two dozen other US government and nongovernmental organizations, including the FBI, and the Treasury, Commerce, and Defense Departments, have initiatives focused specifically on countering adversarial economics. However, these efforts are too disparate and tactically-focused to adequately address or deter the comprehensive gray zone strategies currently deployed against the United States. No single US entity, public or private, is calling the shots overall (let alone has the authority to do so) to counter adversarial economic challenges at the societal level. Subsequently, the government needs an orchestrated operational approach.

An Operational Approach: The EWOC

What sort of organization could address a solution set informed by the global economic, political, and security environment?

Designated the *Economic Warfare Operations Capability (EWOC)*, the concept outlined in this section is a proposed means by which the US government can operationally address the threats and challenges posed by adversarial economic activity.[28] This capability is an imperative if the US expects to remain operationally relevant on the global stage. It is envisioned as agile and responsive to the dynamics of the global economic, political, and security environments to support the strategic posture of the United States.

The overall mission of the EWOC is to ensure access to the industrial base and supply chains critical to preserving operational advantage across the full spectrum of conflict, to include economic warfare. As envisioned, the EWOC will do so by building and leveraging enduring partnerships and operational capacity across the interagency and industry.

The EWOC will bring disparate efforts together, prioritized and orchestrated under one umbrella—a scalable operational approach for decision and action.

The EWOC approach operationalizes the concept of "integrated deterrence" (a key principle of the 2022 National Defense Strategy), providing coordination with the private sector, as well as with vetted allies and partners, to address economic threats across domains and instruments of national power. The EWOC will help deter kinetic conflict with adversaries by virtue of using economic dependencies as a lever of national power, i.e., economic statecraft.

The EWOC has three core mission areas that fuse inputs from across the government, industry, and DOD:

Mission Area 1: Fused Observation and Analysis. Prioritize and conduct observation and analysis of global markets, the industrial base, and supply chains critical to the US government.

Mission Area 2: Industry–Government Partnerships. Shepherd enduring, agile partnerships between industry and the government.

Mission Area 3: Integration and Orchestration for Operations: Decide, Act, Elevate. Provide options to decide and act or elevate action to address threats and risks.

The synchronization of the EWOC's three mission areas is key to addressing the primary challenge: Assurance the US government has enduring, secure access to the industrial products and supply chains vital for success across the spectrum of conflict while maintaining competitive advantage.

The diagram and following section describe each mission area in greater detail, to include explanations of how they work together.

