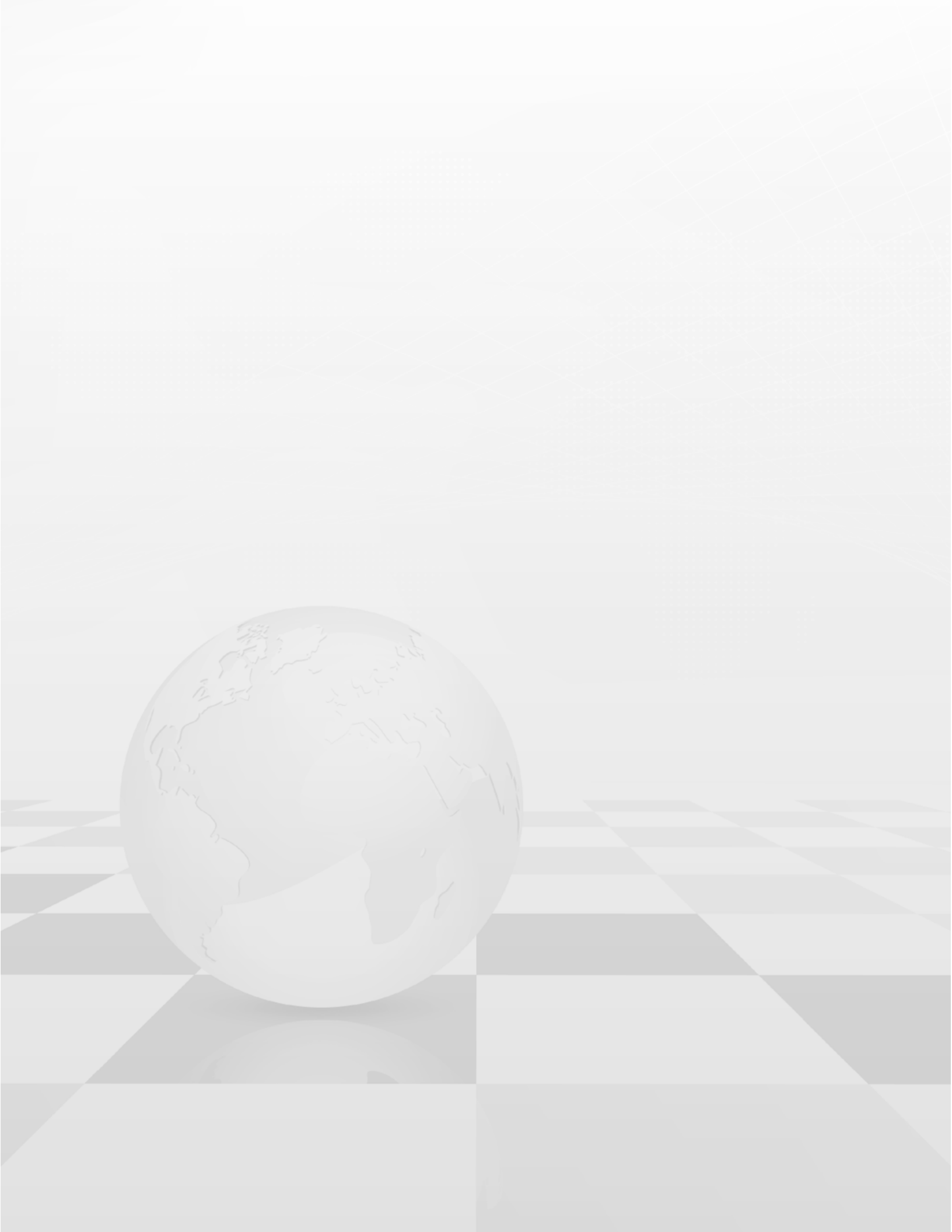
U.S. Department *of* Defense

Strategy for Operations in the Information Environment

July 2023



SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

July 5, 2023

At the Department of Defense, we are driving hard to further strengthen America's deterrence in the 21st-century world. With the National Defense Strategy (NDS) as our North Star, we are taking on the "pacing challenge" of the People's Republic of China, tackling the acute threat of today's highly aggressive Russia, and increasing our vigilance against the persistent threats of North Korea, Iran, and transnational terrorist networks.

As a key part of our ongoing work to implement the NDS, we are updating our strategy for operations in the information environment (OIE) and ensuring that we can deter challenges to U.S. vital national interests in any arena or domain. As this document lays out, the Department has formidable capabilities in the information environment that will help us increase our competitive advantages over our competitors and foes. And by integrating our work with that of our interagency partners, especially the Department of State, we will push hard together to better defend the United States.

As this strategy makes clear, our ability to gain and sustain information advantages at the times and places of our choosing are critical to successful operations in the information space. We must also protect information from external threats and ensure that policies are strictly followed on handling of classified and sensitive information within the Department. That means a renewed commitment to innovation, especially in the ways that the Department acquires and employs cutting edge capabilities. It also means bolstering our capacities, expanding access in allied and partner countries, and better integration of authorities that help us fulfill our objectives.

This strategy also describes the investments that the Department should make to improve its ability to shape the perceptions of our rivals and adversaries, which helps us influence their decisions and behaviors. I'm confident that this strategy matches our resources with innovative new concepts to achieve our security goals.

Make no mistake: America's competitors and enemies are moving quickly in the information environment, hoping to offset our enduring strategic advantages elsewhere. This strategy is an important step forward in swiftly and seamlessly synchronizing and integrating our own operations in the information environment so that we can continue to strengthen our deterrence—and position the United States to lead the way toward a 21st-century world that is more secure and free.

Lloyd J. Austin III
Secretary of Defense

TABLE OF CONTENTS

INTRODUCTION

The purpose of the 2023 Department of Defense (DoD) Strategy for Operations in the Information Environment (SOIE) is to improve the Department's ability to plan, resource, and apply informational power to enable integrated deterrence, campaigning, and building enduring advantages as described in the 2022 National Defense Strategy (NDS). The 2023 DoD SOIE provides a DoD-enterprise approach to ensure improved integration and oversight of information forces and information capabilities, operations, activities, programs, and technologies. This will allow the Department to refine its abilities to campaign in and through the information environment (IE), across all domains, in a global context, using the electromagnetic spectrum (EMS) to enable achievement of enduring strategic outcomes.

