IBM Center for The Business of Government

2023

Managing the New Era of Deterrence and Warfare:

Visualizing the Information Domain

Brian Babcock-Lumish and
Leendert van Bochoven , Stephen Gordon, Tim Hofmockel,
Frederick Kagan, Nils Peterson, and Noah Ringler

ISW INSTITUTE FOR THE STUDY OF WAR

IBM Center for The Business of Government

Managing the New Era of Deterrence and Warfare:

Visualizing the Information Domain

Brian Babcock-Lumish and
Leendert van Bochoven, Stephen Gordon, Tim Hofmockel,
Frederick Kagan, Nils Peterson, and Noah Ringler

MAY 2023

ISW INSTITUTE FOR THE STUDY OF WAR

IBM Center for The Business of Government

Table of Contents

Increasingly, warfare is also engaged through means involving information intended to shape the perspective of adversaries.

Foreword

On behalf of the IBM Center for The Business of Government and the Institute for the Study of War, we are pleased to present this new report, *Managing the New Era of Deterrence and Warfare: Visualizing the Information Domain*.

This report is the capstone of a series that our two organizations led over the past year, which convened leaders from allied, partnered, and U.S. militaries, governments, academia, and industry to envision and shape future strategic advantages through visualizing information operations. The three events gathered experts and practitioners to discuss the topic from a theoretical perspective, as it pertains to the case of Russia, and finally of China.

U.S. and allied leaders increasingly need new solutions for achieving and maintaining a common operating picture that integrates information operations with air, land, sea, space, and cyber domains. This report addresses the unique challenges for understanding and visualizing the information domain and its importance in managing modern defense and intelligence activity. The report also puts forward criteria for how such visualizations could be developed in the future to support managing information activities at the operational, analytical, and decision-maker levels.

We hope that this report helps to increase understanding and collaboration around developing information visualizations that can help the U.S., allies, and partners address ever-accelerating challenges.

Daniel J. Chenok

Dr. Kimberly Kagan

Daniel J. Chenok
Executive Director
IBM Center for The Business of Government
chenokd@us.ibm.com

Dr. Kimberly Kagan
Founder & President,
Institute for the Study of War
kimberlykagan@understandingwar.org

Executive Summary

U.S. military and NATO joint doctrine recognizes five domains of warfare: air, sea, land, space, and cyber.[1] Increasingly, warfare is also engaged through means involving information intended to shape the perspective of adversaries—a domain within which nations maneuver to accomplish strategic and tactical objectives. But there are no well-understood norms or practices to visualize information operations in a way that support command decisions, analytical frameworks, or field operations. Visualizing the information space to inform decisions is the chief challenge that practitioners face in adopting this new domain of warfare. This paper addresses issues involved in developing effective visualizations to manage information operations as another element of warfare.

Indeed, the information space is to policy as terrain is to war. Information can shape, channel, cause, and end military operations. Anything that changes the information space affects military policy, and anything that affects policy affects war. The character of the information space is thus as central to the character of war as technology, social structures, economics, or any other traditional factor.

In a recent series of roundtable discussions, global leaders from the military, government, academia, and technology sectors converged on three core challenges of understanding and visualizing the information domain:

- First, the information space is a chaotic system, in which slight variations in conditions can dramatically impact how information traverses space and time.
- Second, any visualization of this mélange of data points—data from the entire information space that includes mass and social media as well as cultural and socioeconomic networks—must be useful to decision makers at multiple echelons and overlayed onto visualizations of the land, air, sea, air, and cyber domains.
- Third, the vast information domain must remain bounded to build effective visualizations.

Given the recent rise in the scale and scope around information activity as a tool of engagement, information could be considered as a sixth domain of warfare alongside air, sea, land, space, and cyber. The information space exerts a powerful influence on policy and, subsequently, on war. The information domain can be viewed as the sum of the wills, decision capabilities, and subsequent choices to act of each actor, where "will" is a composite of convictions, perceptions, and influences that drive toward action. The information space reflects neither a novel phenomenon nor one only recently relevant to warfare; however, its importance to the modern character of war has grown significantly, especially given new capabilities offered by emerging technologies. "Information operations" describe deliberate campaigns to influence others' wills, in which the mechanism of influence is not the use or threat of violence but rather nonviolent, non-kinetic methods aimed at shaping perceptions, motivations, and convictions. Examples of information operations include military deception, directed persuasion, and narrative construction related to military objectives in some way.

1. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 2016, https://irp.fas.org/doddir/dod/jp1_02.pdf. Accessed 28 Apr. 2022.

Analyzing the capabilities of other major actors involved with information operations can shed light on their impact. Russian information operations take a different approach than Western ones. Russian doctrine holds that the information space represents the domain in which hybrid war achieves *decisive* effects, with other domains subordinate in such conflicts. The Russians have also been engaged in narrative construction. Leaders in Moscow spent years setting informational conditions for the seizure of Crimea and the invasion of eastern Ukraine before acting in 2014; years of similar preparation went into the greater Russian incursion in 2022. The run-up to and invasion of Ukraine saw Russian efforts to shape the information domain from the strategic to the tactical level, as well as Western efforts to counter Russian information condition setting through selective declassification and sharing of intelligence. Throughout the war to-date, the Russians have attempted to set conditions for subsequent actions and to counter Ukraine's own activities in the information domain.

The interplay between the People's Republic of China and Taiwan surrounding U.S. Speaker of the House Nancy Pelosi's visit to Taipei is a useful case study of competing narratives in the information domain. Beijing's leaders sought to degrade the Taiwanese populace's confidence in its armed forces, while Taipei attempted to rebut Chinese disinformation. Chinese government statements before Speaker Pelosi's August 2-3 visit set the conditions necessary for information operations after her departure; disinformation efforts in August 2022 utilized information conditions set in the previous month to put Taiwanese officials on the defensive in the information domain.