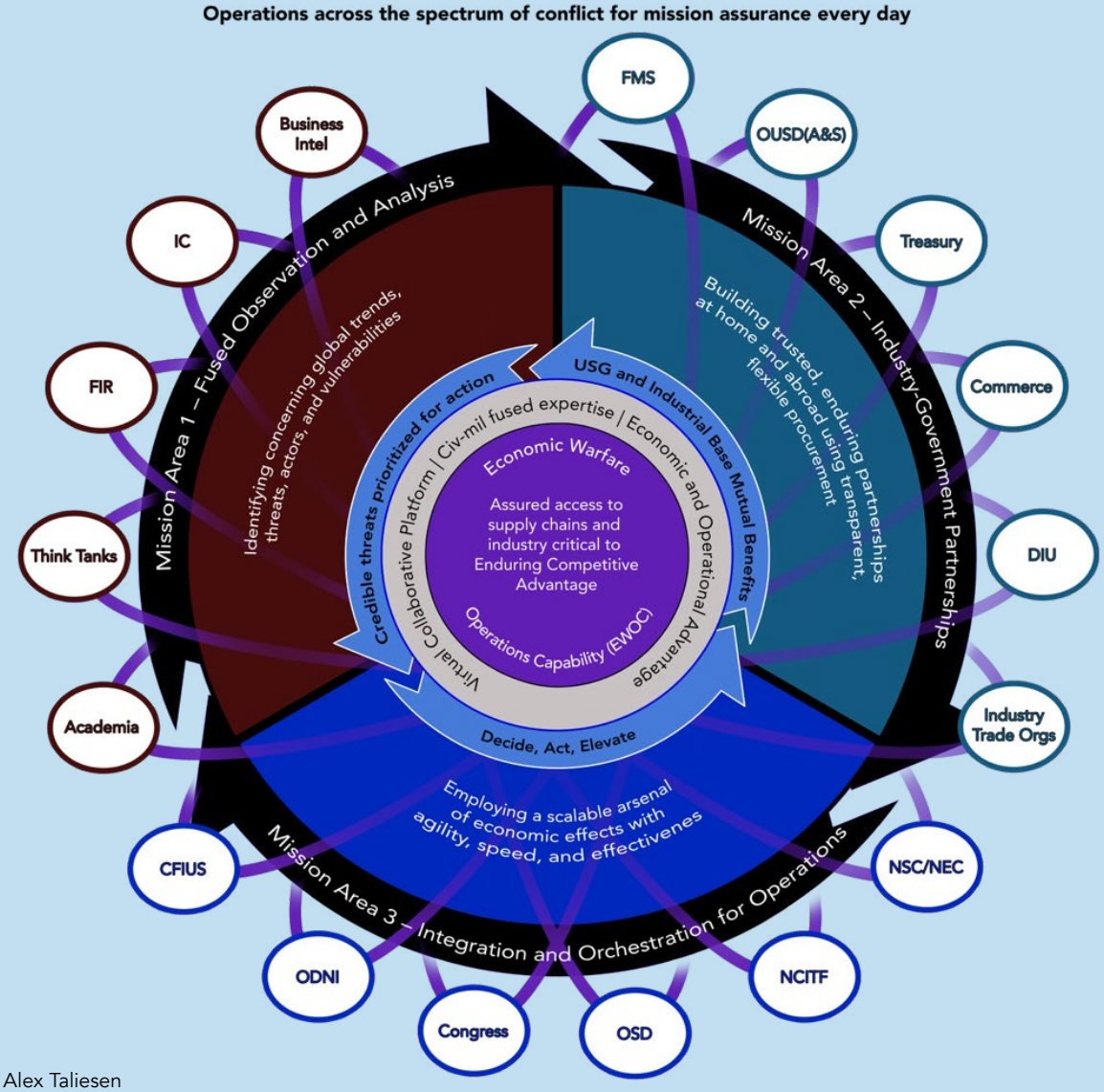


Image credit: Alex Taliesen

Mission Area 1: Fused Observation and Analysis—*Identifying Concerning Global Trends, Threats, Actors, and Vulnerabilities*

Mission Area 1 of the EWOC provides prioritized market intelligence and analysis for decisive operational action. The EWOC will have a dedicated workforce deeply steeped in both business intelligence and military operations, tasked to understand risks and vulnerabilities in supply chain networks impacting the US government.

Mission success will require continuous deep knowledge of global economic trends, investments, and markets and the identification of innovation and technologies vital to national security and US economic wellbeing. Intelligence will be collected from open sources, government sources, and businesses that develop their own intelligence in their respective market sectors.

Currently, information relevant to the problem set is scattered across the private sector, trade publications and associations, various areas of the executive branch and military services, and the intelligence community. Often, the government's awareness of useful information is limited and intelligence fusion capabilities are lacking that could provide comprehensive analytical products to inform decision makers. Therefore, an overarching role of the EWOC is to fuse disparate intelligence analyses together to provide prioritized, actionable options.

The EWOC will help identify sectors worth protecting and the nodes of influence. Analysis of the resulting network will provide critical points of vulnerability and risks in supply chains, driving further focused intelligence collection, sharing, and fusion among industry and government stakeholders.

The key to EWOC's Mission Area 1 is development of a workforce with expertise in researching, analyzing, and using economic market-based intelligence. The workforce would include experience across the financial services, intelligence, and operational national security realms. Expertise would be required in international finance and business, and global logistics coupled with national security savvy. Operators must be able to identify and understand risks and vulnerabilities in supply chain networks impacting US interests and readily leverage a deep knowledge of global economic trends, investments, markets, innovations, and technologies vital to national security and enduring competitive advantage.