> **Information Environment (IE):** The aggregate of social, cultural, linguistic, psychological, technical, and physical factors that affect how humans and automated systems derive meaning from, act upon, and are impacted by information, including the individuals, organizations, and systems that collect, process, disseminate, or use information.
>
> *- JP 3-04, Information in Joint Operations, SEP 2022*

Effective application of informational power must be more broadly understood and deliberately incorporated into the full range of DoD strategies and operations, activities, and investments (OAIs) to support the advancement of national interests across the diplomatic, information, military, and economic instruments of national power in support of specific defense policy objectives. DoD must embrace a cultural shift wherein information is a foundational element of all military strategies and OAIs, and where the consistent integration of informational and physical power becomes the norm (see Figure 1). This change ensures DoD's capability to positively affect the drivers of human and automated system behaviors, shaping operational environments, and reinforcing the strength and credibility of the United States.

> **Informational Power:** The ability to use information to support achievement of objectives and gain an information advantage. The essence of informational power is the ability to exert one's will through the projection, exploitation, denial, and preservation of information in pursuit of objectives.
>
> *- JP 3-04, Information in Joint Operations, SEP 2022*

This 2023 DoD SOIE will be followed by a *DoD Operations in the Information Environment Implementation Plan (OIE I-Plan)* which will inform future policies and guidance, including Program Objective Memorandum submissions and campaign plans. Both the 2023 SOIE and the OIE I-Plan will inform IC efforts to increasingly produce tailored and prioritized intelligence relevant to OIE. The OIE I-Plan will have specific tasks and subtasks, and it will assign specific offices of primary responsibility (OPRs) to each. Timelines and a task tracking process will also be established to ensure accountability.

The 2023 DoD SOIE aligns with the 2022 NDS and *Joint Publication 3-04, Information in Joint Operations*. The 2023 DoD SOIE focus is on increasing and balancing the institutional and operational synergy among military information support operations, civil affairs (CA), public affairs (PA), joint electromagnetic spectrum operations (JEMSO), cyberspace operations, space operations, special technical operations (STO), defense deception activities (DDA), operations security (OPSEC), new and emerging information activities, and other disciplines and the informational aspects of physical power. The 2023 DoD SOIE and the forthcoming OIE I-Plan will address opportunities to strengthen contemporary programs, support the development of new ones, and simultaneously increase DoD OIE efficiency, effectiveness, and unity of effort, while also integrating the IC much more deeply into the planning, execution, and assessment of OIE.

> **Operations in the Information Environment (OIE):** Military actions involving the integrated employment of multiple information forces to affect drivers of behavior by informing audiences; influencing foreign relevant actors; attacking and exploiting relevant actor information, information networks, and information systems; and protecting friendly information, information networks, and information systems.
>
> * Any organization or capability may be tasked to conduct activities to support OIE, whether or not assigned to an OIE unit.
>
> *- JP 3-04, Information in Joint Operations, SEP 2022*

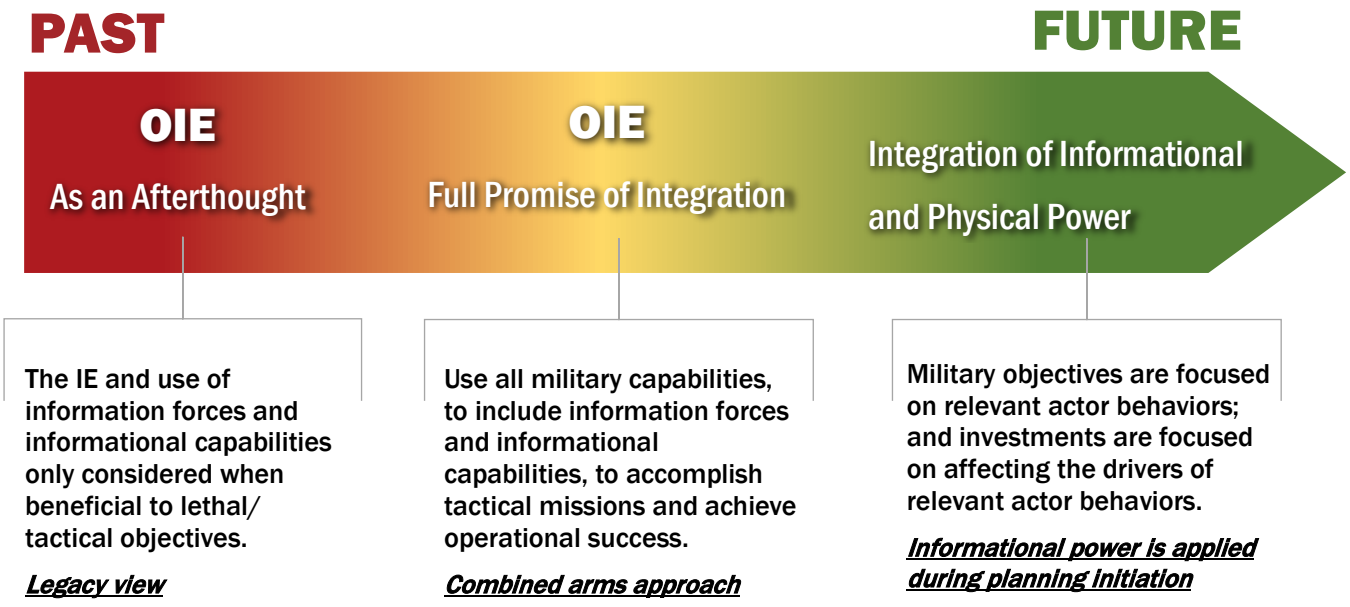


Figure 1. DoD must evolve from the legacy view to integrating informational and physical power

STRATEGIC ENVIRONMENT

For decades, the United States has benefited from diplomatic, economic, and military advantages. However, other governments, industries, institutions, and militaries continue to evolve, becoming more technologically advanced, innovative, and information driven. Foreign actors are harnessing this shift to strengthen their global position and challenge U.S. power and ideals. The 2022 NDS identifies the People's Republic of China (PRC) as the most comprehensive and serious challenge to United States national security and the pacing challenge for DoD. Russia is identified as an acute threat. Iran, North Korea, and violent extremist organizations (VEO) remain persistent threats. All continuously enhance and exercise their diplomatic, military, technological, and informational capabilities to raise the risks to U.S. and allied forces and weaken deterrence. Each is becoming more assertive, using their informational capabilities to deny information accessibility and propagate malign influence, misinformation, disinformation, propaganda, and deception activities to influence and disrupt world order. At the forefront of these efforts is the pursuit of emerging technologies, some of which pose challenging policy, regulatory, and legal issues. These tactics challenge the global security environment and may allow competitors and other relevant actors to contest DoD freedom of action in the EMS and IE. As the global security environment continues to evolve, DoD will need to confront these operational environments and unconventional tactics with all its assets and advantages, notably the inclusion of all dimensions of our diverse total force.