U.S and allied leaders face many challenges in reckoning with the growing importance of the information domain, but one of the most salient dilemmas is that *we have no good way to see it.* Social media facilitates sophisticated visualizations using structured data, but those visualizations are largely confined to social channels and not replicable. Information operations operate beyond social media networks or any one medium of information exchange. Grasping the whole of an information campaign requires structuring data to weigh the level of success or failure of narratives and sentiments within the information operation. Managing in the information domain requires the ability to visualize information campaigns analogously with the way visualizations work in the air, land, and sea domains. And visualizing information operations' effect on the wills of component actors is a key differentiator from the cyber domain. Visualizations of information operations must elucidate how the interaction of component actors' wills can generate strategic decisions and actions.

Visualization must support more than understanding—it must also support decision making in concrete circumstances. Given the complexities and changing nature of modern conflict, future force design must include all domains of warfare. Command, control, intelligence, and operations in information environments will need to detect and respond effectively to first moves during conflict that may originate in the information domain. The U.S. and partners face challenges in keeping up with some adversaries in understanding and operating in the information space. But Western allies have tremendous, indeed unique, advantages in the ability to design, build, field, and use globe-spanning complex systems integrating enormous amounts and varieties of data, platforms, munitions, personnel, doctrines, and ways of thinking. Finally, governments cannot keep pace with the implications of emerging technologies alone, necessitating an unprecedented public-private partnership in developing new information capabilities.

Introduction

> *In making his decision, the adversary uses information about the area of conflict, about his own troops and ours, about their ability to fight, etc. We can influence his channels of information and send messages, which shift the flow of information in a way favorable for us. The adversary uses the most contemporary method of optimization and finds the optimal decision. However, it will not be a true optimum, but a decision predetermined by us. In order to make our own effective decision, we should know how to deduce the adversary's decision based on information he believes is true. The unit modeling the adversary serves the purpose of simulating his decisions under different conditions and choosing the most effective informational influence.*
>
> —Vladimir Lefebvre, Soviet theorist[2]

In a recent series of round table discussions in Washington, D.C., Brussels, and Honolulu, global leaders from the military, government, academia, and technology sectors converged on three core challenges of visualizing and understanding the information domain.

- First, the information space is a chaotic system, as slight variations in conditions can dramatically impact how information traverses space and time. Participants compared information operations to weather forecasting and fluid dynamics: while an actor may set out with a clean narrative, that narrative will likely be disrupted by changing contexts, unanticipated perspectives, and complex interactions with other narratives.
- Second, any visualization of this mélange of data points must be useful to decision makers at multiple echelons. Such a visualization requires a dataset that encompasses data from the entire information space, not just social media, and that can be overlayed onto visualizations of the land, air, sea, air, and cyber domains.
- Finally, although the information domain is large, it must remain bounded. With decades of practice, U.S. adversaries have developed rigorous information warfare doctrines. Delineating activity that does and does not fall within the bounds of information operations allows for more useful understanding and visualization of these activities.

The series of roundtables was guided by three sets of framing questions—the first more general, while the latter two focused on the practical cases of Russia and China.

2. Clifford Reid, "Reflexive Control In Soviet Military Planning," *Soviet Strategic Deception*, Ed. Brian Dailey and Patrick Parker, Lexington Books, 1987, P.294.

General questions:

- How do information operations impact governments and stakeholders in the current era?
- What challenges and opportunities do information operations pose to swift and effective decision making? What interactions do they have with other domains?
- How can emerging technologies provide pathways for faster and more reliable development of a common operating picture and common understanding in order to enable effective decision making?
- How should governments and stakeholders combat misinformation as a tool of modern conflict?
- How can information operations best be visualized alongside other domains?

Russia-focused questions:

- How can we best conceptualize and visualize the interwoven information operations the Russians conducted before the invasion on February 24, 2022?
- How can we best visualize the interactions between those information operations and the counter-information operations conducted by the U.S. and its allies?
- How can we best visualize the interactions between both sets of information operations and the Russian provocations on the ground and then the Russian mobilizations?
- How did the information environment change once war began?
- What are the greatest needs of the West in confronting Russian information operations and other near-peer competitors?
- What are the lessons learned from the answers to the above questions, and what is the best way to visualize information operations alongside other domains of warfare to support effective and efficient decision making?

China-focused questions:

- How can we best visualize the interactions between both sets of information operations and major political events on the ground across the Pacific region?
- How can we best conceptualize and visualize the interwoven information operations conducted by, with, or for the Chinese government in the last decade? What are China's critical capabilities and constraints?
- How can we best visualize the interactions between those information operations and the counter-information operations conducted by the U.S. and its allies?
- What are the greatest needs of the United States, allies, and partners in confronting information operations from China and elsewhere?
- How can we visualize adversaries' use of platforms in the U.S. and allied countries in support of adversary information operations?
- What are the lessons learned from the answers to the above questions, and what is the best way to visualize information operations alongside other domains of warfare to support effective and efficient decision making?

What is the Information Domain?

U.S. military and NATO joint doctrine recognizes five domains of warfare: air, sea, land, space, and cyber.[3] This essay considers the information domain as a sixth domain—an arena within which adversaries maneuver to create effects leading to the accomplishment of objectives at various levels of war from tactical to grand strategic. This essay is not the first to address the creation of an information domain of warfare.[4] Instead, this essay's purpose is to assert that visualizing the information space to inform decisions is the chief challenge that practitioners face in adopting this as a domain or element of warfare.

The information space[5] is to policy as terrain is to war. It shapes it, channels it, causes it, and ends it—in every circumstance, it exerts the most profound influence upon it. Anything that changes the information space affects policy, and anything that affects policy affects war. The character of the information space is as central to the character of war as technology, social structures, economics, or any other traditional factor. It is even more important than all those others, however, because it alone encompasses the collective brain of a polity that decides when to start fighting, what to fight for, how much effort to put into the fight, how much to sacrifice, and when to stop. All those decisions are made by policymakers, influenced by the information available to them and the manner of its presentation.

The military theorist Carl Von Clausewitz first defined war as "an act of force to compel our enemy to do our will."[6] We[7] may understand policy as it relates to war as the whole

3. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 2016, https://irp.fas.org/doddir/dod/jp1_02.pdf. Accessed 28 Apr. 2022.
4. Allen, Patrick D., and Dennis P. Gilbert. "Qualifying the Information Sphere as a Domain." *Journal of Information Warfare*, vol. 9, no. 3, 2010, pp. 39–50, https://www.jstor.org/stable/26487457. Accessed 28 Apr. 2022.
5. This paper uses the terms information space, domain, and operations as similar terms for actions involving information.
6. Clausewitz, Carl von. and Howard, Michael. and Paret, Peter. *On war / Carl von Clausewitz*; edited and translated by Michael Howard and Peter Paret; introductory essays by Peter Paret, Michael Howard, and Bernard Brodie; with a commentary by Bernard Brodie, Princeton University Press Princeton, N.J 1976, pp. 75.
7. In this report, "we" refers to the views of the authors.

effort encompassing both forceful and non-forceful means to compel an enemy to do one's will. **We can view the information domain as the sum of the wills, decision capabilities, and resulting choices to act of each actor, where the will is the composite of convictions, perceptions, and influences that drive toward action.**

This definition distinguishes the information space from cyberspace, which is composed of the electromagnetic spectrum and the physical infrastructure harnessing those wavelengths. Cyberspace contains data that affects the information domain; cyberspace is not the totality of the information domain. Analog containers of information outside cyberspace—such as gestures, conversations, symbols, and press reports—are just as relevant to the information domain as these same data contained within cyberspace.

We must distinguish, moreover, between raw data and data processed to produce information. Raw data gains relevance upon its perception, ingestion, and incorporation by human actors via their cognitive processes. Individual data are thus like grains of sand—inconsequential in isolation and not necessarily relevant even in aggregate. When data is perceived, processed, and incorporated into human cognition, however, it becomes information, as it informs action.

The information space is neither a novel phenomenon nor recently relevant to warfare. Just as the operational level of war existed between tactics and strategy for millennia before anyone thought to define or describe it, so too the information space has always existed without clear and agreed-upon definitions.

Yet its importance to the modern character of war has grown significantly. Modern technology and doctrinal innovations have made possible rapid, decentralized, and large-scale interactions within this space from any location in the world, changing the way information shapes decisions before, during, and after war and in near-real-time. Specifically, emerging technologies around analytics, artificial intelligence, and cloud computing makes the processing and incorporation of data faster, more frequent, and of higher impact.

Technology has also vastly increased the amounts and varieties of information available even to tactical operators. Tactical systems such as the F-35 and even upgraded ground vehicles receive information feeds from many different sources, each carrying far more data and information than in any previous generation. The challenges of receiving, processing, and making sense of those flows in real time during combat are great, and present many opportunities for adversaries to shape perceptions up and down the chain of command to their advantage if they gain an understanding of how our forces use them to obtain situational awareness and make decisions. Such adversary efforts on the tactical level can also constitute information operations.

In this way, "information operations" is a confusing phrase because it encompasses many distinct ideas within the current discourse. We recognize, for instance, that using our definitions, any military action is inevitably an information operation, as it aims to affect the will of the opponent. Military action thus contains an inherent informational component. We gain greater conceptual clarity, however, by distinguishing certain information effects from those that do not immediately stem from the application or threat of violence.

Examples of Information Operations

We use the phrase "information operations," therefore, to describe **deliberate campaigns to influence others' wills in which the mechanism of influence is not the use or threat of violence but rather nonviolent, non-kinetic methods aimed at shaping others' perceptions, motivations, and convictions.** In the information domain, human cognition is key terrain. The weapons used on that terrain include violence, viral memes, speeches, and any other methods by which human cognition may be influenced. We are concerned in this report mainly with the informational effects of three principal methods outside the application of violence: military deception, directed persuasion, and narrative construction.

Military deception operations **describe methods to mislead an enemy about one's military maneuver in wartime.**

Directed persuasion information operations are **nonviolent means of presenting data to convince a person or group of a specific normative view during wartime.** Common methods of directed persuasion include disseminating propaganda, "fake news," and political spin. For our purposes, directed persuasion includes all these methods and more. The key term, however, is "directed," because information operations are optimized for a specific effect—not, for example, to change the general population's view. Similarly, the spread of naturally occurring rumors and sentiment, even if beneficial to a given actor, must not be confused for directed operations.

Narrative construction is a series of directed persuasion information operations that, when combined, form a coherent perspective about policy in wartime. Narrative construction can be one of the most difficult forms of information operations to implement, track, or measure, but it can also be one of the most powerful. Successful narrative construction forms a political theory around tangible aspects of the cultural landscape, and presents self-evident facts about the reality within which the narrative will be propagated. Such campaigns incorporate passive and active operations to shape discourse within and between societies. The success of this kind of societal effort is not total or

verifiable, as competition between political ideas is iterative, but these information operations promise to align large swaths of people and communities with a political theory of action. In the military context, successfully constructed narratives can shift actors from adversaries to allies or transform cultures.[8]

Russian Information Operations

Russian theory and doctrine regarding the information domain are the most advanced in the world, but China, Iran, and other U.S. adversaries are adopting similar approaches. Russian hybrid war doctrine goes so far as to declare that the information space is the domain in which hybrid war achieves *decisive* effects, and that other domains are subordinated to it in such conflicts.[9] Russian hybrid warfare doctrine requires setting conditions within the information domain prior to conducting decisive operations in any domain.

Consider Lefebvre's quote introduced at the beginning of this essay: Soviet theorists believed that the state could maneuver in the information space to optimize the adversary's decision making for Soviet interests. How could this work? The information operation Russia conducted against the Ukrainian government early in the COVID crisis provides a good case study of such targeted efforts: Russian agents on the ground and in cyberspace falsely asserted that the Ukrainian government was bringing infected Ukrainian citizens home from China to several locations in Ukraine, where medical authorities were unprepared to handle them. An example of "directed persuasion," this campaign disrupted the Ukrainian response to the crisis and harmed the credibility of that government in the eyes of its people, a core objective of Russia's efforts in Ukraine.[10]

The Russians have also been engaged in narrative construction. Moscow spent years setting informational conditions for the seizure of Crimea and the invasion of eastern Ukraine before it acted in 2014; years of similar preparation went into the greater Russian invasion in 2022. Deliberate information operations stoked pro-Russian and anti-Kyiv sentiment in those areas starting at least in 2004, fueling support for Russian military and paramilitary operations a decade later. Those information operations also acted on Western audiences, spreading a belief that both Crimea and eastern Ukraine are "naturally" part of Russia, and that Kyiv should come to some accommodation to "satisfy" the "ethnic Russian" population in the east (and, of course, accept the fait accompli of the annexation of Crimea, which is said to be "rightfully" part of Russia). These operations were not effective enough to prevent or terminate Western sanctions imposed after 2014 or allow Russia to gain political control of the rest of Ukraine, which is likely Russia's ultimate objective, as demonstrated by the initial thrust of the invasion in February. But they secured Russia a formal position as a *mediator* in a conflict that Russia itself initiated as the *aggressor* under international law. However, Russia's 2022 invasion of Ukraine undid much of the informational groundwork their agents had so painstakingly laid.

8. "Joint Concept for Operating in the Information Environment (JCOIE)," Department of Defense, 25 Jul. 201.8. https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf?ver=2018-08-01-142119-830. Accessed 30 Aug. 2022.
9. Snegovaya, Maria, "Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare," Institute for the Study of War, September 2015. https://www.understandingwar.org/sites/default/files/Russian%20Report%201%20Putin%27s%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf. Accessed 30 Aug. 2022.
10. George Barros, "Viral Disinformation: The Kremlin's Coronavirus Information Operation in Ukraine," Institute for the Study of War, 11 Mar. 2020. https://www.understandingwar.org/backgrounder/viral-disinformation-kremlin%E2%80%99s-coronavirus-information-operation-ukraine. Accessed 27 Aug. 2022.

2022 Russian Invasion of Ukraine

The run-up to the invasion and the conduct of the war both illustrate the centrality of the information domain in Russian thinking about war. Russia prepared false flag operations to justify the invasion that the West then "prebutted" by selectively declassifying intelligence that undermined the effectiveness of Russian information operations.[11] The Russians were clearly attempting to set the conditions for the military campaign, and the United States and its allies worked to undermine it in advance. In December 2021, the United States revealed the scale of the Russian build-up in greater detail than previously in public. In January, the British revealed Russian intentions to install a puppet regime in Kyiv. In early February, the Biden administration revealed the plan to film a false flag attack against either Russian territory or Russian-speaking people.[12]

On the eve of the invasion, "Putin . . . recognized the Donetsk and Luhansk People's Republics . . . as covering the entirety of Donetsk and Luhansk Oblasts (provinces)," which at the time were only partially under separatists' control.[13] This was likely an attempt to justify to the Russian people the need to defend Russian speakers in eastern Ukraine and set the conditions for the regions' eventual absorption into Russia itself. The recognition served as part of the justification for the subsequent invasion. Russia attempted to reshape the information space after the unsuccessful initial invasion, claiming in late March that the "primary objective is to capture the entirety of Donetsk and Luhansk Oblasts," after the initial thrust toward Kyiv clearly suggested otherwise.[14]

At the strategic level, Russia is attempting to set the conditions for the annexation of Ukrainian territory in such a manner that the Russians can claim it to be an organic, locally-driven phenomenon. The Ukrainians resisted such efforts, both by refusing to cooperate with the preparations for the referenda and by engaging in partisan attacks.[15] There is likewise an information domain aspect to the expected show trials of Ukrainian POWs from the siege of Mariupol, both to demoralize Ukrainian troops and to demonstrate to the Russian public that Russia has secured the regions now under occupation.[16]

11. Connor O'Brien, "U.S. 'watching very carefully' for phony Russian reason to kick off Ukraine invasion," Politico, 13 Feb. 2022, https://www.politico.com/news/2022/02/13/ukraine-invasion-false-flag-00008470. Accessed 26 Aug. 2022.
12. Shane Harris, Karen DeYoung, Isabelle Khurshudyan, Ashley Parker, and Liz Sly, "Road to war: U.S. struggled to convince allies, and Zelensky, of risk of invasion," *Washington Post*, 16 Aug. 2022. https://www.washingtonpost.com/national-security/interactive/2022/ukraine-road-to-war/. Accessed 26 Aug. 2022.
13. Mason Clark and Frederick W. Kagan, "Russia-Ukraine Warning Update: Russia Likely to Pursue Phased Invasion of Unoccupied Ukrainian Territory," Institute for the Study of War, 22 Feb. 2022. https://www.understandingwar.org/backgrounder/russia-ukraine-warning-update-russia-likely-pursue-phased-invasion-unoccupied-ukrainian. Accessed 26 Aug. 2022.
14. Mason Clark, Frederick W. Kagan, and George Barros, "Russian Offensive Campaign Assessment, March 25," Institute for the Study of War, 25 Mar. 2022. https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-march-25. Accessed 27 Aug. 2022.
15. Karolina Hird, Grace Mappes, Angela Howard, George Barros, and Mason Clark, "Russian Offensive Campaign Assessment, August 26," Institute for the Study of War, 26 Aug. 2022. https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-august-26. Accessed 27 Aug. 2022.
16. Karolina Hird, Grace Mappes, Layne Philipson, George Barros, and Frederick W. Kagan, "Russian Offensive Campaign Assessment, August 19," Institute for the Study of War, 19 Aug. 2022. https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-august-19. Accessed 27 Aug. 2022.

As Ukrainians have conducted attacks deeper into Russian held territory, Russia has also attempted to shape the information domain by characterizing such attacks as "terrorism," rather than the military attacks they are.[17] Such characterization is also likely an attempt to deflect Western accusations that Russia is state sponsor of terrorism, based on how it has conducted the invasion, targeting civilians indiscriminately. It is also likely an attempt to coopt the international legal framework around terrorism in a bad faith effort to paralyze Western structures with a high volume of allegations against the Ukrainians.

The conflict surrounding the Zaporizhzhia Nuclear Power Plant has also seen the importance of the information domain. The Russians, using the plant as a stronghold from which to launch artillery strikes into surrounding areas, have accused the Ukrainians of preparing to conduct false flag attacks on the plant in order to blame the Russians for any—possibly literal—fallout from the attacks.[18] The Russians will likely attempt to portray disconnecting the plant from the Ukrainian grid as a necessary response to purported Ukrainian shelling, and will use the connection as leverage in negotiations with the United Nations and International Atomic Energy Agency. Both the Ukrainians and Russians are shaping the information space so that the other takes the blame for any disasters surrounding the plant.

At the more tactical level, Russian forces used information operations to degrade Ukrainian troops' morale. "The Ukrainian Main Intelligence Directorate (GUR) reported on June 8 that Russian forces are sending threatening messages to the personal devices of Ukrainian servicemen calling on them to betray their service oaths, lay down their arms, surrender, or defect to Russia."[19] In occupied areas of Ukraine, the Russian-backed administrators have also attempted to isolate Ukrainians from the non-Russian information space, blocking access to Google and YouTube, for example.[20] In many occupied areas, Russia has rerouted all internet traffic to flow through Russian infrastructure, rather than Ukrainian, which allows the Russian occupiers to exercise even greater control over which sites Ukrainians under occupation can access.[21]

The information domain has been a key component of the Russian campaign to occupy Ukraine and overthrow the government. While the West was successful in mitigating some of Russia's efforts prior to the invasion, Russia will continue to use the information domain to set conditions for military operations. One of the greatest challenges is the difficulty in visualizing these efforts in real time, to inform options for U.S. and allied decision makers to manage information operations effectively at the national levels and in the field.

17. Karolina Hird, Kateryna Stepanenko, Angela Howard, George Barros, and Frederick W. Kagan, "Russian Offensive Campaign Assessment, August 17," Institute for the Study of War, 17 Aug. 2022. https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-august-17. Accessed 26 Aug. 2022.
18. Karolina Hird, Layne Philipson, Angela Howard, Katherine Lawlor, George Barros, and Frederick W. Kagan, "Russian Offensive Campaign Assessment, August 18," Institute for the Study of War, 18 Aug. 2022. https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-august-18. Accessed 27 Aug. 2022.
19. Kateryna Stepanenko, Karolina Hird, Mason Clark, and George Barros, "Russian Offensive Campaign Assessment, June 8," Institute for the Study of War, 8 Jun. 2022. https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-june-8. Accessed 26 Aug. 2022.
20. Karolina Hird, Grace Mappes, George Barros, and Frederick W. Kagan, "Russian Offensive Campaign Assessment, July 23," Institute for the Study of War, 23 Jul. 2022. https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-july-23. Accessed 26 Aug. 2022.
21. Adam Satariano and Scott Reinhard, "How Russia Took Over Ukraine's Internet in Occupied Territories," *New York Times*, 9 Aug. 2022. https://www.nytimes.com/interactive/2022/08/09/technology/ukraine-internet-russia-censorship.html. Accessed 28 Aug. 2022.

Chinese Information Operations

The interplay between the People's Republic of China and Taiwan surrounding U.S. Speaker of the House Nancy Pelosi's 2022 visit to Taipei is a useful case study of competing narratives in the information domain. Beijing's objective was to degrade the Taiwanese populace's confidence in its armed forces, while Taipei was attempting to rebut Chinese disinformation. The case highlights the way in which operations in the conventional domains can be in support of operations in the information domain, which was, in this case, the center of gravity.

Chinese government statements before Speaker Pelosi's August 2-3 visit set the conditions necessary for information operations after her departure that targeted the Taiwanese populace's confidence in its armed forces. On July 26, Chinese Ministry of National Defense Spokesman Senior Colonel Tan Kefei warned that the People's Liberation Army (PLA) would "never sit idly by" during the Speaker's visit.[22] Chinese President Xi Jinping then warned President Biden via phone call on July 28 to not "play with fire" over Taiwan.[23] The following day, July 29, the PLA posted the message "Prepare for War!" on the Chinese social media site Sina Weibo.[24] These combined statements created an information environment where individuals expected forthcoming PLA activity. That expectation led to a greater willingness to accept PLA claims of miliary activity without substantial research. This environment buttressed Chinese capacity to conduct information operations regarding the Penghu Islands.

The PLA released claimed footage of PLA Air Force (PLAAF) fighters operating near the Penghu Islands in mid-August as part of an information effort to discredit Taiwanese defense capabilities.[25] The Penghu Islands sit approximately 30 miles to the west of the Taiwanese mainland. If not countered in the information domain, the released PLAAF footage would signal Taiwanese ineffectiveness against PRC aggression and severely degrade the already flagging Taiwanese populace's belief that they could win a war against China.[26] Taiwanese Air Force Vice Chief of Staff for Operations Tung Pei-lun cited publicly released Taiwanese Ministry of Defense graphics of PLAAF flight paths to rebut the PLA claim. He also accused the PLA of engaging in information warfare with the release of the video.[27] This counter-narrative effort did not effectively rebut Chinese disinformation claims to the degree necessary to allow Taiwanese officials to engage in offensive information efforts.

PLA disinformation efforts in August 2022 utilized information conditions set in the previous month to put Taiwanese officials like Tung Pei-lun on the defensive in the information domain. U.S. and allied partners could collaborate on decision options in the region as Taiwan develops the capacity to neutralize future PRC narratives in the information domain in order to avoid undesired crises, even as Taiwan will likely simultaneously wish to avoid rhetorical claims that Beijing sees as a "provocation" requiring an escalatory response outside the information domain.

22. http://eng.mod.gov.cn/news/2022-07/26/content_4916547.htm.
23. http://eng.mod.gov.cn/news/2022-07/28/content_4916911.htm. https://www.reuters.com/world/biden-looks-tamp-down-taiwan-tension-during-china-xi-call-2022-07-28/.
24. https://www.globaltimes.cn/page/202207/1271742.shtml.
25. https://www.reuters.com/world/asia-pacific/taiwan-says-china-air-force-video-islands-is-information-warfare-2022-08-16/ https://www.youtube.com/watch?v=wzZOUmqPDFE. https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/202208/t20220816_10744243.html.
26. https://www.taiwannews.com.tw/en/news/4663330. https://www.tpof.org/%e7%b2%be%e9%81%b8%e6%96%87%e7%ab%a0/2022%e5%b9%b49%e6%9c%88%e3%80%8c%e5%9c%8b%e9%9a%9b%e5%bd%a2%e5%8b%a2%e3%80%81%e7%b8%bd%e7%b5%b1%e8%81%b2%e6%9c%9b%e8%88%87%e9%81%b8%e8%88%89%e7%ab%b6%e7%88%ad%e3%80%8d/.
27. https://twitter.com/MoNDefense/status/1559129378004832256. https://taipeitimes.com/News/taiwan/archives/2022/08/17/2003783678.

Visualizing the Information Domain—Findings and Recommendations

The West faces many challenges in reckoning with the growing importance of the information domain. One of the most salient dilemmas, however, is that *there is no good way to see it.* Many visualizations of information campaigns are available in academic, policy, and media documents. Some show the evolution of storylines over time. Others try to relate the publication of stories or memes with other events on timelines. In some cases, node-link diagrams depict humans and organizations engaged in conducting information operations. Research into the spread of messages on social media platforms is vast and growing. It often generates fascinating visualizations of social media formal and informal networks, message dissemination, and many other dimensions of the interactions of human beings (and bots) in the social media space.

The differential timescales on which information operations can run poses one major dilemma for analysts and decision-makers. Information operations can run at network speed when they involve spreading memes or stories directly through the internet via social media platforms, cyber operations, or just the propagation of information across the network. They can also run for decades, evolving to meet the contemporary contexts of long-term strategic interests in the information domain. The first major dilemma facing analysts and decision makers in the information domain is the challenge of interacting with operations moving at nearly the speed of light, while simultaneously maintaining awareness of and interacting with decades-long informational efforts.

Social media facilitates sophisticated visualizations because it contains structured data, *but those visualizations are largely confined to social media and not replicable beyond it.* Information operations are not confined to this space. In the cases where we have structured data from digital influence vectors (say, online journalism), the metadata from those sources is not normalized, is inconsistent, can be deliberately falsified and manip-

ulated, and simply does not add up to a data layer with anything like the analytical power or visualization potential of, say, activity on Twitter. Non-digital vectors—such as newspapers, billboards, or even slogans chanted at protests—usually come with no direct metadata layer at all.

Grasping the whole of an information campaign thus requires structuring data to weigh the level of success or failure of narratives and sentiments within the information domain. Tools to grapple with this problem are evolving, but slowly. Natural language processing and entity and event extraction algorithms have improved, but unevenly across languages. A concerted effort by governments and commercial partners will help to complete the development and integration of tools needed to wrestle with multilingual content across many language groups—and then to move beyond language to the abstractions of semantic analysis that can support tracking information operations as they traverse from one language to another.

These tools alone, however, will not enable visualizing information operations' results. Node-link charts, timelines with events, and color-coded dynamic graphics showing the spread of memes and their transitions from language to language are important but insufficient. The information domain requires the ability to visualize information campaigns analogously with visualizations of military campaigns in the air, land, and sea domains. Visualization must start with the assessed objectives of the campaign, and then move through conditions-setting, initial undertakings, adjustments and inflections over time, and setbacks and counterattacks from the assessed campaign objectives to the supporting lines of effort. All these phases and activities occur in well-designed information operations.

Visualizing information operations' effect on the wills of component actors is key. None of the methods discussed above facilitates knowledge or representation of the results of information operations. The mere spread of a story across social media or news outlets does not validate that the story influenced its readers toward a specific action. A more dynamic approach can integrate localized undertakings with larger country-level information operations nested within the global set of information operations, all changing over time and showing key inflections. The challenge becomes even greater given the need to visualize the information domain in relation to the other domains of war.

In addition, visualizations of information operations must elucidate how the interaction of component actors' wills can generate strategic effects. Different actors will have more or less potential to impact an adversary's policy decisions. These actors need the capability to amplify, suppress, or disrupt narratives subordinate to an information campaign, as well as explain how those tactical tasks impact other narratives, events, and actors in the battlespace. The interaction of narratives will be a critical element of this visualization and should go beyond traditional sentiment-analysis scoring to measure an operation's successive and cumulating supporting efforts. Such analysis should incorporate numerous sentiments and display their causal impact (gaining or losing strength) based on the resourcing, perception, and formulation of supporting or competing narratives.

Finally, visualizations should involve a suite of solutions for multiple echelons, able to zoom in and out both functionally and geographically. This is especially important because analysts, commanders, and policymakers need different kinds of inputs and

access to visualizations—the information domain is so inherently complex that visualizing it must address multiple actions for multiple audiences, with the ability to tailor the visualization to the relevant user. This allows for staffs to monitor the day-to-day activities in the information domain, but also to develop a narrative about information operations and to elevate activity to a policymaker or commander to inform their decision making.

Other criteria that can enable governments and partners to meet the challenge of visualizing information operations include the following:

- Automated translation and entity and event extraction from unstructured text or images in any major language at the level of a human expert translator or analyst
- Static visualization of an information campaign depicting its initial state, assessed objectives, major lines of effort, and progress along each line
- Static visualization of multiple information campaigns nested under strategic and grand strategic objectives
- Dynamic visualizations of individual and multiple information operations from their preparation stages to their completion
- Visualization of adversarial information campaigns operating against one another
- Integrated static and dynamic visualizations of information campaigns with undertakings in the air, sea, and land, space, and cyber domains
- Automated detection of inflections in information campaigns
- Assessment and visualization of information campaigns moving from language to language and region to region
- Identification and visualization of indicators and warnings within the information domain
- Identification and visualization of cross-domain indicators and warning
- Data collection and processing mechanisms to facilitate the above visualizations

Leaders from the U.S., allies, and partners can work together with industry and academic experts to develop initial visualization frameworks that address these and related criteria. An open ecosystem to collaborate on solutions can draw out innovative models to facilitate collection and operations in the field, narrative explanations by analysts, and ultimately decisions by leaders at the national level.

Conclusion

Visualization must support more than understanding. It must also support decision making in concrete circumstances. Efforts to develop effective visualizations must also, therefore, take into account the critical requirements of operations, experimentation, and modeling and simulation to support preparing and training the military to function well in an increasingly complicated multidomain environment.

Given the complexities and changing nature of modern conflict considered above, future force design concepts must expand the concept of operational readiness to include all domains of warfare. They in particular must develop accurate models of influence campaigns, information operations, counter-influence operations, and their interactions with and impacts on land, air, sea, space, and cyber domains.

These capabilities are particularly important where future force design models demand tighter integration and pre-positioning strategies, such as in the U.S. Indo-Pacific Command area of responsibility, where policymakers and commanders must contend with the tyranny of great distances. Command, control, intelligence, and operations in information environments will need to be able to detect and respond effectively to first moves in conflict with peer adversaries that may originate in the information domain. The May 2022 Marine Corps Force 2030 update highlights the need to improve this domain calling for the creation of an information command, stating: "The service lacks adequate OIE (Operational Information Environment) doctrine or training standards. This leads to a lack of awareness, education, and experience, often reflected in commanders and staffs grappling with operating in a multi-domain environment and applying and integrating information capabilities."[28]

Developing effective visualization can support managing in the information domain, as evidenced by the need to address and learn from current events in Eastern Europe. Governments need both a coherent understanding of the information domain and information operations, and ways of visualizing such operations in conjunction with the other domains of war—and then need to bring those insights through force conceptualization and force design to experimentation, wargaming, preparation, and training of forces and leaders. Nations who can better operationalize their understanding of information operations will be more likely to prevail.

The U.S., its allies, and partners can accelerate activity in these areas to keep pace with adversaries in understanding and manipulating the information space. Moreover, governments cannot keep pace with the implications of emerging technologies alone, necessitating an unprecedented public-private partnership. The U.S., its allies, and partners have tremendous, indeed unique, advantages in the ability to design, build, field, and use globe-spanning complex systems integrating enormous amounts and varieties of data, platforms, munitions, personnel, doctrines, and ways of thinking. Governments have the opportunity to act now to succeed in the future, by bringing these skills and capabilities to addressing the challenges posed by technological changes and by raising the prominence and importance of information operations.

28. United States Marine Corps, Force Design 2030 Annual Update, May 2022, p7.

About the Authors

Brian Babcock-Lumish is the Recanati-Kaplan Chair and director of the General David H. Petraeus Center for Emerging Leaders at the Institute for the Study of War. Prior to joining the Institute, he served as a U.S. Army military intelligence officer, retiring after 24 years in uniform.

Dr. Babcock-Lumish twice deployed as a part of Multi-National Force-Iraq, first leading a team training Iraqi intelligence collectors, and later serving for a year as a strategic intelligence analyst and General Petraeus' daily intelligence briefer during "The Surge" in 2007. During his assignment at U.S. Army Pacific, he served as General Vincent Brooks' analysis chief, leading 200 analysts watching the 36 countries of the Indo-Pacific, and as a strategic planner in General Robert Brown's commander's action group.

Dr. Babcock-Lumish served two tours teaching international relations in the Department of Social Sciences at the United States Military Academy at West Point where he also led the Academy's graduate scholarship program. Throughout his career, he served in various command and staff positions, including a company of command training intelligence analysts at Fort Huachuca, Arizona, and as the battalion executive officer of the 205th Military Intelligence Battalion at Fort Shafter, Hawaii.

Formerly an enlisted Russian linguist, Dr. Babcock-Lumish double majored in International & Strategic History and International Politics and received his commission from West Point. Upon graduation, he earned a Masters of Philosophy in Russian and East European Studies at Oxford University as a U.S. Marshall Scholar. Prior to his first tour on faculty at West Point, he completed his PhD in War Studies at King's College London as a Harry S. Truman Scholar.

Brian Babcock-Lumish

Recanati-Kaplan Chair and Director of the General David H. Petraeus Center for Emerging Leaders

Leendert van Bochoven is a global executive serving defense and intelligence clients with their essential work. For 23 years, Mr. van Bochoven has worked with this community and NATO to improve mission readiness. He was appointed Distinguished Industry Leader in 2022. Prior to working with IBM, he was a director with the Baan Institute.

Mr. van Bochoven attended the Harvard Kennedy School's Executive Education program and earned certificates in National and International Security and Leadership Decision-Making. He received his master's in Business Economics from Erasmus University, Rotterdam.

Leendert van Bochoven

Global Defense and Intelligence Leader
IBM, Netherlands

Stephen Gordon

Red Hat Strategic Accounts Director,
DoD & Joint Agencies
Washington, D.C.

Stephen Gordon is a strategic accounts director in Red Hat U.S. Public Sector, managing a portfolio of customers in U.S. Department of Defense, Joint Agencies, and Fourth Estate.

Previously, he led business development for Microsoft's Digital Transformation and Cloud team, leading Microsoft Federal entrance into the modeling and simulation market, creating a unified digital platform and studio for simulating, designing, rehearsing, visualizing, and analyzing complex global conflict scenarios (wargames). He worked inside Xbox Research and Xbox Game Studios with Microsoft Azure and AI product teams, streaming services (XCloud), content creators, and game operations (PlayFab) to adapt these and other innovative gaming technologies to serious gaming, initially for U.S. Marine Corps, Navy, Army, and U.S. Special Operations.

During his time at Microsoft, he created a program for inner-city NYC schools, "Summer Challenge," providing 9th-11th grade students a six-week experience teamed with corporate volunteers to develop creative solutions to a real-world business problem. The program recognized all participant student with a monetary award, and proved to motivate students to go on to college and pursue fulfilling, happy careers and lives.

Mr. Gordon is also a fellow at the Institute for the Study of War in Washington D.C., a nonpartisan, nonprofit, public policy research organization, advancing the understanding of military affairs through reliable research, where he focused on the impact of information operations and influence campaigns on contemporary and future conflict.

Tim Hofmockel

Research Engineering Manager at
Palo Alto Networks

Tim Hofmockel leads a research engineering team at Palo Alto Networks, where he supports USG customers in countering cyberattacks and espionage operations conducted by malicious actors. He is concurrently pursuing his Master of Arts in Security Studies at the Georgetown University Walsh School of Foreign Service. Mr. Hofmocket participated in the 2017 Hertog War Studies Program and subsequent seminars hosted by the Institute for the Study of War.

Frederick W. Kagan, author of the 2007 report Choosing Victory: A Plan for Success in Iraq, is one of the intellectual architects of the successful "surge" strategy in Iraq. He is the director of AEI's Critical Threats Project and a former professor of military history at the U.S. Military Academy at West Point. His books range from *Lessons for a Long War* (AEI Press, 2010), coauthored with Thomas Donnelly, to the *End of the Old Order: Napoleon and Europe, 1801-1805* (Da Capo, 2006).

Frederick W. Kagan

Senior Fellow and Director of the Critical Threats Project

Nils Peterson is a China researcher and war studies fellow at ISW. He is a graduate of the University of Wisconsin-Madison with a Bachelor of Arts in History and Chinese. Mr. Peterson previously conducted research on the historical development of Chinese law. He is a 2021 alumnus of ISW's Hertog War Studies program.

Nils Peterson

China Researcher and War Studies Fellow at ISW

Noah Ringler is a scientist at Booz Allen Hamilton and a 2021 graduate of Georgetown University's Security Studies Program, where he concentrated on artificial intelligence and national security. He is a 2017 alumnus of the Hertog War Studies Program at the Institute for the Study of War.

Noah Ringler

Scientist at Booze Allen Hamilton

Recent Reports from the IBM Center for The Business of Government

A Guide to Adaptive Government: Preparing for Disruption

by Nicholas D. Evans

Leveraging Data for Racial Equity in Workforce Opportunity

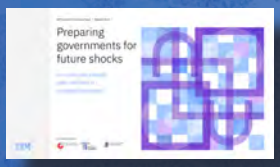
by Temilola Afolabi

Off to a Running State Capital Start: A Guide for New Governors and Their Teams

by Katherine Barrett and Richard Greene

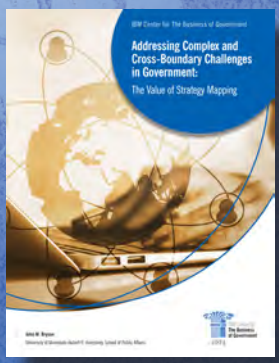
Mobilizing Cloud Computing for Public Service

by Amanda Starling Gould



Preparing governments for future shocks: An action plan to build cyber resilience in a world of uncertainty

by Tony Scott



Addressing Complex and Cross-Boundary Challenges in Government: The Value of Strategy Mapping

by John M Bryson, Report Contributors

The Future of AGILE GOVERNMENT

by G. Edward DeSeve

Partnering for Resilience

by Chris Mihm

For a full listing of our reports, visit www.businessofgovernment.org/reports

About the IBM Center for The Business of Government

Through research stipends and events, the IBM Center for The Business of Government stimulates research and facilitates discussion of new approaches to improving the effectiveness of government at the federal, state, local, and international levels.

About IBM Consulting

With consultants and professional staff in more than 160 countries globally, IBM Consulting is the world's largest consulting services organization. IBM Consulting provides clients with business process and industry expertise, a deep understanding of technology solutions that address specific industry issues, and the ability to design, build, and run those solutions in a way that delivers bottom-line value. To learn more visit ibm.com.

For more information:
Daniel J. Chenok
Executive Director
IBM Center for The Business of Government

600 14th Street NW
Second Floor
Washington, D.C. 20005
(202) 551-9342

website: www.businessofgovernment.org
e-mail: businessofgovernment@us.ibm.com

Stay connected with the IBM Center on:

or, send us your name and e-mail to receive our newsletters.

IBM Center for **The Business of Government**