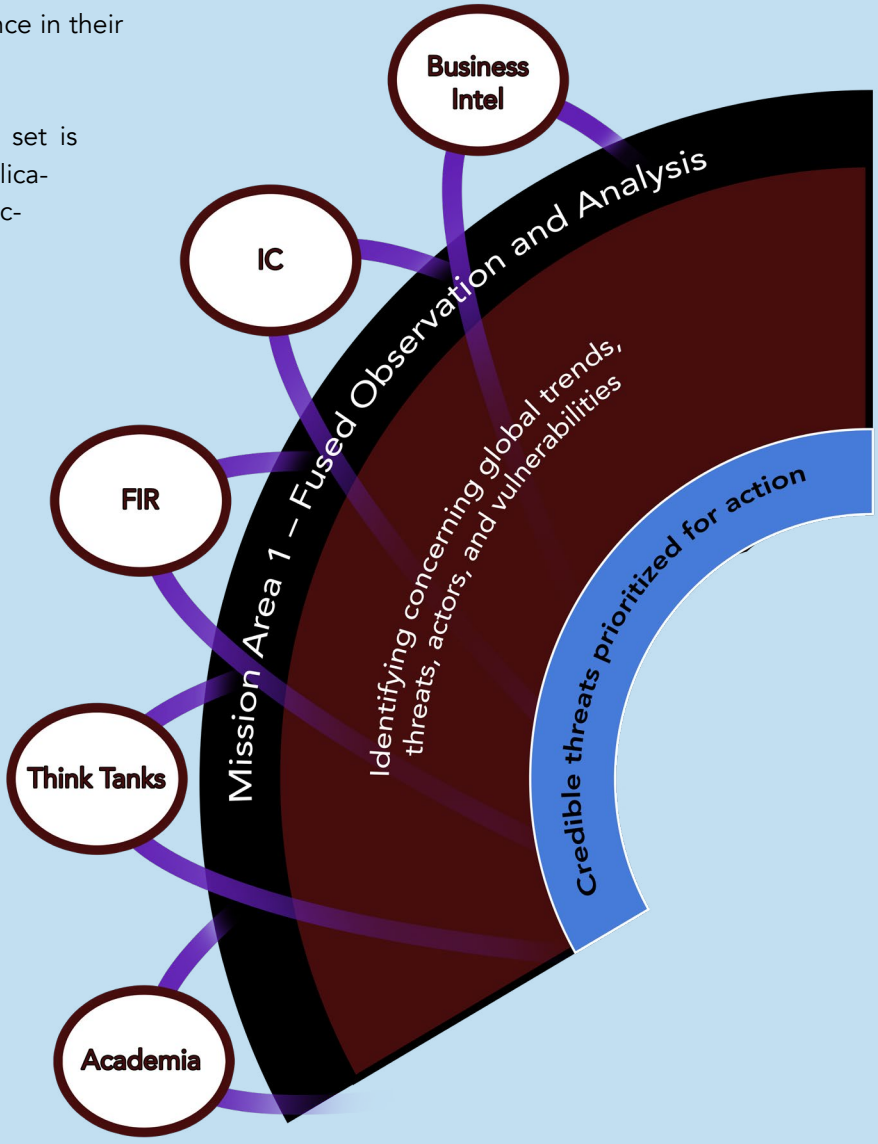
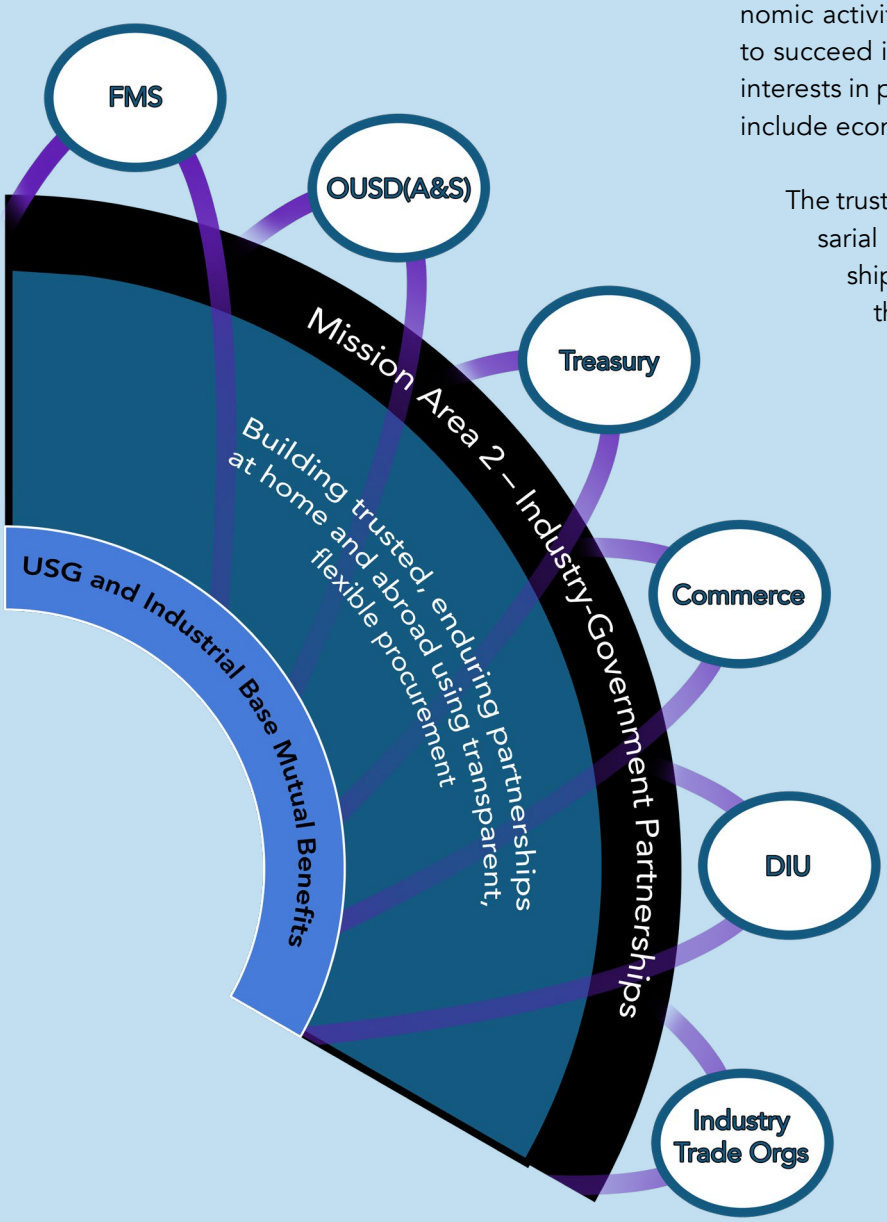