PEOPLE'S REPUBLIC OF CHINA

The PRC's goal is "to achieve the great rejuvenation of the Chinese nation by 2049."[1] In 2017, the PRC laid out a plan to become more engaged in world affairs, further its economic and social development, grow a more robust military, and focus more stringently on industrial and technological innovations. The Chinese Communist Party (CCP) prioritized its economic strategy by instigating more aggressive trade policies, bolstering investments, lending to developing nations' infrastructure projects, and promoting economic programs such as the Belt and Road Initiative. Beijing understands it must leverage information and apply asymmetric techniques to counter and dominate its adversaries.

According to the *2023 Annual Threat Assessment of the United States Intelligence Community* (ATA), "Beijing will continue expanding its global intelligence and covert influence posture to better support the CCP's political, economic, and security goals. Beijing's growing efforts to actively exploit perceived U.S. societal divisions using its online personas move it closer to Moscow's playbook for influence operations."[2]

[1] Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China*, Annual Report to Congress, Washington, DC: 3 NOV 2021, III, https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF

[2] Office of the Director of National Intelligence, *2023 Annual Threat Assessment of the U.S. Intelligence Community*, February 6, 2023, 10.

PRC ACTIVITIES IN THE IE

DISINFORMATION: In 2018, Typhoon Jebi stranded thousands of tourists, including holders of PRC and Taiwan passports, at Kansai International Airport in Osaka, Japan. Social media posts circulated criticizing the Osaka-stationed Taiwanese Director of the Taipei Economic and Cultural Representatives Office for not taking action to help stranded Taiwan citizens, while the PRC Consulate in Osaka reportedly dispatched buses to support rescue efforts. Due to the intense criticism online, the Director committed suicide. An investigation uncovered that Japanese airport authorities arranged evacuation buses for all stranded passengers and rejected a request by the Chinese Consulate to send their own buses. During evacuation procedures though, representatives from China Southern Airlines pulled mainland Chinese tourists into buses. PRC media promoted narratives praising the Chinese Consulate in Japan. Global press reports and social media posts circulated those narratives, publicizing that the Chinese Consulate negotiations saved tourists and that the Taiwanese had to rely on the Chinese to survive.

PROPAGANDA: The PRC claims historical ownership over an area in the South China Sea (SCS) within the PRC-asserted "nine-dash line," an area which overlaps with reefs, islands, and claimed exclusive economic zones of the Philippines, Indonesia, Vietnam, Brunei, Malaysia, and Taiwan. These areas harbor natural gas, crude oil, and significant fishing stocks. Since 2010, maps, globes, postcards, T-shirts, video games, and at least one blockbuster film (the animated movie "Abominable") depict or refer to the nine-dash line. The CCP uses the IE to disseminate propaganda promoting their SCS claims and the nine-dash line to attempt to "normalize" their claims to the area.

RUSSIA

According to the ATA, "Russia presents one of the most serious foreign influence threats to the United States, because it uses its intelligence services, proxies, and wide-ranging influence tools to try to divide Western alliances and increase its sway around the world, while attempting to undermine U.S. global standing, sow discord inside the United States, and influence U.S. voters and decision-making.

Russia's influence actors have adapted their efforts to increasingly hide their hand, laundering their preferred messaging through a vast ecosystem of Russian proxy websites, individuals, and organizations that appear to be independent news sources."[3]

RUSSIAN INFORMATION CONFRONTATION

MALIGN INFLUENCE: On February 24, 2022, the day Russia invaded Ukraine, a Berlin-based/Kremlin-run media outlet masquerading as a reputable news source posted a map on social media showing Europe, the Middle East, and Africa with a label that reads, "Airstrikes in the last 48 hours." The post warns, "Don't let the mainstream media's Eurocentrism dictate your moral support for victims of war. A human life is a human life. Condemn war everywhere." The map labeled Syria with Israeli airstrikes, omitting any Russian role in those bombings. It points out a United States airstrike in Somalia and Saudi airstrikes in Yemen with only a dozen noted by Russia in Ukraine. A video was also posted showing Western TV journalists saying how terrible it was that a "civilized country" like Ukraine was invaded rather than a "Middle Eastern country like Afghanistan [sic] or Iraq." The intent was to incite arguments about equality and alleged oppression by Western cultures and to deflect criticism away from the Kremlin.

[3] Ibid, 12.

IRAN AND NORTH KOREA

Iran and North Korea use tactics designed to create regional instability and threaten United States' interests, allies, and partners. Iran and North Korea have increased their informational capabilities, operations, and activities focusing heavily on the cyber domain, deception, and malign influence. Both Iran and North Korea employ civilian, military, and third-party resources in their attempts to manipulate the IE and often link their efforts to diplomatic and/or strategic actions.

"Iran will continue to threaten U.S. interests as it tries to erode U.S. influence in the Middle East, entrench its influence and project power in neighboring states, and minimize threats to the regime. Tehran will try to leverage diplomacy, its expanding nuclear program, its conventional, proxy, and partner forces, and its military sales and acquisitions to advance its goals. The Iranian regime sees itself as locked in an existential struggle with the United States and its regional allies, while it pursues its longstanding ambitions for regional leadership."[4]

"North Korean leader Kim Jong Un is continuing efforts to enhance North Korea's nuclear and conventional capabilities targeting the United States and its allies, which will enable periodic aggressive actions to try to reshape the regional security environment in his favor. Kim probably is attempting to secure North Korea's position in what he perceives to be an international environment conducive to his brutal authoritarian system, as demonstrated by North Korea's repeated public support for Beijing and Moscow's foreign policy priorities."[5]

IRAN AND NORTH KOREA IE ACTIVITIES

IRAN DISINFORMATION: After a January 2, 2020, United States drone attack killed Iranian military general Qasem Soleimani, Iran retaliated by shooting ballistic missiles at bases in Iraq that housed American military troops. Social media posts used images from unrelated events to perpetuate the narrative that the missile strikes were more successful than reported, along with statements to scare American audiences, warning that America "was on the precipice of another horrible war in the Middle East."

NORTH KOREA DECEPTION ACTIVITES: In 2012, North Korea gave indications of a missile launch, but then announced it was experiencing technical issues. Open-source reports indicated parts of the rocket were taken from the launch pad, reinforcing the understanding that the launch was canceled. The missile was then indeed launched on its originally scheduled day and time, deceiving intelligence communities, and thereby limiting intelligence collection opportunities.

TRENDS IN DIGITAL AUTHORITARIANISM AND MALIGN INFLUENCE

[4] Ibid, 17.
[5] Ibid, 20.

According to the ATA, "Globally, foreign states' malicious use of digital information and communication technologies will become more pervasive, automated, targeted, and complex during the next few years, further threatening to distort publicly available information and probably will outpace efforts to protect digital freedoms. The exploitation of U.S. citizens' sensitive data and illegitimate use of technology, including commercial spyware and surveillance technology, probably will continue to threaten U.S. interests.

Authoritarian governments usually are the principal offenders of digital repression, but some democratic states have engaged in similar approaches, contributing to democratic backsliding and erosion."[6]

TRANSNATIONAL ISSUES

While climate change and the COVID-19 pandemic highlight the challenges that a wide range of transnational issues pose to U.S. national security, other priority issues, such as narcotics trafficking and terrorism, have a direct and immediate impact on U.S. interests. Vulnerabilities in our supply chain, Internet governance, and global economic shocks seem to be building, or posing chronic, indirect challenges to U.S. interests. These issues also vary in the scope of the consequences they pose, having broad, global impact or causing local, even individual effects.

According to the ATA, "Transnational threats interact in a complex system along with more traditional threats such as strategic competition, often reinforcing each other and creating compounding and cascading risks to U.S. national security. Increasing interconnections among countries—ranging from supply chains to social media—also have created new opportunities for transnational interference and conflict. The rapid development of technologies, the spread of digital repression on the Internet, the threats posed by transnational organized crime and terrorism, and the societal effects of international migration stand out for the clear and direct threats they will pose to U.S. interests during the coming years."[7]

[6] Kali Robinson, "How Israel's Pegasus Spyware Stoked the Surveillance Debate," *Council on Foreign Relations,* March 8, 2022, https://www.cfr.org/in-brief/how-israels-pegasus-spyware-stoked-surveillance-debate.
[7] 2023 Annual Threat Assessment, 26.

KEY OIE PRINCIPLES

OIE must be aligned within a spectrum of other government informational capabilities, operations, and activities that span public diplomacy and public affairs to intelligence. The key planning considerations of the 2023 DoD SOIE include:

- The Department of State is lead for public diplomacy. DoD collaborates with interagency partners and offers planning and synchronization support and other resources to enable the effective, whole-of-government integration of informational power.
- Joint force commanders' requirements for organic capability and capacity to conduct OIE as part of campaigning and integrated deterrence require informed resource prioritization or offsets.
- All military operations and activities affect the information environment. The integration of informational power into strategy, strategic art, operational art, operational design, and operational planning, from the onset of planning initiation, enables effective OIE and information advantage.
- Maintaining an updated joint lexicon for terms related to OIE is critical.
- DoD integration of PA is a key component of OIE across the competition continuum.
- Military Departments/Services continue to provide forces and capabilities for integration into the joint force including for the information joint function. Future joint integration models for effective, efficient, and agile information capability and capacity are continually maturing to match DoD needs.
- Each Service has defined and organized their information forces and capabilities differently. Therefore, OIE units may be comprised of varying information forces and associated capabilities and competencies that include but are not limited to psychological operations (PSYOP) forces, Civil Affairs (CA), Public Affairs (PA), Joint Electromagnetic Spectrum Operations (JEMSO) elements, cyberspace forces, space operations elements, with information planners skilled in Special Technical Operations (STO), DoD deception activities (DDA), and Operational Security (OPSEC).
- Maintaining up-to-date architectures and standards in order to assess the efficacy of DoD activities in this space and to enable interoperability, efficiency, information sharing, and cybersecurity[8].

[8] The role of cybersecurity is expounded in the National Cybersecurity Strategy (March 2023) and the 2023 DoD Cyber Strategy.

STRATEGIC APPROACH

The 2023 DoD SOIE lays out how the Department will comprehensively consider the informational, physical, and human aspects of the environment. A coherent strategy requires a clear understanding of the drivers that shape relevant actors' perceptions and behaviors. The IC must identify and better understand individuals, groups, and populations critical and influential to partners, adversaries, and/or relevant foreign actors. The IC must apply an analysis and assessment methodology of the informational, physical, and human aspects of the environment to gain a better grasp on the motivations that drive behaviors. Once DoD planning, execution, and assessment incorporate the factors that drive target audience behavior, informational power can be effectively applied. DoD must address these challenges and limitations identified in multiple United States Government Accountability Office (GAO) reports on the IE and OIE[9] and other supporting documents of the *2023 Information Operations Posture Review (IOPR)*.