Image credit: Alex Taliesen

Mission Area 2: Industry-Government Partnerships—*Building Trusted, Mutually Beneficial Enduring Partnerships at Home and Abroad Using Transparent, Flexible Procurement*

Mission Area 2 of the EWOC is focused on developing and harnessing mutually beneficial relationships between the government and industry. It provides a virtual collaborative platform for consistent engagement between the two—domestically and with allies and partners—rendering enduring partnerships built on countering common gray zone economic threats. This mission area is fueled by assuring that businesses are properly incentivized and sufficiently equipped to identify and share information about economic threats for assistance from the US government.

Fusing the efforts of extant organizations, the EWOC will help orchestrate a cohort of invested parties from within the government and across industry to establish a distributed public-private partnership. It aims to transcend transaction-focused relationships through the sharing of information to benefit economic sectors while also preserving individual industry's competitive advantages over their competitors. In many cases, the EWOC will fuse products from multiple anonymized entities to inform operational decisions for action against adversarial economic activities. The partnerships will enable businesses to succeed in their endeavors, while also serving national interests in providing for common defense and security, to include economic security.



The trust established by collaborating to counter adversarial economic activities will strengthen relationships. Industry can be incentivized to participate through more transparent and flexible acquisitions practices, sharing of business intelligence, and broader access to government needs and resources.

The EWOC's role is to serve as an information clearinghouse between the government and industry. The EWOC should be the venue for sharing information on emerging economic threats so nefarious actors or suspicious activity may be identified, deterred, and countered with decisive action. Participants would gain market and industry insights unavailable elsewhere. The outcome will be a protected and strengthened industrial base critical to national interests while addressing the pace and character of security challenges of the global competitive environment.

Image credit: Alex Taliesen

Mission Area 3: Integration and Orchestration for Operations: Decide, Act, Elevate—*Employing a Scalable Arsenal of Economic Effects With Agility, Speed, and Effectiveness*

Mission Area 3 of the EWOC is the operational arm. It will develop and recommend actions from an arsenal of economic levers to act on the market intelligence and fused analysis from Mission Area 1, in concert with the partnerships established by Mission Area 2. Actions may be recommended to the executive branch, to be orchestrated by departments and agencies at the direction of the chief executive (the president), or National Security Council, or the legislative branch through proposed legislation. The EWOC itself might have limited operational authorities by virtue of association with interagency stakeholders. With integrated information, integrated deterrence is possible. Effects will be used to address threats with agility, speed, and impact, ultimately assuring competitive and decision advantage across the spectrum of conflict—from competition to crisis.

The US government currently employs various levers to identify, analyze, and address mission critical industry and supply chain vulnerabilities. Trade controls are typical capabilities employed in this domain. However, no agency currently takes an orchestrated operational approach to their employment, bringing disparate efforts together for decision and action. Identifying an arsenal of gray zone economic levers will enable an operational decision framework to be developed. The framework would include guidance on when to make decisions based on analysis of threats, when and how to act upon threats, and when to elevate actions to higher levels of authority for further actions. The arsenal would include a suite of effects to create specific desired outcomes in both defensive and offensive operations.

Defensive measures might be designed to protect companies from malign foreign influence. Defensive operations include changes to policy, regulations, and procedures that make it easier for industry partners to work with the US government, as opposed to working with entities beholden to

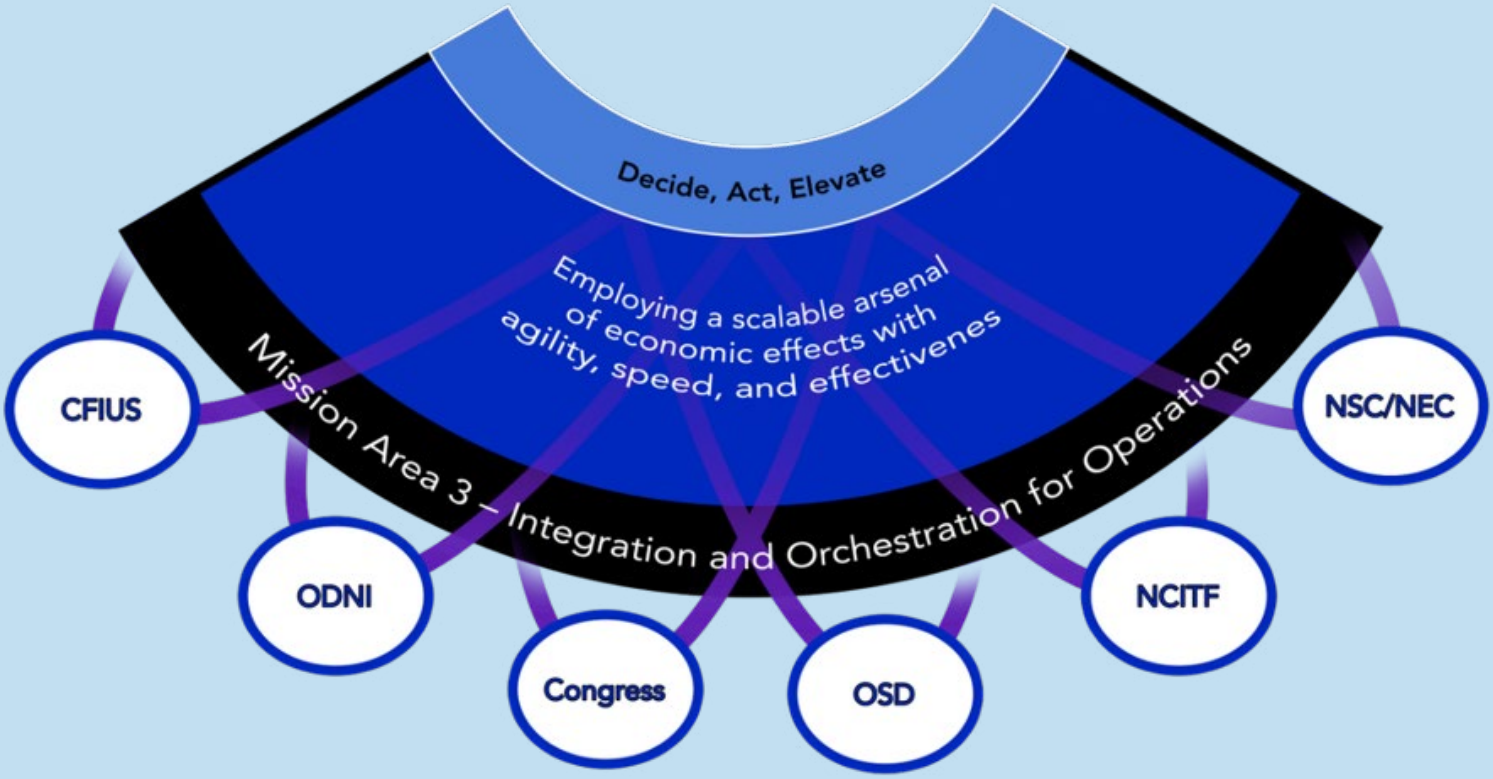


Image credit: Alex Taliesen

rival governments. They might involve reducing hurdles for companies to accept US government funding (as with the DoD's OSC). It could also be manifested in the creation of tax incentives for US companies to remain in the US or it could facilitate the availability of services that enable small companies to better compete.

Offensive operations generally involve asymmetric effects that negatively impact an adversary's global economic enterprise. For example, introducing capital investments in an alternative to rare earth elements (REEs) could disrupt China's dominant share of the world's processing capability, (which they exploit to threaten supply chains.

Summary

Development and employment of a scalable arsenal of economic effects that leverage market intelligence and analysis, as well as government-industry partnerships, will support the new reality of national security. Fusion of these elements provides a means for government leaders to decide to act on looming threats in a deliberately orchestrated, operational manner. The US needs an effective whole-of-government approach to countering adversarial economic activity across domains and instruments of national power.

National interests are vulnerable to unchecked adversarial economic activities. While there are efforts underway to identify and analyze those threats, such information is not prioritized, fused, and orchestrated across the entirety of the government for decision and action. When an action is taken it is usually at the tactical level, disconnected from a broader strategy and from industry partners. Here, we have outlined the concept of an Economic Warfare Operations Capability, an EWOC, to provide a unique but mutually beneficial opportunity for industry and government to strengthen their relationships and work together with partners to counter threats and serve the common good.

Development and fielding of an EWOC-type capability will help preserve the ability of the US government to carry out its core missions at the most basic level—by securing the industrial base and supply chains they depend upon—while providing the opportunity to build enduring partnerships and operational capability to assure competitive advantage on the global stage.

Acknowledgements

The author declares that the views expressed in this article reflects the author's personal thoughts and do not represent the position of the Department of the Air Force or the Department of Defense, with whom the author is also affiliated. He is grateful to the many contributors of the staff of the Potomac Institute for Policy studies, and thanks the editors of Potomac Institute press for their assistance in the preparation of this article.

Endnotes

1 "Fact Sheet: The Biden-Harris Administration's National Security Strategy." The White House. October 12, 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/12/fact-sheet-the-biden-harris-administrations-national-security-strategy/.

2 John Knefel. "The 'Gray Zone' Is the Future of War: Ongoing, Low-level, and Undeclared." *Inverse*. December 7, 2015. https://www.inverse.com/article/8838-the-gray zone-is-the-future-of-war-ongoing-low-level-and-undeclared.

3 Center for Strategic and International Studies. "Competing in the Gray Zone: Countering Competition in the Space between War and Peace." CSIS. 2023. https://www.csis.org/analysis/competing-gray-zone-countering-competition-space-between-war-and-peace.

4 "How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World." The White House. June 2018. https://trumpwhitehouse.archives.gov/briefings-statements/office-trade-manufacturing-policy-report-chinas-economic-aggression-threatens-technologies-intellectual-property-united-states-world/

5 Will Weissert. "DHS Report: China Hid Virus' Severity to Hoard Supplies." *AP News*. May 4, 2020. https://apnews.com/article/us-news-ap-top-news-international-news-global-trade-virus-outbreak-bf685dcf52125be54e030834ab7062a8.

6 "National Security Strategy of the United States of America." The White House. December 2017. https://history.defense.gov/Portals/70/Documents/nss/NSS2017.pdf?ver=CnFwURrw09pJ0q5EogFpwg%3d%3d

7 US Mission Japan. "Remarks by Secretary of Commerce Gina Raimondo on US Competitiveness and the China Challenge." US Embassy and Consulates in Japan. November 30, 2022. https://jp.usembassy.gov/commerce-secretary-raimondo-on-us-competitiveness-and-chinas-challenge/.

8 David Rader. "Dollars, Tanks, and Banks: Modernizing the Economic Warfighting Domain." *The Hamiltonian.* 2022. https://hamiltonian.alexanderhamiltonsociety.org/security-and-strategy/dollars-tanks-and-banks/.

9 Philip Kapusta. "The Gray Zone." *Special Warfare*. October 2015. https://www.proquest.com/trade-journals/gray-zone/docview/1750033789/se-2.

10 Ben Connable, Stephanie Young, Stephanie Pezard, Andrew Radin, Raphael S. Cohen, Katya Migacheva, and James Sladden, Russia's Hostile Measures: Combating Russian Gray Zone Aggression Against NATO in the Contact, Blunt, and Surge Layers of Competition. Santa Monica, CA: RAND Corporation, 2020. https://www.rand.org/pubs/research_reports/RR2539.html. Also available in print form.

11 Elisabeth Braw. "The Defender's Dilemma: Identifying and Deterring Gray Zone Aggression." American Enterprise Institute. 2022. https://www.aei.org/the-defenders-dilemma/.

12 Christopher Wray. "Countering Threats Posed by the Chinese Government Inside the US" Federal Bureau of Investigation. January 31, 2022. https://www.fbi.gov/news/speeches/countering-threats-posed-by-the-chinese-government-inside-the-us-wray-013122.

13 Per Covington, a firm providing legal and policy advice to those seeking to do business in China.

14 Kaja Ashwin, Sean Stein, and Ting Xiang. "China's 14th Five-Year Plan (2021-2025): Signposts for Doing Business in China." *Global Policy Watch*. April 6, 2021. https://www.globalpolicywatch.com/2021/04/chinas-14th-five-year-plan-2021-2025-signposts-for-doing-business-in-china/.
15 Remarks by U.S. Secretary of Commerce Gina Raimondo on the U.S. Competitiveness and the China Challenge, November 30, 2022, https://www.commerce.gov/news/speeches/2022/11/remarks-us-secretary-commerce-gina-raimondo-us-competitiveness-and-china.
16 Elisabeth Braw. "The Defender's Dilemma: Identifying and Deterring Gray Zone Aggression." American Enterprise Institute. 2022. https://www.aei.org/the-defenders-dilemma/.
17 The Defender's Dilemma: Identifying and Deterring Gray Zone Aggression.
18 The Defender's Dilemma: Identifying and Deterring Gray Zone Aggression.
19 Christopher Wray. "Countering Threats Posed by the Chinese Government Inside the US" Federal Bureau of Investigation. January 31, 2022. https://www.fbi.gov/news/speeches/countering-threats-posed-by-the-chinese-government-inside-the-us-wray-013122.
20 Lucie Béraud-Sudreau, David Brewster, Christopher Cairns, Roger Cliff, R. Evan Ellis, April Herlevi, Roy Kamphausen Mr., Roderick Lee, Paul Nantulya, Meia Nouwens, Rebecca Pincus, and Joel Wuthnow, Enabling a More Externally Focused and Operational PLA – 2020 PLA Conference Papers (Carlisle Barracks, PA: US Army War College Press, 2022), https://press.armywarcollege.edu/monographs/951.
21 "Executive Summary: China: The Risk to Corporate America." Federal Bureau of Investigation. 2022. https://www.fbi.gov/file-repository/china-exec-summary-risk-to-corporate-america-2019.pdf.
22 Sakshi Tiwari. "Chinese 'Stealth' Espionage! How Beijing-Backed Hackers 'Acquired' Sensitive US Tech Used In Its F-35 Fighter Jet?" February 3, 2022. https://eurasiantimes.com/chinese-stealth-espionage-us-tech-used-in-its-f-22-f-35-fighter/.
23 Ellen Ione. "China Steals US Designs for New Weapons, and It's Getting Away with 'The Greatest Intellectual Property Theft in Human History." *Business Insider*. September 24, 2019. https://www.businessinsider.com/esper-warning-china-intellectual-property-theft-greatest-in-history-2019-9#the-plas-j-20-looks-extremely-similar-to-the-us-air-forces-f-22-raptor-1.
24 Jeff Jones. "Confronting China's Efforts to Steal Defense Information." Harvard Kennedy School's Belfer Center for Science and International Affairs. May 2020. https://www.belfercenter.org/publication/confronting-chinas-efforts-steal-defense-information.
25 "Annual Report to Congress: Report Period: CY 2021." Committee on Foreign Investment in the United States. 2022. https://home.treasury.gov/system/files/206/CFIUS-Public-AnnualReporttoCongressCY2021.pdf.
26 Meredith Roaten. "AFA News: 'Integrated Deterrence' to Drive National Defense Strategy." *National Defense Magazine*. September 22, 2021. https://www.nationaldefensemagazine.org/articles/2021/9/22/integrated-deterrence-to-drive-national-defense-strategy.
27 "Fact Sheet: CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China." The White House. August 9, 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/.
28 Distinct from, but not unrelated to the independently proposed Office of Economic Warfare and Competition (OEWC).