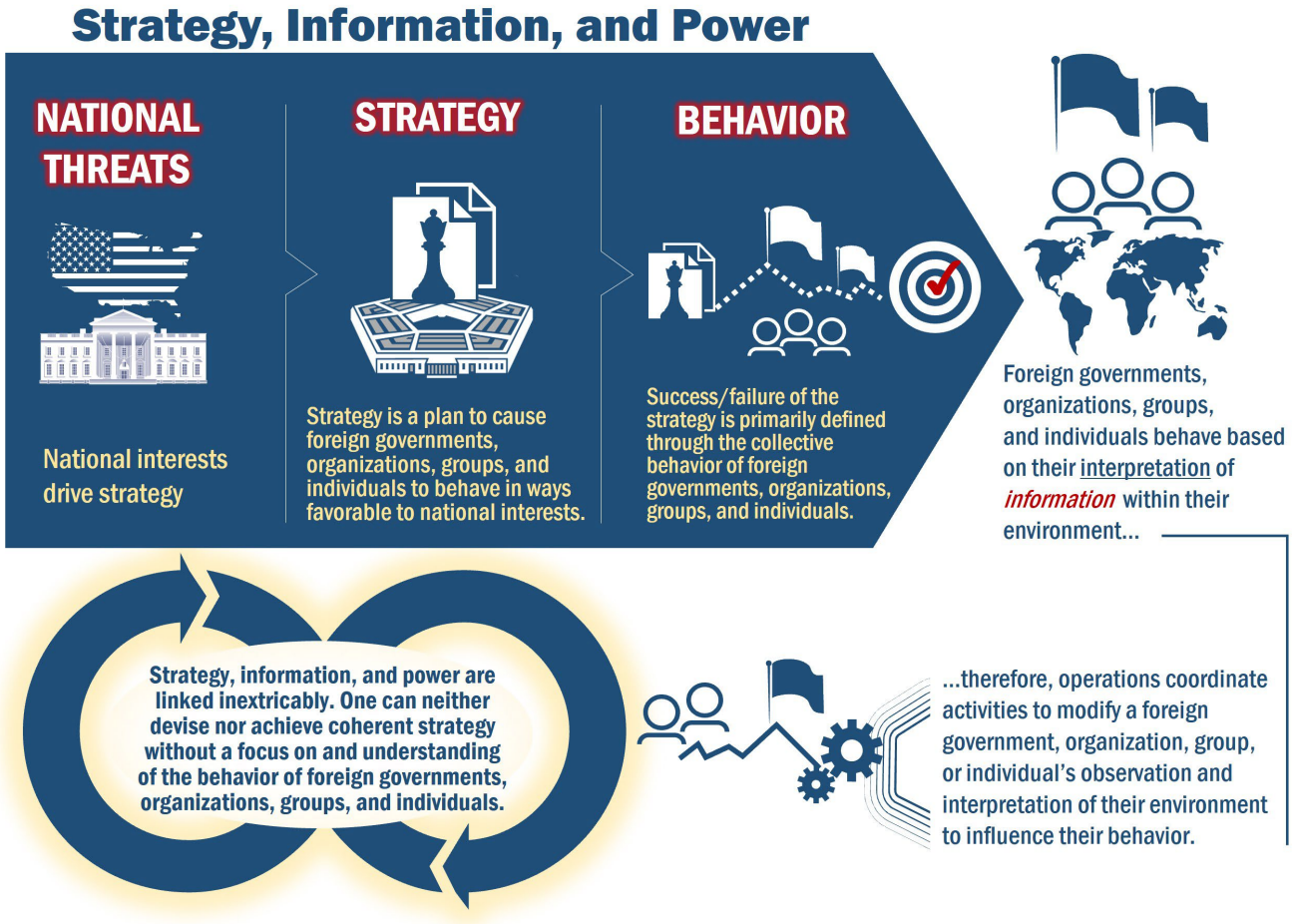


Figure 2. Strategy, Information, and Power are Inextricably Linked

[9] U.S. Government Accountability Office, *Information Environment: Opportunities and Threats to DoD's National Security Mission,* Washington DC: GAO, September 21, 2022, https://www.gao.gov/products/gao-22-104714.

SCOPE

The objective of the 2023 DoD SOIE is to guide the Department to effectively plan, resource, and apply informational power to enable integrated deterrence, promote campaigning, build enduring advantages, compete against strategic adversaries, and support allies and partners, as described in the 2022 National Defense Strategy. The 2023 DoD SOIE focuses on OIE policy, planning, resource management, operational considerations, personnel, technology development, and risk management to address identified gaps and ensure DoD possesses the appropriate capabilities and capacities necessary to deliver globally integrated and effective informational power and physical power to achieve DoD objectives.

Title 10 United States Code §397 assigns responsibilities to DoD Principal Information Operations Advisor (PIOA) related to the areas described in the previous paragraph. In October 2020, the Secretary of Defense designated the Under Secretary of Defense for Policy (USD(P)) the PIOA. To support the assigned responsibilities, the USD(P) formed the Office of Information Operations Policy (OIOP) and established a PIOA cross-functional team (CFT) with Military Service representatives. The PIOA CFT studied the 2022 NDS, the *Joint Publication 3-04, Information in Joint Operations,* and collected inputs from multiple information forces' strategies and foundational documents. This was done to align the 2023 DoD SOIE with the 2022 NDS and focus on building DoD capabilities and capacities to execute OIE in support of integrated deterrence, campaigning, and building enduring advantages – the three approaches needed to advance United States national defense priorities and defend/promote United States national interests[10]. Integrated deterrence requires working seamlessly across all instruments of national power to dissuade competitors of the net benefits of aggression over restraint. DoD's ability to use information, including for signaling, is critical to this approach. Integrating informational activities with sequenced operations allows DoD to leverage campaigning to advance its priorities over time. To bolster the foundations of the United States' ability to deter and campaign, DoD will build enduring advantages modernizing the joint force and defense enterprise with new capabilities to conduct OIE. Shared domain awareness, promoting international norms, and building allies and partners are key to establishing and maintaining those advantages.

CURRENT ACTIONS

As directed by the Secretary of Defense, the Department has established the Strategic Information Oversight Board (SIOB), which directed the SIOB to "serve as the senior forum for strategic information operations (IO), information-related capabilities (IRCs), and concepts that require coordination at the highest levels of DoD." The SIOB tri-chairs, the USD(P), the Under Secretary for Intelligence and Security (USD(I&S)), and the Vice Chairman of the Joint Chiefs of Staff, may resolve issues that fall within their purview, or propose topics for discussion and decision to the Secretary of Defense. Other standing members include: the Secretaries of the Military Departments; the Under Secretaries of Defense for Research & Engineering (USD(R&E)), Acquisition & Sustainment, and Comptroller; Chiefs of the Military Services, members of the Joint Staff (JS), Director of Cost Assessment and Program Evaluation, Assistant Secretary of Defense (ASD) for Special Operations/Low-Intensity Conflict, Assistant to the Secretary of Defense for Public Affairs (ATSD(PA)), and Commanders of the Combatant Commands.

[10] Department of Defense, *National Defense Strategy of the United States of America,* Washington, DC: Department of Defense, 2022, https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF

The Department also reinvigorated multiple symposia, featuring collaboration among information planners, forces, developers, and leaders across government, industry, academia, and allies. Those events will be increasingly complementary and outputs from each will inform this and future strategies for OIE.

These OIE oversight and collaboration efforts, along with the 2022 NDS, IOPR, *Joint Publication 3-04, Information in Joint Operations*, and GAO reports resulted in the identification of four lines of effort (LOEs) to enable DoD to fully integrate and modernize OIE across DoD: **1. People & Organizations, 2. Programs, 3. Policies & Governance, 4. Partnerships.** These four LOEs support DoD's focus on integrated deterrence, campaigning, and building enduring advantages. They are broad in scope and described in more detail later in this strategy. Each LOE is followed by a series of high-level implementation tasks. These tasks will be subdivided into sub-tasks and lower-level activities and investments in the OIE I-Plan.

Each of these LOEs require collaboration, integration, and synchronization of OIE throughout DoD and in coordination with other United States Government departments and agencies, international and nongovernmental organizations (NGOs), government agencies of allied and partner nations, State, Local, Tribal, and Territorial government departments, academia, and elements of the private sector. The OIOP, Office of the USD(I&S), USD(R&E), and the JS already collaborate on a regular basis to drive investments. Each of these offices participate in different OIE focused fora. For example, the Defense Intelligence Support to Operations in the Information Environment Working Group is shaping how the IC provides support to OIE. OUSD(R&E) stakeholder meetings provide an opportunity for input into the development of the OIE technological roadmap. The Joint Information Force Development and Design Working Group supports OIE joint force capabilities and requirements development. The OIOP maintains a strong partnership with the Joint Information Operations Warfare Center, which provides a dedicated and enduring capability to facilitate coordinated and sustained joint force efforts in execution of this 2023 DoD SOIE and the development of the follow-on OIE I-Plan.

FUTURE ACTIONS

In the near term, the 2023 DoD SOIE and associated implementation plan will detail the objectives, tasks, and sub-tasks that will be assigned to specific OPRs. The OIOP, OUSD(I&S), OUSD(R&E), JS, in coordination with the Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, the Office of the Chief Information Officer, the Office of the Chief Digital and Artificial Intelligence Officer, OUSD for Personnel & Readiness, OUSD Comptroller, and the Office of the Director of Cost Assessment and Program Evaluation will sustain and increase collaboration with OIE I-Plan designated OPRs to support the execution of this 2023 DoD SOIE.

Over the long term the OIE I-Plan will focus on the institutionalization of the information joint function and synchronization of OIE. Leaders across the DoD will build strength and capability to compete against adversary information warfare by improving the Department's ability to integrate, validate, employ, and assess OIE operations, activities, and investments. For example, all of DoD will be educated on foreign malign influence, consistent with section 549N of the National Defense Authorization Act for fiscal year 2022, and on the significance of integrating information into planning, execution, and assessment. Commanders across all Military Services will increase training to promote awareness of all personnel on how to integrate OIE across the joint functions, how to measure and assess outcomes, and how to ensure tactical activities are synchronized with operational and strategic OIE objectives. Research and

development efforts will also evolve and will identify, develop, adapt, and test new technologies and preserve the effectiveness of current ones to better enable information advantage.

The tasks for this Strategy are listed below after each LOE. The specific sub-tasks and OPRs will be described in the forthcoming OIE I-Plan.

LOE 1. PEOPLE & ORGANIZATIONS

As the global security environment continues to evolve, DoD will need to confront evolving challenges with the assets and advantages that come from the inclusion of all capabilities across DoD's diverse total force. The Joint Force consists of many different types of information forces operating across the air, land, sea, space, and cyberspace domains, which will provide subject matter expertise and capabilities to DoD, the joint force, and joint force commanders. Information forces possess unique skills that require an emphasis by DoD regarding recruitment, talent management, and retention of a highly diverse and inclusive workforce. It is DoD's responsibility to provide all its members, including those assigned to the Services, joint organizations, and combat support agencies, with the training and resources needed to be resilient to foreign malign influence and to improve their understanding of the informational aspects of military activities. DoD implements force development and design initiatives in education and training and organizes DoD to enable effective OIE.

DoD requires a force trained and educated in the information joint function. This education and training will require commanders, staffs, and personnel carrying out information activities to have a full understanding of how to integrate the information joint function at the onset of planning initiation and throughout execution and assessment. Additionally, DoD must educate the force on how information can be used to benefit joint force operations and how competitors can use this same information for malign purposes to undermine the United States.

DoD needs the ability to surge capability and capacity to quickly respond and maneuver in and through the IE. As such, DoD must build a process to rapidly deploy teams of information forces, including the reserve force.

As we have done across DoD with other functional professional communities, DoD will fully develop an information workforce composed of uniformed and DoD Civilian members and execute the full range of the human resource and talent management lifecycle for this workforce, including active recruiting and accession, training/education, career path development including equitable competitive opportunity for command and GO/FO/SES leadership development and assignment, and broadening/retention.

Task A – Educate and Train DoD to Lead and Conduct OIE.

Task B – Cultivate, Retain, and Track Information Forces and Planners to Enable Effective OIE.

Task C – Designate Information Force Providers and Joint Information Force Trainers as required by Section 1631(g) of the National Defense Authorization Act for Fiscal Year 2022 (Public Law 116-92; 10 U.S.C. 397 note)**.**

LOE 2. PROGRAMS

Today's strategic environment requires DoD to improve the tools and infrastructure that commanders, their staffs, planners, and forces use to characterize and operate in the IE and assess the effectiveness of those operations. DoD will need to invest in, secure, and integrate the research, development, maintenance, and sustainment of information capabilities and capacities to successfully conduct OIE and achieve and sustain information advantage.

DoD will habitually study and account for the effects of the IE on the Department's activities and will foundationally and deliberately integrate the information function in all activities via existing DoD and Joint processes. Commanders and leaders at all levels will address information in strategy, campaign design, plans, targeting, and assessments. DoD will need to invest in systems that can characterize the IE, sharing large amounts of data that is easily discoverable and can be ingested into different programs for analysis. The system requirements will need to fit into joint force training and support interoperability with the entire joint force, partners, and allies.

Task A – Improve Development of OIE Capabilities.

Task B – Evolve to an Agile, Fully Integrated OIE Infrastructure.

Task C – Integrate OIE into Planning, Operations, and Assessments.

Task D – Provide Intelligence Support to Enable OIE.

LOE 3. POLICIES & GOVERNANCE

Well-articulated and timely policy and guidance are necessary to execute deliberate OIE. This requires not only review and maintenance of policy, concepts, doctrine, legal frameworks, and authorities, but also assessments to evaluate and monitor OIE and understand the return on investment in campaigning. This includes a rigorous risk management process to manage the risk of potential exposure of United States persons to information intended exclusively for foreign audiences. Oversight boards and accountability processes will ensure OIE remain effective, agile, and adaptable to rapid changes in the IE.

Senior leaders and standardized accountability processes will ensure OIE remain strategically and legally sound, ethically acceptable, demonstrate appropriate return on investment, and are agile and adaptable to rapid changes in the IE. DoD and the joint force must provide a framework to support the integration of policy and doctrine development, assessing and managing risk, and evaluating authorities to support operations.

DoD will continue to mature the structure surrounding the SIOB to identify optimal organization, to maximize information flow across components, and to strengthen ability of leadership to make more informed decisions regarding DoD's strategic approach and investments. The SIOB will provide oversight and can support the PIOA's efforts to improve specific capabilities and processes, including processes for coordinating and monitoring strategic OIE; development and adaptation of Information concepts, policies, priorities, and guidance; continuous assessment and evolution of processes, doctrine, the posture of Information forces and the overall effectiveness of Information as a joint function.

Task A – Monitor and Improve DoD's Ability to Conduct OIE.

Task B – Develop and Adapt OIE Related Concepts, Policies, Priorities, and Guidance.

Task C – Continuously Assess and Update the Current Processes, Doctrine, Posture of Information Forces, and their Effectiveness in Supporting OIE.

Task D – Develop, Update, and Deconflict Authorities and Permissions to Enable Effective OIE.

Task E – Ensure OIE are Synchronized and Managed to Protect United States Persons and Interests.

LOE 4. PARTNERSHIPS

The IE knows few boundaries, and the Department's approach to OIE must reflect this reality. The competition for information advantage is an inherently global, joint, combined, interagency, and whole-of-society one. The United States military's capability and capacity to operate globally in the IE will be contingent on its ability to establish and maintain situational and enduring partnerships. Integration with allies and partners provides a critical warfighting capability. Our allies and partners around the world have incredible capability, understanding of regional and local language and culture, and can better communicate within their respective regions and with their partners than can DoD. DoD will eliminate barriers to cooperation and combined action with our allies and partners.

To truly make OIE an effective national capability it must be applied by DoD in a deliberate and unified manner; remain aligned with the interagency; and consider the viewpoints and activities of academia to include university-affiliated research centers (UARCs), commercial entities, industry, federally funded research and development centers (FFRDCs); NGOs; and State, Local, Tribal, and Territorial governments and agencies. The United States must embrace a whole-of-government approach to the development and employment of Information as an instrument of national power. In addition to its statutory and traditional military role and functions, DoD can provide planning support to help coordinate, synchronize, reinforce, and deconflict interagency information activities, as well as provide thematic reinforcement and mutual support across agencies.

Integration with allies and partners will be critical to effective warfighting capabilities. DoD partners around the world have incredible capability, understanding of local language and culture, and can better communicate with their respective regions. To that end, with an emphasis on people, processes and capabilities, DoD must facilitate the integration of our partners into our military and our military into theirs. This will be imperative to truly understand the diverse information environment that meld together across the areas of responsibilities around the globe.

Task A – Establish and Maintain Partnerships within DoD and Among United States Government Interagency Partners, Appropriate Non-United States Government Entities, and International Partners to Enable More Effective Whole-of-Government OIE.

Task B – Foster and Enhance Partnership Capabilities and Capacities.

CONCLUSION

DoD operates in a world evolving both technologically and socially at an ever-accelerating pace. Adversaries and others are effectively leveraging the IE to advance their objectives. This 2023 DoD SOIE is part of several efforts to enable integrated deterrence, campaigning, and building enduring advantages as described in the 2022 NDS. The LOEs, "People & Organizations," "Programs," "Policies & Governance," and "Partnerships," begin to address the OIE challenges of gaining and sustaining information advantages at times and places of our choosing. This strategy informs and guides the investments that the Department should make to improve its abilities to influence our rivals and adversaries' decisions and behaviors, while protecting DoD personnel and institutions against foreign malign influence. This is an enduring effort and significant work remains.

GLOSSARY

This glossary serves to clarify the 2023 DoD SOIE content. The 2023 DoD SOIE uses terms listed below with the intent of communicating the associated descriptions. Most are derived from *Joint Publication 3-04, Information in Joint Operations* (JP 3-04). While some other terms in the SOIE have not been formally defined in the DoD Dictionary of Military and Associated Terms, they are not included in this glossary as they are already in common use.

Foreign Malign Influence: Any hostile effort undertaken by, at the direction of, or on behalf of or with the substantial support of, the government of a covered foreign country with the objective of influencing, through overt or covert means the political, military, economic, or other policies or activities of United States or State or local governments, including any election within the United States; or the public opinion within the United States. (See section 359 of 50 U.S.C., "Foreign Malign Influence Response Center").

Human Aspects: The interactions among and between people and the environment that shape human behavior and decision making. Those interactions are based upon the linguistic, social, cultural, psychological, and physical elements.

Information Advantage: The operational advantage gained through the joint force's use of information for decision-making and its ability to leverage information to create effects on the IE.

Information Environment (IE): The aggregate of social, cultural, linguistic, psychological, technical, and physical factors that affect how humans and automated systems derive meaning from, act upon, and are impacted by information, including the individuals, organizations, and systems that collect, process, disseminate, or use information (Joint Chiefs of Staff, Joint Publication 3-04, *Information in Joint Operations*).

Information Forces: Active Component and Reserve Component forces of the Services specifically organized, trained, and equipped to create effects in the IE. These forces provide expertise and specialized capabilities that leverage information and can be aggregated as components of an OIE unit to conduct OIE. Information forces are available to the joint force through the request for forces (RFF) process. OIE units may be composed of the following types of information forces: PSYOP, CA, PA, Electromagnetic Spectrum Operations Elements, Cyberspace Forces, and Space Operations Elements (*Joint Publication 3-04*). Many of these information forces are also trained on how to plan and execute OPSEC and military deception.

Information Joint Function: The intellectual organization of the tasks required to use information during all operations—understand how information impacts the operational environment, support human and automated decision making, and leverage information. The information joint function encompasses the management and application of information to change or maintain perceptions, attitudes, and other drivers of behavior and to support human and automated decision-making.

Information Planners: Trained information force professionals that have subject matter expertise with specialized capabilities, experience working with and in OIE units, and an understanding of the inherent informational aspects of capabilities and activities of other units. Information planners collaborate with all members of the joint force staff to develop and plan activities in a manner that most effectively leverages the informational aspects of joint force operations, as well as planning OIE to support achieving the Joint Force Commander's objectives.

Informational Aspects: Describe how individuals, information systems, and groups communicate and exchange information. This description includes the collected, transmitted, processed, stored, and displayed informational content. The formal and informal communication infrastructure and networks, kinship and descent relationships, licit and illicit commercial relationships, and social affiliations and contacts that

collectively create, process, manipulate, transmit, and share information in an operational area and among relevant actors. These also include the inherent informational aspects of activities (i.e., the "body language" of activities), the features and details, which include, but are not limited to, the size of a force and its types of capabilities; the communications about an activity (e.g. verbal and nonverbal communication, images, credible voice); and the duration, location, and timing of the activity.

Informational Capabilities, Operations, and Activities: Describe capabilities, operations, and activities that use and leverage information to affect behavior and impact the operational environment.

Informational Power: The ability to use and leverage information to support achievement of objectives and gain an informational advantage. The essence of informational power is the ability to exert one's will through the projection, exploitation, denial, and preservation of information in pursuit of objectives**.**

Operational Art: The cognitive approach used by commanders and staffs— supported by their skill, knowledge, experience, creativity, and judgment—to develop strategies, campaigns, and operations to organize and employ military forces by integrating ends, ways, means, and evaluating risks. (Joint Chiefs of Staff, *Joint Planning*, Joint Publication 5-0).

Operational Design: The conception and construction of the framework that underpins a campaign or operation and its subsequent execution. The framework is built upon an iterative process that creates a shared understanding of the OE; identifies and frames problems within that OE; and develops approaches, through the application of operational art, to resolving those problems, consistent with strategic guidance and/or policy.

Operations in the Information Environment (OIE): Military actions involving the integrated employment of multiple information forces to affect drivers of behavior.

Operations in the Information Environment Unit: Those service provided organizations that are trained and equipped to conduct OIE. An OIE unit consists of a headquarters organization with command and control of assigned and attached information forces. The two core activities of OIE units are to conduct OIE and to facilitate the Joint Force Commander's integration of information into joint force operations.

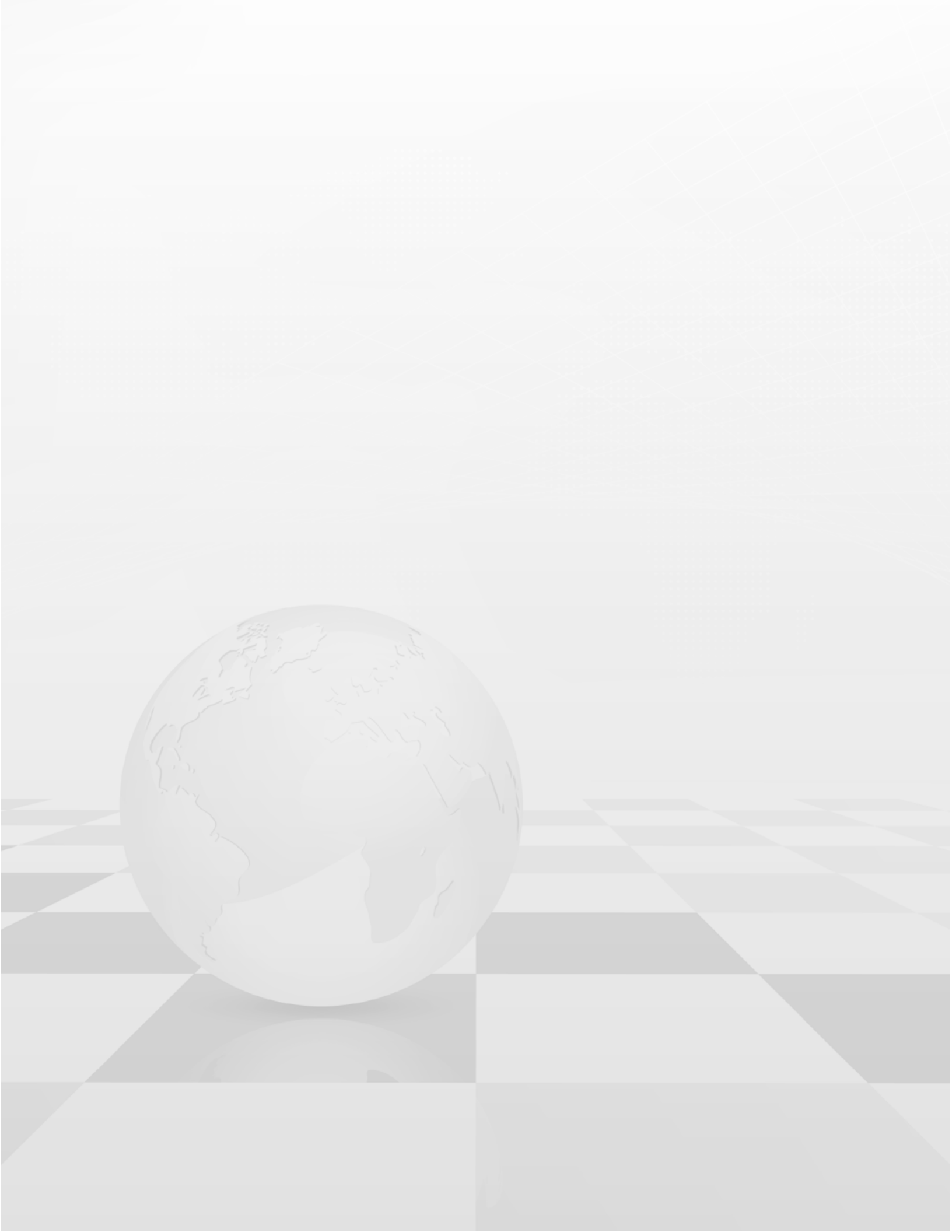
Operational Planning: Translates the commander's concepts into executable activities, operations, and campaigns, within resource and policy limitations to achieve objectives. (Joint Chiefs of Staff, *Joint Planning*, Joint Publication 5-0).

Physical Aspects: Describe the material characteristics of a joint operating environment, natural and manufactured, that inhibit or enhance communication between people and between information systems. This includes physical features such as terrain and lines of communication that impact the transmission and processing of information, territorial boundaries associated with governments' obligations to provide security for their people, the medium used in communication (material on which something is printed or the radio frequency and bandwidth used during broadcast), and information infrastructure. Physical aspects are critical elements of group identity and frame how tribes and communities form.

Propaganda: "Ideas, facts, or allegations spread deliberately to further one's cause or to damage an opposing cause." (Merriam-Webster Dictionary).

Relevant Actors: Relevant actors include individuals, groups, populations, or automated systems whose capabilities or behaviors have the potential to affect the success of a particular campaign, operation, or tactical action (Joint Chiefs of Staff, Joint Publication 3-04, *Information in Joint Operations*).

Strategic Art: The formulation, coordination, and application of ends, ways, and means to implement policy and promote national interests. (Joint Chiefs of Staff, *Joint Planning*, Joint Publication 5-0).




DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA