MITRE

MP210039
MITRE PRODUCT

Structured Process for Information Campaign Evaluation (SP!CE™)

An Analytic Framework, Knowledge Base, and Scoring Rubric for Operations in the Information Environment

Author(s): Matt Venhaus, The MITRE Corporation
Mike Fulk, The MITRE Coporation
Mark A. Finlayson, Ph.D, Florida International University
Brian Fonseca, Florida International University
Zue Lopez Diaz, The MITRE Corporation
Daniel Sixto, Florida International University
Savina Koda, The MITRE Corporation

November 2021

Approved for Public Release; Distribution Unlimited.

Public Release Case Number 21-1184.

Annapolis Junction, MD

Abstract

In an increasingly information-driven world, individuals simultaneously produce, distribute, and consume information. The demand to use the information to conduct and counter influence campaigns is increasing. To address this demand, MITRE built upon an existing framework, Adversarial Misinformation and Influence Tactics and Techniques (AMITT)[1], to analyze, categorize, and conduct operations in the information environment. The resulting Structured Process for Influence Campaign Evaluation (SP!CE™) extends AMITT to provide a further strengthened, solid foundation for the growing community of analysts, policymakers, planners, and operators interested in information campaigning, malign foreign influence, information operations, and cognitive security. The standardized, rigorous, repeatable framework that SP!CE™ provides fosters better decisions about influence campaigns. SP!CE™ examines influence at the campaign level, where multiple information actions, coordinated in time, space, and purpose, endeavor to advance an entity's interests and strategic objectives. The SP!CE™ Framework organizes influence campaign strategies, tactics, and techniques. The SP!CE™ evaluation methodology provides complete scoring rubrics for every phase of an information campaign. With these rubrics, analysts can fully evaluate adversary campaigns, and planners can improve in stride ongoing campaigns. The SP!CE™ curated knowledge base, using the AMITT base, contains clear definitions of all tactics and techniques and documented examples of tradecraft used in recent information campaigns. As this knowledge base grows, trends in adversary behavior emerge, and opportunities to present and disrupt future campaigns develop.

[1] Gray & Terp "Misinformation: we're 4 steps behind its creators" https://cyber.harvard.edu/sites/default/files/2019-11/Comparative%20Approaches%20to%20Disinformation%20-%20John%20Gray%20Abstract.pdf; Terp, S. AMITT red framework: Latest framework. Retrieved from https://github.com/cogsec-collaborative/AMITT/commits/main/amitt_red_framework.md; Presented at a variety of talks given by Pablo Breuer, Sarah-Jane Terp, John F. Gray, and Christopher R. Walker

This page intentionally left blank.

Executive Summary

MITRE's Structured Process for Information Campaign Evaluation (SP!CE™) provides a solid foundation for the growing community of analysts, policymakers, planners, and operators interested in information campaigning, malign foreign influence, information operations, and cognitive security.

SP!CE™ provides a standardized, rigorous, repeatable framework to:

- Recognize, organize, analyze, and assess information activities.
- Maintain a curated knowledge base of observed tradecraft, tactics, and techniques.
- Highlight opportunities to deter, detect, mitigate, or pre-empt foreign influence.
- Evaluate the effectiveness of operations in the information environment.
- Enumerate areas to improve U.S. influence campaigns' design and execution.
- Inform future investments in supporting technologies.

Three fundamental philosophical underpinnings guide SP!CE™'s development. First, information campaigns combine the technical and cyber actions taken on information systems ***and*** the persuasive cognitive effects information exerts on humans. Second, examining all aspects of planning, enabling, and executing information activities is essential. Finally, continuous assessment of each phase of an information campaign is more useful than post facto measures of effectiveness alone.

SP!CE™ examines influence at the campaign level, where multiple information actions, coordinated in time, space, and purpose, endeavor to advance an entity's interests and strategic objectives. The methodology is consistent with the Department of Defense's *Joint Concept for Integrated Campaigning* and the *Joint Concept for Operating in the Information Environment.* SP!CE™ provides more detail on specific actions than is currently available from published military doctrine and incorporates best practices from social movements, political campaigns and commercial advertising.

SP!CE™ and its AMITT basis are distinctive from high-level models such as the Department of Justice Malign Foreign Influence Campaign Cycle[2] and the Carnegie Endowment's ABCDE Framework proposed for the European Union.[3] High-level models illuminate high-level processes and goals but do not effectively convey individual actions, how one action relates to another, how sequences of activities relate to objectives, and how they correlate with data sources, mitigation strategies, and countermeasures. SP!CE™ focuses on accurately representing information campaigns in a way that is easy to categorize.

[2] U.S. Department of Justice, *Report of the Attorney General's Cyber Digital Task Force,* 2018

[3] Carnegie Endowment for International Peace, *The EU's Role in Fighting Disinformation: Crafting a Disinformation Framework,* 2020.

The SP!CE™ curated knowledge base contains clear definitions of all tactics and techniques and documented examples of tradecraft used in recent information campaigns.

As this knowledge base grows, trends in adversary behavior emerge, and opportunities to present and disrupt future campaigns develop.

SP!CE™ provides complete scoring rubrics for every phase of an information campaign. With these rubrics, analysts can fully evaluate adversary campaigns, and planners can improve in stride ongoing campaigns.

Instead of calling additional attention to adversary information campaigns, planners, policymakers, and operators should use knowledge gleaned in the assessment process to reverse information flows, disrupt enabling activities, deliver alternative behaviors to the target audience, enhance target audience resilience, and threaten adversary objectives.

MITRE designed the SP!CE™ enhancements to AMITT to provide a more solid foundation for the growing community of interest in influence campaigning, malign foreign influence, and cognitive security. As the community grows and coalesces, MITRE wants SP!CE™ to:

- Highlight opportunities to deter, detect, mitigate, or pre-empt foreign influence.
- Enumerate areas of improvement for U.S. influence campaigns.
- Provide a rigorous, repeatable process for evaluating campaign effectiveness.
- Inform future investments in supporting technologies.

  When properly applied, SP!CE™ can identify a critical set of relevant factors to address specific issues against which U.S. government decision makers may employ appropriate levers to compete effectively below the armed conflict threshold.

Acknowledgments

Besides the behavioral and social sciences, this research borrows extensively from the cybersecurity community. The MITRE ATT&CK® global knowledge base of cyber adversary tactics and techniques brings private sector, government, and cybersecurity product and service communities together to develop more effective cybersecurity. The success of ATT&CK® led to it being used as an inspiration for the categorization of the different types of online influence tactics in the AMITT framework, effectively extending the concepts of ATT&CK® beyond the purely cyber domain. AMITT is a framework that provides the ability to rapidly describe, understand, communicate, and counter misinformation-based incidents. The United Kingdom Government Communications Service created another framework, known as RESIST. It includes a counter disinformation toolkit that helps government and public sector communications professionals prevent the spread of mis/disinformation. This toolkit provides practical approaches to identifying and tackling disinformation as an early warning system.

MITRE has additionally been working on a further enhancement and expansion of SP!CE™ in partnership with Florida International University. The MITRE Corporation and Florida International University (FIU) entered into a strategic partnership in 2019 to work on the nation's most significant challenges. In the 2020-21 SP!CE™ project, FIU has been working collaboratively with MITRE to evaluate existing information conflict frameworks and implementations. Together, MITRE and FIU have expanded SP!CE™, clarified definitions, researched recent influence campaigns, and designed and developed a set of knowledge bases to accompany SP!CE™. As a result of this collaboration, SP!CE™ is grounded in academic research, and has been reviewed by career practitioners and validated against observed and documented actions "in the wild." This learning also supports and enhances the learning from deployments of the AMITT framework across NATO, The European Union, UN Agencies, and national domains.

MITRE would like to offer special thanks to FIU students Brandon Lee and Amelia Raudales whose tireless research efforts and passion for excellence enhanced the scope and quality of this work. Their faculty advisors Dr. Mark Finlayson, Dr. Alex Crowther, and Mr. Brian Fonseca went beyond simply providing mentorship and guidance to the students as they directly contributed their significant intellectual prowess to the collaborative effort.

Table of Contents

List of Figures

List of Tables

This page intentionally left blank.

1 Introduction

Recent and widely publicized media manipulation incidents have focused the U.S. national security establishment on improving capabilities to conduct information-centered influence operations, understand adversary information campaigns, and thwart foreign governments' attempts to conduct malicious influence activities.[3] [4] In a recent paper on communications strategy and synchronization, the Joint Chiefs of Staff wrote:

> "Today's information environment complicates the security environment and affects the way we operate. It is a decisive realm of competition for us and for our adversaries in the fight for legitimacy and influence. This has amplified the importance and urgency by which we plan and how we align and synchronize our actions and words to educate, inform, and influence different audiences and engage the media."[5]

State and non-state actors use information and related efforts to advance their interests. America has re-entered an era of strategic competition across the globe, often in non-permissive environments, particularly in conflict with Chinese and Russian interests and information. China and Russia are highly capable adversaries that a 2019 Joint Doctrine Note described as "willing and able to employ a mixture of instruments of national power to achieve significant strategic advantages in a manner calculated not to trigger our legal or institutional thresholds for armed conflict."[6] Both nations exert control over the information environment within their borders and endeavor to exert control externally. In short, they are seeking to dominate the 21st century information environment.

Influence campaigns use multiple information actions, coordinated in time, space, and purpose, to advance an entity's interests and strategic objectives. Effective competition requires a standardized, rigorous, repeatable methodology to recognize, organize, analyze, and assess influence campaigns and provide the critical underlying context to explain actors' actual or potential actions more fully. Many analysts, policymakers, and operational elements find it challenging to consistently integrate information activities into their work or to organize and evaluate influence campaigns in their totality.

Influence continuously occurs at strategic, operational, and tactical levels. Tools and resources available at each level vary greatly, and a wide variety of actors employ them. For example, those interacting directly with an audience face-to-face likely are not the same people who are in a position to impose international economic sanctions. However, within the context of their decision-making system, the audience takes both inputs to formulate their behavioral output. The breadth of actors and capabilities that contribute to influence activities ranges from diplomats,

---

[3] For purposes of this report, the term "influence" is an umbrella term that includes, but is not limited to, information operations, public diplomacy, active measures, information statecraft, strategic communication, information warfare, disinformation, misinformation, political warfare, propaganda, cognitive security, and operations in the information environment.

[4] Summaries of recent incidents of media manipulation can be found at https://www.brookings.edu/blog/order-from-chaos/2020/05/19/the-kremlins-disinformation-playbook-goes-to-beijing/, https://www.americanprogress.org/issues/security/reports/2019/02/28/466669/understanding-combating-russian-chinese-influence-operations/ and https://www.rand.org/news/press/2019/09/04.html

[5] Joint Staff, *Insights and Best Practices Focus Paper: Communication Strategy and Synchronization.* Suffolk: Joint Chiefs of Staff, 2016, retrieved 2020 from https://www.jcs.mil/Portals/36/Documents/Doctrine/fp/comm_strategy_and_sync_fp.pdf

[6] Joint Staff, *Joint Doctrine Note 1-19: Competition Continuum.* Joint Chiefs of Staff, 2019 retrieved 2020 from https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn1_19.pdf

trade negotiators, and heads of state through public relations, marketing, and advertising professionals to psychological operators, cyber-attackers, and electronic warfare specialists. In addition to traditional influencers, today's information environment includes new influence actors. For example, "Coordinated Inauthentic Behavior," implemented through social media platforms, means a very loosely organized group (e.g., teen-age fans of Korean pop groups) who may directly or indirectly influence an individual (e.g., doxing), another group (conveying a hoax threat of flag-burning to right-wing militias), or influence through the environment (signing up for rally tickets to frustrate authentic potential attendees to make rally attendance low), or hinder opponent supply chains and inventories (massively loading up shopping carts with merchandise but not purchasing). Each can have a role in influence, just as changes in the physical environment and traditional influence actors can change an audience's perception of a situation.

To maintain an advantage in the influence campaign aspects of strategic competition, the United States must solidify its understanding of how these campaigns are conducted in today's information environment. Accurately assessing influence activities and their effectiveness, both those that the United States and its allies run and those attempted by our adversaries, is central to advance that understanding.[7] These assessments are notoriously challenging because of the often abstract, complex, and dynamic nature of the information environment.[8] Humans tend to believe or seek out information that preserves or reinforces their opinions or beliefs, which often results in knowledge gaps leading to questionable reasoning and poor decision making. Additionally, biases often enter the assessment process unconsciously. Long-term influence practitioners note that those conducting influence operations often overstate their efforts' impact.

In contrast, the targets and victims of influence operations often understate those operations' effects on their actions, behaviors, and beliefs. These compound over time and scale up as decisions are adjusted based on these inaccurate assessments. These complicating factors have implications for policymakers, planners, and operators. As influence operations become increasingly common, they will play a more critical and strategic role in complex global political, military, economic, and social affairs. Thus, an improved ability to effectively assess and adjust affords a distinct advantage in international competition.

MITRE designed the Structured Process for Influence Campaign Evaluation (SP!CE™) to provide a solid foundation for the growing community of interest in influence campaigning, malign foreign influence, and cognitive security. Unlike most current analytic methodologies that concentrate on traditional political science, science, technology, and military actions, SP!CE™ seeks to identify, interpret, and evaluate efforts in and concerning the information environment, and explore how those efforts surround and contextualize the physical world.[9] SP!CE™ provides more detail on specific actions than is currently available from published military doctrine.

---

[7] For purposes of this paper, the term "assessment" is defined using the standard Department of Defense (DoD) definition from Joint Pub 5-0 as "A continuous activity that supports decision making by ascertaining progress toward accomplishing a task, creating an effect, achieving an objective, or attaining an end state for the purpose of developing, adapting, and refining plans and for making campaigns and operations more effective."

[8] S. B. King, "Military Social Influence in the Global Information Environment." p. 7. See also J. Jones, D. Kuehl, D, Burgess, and R. Rochte, "Strategic Communication and the Combatant Commander," *Joint Force Quarterly*, vol. 55, no. 4, 2009; C. Lamb, Review of Psychological Lessons Learned from Recent Experience; T. Shanker and M. Hertling, "The Military-media Relationship: A Dysfunctional Marriage?" *Military Review*, vol. 89, no. 5, Sept.-Oct. 2009.

[9] The methodology is consistent with DoD's *Joint Concept for Integrated Campaigning* and the *Joint Concept for Operating in the Information Environment*.

2 Purpose

SP!CE™ provides a solid foundation for the growing community of analysts, policymakers, planners, and operators interested in information campaigning, malign foreign influence, information operations, and cognitive security. The standardized, rigorous, repeatable framework that SP!CE™ provides helps users make better decisions about influence campaigns in an increasingly information-driven world.

The SP!CE™ Framework's first purpose is to establish a baseline for conducting influence campaigns rooted in social science and psychological theories from seminal works in Western and non-Western perspectives. The second is to provide a framework for analysis that categorizes observed tactics from all phases of a wide variety of influence campaigns. The tactics documented in the framework form a publicly available curated knowledge base and model of information activities.

The most significant purpose of SP!CE™ is to outline a methodology to measure influence campaigns' efficacy that is equally applicable to those assessing adversary campaigns and those planning and conducting U.S. influence operations. The assessment scoring methodology allows planners to identify and correct problems earlier in a campaign and enables analysts to focus chronologically earlier in the influence cycle to provide stakeholders with the maximum time and flexibility to apply traditional and non-traditional levers against adversary campaigns.

Vagueness is the enemy of measurement. Indeed, ambiguity is often the reason those hard-to-measure things appear to be immeasurable. The SP!CE™ evaluation rubrics for measuring influence campaigns and their impact overcome the abstract, complex, and dynamic nature of the information environment and the paucity of data available during an event with a repeatable process for a wide range of influence activities. This rigorous approach to measurement informs sensor strategies and data collection plans essential to successful influence campaigns.

Professionals who conduct influence may have different terms for some of the processes reinforced by centuries of thought on the topic. This framework is not intended to challenge or replace those documents but rather to create a common point of reference for concepts and ideas needed to assess all changes in the information environment's cumulative effects on a target audience.

3 Approach

This paper uses the term "information" in the broadest possible sense to denote that which can be perceived and transmitted in any form or through any means. This definition is intentionally free of reference to intent, truth, origin, or legitimacy to avoid the pitfalls of pre-judging or arbitrating information on its content.[10] "Information activities" are discreet events where one or more actors undertake a discernable endeavor using information (i.e., transmit it, process it, alter it, broadcast it, etc.). "Influence campaigns" involve multiple coordinated information actions to advance an entity's interests and strategic objectives. SP!CE™ primarily focuses on campaign-level understanding, analysis, and assessment.[11]

Three fundamental philosophical underpinnings guide SP!CE™'s development. First, influence campaigns combine the technical and cyber actions taken on information systems and the persuasive cognitive effects information exerts on humans (Figure 3-1). The technical effects on information manipulate the flow, content, or composition of information as it exists in the information environment. The effects of information change the perceptions, emotions, and objective reasoning within the target audience. Figure 3-1 shows that cognitive and technical actions combine to produce effects.

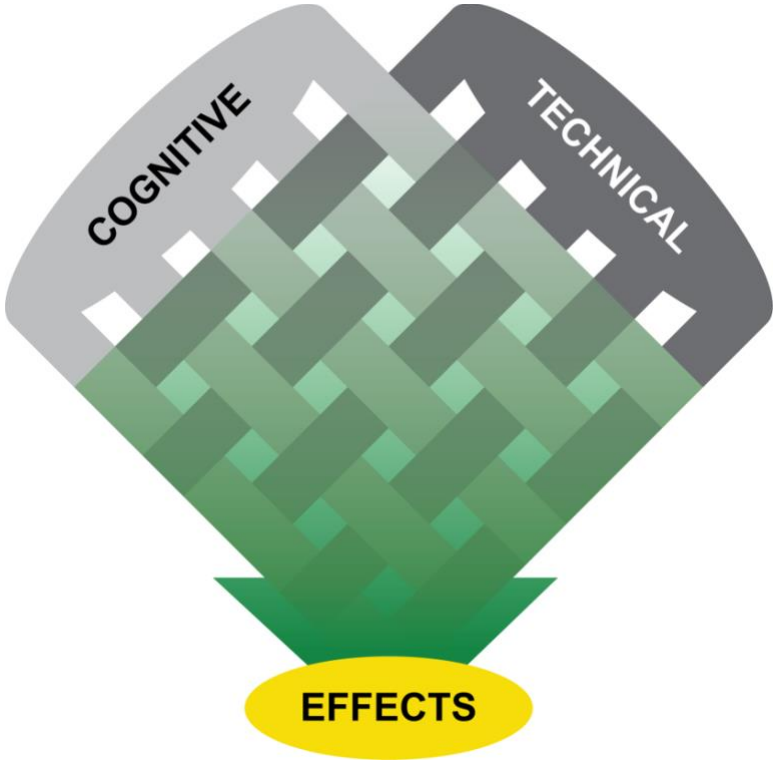

Figure 3-1. Combining Capabilities Generates Effects

[10] For a more complete discussion of the challenge of terminology to accurately represent information and influence, see A. Wanless and J. Pamment, "How Do You Define a Problem Like Influence?" *Journal of Information Warfare,* vol. 18, no. 3, pp. 1-14, 2019.

[11] Professionals who conduct influence may have different terms for some of the process, which are reinforced by centuries of thought on the topic. This framework is not intended to challenge or replace those documents, but rather to create a common point of reference for concepts and ideas needed to assess all changes in the information environment's cumulative effects on a target audience.

The second guidepost for SP!CE™ is that all aspects of planning, enabling, and executing information activities, not just information when it appears in front of an audience, must be examined. Finally, continuous assessment of each phase of an influence campaign is more useful than post facto measures of effectiveness alone.

This paper presents the characteristics of the modern information environment and decision-making process by drawing on a body of literature on human behavior and decision science, coupled with more recent developments in the field. Using that process as a base, MITRE created an influence chain that explains the steps taken in influence campaigns to affect audience behavior. Like the kinetic Find, Fix, Track, Target, Engage, Assess (F2T2EA) kill chain, and cyber kill chains, the influence chain is an integrated, end-to-end process described as a "chain" because interruption at any stage can disrupt the entire process. [1213]

MITRE presents the tactics and techniques in a matrix like the MITRE ATT&CK® framework for cybersecurity to help catalog actions using standard terminology and provide structure for an online knowledge base. MITRE's methodology to assess the performance and effectiveness of both U.S.-supported and adversary influence campaigns includes both qualitative and quantitative measures. The paper concludes with suggested actions to respond to, prevent, or deter influence campaigns and recommendations for technological development to enhance the conduct, analysis, and evaluation of influence campaigns. The appendices provide detailed scoring rubrics and assessment criteria for adversary influence campaigns and U.S. campaigns.

[12] J. A. Tirpak, "Find, Fix, Track, Target, Engage, Assess," *Air Force Magazine,* July 1, 2000,https://www.airforcemag.com/article/0700find/.

[13] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

4 Decision Making and the Information Environment

> **"Individuals and groups today have access to more information than entire governments once possessed. They can swiftly organize and act on what they learn."** *– from the Joint Concept for Operating in the Information Environment*[14]

Describing information activities and influence campaigns centers on the effect that information has on a person or group's decision to act or not act in a manner consistent with the influencer's objective. Despite dramatic increases in the technology to conduct influence activities, influencing audiences is still a human-centered phenomenon. Harold Laswell, one of the 20th century's most noteworthy influence researchers, opined that:

> "Whatever the 'ultimate' theory of communication may be, it will no doubt continue to underline the creative role of 'central process' ('brain,' 'mind') in guiding man's impact on his cultural and biological evolution."[15]

Much has changed since Laswell's day. The speed, scale, and precision with which targeted information can be delivered has increased. Information can go viral today at a speed and scale unimaginable 15 years ago, and it can be shared by people who previously would not have had a platform to achieve such reach. Artificial intelligence, social media, machine learning, and autonomous communications are tools for creating, delivering, and measuring information but do not themselves perform influence. Sophisticated tools exist to manipulate the flow, content, and accessibility of information. Echo chambers, which might only have existed due to lack of information, can now be artificially created within an environment where information is seemingly ubiquitous. This technology contributes to efficient operations, better understanding, and improved analytic fidelity, ultimately influencing campaigns targeting humans.

Whether the target audience is an individual or a group, SP!CE™ treats the human target audience as part of a system that takes information as an input, processes it into a decision, and produces observable behavior and new information as an output. When an influencer takes actions on and with information, it alters the input (information) and manipulates the output (behavior). (**Figure** 4-1). Regardless of whether the decision is to vote for a candidate, support a regime, buy a product, or invade a neighboring country, the decision is built upon the information presented to the target.

[14] Joint Staff, *Joint Concept for Operating in the Information Environment (JCOIE,)* Suffolk: Joint Chiefs of Staff, 2018,retrieved 2020 from https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf

[15] H. D. Laswell, "The Theory of Political Propaganda," *The American Political Science Review*, vol. 21, ,o. 3, pp. 627-631, Aug. 1927.

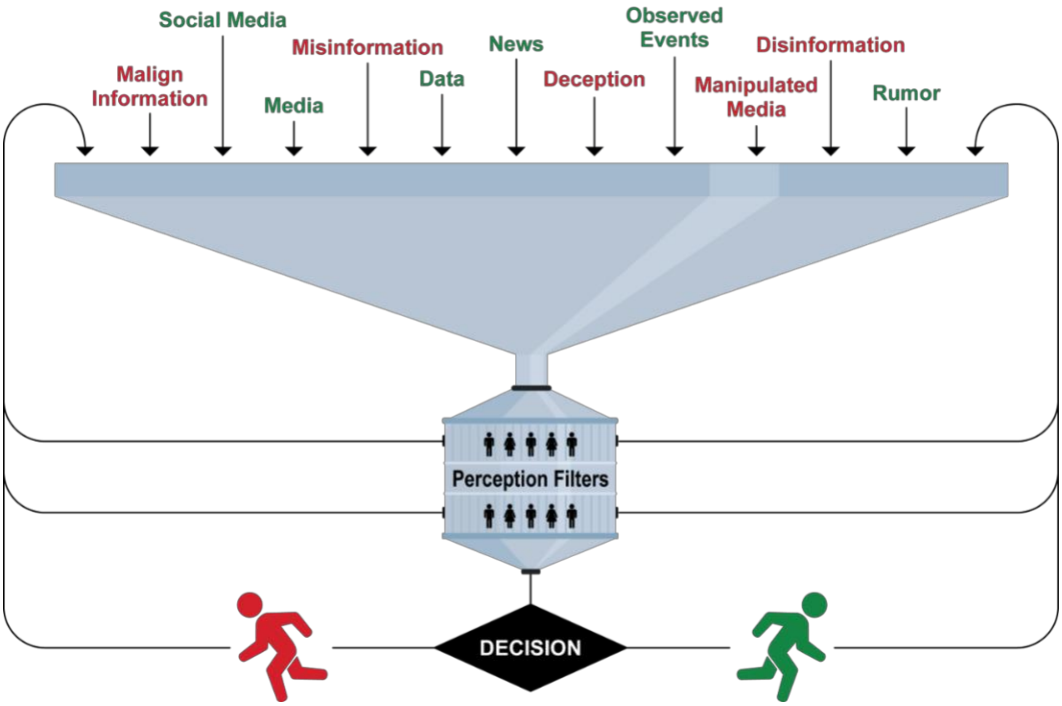

Figure 4-1. Decision Making and the Information Environment

The target audience constantly interacts with information through simultaneous information production, consumption, and processing. Using technology to manipulate the flow and content of information changes the information environment, has the potential to result in an alteration of the target's beliefs, decisions, and ultimately, behaviors. The target audience is subject to human circumstances such as bias, culture, decision heuristics, history, physical conditions, misconceptions, peer pressure, emotions, logic, and environment. These perception filters can alter both the inputs and outputs of human decision making. The behaviors exhibited by a target audience can, over time, create patterns and habits through reinforcement and repetition.

The steps in the SP!CE™ influence chain describe how influence happens within a target audience's decision-making system. The information input can be many-dimensional and complex.

4.1 Applicability to Autonomous Systems

Replacing the human target audience with an autonomous system or other technical information processing system does not alter the fundamental model. Whether accurate or manipulated, information input changes the decision system of any algorithmically designed system that replaces a human in the loop. Manipulating machine-learning training data sets can introduce the same bias and perceptual flaws that humans exhibit. Similarly, limiting or altering data flow to the decision-making system can affect the behavioral output. In short, the machines are not any less susceptible to influence campaigns than the humans who designed them or the ones that they are designated to replace.

5 The Steps in the Process—the "Influence Chain"

The term "kill chain" refers to the process a military force undertakes to achieve an objective. It is also a methodology to decompose adversary processes to disrupt or defeat their intended actions. Technologist Bruce Schneier advocated for the development of an influence kill chain because, as he states:

> "Information attacks against democracies, whether they're attempts to polarize political processes or to increase mistrust in social institutions, also involve a series of steps… These attacks have been so effective in part because, as victims, we were not aware of how they worked. Identifying these steps makes it possible to conceptualize—and develop—countermeasures designed to disrupt information operations."[16]

Influence is much broader than just military information operations, so constructing an "influence chain" is useful for understanding and assessing information campaigns. Like the kinetic F2T2EA kill chain, or the Lockheed Martin cyber kill chain, the SP!CE™ Influence Chain (**Figure** 5-1) is an integrated, end-to-end process described as a "chain" because an interruption at any stage can disrupt the entire process. The steps in the process explain how influence occurs within a target audience's decision-making system. In addition to its utility in describing adversary activities, the influence chain also provides a framework for friendly planners to design influence campaigns supporting U.S. national objectives. The methodology is consistent with DoD's *Joint Concept for Integrated Campaigning*[17] and the *Joint Concept for Operating in the Information Environment.*[18] The influence chain provides more detail on specific actions than is currently available from published military doctrine.

The influence chain steps are grouped into four main components—plan, enable, engage, and assess—each of which is described in detail below. **Figure** 5-1 depicts the flow from planning to enabling to engagement sequentially to aid understanding, but many of the steps may occur concurrently. The recursive arrows represent the revisions and adjustments made throughout a campaign as the situation and information environment change. The influence chain's recursive nature is most pronounced during the engagement phase, wherein multiple information activities co-occur, and reinforcement of information enhances the persuasive effects. Assessment is continuous throughout the process. When assessing friendly influence campaigns, significant portions of the evaluation are conducted at each component's conclusion. For the assessment of an adversary campaign, where access to the planning phase is less likely, the analyst starts at the first indication of influence activity and builds out to complete the overall campaign's picture.

[16] B. Schneier, "Toward an Information Operations Kill Chain," *LAWFARE,* Apr. 24, 2019, retrieved May 29, 2020, from https://www.lawfareblog.com/toward-information-operations-kill-chain#

[17] Joint Staff, *Joint Concept for Integrated Campaigning*, Joint Chiefs of Staff, 2018, retrieved 2020 from www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concept_integrated_campaign.pdf?ver=2018-03-28-102833-257

[18] Joint Staff, *Joint Concept for Operating in the Information Environment,* Joint Chiefs of Staff, 2018, retrieved 2020 from www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf?ver=2018-08-01-142119-830

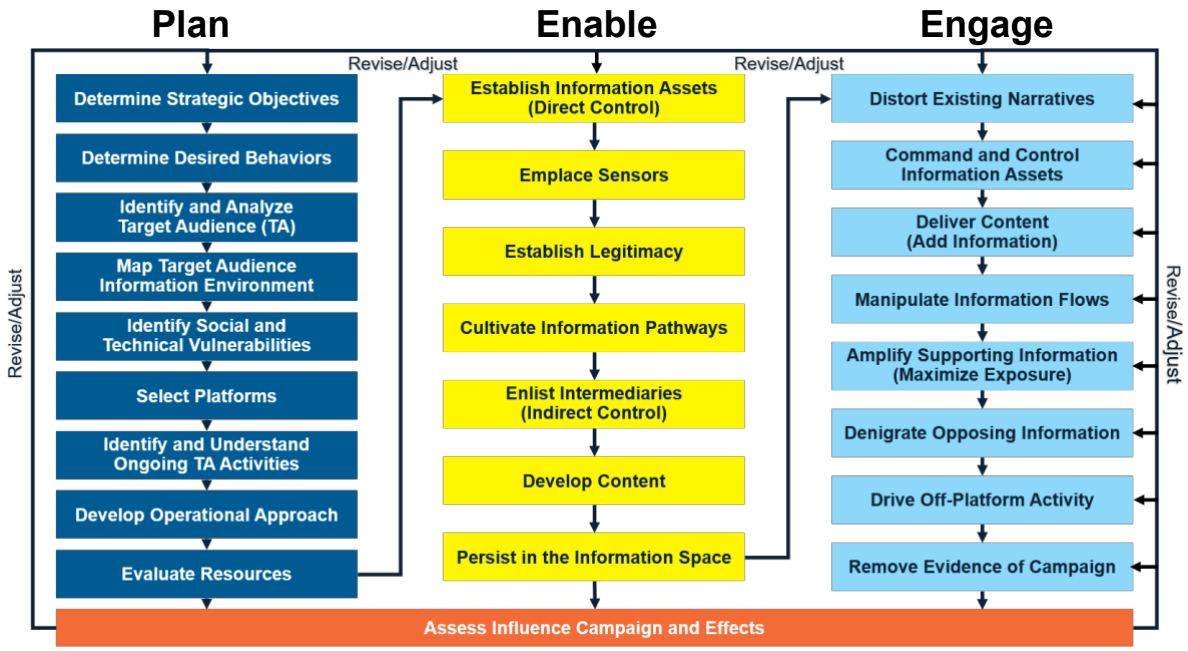

Figure 5-1. SP!CE™ Influence Chain

5.1 Planning Influence

Influence planning follows planning and targeting processes used for other U.S. and allied national security activities. These vary by department, agency, or ally. However, the steps outlined in this section integrate with standard planning processes to construct an influence campaign, as depicted in **Figure** 5-1. The evidence in the SP!CE™ knowledge base shows that adversary influence campaigns follow the process in **Figure** 5-1 as well. However, some steps may not be visible to analysts investigating a campaign until the campaign enters the enable or engage phase.

5.1.1 Determine Strategic Objectives

The first step is to determine the strategic objectives, which are the primary focus of information- and non-information-related activities to advance a state or non-state actor's interests. The strategic objectives provide the purpose behind conducting an influence campaign. Many non-information-related actions may accompany an influence campaign to achieve strategic objectives. Campaign designers use the strategic objectives as guideposts for the remainder of the campaign design. Analysts who understand an adversary's strategic objectives may discern asymmetric countermeasures to thwart the effects of an influence campaign more broadly. Examples of influence objectives include deterring aggression, making a profit, electing a candidate, or improving the economy. An objective is usually more descriptive of the desired situation at the end of a campaign than of specific behavior.

5.1.2 Determine Desired Behaviors

The desired behaviors are those actions that are most likely to lead to the desired objectives if executed by the target audience. In some cases, it may not be the behavior of the largest audience. For example, when seeking to deter cross-border aggression, it is more important to cause a military commander to direct forces to return to their garrisons than to make all soldiers abandon their equipment. While both may lead to the outcome, it is more effective to address them separately, as influence activities for each will be different. Influence is most likely to be

effective if the activities are focused on a specific, measurable, and distinct behavior. The selected measurable behavior forms the basis for the campaign's overall measure of effectiveness.

Analysts investigating adversary influence campaigns will likely infer the desired behavior from the content of information employed. When the desired behavior is known, measures can be taken to protect a vulnerable target audience from an adversary influence campaign.

5.1.3 Identify and Analyze the Target Audience

The target audience is the individual or group best positioned to modify their behavior to achieve the strategic objectives. Getting the target audience to perform the desired behavior drives every other aspect of the campaign. Social or physical characteristics (i.e., geography, language, age, gender, race, occupation, etc.) factor into selection; however, a target audience whose thoughts, beliefs, opinions, and other cognitive characteristics are closely aligned is more susceptible to influence than one solely selected on demographics. Selecting a target audience based on cognitive alignments is cognitive clustering, and it identifies those within the larger population most likely to have the same reaction if presented with similar information. The more tightly clustered an audience is, the more homogeneous their behavior will be in response to a given input. In short, it is more important that a target thinks alike than that they look alike. It is also important to note that target audiences may not always be the largest or most senior audiences related to a specific issue.

Once the target audience has been identified, campaign planners analyze the audience, seeking to determine their barriers to executing the desired behavior, social and cultural biases, and most salient issues or concerns. Further analysis specific to individual information capabilities or activities occurs below the campaign level.

This step also includes documenting an initial baseline of relevant target audience behaviors before influence activities are developed and executed. Without a baseline, it is impossible to accurately assess the behavioral changes an influence campaign intends to induce. Dedicating purpose-built assets during planning to establish this baseline allows policymakers, planners, analysts, and operators to measure the change in target audience behavior throughout the campaign and assess progress toward influence objectives and strategic goals.

5.1.4 Map Target Audience Information Environment

This step produces an audience-specific information map that displays the sources of information the target audience primarily uses and trusts. The information environment map, which is specific to the target audience, forms the cognitive terrain on which the battle of ideas occurs. For the information campaign to succeed, each identified information pathway to the target audience serves as a potential to either add new information or reduce information flow in service of the campaign's objectives. As shown in **Figure** 4-1, the target audience will output information that feeds back into their information environment, so this path is also included on their information environment map.

Micro-targeting, target systems analysis, nodal and social networking analysis, and other tools describe how the audience receives information. This allows influence activities to be planned more effectively toward the most significant information receptors for an audience (i.e., key communicators or trusted news sources, information bubbles on social media, etc.). Adversary influence campaigns generally employ multiple information pathways, so analysts cross-

correlate information from one pathway to another to help identify adversary activities' extent and penetration.

5.1.5 Identify and Analyze Social and Technical Vulnerabilities

This step illuminates opportunities to conduct more effective influence. A target audience's vulnerabilities are those that make it more susceptible to influence. Social vulnerabilities include personal, cultural, and historical biases, predispositions, rituals, and other characteristics that increase their susceptibility to influence. Technical vulnerabilities range from poor cyber hygiene, making private information publicly available to platform rules, and standards that can be exploited for influence advantage. For example, a target audience's racial bias may make them likely to believe information that reinforces their beliefs (aka confirmation bias). Technically, the same audience may be susceptible to influence on a platform that does not censor racially inflammatory content or emanates from a place out of reach of law enforcement.

5.1.6 Select Platforms

To complete this step, campaign planners choose those platforms on which to employ information activities. This includes both the platforms that will be used to add information to the environment and those that must be restricted to accomplish the influencer's objective. The goal is to select platforms that maximize reach into the target audience, contain necessary technical vulnerabilities, and to which the influencer has or can have access. Constraints of access or resource limitations make the selected platforms a subset of the entire information map.

An information campaign may analyze platform algorithms to determine which to utilize based on content promotion, fact-checking technology, and other factors. Often, platform algorithms can aid information campaigns by creating "echo chambers," online environments where users are exposed to content that reinforces their views. Human psychological weaknesses, such as confirmation bias and the illusory truth effect, amplify echo chambers' effect.

5.1.7 Identify and Understand Ongoing Target Audience Activities

This step, also called strategic listening, involves monitoring a target audience to determine the issues at hand, the tone and tenor of conversations, and the identifying characteristics shared between members of the audience to authenticate one another. Establishing a credible voice with the target audience is essential to influence and may even be a pre-condition for admission into closed groups. Success in this step relies heavily on the target audience analysis previously conducted. A cohesive group or community of like-minded individuals often prefers, and indeed protects, a safe environment where they feel they can reveal a bit more, test theories without backlash or retribution, be among the first to hear breaking news, or share fresh ideas with others who share their views.

From this step, the influencer can design information to be presented to the target audience that gains their trust through shared opinions, ideas, and topics. People tend to join groups around topics they are passionate about and subjects they are interested in; building the appearance of shared passion and interest is a catalyst for engagement and gaining access.

5.1.8 Develop Operational Approach

This step creates the information campaign's conceptual framework, including framing the situation and orchestrating the sequence and timing of significant portions of the information

campaign to maximize their combined effect. Organizations and individuals assigned to carry out information activities follow the operational approach to develop detailed plans for individual actions. Essential components of the operational approach include the main themes and types of information to promote or deny to the audience, the barriers to performing the desired behavior to overcome for the campaign to be successful, and the sensor strategy to collect data about the audience and their reactions to information activities. Developing the operational approach is a critical step for friendly planners. It is useful for analysts to evaluate an adversary campaign, as a thorough understanding of the adversary's operational approach lends predictive power to analytic judgments.

5.1.9 Evaluate Resources

To complete this step, planners evaluate both the traditional funding and equipment resources and, more important, the information and cognitive resources available. Information resources include access to platforms, raw data, previously emplaced information assets, aged accounts, existing information infrastructure, or media outlets. Resources also include any relationships with key communicators and other existing means of amplifying. Access to the information pathways that will be blocked or disrupted is especially noteworthy.

5.1.10 Assess Plan Phase

In this step, each of the previous nine steps in the chain is evaluated and scored. When the United States is conducting influence, planners assess before starting information activities. From that assessment, planners revisit previous steps as necessary to improve the plan. The scoring rubrics in Appendix A (table A-1) provide the minimum criteria to consider each step successful and thresholds to meet that add higher confidence levels in the plan.

Assessing adversary planning activities will likely come later because most adversary planning is undetectable. When assessing adversary influence, Appendix B's table B-1 criteria reflect how well an analyst understands an adversary's influence campaign. Higher levels of understanding are necessary for more effective protective and countermeasures.

5.2 Enabling Influence

Enabling activities are necessary precursors to conducting influence activities against a target audience. For the actor conducting the influence campaign, these steps supply essential access to the target audience and adequate coverage of the information spectrum. For analysts attempting to assess adversary influence, enabling activities represent significant indicators of imminent adversary influence activity. Detecting enabling activities is crucial to pre-emption or mitigations of adversary influence campaigns.

Enabling influence is the informational equivalent of military forward basing. Occurring both clandestinely and overtly, forward basing can signal capability and intent, establish proximate access to a disputed domain, and provide options in the event of a conflict.

Effective influence operations take a similar approach in the cognitive and cyberspace domains. Russian media manipulation through Facebook by posting stories, buying content, and trolling comments to influence American political processes did not happen overnight. Russian actors set up a presence on Facebook well in advance by creating account profiles, pages, groups, events,

and content.[19] The Russians "forward-based" information forces in chat rooms, on Facebook, and in Twitter accounts. They also established themselves as legitimate distributors of press releases and other information to traditional media outlets with routine news and information before the commencement of active operations to influence U.S. audiences. By engaging in relatively benign public discourse within U.S. media, they created freedom of movement in the information space. They attained on-demand access to the American cognitive domain to conduct influence. The open nature of U.S. media and personal information for sale from social media providers facilitated Russian access. It would be far more challenging for an influence campaign targeting a country where restrictive privacy laws (like those in the E.U.) or outright blockage of external content (as exists behind China's great firewall) were in place. Therefore, U.S. and allied influence campaign planners must give extra attention to enabling activities.

While separate from the much-needed persistence and access in the cyber domain, establishing persistent access to the cognitive domain is enabled by, and increasingly dependent on, operations in and through cyberspace. Within DoD, the relationship between Cyberspace Operations and Information Operations is both an interdependency and a hierarchy; cyberspace is a medium through which other information activities and capabilities may operate. Cyberspace operations and capabilities create effects in the information environment.[20]

Forces in close (cognitive) proximity to the adversary can deliver influence effects in a prompt and mission-relevant manner. Given the fast-paced cycle of reporting and audience consumption of news in the Information Age, where many stories compete for attention before they fade from relevancy, developing access to the target audience's cognitive space is essential. Early access development is especially crucial when establishing a credible presence within a foreign-owned and -operated information platform. Establishing and keeping a forward presence in the cognitive domain can be more difficult than establishing physical presence due to the alterability of the information terrain and lower costs for adversaries to counter these access points than to remove physical bases abroad.

The enabling phase steps described below detail the actions necessary to establish and maintain a cognitive forward base supporting an influence campaign. Although this phase has the fewest steps, accomplishing them has the most significant impact on influence campaign accomplishment.

5.2.1 Establish Information Assets (Direct Control)

In this step, the influencer emplaces the assets that they will directly control throughout the campaign. They may include setting up social media accounts, establishing web presences, buying internet and physical advertising space, moving electronic attack assets, co-opting media outlets, and establishing cyberspace access, embedded journalists, or even complete media outlets. The influencer places information assets into existing information paths known and used by the target audience, because establishing a completely new path is usually cost and time prohibitive. The Chinese Communist Party established an elaborate network of proxies, front organizations, and media outlets outside of China to unify overseas Chinese, quell dissent, and

[19] *Report of the Select Committee on Intelligence, United States Senate on Russian Active Measures Campaigns, and Interference in the 2016 U.S. Election. Volume 2: Russia's Use of Social Media with Additional Views*, retrieved July 15, 2020, from https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures .

[20] Joint Staff, *Cyberspace Operations*, Joint Chiefs of Staff, 2018, retrieved 2020 from www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

tame debate on China. President Xi Jinping refers to this work as the "magic weapon" for the Chinese people's great rejuvenation.[21] Iran maintains 37 news and information websites to promote its interests abroad without open acknowledgment of their association with the Iranian government. Many of these sites produce English-language content under innocuous names like usjournal.net and newsstand7.com[22]

5.2.2 Emplace Sensors

An information sensor is a device, module, machine, subsystem, or activity whose purpose is to detect events or changes in the information environment. Sensors include electronic sensors on networks and survey instruments administered manually. Within an information campaign, sensors detect the target audience's activities and sentiments, reveal media usage changes, gather feedback on information activities, look for evidence of counter-information in the environment, and reveal the presence of opposing information assets. According to a 2019 Oxford University inventory, 70 countries conduct organized social media manipulation, more than half of which have permanent monitoring capabilities in place.[23]

5.2.3 Establish Legitimacy

Actions to increase the likelihood that the target audience perceives information as credible establish the influencer's legitimacy. Some activities in this step are relatively benign, such as using the target audience's local language and dialect. Other activities may be more nefarious, such as impersonating an expert in the field or establishing a phony organization with an official-sounding title. In the run-up to the 2020 Taiwan elections, China created online accounts that appeared to represent independent think tanks and other regionally focused independent organizations to spread information that supported China's position.[24] In eastern Ukraine, Russian-controlled outlets posed as local partisan groups to increase their legitimacy with the population.[25]

5.2.4 Cultivate Information Pathways

In this step, the influencer takes action to increase the diversity of pathways through which information can travel to the target audience. Information campaigns build new outlets to increase the percentage of the target audience reached and increase delivery mechanisms' diversity. This step enables the influence campaign to engage the maximum portion of the target audience and control the highest number of information conduits. It allows the influence campaign to deliver tailored, audience-relevant content or pre-emptively defend against adversary attempts to disrupt the campaign. To bolster its ongoing anti-NATO influence

---

[21] A. Brady, *Magic weapons: China's political influence activities under Xi Jinping,* Washington, DC: Wilson Center, 2017, hhttps://www.wilsoncenter.org/sites/default/files/media/documents/article/magic_weapons.pdf

[22] FireEye, Inc., *Suspected Iranian Influence Operation Leveraging Inauthentic News Sites and Social Media Aimed at U.S., U.K., Other Audiences,* Milpitas, CA, 2018, https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-FireEye-Iranian-IO.pdf

[23] S. Bradshaw and P. N. Howard, *The Global Disinformation Order: 2019 Global inventory of organized social media manipulation,* Oxford, UK: Computational Propaganda Research Project, 2019, https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf

[24] B. Nimmo et al., "Secondary Infektion," *Graphika*, 2020, https://secondaryinfektion.org/downloads/secondary-infektion-report.pdf

[25] M. Kofman, K. Migacheva, B. Nichiporuk, A. Radin, O. Tkacheva, and J. Oberholtzer, *Lessons from Russia's operations in Crimea and Eastern Ukraine*, RAND Corporation, 2017

campaign, Russia established accounts on Facebook, Twitter, YouTube, Medium, Tumblr, Reddit, Telegram, Pinterest, Wordpress, Blogspot, and other smaller sites.[26] All of these accounts shared content and reinforced one another's messages with supporting information. In its efforts to sway American public opinion, China initiates messages on state-run media. A network of social media accounts combines with paid advertisements to expand the pro-Chinese message's reach beyond the original sources.[27]

5.2.5 Enlist Intermediaries (Indirect Control)

At this step in the process, the influencer connects to individuals, groups, or information assets outside of direct control that will either further disseminate the campaign's content or produce amplifying or supportive messages of their own. Intermediaries may include local influencers, celebrities, subject matter experts, or powerful voices within the community. The influencer may also have automated reposting accounts (aka amplifier bots), useful idiots, or like-minded groups within the target audience's information environment. In response to the 2019 Hong Kong protests, China enlisted organized groups of "fangirls" known for their online passion and crazy off-line stunts to support pop culture icons over whom they obsess.[28] These fangirls brought with them a sizable following and a furious pace of online posting when they began to denounce young people who were protesting. Journalists are often unwitting intermediaries. In a study of domestic radical organizations, Donovan and Friedburg (2019) found that organizations often packaged materials with ready-made graphics, evidence, and bombastic headlines that enticed journalists to use material without revision.[29]

5.2.6 Develop Content

In this step, the influencer generates previously nonexistent information or repackages and repurposes existing information. New content can be simple memes, complex news stories, or purpose-built deepfake media.[30] Any information that the influencer intends to present to the target audience is content. As the campaign develops and the target audience responds to the initial content delivered, the influencer may return to this step to generate new content or modify previously used content. Beyond the well-documented activities of the Russian Internet Research Institute's troll farms, influencers are devising new techniques to develop content rapidly. Chinese content producers use artificial intelligence to generate massive volumes of content with a system that crawls the internet, gathering articles and posts, then reorganizes the words and sentences into thousands of new items per day.[31]

---

[26] B. Nimmo et al., "Secondary Infektion," *Graphika*, 2020, https://secondaryinfektion.org/downloads/secondary-infektion-report.pdf

[27] Insikt Group, "Beyond Hybrid War: How China Exploits Social Media to Sway American Opinion," *Recorded Future,* 2019, https://go.recordedfuture.com/hubfs/reports/cta-2019-0306.pdf

[28] Insikt Group, "Chinese Influence Operations Evolve in Campaigns Targeting Taiwanese Elections, Hong Kong Protests," *Recorded Future,* 2020, https://go.recordedfuture.com/hubfs/reports/cta-2020-0429.pdf

[29] J. Donovan and B. Friedberg, *Source hacking: media manipulation in practice,* Data & Society Research Institute, retrieved from Informit Analysis and Policy Observatory (APO), 2019, https://search.informit.org/documentSummary;res=APO;dn=257046

[30] "Deepfake is a term for videos and presentations enhanced by artificial intelligence and other modern technology to present falsified results. One of the best examples of deepfakes involves the use of image processing to produce video of celebrities, politicians or others saying or doing things that they never actually said or did." "Deepfakes," Technopedia.com, retrieved from https://www.techopedia.com/definition/33835/deepfake

[31] Insikt Group, "Chinese Influence Operations Evolve in Campaigns Targeting Taiwanese Elections, Hong Kong Protests," *Recorded Future,* 2020, https://go.recordedfuture.com/hubfs/reports/cta-2020-0429.pdf

5.2.7 Persist in the Information Space

This step in the process includes actions that allow the influencer's assets to operate without detection or be considered legitimate participants within an existing information channel. For traditional broadcast media, persistence may include ensuring that no one jams their signals or censors content. In social media, actions include steps to evade detection by platforms and providers whose algorithms attempt to identify inauthentic behaviors. Chinese actors use a technique called "Spamouflage" to hide their controversial content within a large volume of innocuous content such as landscape photos or weather sightings.[32] To evade detection, Russian social media accounts are either artificially "aged" to present a seemingly long history of existence or hijacked from well-established accounts.[33]

5.2.8 Assess Enable Phase

Each of the enable phase's seven steps in the influence chain is evaluated and scored. When the United States is conducting influence, influencers assess before starting engagement activities. From that assessment, the influencers revisit previous steps as necessary to ensure that conditions for the most effective engagement are in place. The scoring rubrics in Appendix A (table A-2) provide the minimum criteria to consider each step successful and thresholds to meet that add higher confidence levels.

Assessing adversary enabling activities can begin immediately upon detection. When assessing adversary influence, Appendix B's table B-2 criteria reflect how well an adversary is prepared to conduct influence. Disrupting an adversary's enabling phase is the most likely to disrupt the entire campaign.

5.3 Engaging the Audience

Simultaneously affecting multiple aspects or elements of the information environment along multiple information pathways is the key to successful influence. Influence campaigns combine the technical and cyber actions taken on information systems and the persuasive cognitive effects information exerts on humans (Figure 3-1). The technical effects on information manipulate the flow, content, or composition of information as it exists in the information environment. The effects of information change the perceptions, emotions, and objective reasoning within the target audience. For example, to deceive an enemy commander into believing that an attack from the north is imminent, false reports from sentries on the northern flank may lead to a desired behavior such as removing forces from southern defensive positions. A single influence activity that leaves backdoors open to competing information is insufficient in the highly contested and information-saturated modern world. Instead, the influencer must account for and affect multiple information streams simultaneously. For example, the north's misleading reports cannot succeed unless the visible presence of forces in the south is masked and the link to overhead imagery is severed. The eight steps of the engage phase described below are mutually reinforcing and frequently co-occur.

[32] B. Nimmo et al., "Secondary Infektion," *Graphika*, 2020, https://secondaryinfektion.org/downloads/secondary-infektion-report.pdf

[33] E. Bodine-Baron, T. C. Helmus, A. Radin, and E. Treyger, *Countering Russian social media influence,* RAND Corporation, 2018.

5.3.1 Distort Existing Narratives

This step involves information activities designed to disrupt the information status quo. Enhancing confusion, sowing doubt, triggering bias, inflaming emotions, and questioning assumptions create opportunities to present new information and ideas to the target audience. The turbulent information environment created in this step reduces the target audience's perceived barriers to the behavior.[34] This step also seeks to increase target audience participation and activity around a specific topic. A 2020 Institute for Public Relations study found that 20 percent of Americans "rarely" or "never" check alternative information sources.[35] Russia and other malicious actors distort existing narratives on race, politics, healthcare, and a wide range of topics with fake entities, false grassroots movements, and effective hack, forge, and leak operations to hypercharge the marketplace of ideas.[36]

5.3.2 Command and Control Information Assets

Throughout the campaign, the influencer must orchestrate information actions in time and space to ensure maximum effectiveness. In this step, the influencer uses various techniques to guide and direct the campaign either directly or through proxies. Public relations firms, military units, fake companies, and algorithmic programs can all keep the campaign synchronized. Techniques to command and control information activities vary widely by actor and campaign. A single Russian case officer used Skype to prescribe the content and editorial decisions of three editors of news websites in the Baltic states.[37] In contrast, the United Work Front Department of the Chinese Communist Party manages a global network with tight centralized control.[38]

5.3.3 Deliver Content

This step introduces new or existing information from outside of the target's current environment. It aims to introduce information to the target audience on as many channels identified in the information environment map created during planning as possible. Content introduced in this step persuades the target to perform the behavior with reason, logic, and emotion.[39] It focuses on changing attitudes, perceptions, and beliefs. Content delivered in this step links to content in later steps that reinforce supportive opinions, while others castigate

---

[34] The importance of empowering the target is most strongly associated with the Theory of Planned Behavior. For further discussion of the theory and its application, see I. Ajzen, "The theory of planned behavior," *Organizational Behavior and Human Decision Processes,* vol. 50, pp. 179-211, 1991.

[35] T. McCorkindale, *2020 IPR Disinformation in Society Report,* Institute for Public Relations, 2020, https://instituteforpr.org/wp-content/uploads/Disinformation-In-Society-2020-v6-min-1.pdf

[36] R. Diresta and S. Grossman, *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014-2019,* Stanford Internet Observatory, 2019, https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/potemkin-pages-personas-sio-wp.pdf

[37] H. Roonemaa and I. Springe, "This is How Russian Propaganda Actually Works in the 21st Century," BuzzFeed News, Aug. 31, 2018, https://www.buzzfeednews.com/article/holgerroonemaa/russia-propaganda-baltics-baltnews

[38] A. Searight, *Countering China's Influence Activities: Lessons from Australia*, Center for Strategic and International Studies, 2020, retrieved from Informit Analysis and Policy Observatory (APO) https://search.informit.org/documentSummary;res=APO;dn=307243

[39] Theories of persuasion abound, from Social Judgement and Elaboration Likelihood to Theories of Reasoned Action, Expectancy-Value, and Cognitive Dissonance. It is not the intent of this paper to engage in a debate over the correct theory of persuasion, but rather to acknowledge that persuasive information is a portion of the information environment and its efficacy must be measured.

opposing views.[40] Many influencers follow the Russian model of delivering content openly through attributed news sources that they rebroadcast, repurpose, and deliver through user-generated media sites where non-Russia-affiliated information providers can pick it up.[41]

5.3.4 Amplify Supporting Information (Maximize Exposure)

This step includes information actions to create a perception in the target audience that most of the population supports the influencer's desired behavior. Its techniques range from automated reposting that popularizes a topic to pushing information from fringe outlets into mainstream media. Intermediaries enlisted during the enable phase are most active during this step. This step aims to normalize the behavior within the target audience. It is essential, especially when the behavior is dramatically different from the target's earlier actions—for example, indoctrinating terror group members to become suicide bombers or changing from supporting a regime to opposing it.[42] Many influencers use automated bot accounts to amplify published content that reinforces their objective. Chinese-developed software called "Cross Border Cloud/Mass Management System" allows users to batch manage thousands of social media accounts at once.[43] Besides bots, Russian influencers have used false think tanks and journals with names like "The Strategic Culture Foundation" to further distribute their messages without attribution to the Russian state.[44]

5.3.5 Manipulate Information Flow

This step includes actions that affect the flow, content, or composition of information to manipulate information flow to and from the target audience. Some actions in this step eliminate information so that it is not present in any information environment. Other actions may alter existing information before introducing it into the environment—for example, Man-in-the-Middle Attack[45] or Deepfakes.[46] Activities may also include those that prevent the target audience

---

[40] An example from technology: If social bots advocating a certain opinion spread over a network, this could lead to the false impression that the "bot opinion" is shared by more humans than it really is. Consequently, people who agree with this opinion gain the confidence to speak about it publicly, while those who disagree keep silent out of fear of being socially isolated—this is the Spiral of Silence theory. See B. Ross, L. Pilz, B. Cabrera, F. Brachten, G. Neubaum, and S. Stieglitz, "Are social bots a real threat? An agent-based model of the spiral of silence to analyze the impact of manipulative actors in social networks," *European Journal of Information Systems,* vol. 28, no. 4, pp. 394-412, 2019,retrieved from https://doi.org/10.1080/0960085X.2018.1560920

[41] T. C. Helmus et al., *Russian Social Media Influence*. RAND Corporation, 2018

[42] For an explanation of this type of conditioned behavior, see Hafez, M. M., "Rationality, Culture, and Structure in the Making of Suicide Bombers: A Preliminary Theoretical Synthesis and Illustrative Case Study," *Studies in Conflict & Terrorism*, vol 29, no. 2, pp. 165-185, 2006

[43] Insikt Group, "Chinese Influence Operations Evolve in Campaigns Targeting Taiwanese Elections, Hong Kong Protests," *Recorded Future,* 2020, https://go.recordedfuture.com/hubfs/reports/cta-2020-0429.pdf

[44] Global Engagement Center, *GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem; 2020 ASI 7008-84,* Washington, DC: U.S. Department of State, 2020, https://statistical.proquest.com/statisticalinsight/result/pqpresultpage.previewtitle?docType=PQSI&titleUri=/content/2020/7008-84.xml

[45] "In cryptography and computer security, a man-in-the-middle attack (MITM), also known as a hijack attack is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other." "Man-in-the-middle attack," Wikipedia, retrieved from https://en.wikipedia.org/wiki/Man-in-the-middle_attack

[46] "Deepfake is a term for videos and presentations enhanced by artificial intelligence and other modern technology to present falsified results. One of the best examples of deepfakes involves the use of image processing to produce video of celebrities, politicians or others saying or doing things that they never actually said or did." "Deepfakes," Technopedia.com, retrieved from https://www.techopedia.com/definition/33835/deepfake

from accessing existing information—for example, censorship or electronic jamming. Finally, some actions will cause the target to be unable to use the information presented—for example, cognitive information overload, or physical overloads like a stack[47] or buffer[48] overflow. The cumulative effects of manipulating information flows create an environment in which a member of the target audience encounters only beliefs or opinions that coincide with the desired behavior. This step aims to isolate the target audience by creating an echo chamber where information constantly reinforces supportive views and makes alternative ideas unavailable. Manipulating information flow includes technical means like the Great Firewall of China[49] and other means such as fining U.S. International Broadcasting and intimidating journalists in Russia.[50]

5.3.6 Denigrate Opposing Information

This step reduces the appeal of any information contrary to the desired behavior that reaches the target audience. Manipulating information flow may not isolate the target audience entirely or may not be sustainable for long periods. Actions taken during this step complement action in the amplify supporting information step by showing a negative consequence of failing to perform the behavior or associating negative attributes to information that contravenes the desired behavior. According to Oxford University's 2019 report on computational propaganda, 26 different countries employ techniques to suppress, discredit, or drown out competing information, with most using these techniques both within their countries and externally.[51] Iranian actors frequently and acridly denounce those who oppose the regime as "un-Islamic" or "agents of the American Satan."[52]

5.3.7 Drive Off-Platform Activity

This step aims to convert the attitudes, perceptions, and beliefs created during the previous steps into behaviors in the physical environment. When some of the target audience begins the physical behaviors elicited in this step, it reinforces support for the behavior in other members of the target audience. For example, when members of the target audience see others demonstrating in the streets against the current government, their perception of the government's competence will diminish. Influencers also use offline activities to damage opponents. In response to the

[47] "A stack overflow is a runtime error that happens when a program runs out of memory in the call stack. The stack overflow generally signals a problem in resource provisioning and has to be fixed to allow the program to run and use memory properly." "Stack Overflow, Technopedia.com, retrieved from https://www.techopedia.com/definition/9522/stack-overflow

[48] "A buffer overflow occurs when more data are written to a buffer than it can hold. The excess data is written to the adjacent memory, overwriting the contents of that location and causing unpredictable results in a program. Buffer overflows happen when there is improper validation (no bounds prior to the data being written). It is considered a bug or weakness in the software." "Buffer Overflow," Technopedia.com, retrieved from https://www.techopedia.com/definition/2760/buffer-overflow

[49] Committee to Protect Journalists, *One Country, One Censor: How China undermines media freedom in Hong Kong and Taiwan,* 2019, https://cpj.org/?p=36113

[50] T. Kent, *Striking Back*, The Jamestown Foundation, 2020

[51] S. Bradshaw and P. N. Howard, *The Global Disinformation Order: 2019 Global inventory of organized social media manipulation*, Oxford, UK: Computational Propaganda Research Project, 2019, https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf

[52] E. T. Brooking and S. Kianpour, *Iranian Digital Influence Efforts: Guerrilla Broadcasting for the Twenty-First Century,* Atlantic Council, 2020, https://www.atlanticcouncil.org/wp-content/uploads/2020/02/IRAN-DIGITAL.pdf

Hong Kong protests, the Chinese government secretly sponsored HKLeaks, which doxed[53] many of the protesters—some were physically attacked, and others lost jobs.[54]

5.3.8 Remove Evidence of the Campaign

After the campaign, the influencer removes the assets previously created and any links that may attribute information activities to their sponsor. This step aims to ensure that the target audience is unaware of any manipulation and prevent opposing nations or entities from taking action against the influencer.

5.3.9 Assess Engage Phase

Each of the engage phase's eight steps in the influence chain is evaluated and scored. When the United States is conducting influence, influencers assess continuously throughout the engagement phase, revisiting, revising, and reinforcing steps to maximize their impact. The scoring rubrics in Appendix A (table A-3) provide the minimum criteria to consider each step successful and thresholds to meet that add higher confidence levels. They are useful to measure the performance of the campaign and highlight areas for improvement.

Assessing each adversary engage step begins immediately upon detection. When assessing adversary influence, Appendix B's table B-3 criteria reflect how well coordinated an adversary's campaign is and point to areas where the campaign's weaknesses are exploitable. Disrupting an adversary's engagement phase is the most challenging because it requires competition between information activities in front of the target audience.

[53] Doxing (sometimes written as doxxing) is the act of revealing identifying information about someone online, such as their real name, home address, workplace, phone, financial, and other personal information.

[54] Insikt Group, "Chinese Influence Operations Evolve in Campaigns Targeting Taiwanese Elections, Hong Kong Protests," *Recorded Future,* 2020, https://go.recordedfuture.com/hubfs/reports/cta-2020-0429.pdf

6 Assessments

Besides the assessments completed with each phase of an influence campaign, SP!CE™ provides a methodology for overall campaign evaluation.[55] After assessing each campaign phase, planners, operators, and analysts evaluate the entire campaign using SP!CE™ methodologies to calculate the campaign's conduct and impact. Both conduct and impact assessments create numerical scores.

6.1 Evaluating Information Campaign Conduct

The campaign score (C_S) is a subjective analysis of campaign design and execution. It measures the performance of the influencer who owns the campaign. When calculated, C_S yields a percentage. Scores of 80 percent and above indicate a campaign that is well designed and executed. These high-scoring campaigns have the greatest potential for impact. Campaigns scoring between 40 and 79 percent have flaws that can be improved by the influencer or exploited by an opponent. A campaign scoring below 40 percent is least likely to be effective without major revision. More importantly than the score itself, the campaign evaluation process is valuable in thinking critically about the campaign's strengths and weaknesses.

6.1.1 Calculating the U.S. or Allied Influence Campaign Score

To calculate friendly C_S, evaluate each step in the influence chain using the tables in Appendix A. The assessor considers other friendly influence activities under their government's control as they contribute to completing a step. The assessor selects the statement in Appendix A's table that best describes how the campaign performed that step and assigns the corresponding score. Record each score to represent the results graphically. The example chart (**Figure** 6-1) colors a step's box to correspond with its assessed score: Red = 1, Yellow = 3, Green = 5. Lower individual step scores highlight areas to add resources, increase levels of effort, or alter the approach. The assessor records the step scores in a chart similar to **Figure** 6-1. The assessor divides the sum of the step scores by 120 to determine C_S.

$$C_S = \frac{\sum_{n=1}^{24} Step\ score}{120}$$

[55] DoD defines an assessment as a "continuous activity that supports decision making by ascertaining progress toward accomplishing a task, creating an effect, achieving an objective, or attaining an end state for the purpose of developing, adapting, and refining plans and for making campaigns and operations more effective." Joint Staff, *JP 5-0, Joint Planning*, Joint Chiefs of Staff, 2018, retrieved 2020 from www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp5_0_20171606.pdf

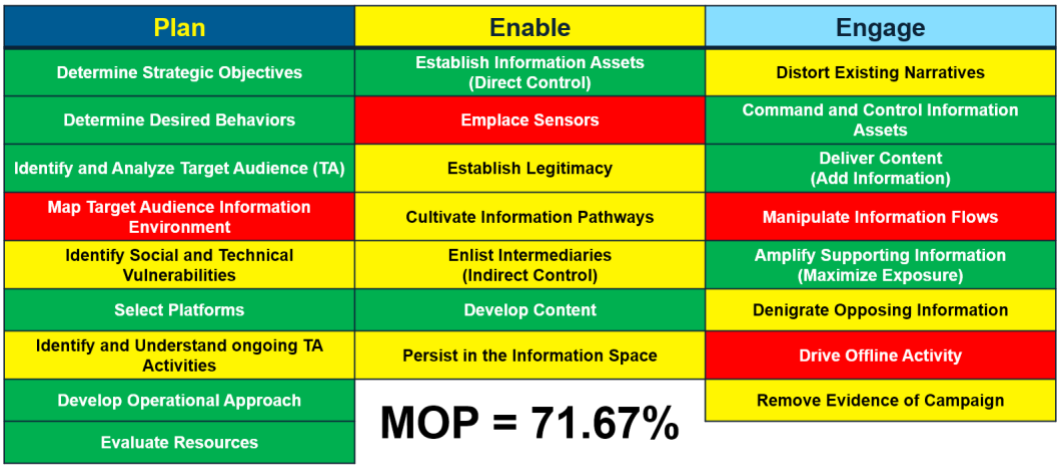

Figure 6-1. Example Friendly Campaign Results

Reviewing the assessment results, planners, policymakers, and operators conducting influence can refine and adjust a campaign to increase efficiency. Individual step scores point to areas that need further development, are poorly performed, need additional resources, or require innovative approaches to dominate an audience's information environment more successfully. Additionally, campaign assessments point to areas where the activities of other friendly actors, echelons, or other departments or government agencies are required.

6.1.2 Calculating Adversary Influence Campaign Score

When adversary influence activities are detected, analysts work laterally throughout the framework to fully describe and assess an adversary's campaign. For example, an adversary using a falsely attributed account to deliver content about the attractiveness of a behavior is probably simultaneously trying to block or otherwise degrade the flow of information about the alternative to that behavior. Analysts who have only found one of the instances can piece together the totality of the campaign, as each new instance helps to show a portion of the adversary's targeting and desired behaviors. Once sufficient pieces of the puzzle come together, the analyst calculates the adversary campaign score (C_S) similarly to friendly calculations, adjusting for unknowns.

To calculate the adversary C_S, the assessor determines which steps in the influence chain have sufficient evidence to confirm or infer activities that the adversary has conducted. For each confirmed step, the assessor evaluates the step using the tables in Appendix B. The assessor selects the statement in Appendix B's table that best describes how the campaign performed that step and assigns the corresponding score. Record each score to represent the results graphically. The example chart (**Figure** 6-2) colors a step's box to correspond with its assessed score: Red = 1, Yellow = 3, Green = 5, Black = insufficient data to assess. Assessments of adversary campaigns help focus resources on detecting other campaign activities and point to the areas where a campaign is most likely to be effectively countered. More importantly than the score itself, the campaign evaluation process is valuable in thinking critically about the adversary campaign's vulnerabilities. Higher step scores highlight areas of adversary strength that may require significant effort to counter. Lower step scores are areas of adversary weakness that friendly influencers may seek to exploit. The assessor records the step scores in a chart similar to

Figure 6-2. The assessor divides the sum of the step scores by five times the number of steps evaluated to determine the C_S.

$$MOP = \frac{\sum_{n=1}^{\#\ Steps\ evaluated} Step\ score}{5(\#\ Steps\ evaluated)}$$

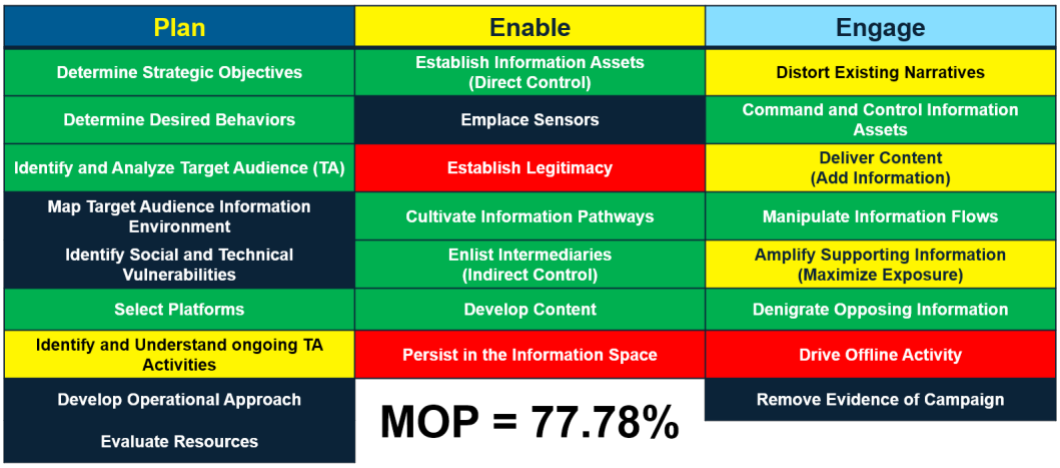

Figure 6-2. Example Adversary Campaign Results

6.2 Evaluating Campaign Impact—Key Performance Indicators

The impact score (K) evaluates the impact that the influence campaign had on the target audience. The score can be positive (successful), zero (neutral), or negative (failing). The impact score is an objective score composed of six key performance indicators (KPI): penetrate, isolate, activate, resonate, persuade, and motivate. **Figure** 6-3 shows the influence campaign's target audience identified during planning and the six KPI of the impact score; some are external forces acting on the target audience, while others operate within it.

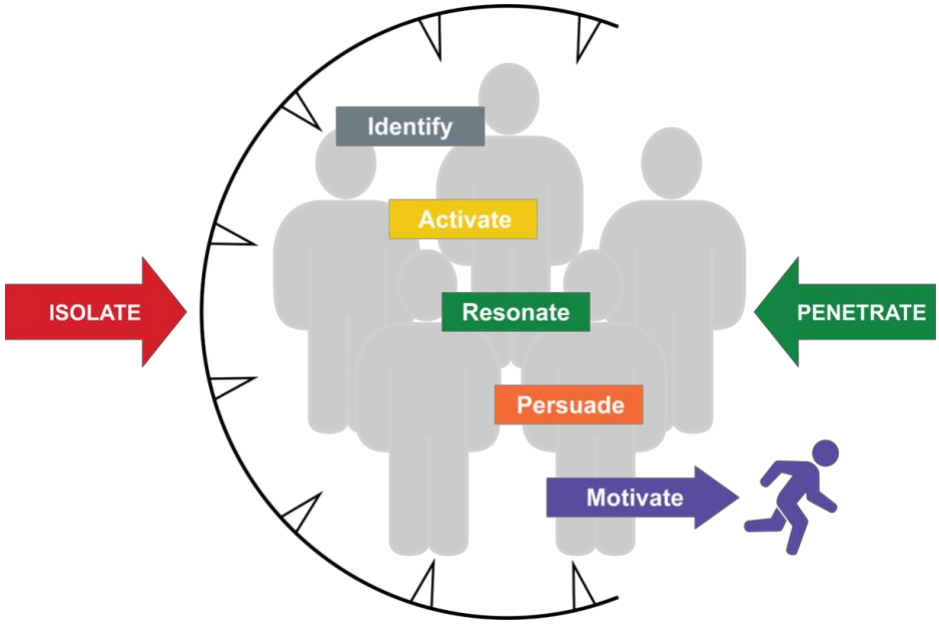

Figure 6-3. Impact Score Key Performance Indicators (KPI)

6.2.1 Calculating Influence Campaign Impact Score

The assessor uses the same calculations for adversary or friendly campaigns since the impact score focuses on the target audience, not the influencer. Assessors gather data to calculate each KPI's score separately. The six scores help the influencer determine the reason for success or failure in a campaign more accurately than merely observing the target audience's behavior. The total impact score (*K*) is a weighted average of the element scores. The assessor calculates the impact score at regular intervals to track the change over time. Below are the formulas to calculate each score (T.A. = Target Audience).

6.2.1.1 Penetrate

Increasing the portion of the target audience exposed to an influence campaign improves its effectiveness. The penetrate score measures the amount of the target audience receiving campaign-directed or supporting information.[56] It is similar to "reach," which is a term used in marketing, but it is focused only on the designated target audience and not a broader population. The term *impressions* refers to the number of times during the reporting period that the target audience encountered the information. It may be once for a fleeting social media post or every day during the reporting period for information that is in constant view or is repeatedly transmitted. Lower penetrate scores most often result from deficiencies in the "Cultivate Information Pathways," "Select Platforms," "Deliver Content," and "Amplify Supporting Information" tactics and techniques in the SP!CE™ framework. Adjusting those activities is the most effective way to raise the friendly Penetrate score and countering activities in those tactics the most effective way to reduce an adversary's penetrate score.

Penetrate (*P*) =

$$\frac{\sum_{n=1}^{\#\ Channels}(\%\ TA\ reached\ \times\ \#\ Impressions)}{\#\ Channels}$$

6.2.1.2 Isolate

Preventing an audience from seeing information that conflicts with the influencer's objective is as important as reaching them. Whether through the active blocking of data flows or encouraging the audience to close one of its information pathways, the effect of isolation magnifies the impact of an influence campaign. The isolate score measures the amount of competing, confusing, or negative information withheld from the target audience.[57] Actions from the "Manipulate Information Flows" tactic in the SP!CE™ framework have the greatest effect on Isolate scores because those techniques make information unavailable to the target audience. Actions from the

[56] Extensive research exists on the optimum amount of exposure to information to affect change in thinking. The numbers are different for different media, but the research universally agrees that increased exposure to information increases the likelihood of performing the behavior up to a point before diminishing and eventually producing a negative response in the audience. For the purposes of the assessment framework, it is assumed that the professional influencers conducting the activities understand the inverted-U relationship between number of exposures and message impact, and that they seek to optimize their impact where possible.

[57] If, in the professional judgment of the influence practitioners, one or more of the information pathways is dramatically more important, this can be a weighted average. Generally speaking, weighting one effect more heavily than others undermines the combined power of effects delivered through multiple pathways and may lead planners to more heavily weight only those pathways on which they are currently operating rather than identifying those where they are absent and seeking to gain access.

"Denigrate Opposing Information" tactic in the SP!CE™ framework can also affect because they cause the target audience to voluntarily disengage from content, but the effect is much less pronounced than the "Manipulate Information Flows" techniques.

Isolate (*I*) =

$$\frac{\sum_{n=1}^{\#\ Channels}(\%\ TA\ affected\ \times \%\ Time\ denied)}{\#\ Channels}$$

6.2.1.3 Activate

Before an audience considers performing the desired behavior, they will begin to demonstrate interest in the broader topic. For example, before deciding how they will vote, a political campaign's target audience will discuss politics and issues related to the candidates. The activate score measures interest, attention, and discussion about a topic (aka buzz or virality). When two or more influencers compete for opposing behaviors in the same target audience, their activate scores will be identical. Candidate A's campaign is equally interested in generating buzz about the political race as the opponent's campaign. The techniques listed under the "Establish Legitimacy," "Enlist Intermediaries," and "Develop Content" tactics in the SP!CE™ framework have the most significant impact on the activate score.

Activate (*A*) =

$$\sum_{n=1}^{\#\ Channels} (\%\ TA\ activities\ related\ to\ topic\ (post,\ like,\ share,\ respond,\ link,\ re - distribute))$$

6.2.1.4 Resonate

A target audience's initial response to the information presented is an early indicator of their likelihood of being influenced. The resonate score measures the reaction to information presented (aka content). Even when they disagree with the line of argument, a target audience that finds a message visually appealing, funny, exciting, or has other positive responses to it remains open to further considering the behavior in the future. Conversely, when the audience finds a message offensive, inappropriate, poorly translated, or otherwise views it negatively, they are much less likely to consider performing the requested behavior. The most likely proximate causes of negative resonate scores are the failure to execute the "Establish Legitimacy" and "Develop Content" tactics correctly in the SP!CE™ framework. The Resonate score may also be affected by others under the "Denigrate Opposing Information" tactic in the SP!CE™ framework.

Resonate (*R*) =

$$\frac{\sum_{n=1}^{\#\ Channels} (\#\ Positive\ responses\ to\ content + \#\ Positive\ amplifications) - (\ Negative\ responses\ to\ content + Negative\ amplifications)}{Total\ responses}$$

6.2.1.5 Persuade

Short-term behavior change is possible with coercive force, threat, bribes, and violence, but sustained behavior changes require changes in the target audience's attitudes, perceptions, and beliefs. Often measured using survey instruments, the persuade score measures the change in

attitude or perception of the desired behavior. These changes are a precursor to action; thus, low persuade scores usually presage low adoption of the desired behavior.

Persuade (S) =

$$\sum_{n=1}^{\#\ Channels} (\%\ T.A.\ positive\ towards\ behavior_{\ Observed} - \%\ T.A.\ positive\ towards\ behavior_{\ Baseline})$$

6.2.1.6 Motivate

The motivate score is the most direct measure of campaign impact because it measures the target audience's performance of the desired behavior. Influencers measure baseline percentages during the planning phase of an influence campaign, which they compare against the measured behavior for the first evaluation. For subsequent evaluations, the previous time period's behavior observation becomes the new baseline.

Motivate (M) =

$$\%\ T.A.\ Performing\ Behavior\ Observed - \%\ T.A.\ Performing\ Behavior\ Baseline$$

6.2.1.7 Total Impact Score

The total impact score (K) is a weighted average of the KPI scores. The impact score is most useful for tracking the success or failure of a campaign over time.

Impact Score (K) =

$$\frac{P + I + A + R + S + 5(M)}{10}$$

6.2.2 Interpreting Impact Scores

"Good" impact scores depend on the influence objective and size of the target audience. For example, an effective influence campaign to deter aggression from a rival great power may require an extremely high percentage of a smaller target audience to change their behavior until a strategic shift in the balance of power occurs. Conversely, influencing a larger target audience to support a national referendum may only require 51 percent of the audience to perform the desired behavior on voting day. The numerical values are also relative to the influencer's goal. A three percent change in the votes of a key demographic may get a candidate elected, but a three percent increase in the number of forces retreating may not halt a military attack in progress. "Good" impact scores are relative to time. For example, an effective influence campaign against an enemy integrated air defense system may require a very high percentage of the target audience to change their behavior briefly while friendly aircraft transit the system's engagement range. Conversely, influencing one member of the 12-person governing council to veto the use of nuclear weapons may require only an 8.3 percent change in behavior (1/12) sustained over a much longer duration.

The individual KPI scores point to specific changes needed to improve the campaign's effectiveness. For example, an influencer whose impact score was unacceptably low might, without considering the individual KPI scores, decide to double the amount of broadcast time and blanket the target audience with information. Providing more information to the target

audience would be the right course of action if the low impact score resulted from a low penetrate score. However, if the low impact score derived from a low resonate score (due to offensive messages) or a low isolate score (because too much adversary information was reaching the target audience), increasing broadcasts would have little effect on the campaign's success. Table 6-1 shows each Key Performance Indicator, its measurement limits, reasons for low sores, and specific SP!CETM tactics associated with each KPI.

Appendix C provides an example of how an assessor applies the formulas to a specific use case.

Table 6-1. Relationship between Key Performance Indicators and SP!CE™ Tactics

KPI	What it Measures	Reasons for Low Scores	SP!CE™ Tactics to Revisit
Penetrate	Percentage of the target audience receiving information and the frequency of presentation	Wrong platforms selected Low message frequency Insufficient information pathways	Cultivate Information Pathways Select Platforms Deliver Content Amplify Supporting Information
Isolate	Degree to which the target audience is **prevented** from receiving contrary information	Too much negative or contrary information reaching the target audience Information following unexpected paths	Manipulate Information Flows Denigrate Opposing Information Map Target Audience Information Environment
Activate	Interest, attention, and discussion about a **topic** (aka buzz or virality)	Other topics have the audience's interest Information sources not trusted No key influencers disseminating content	Establish Legitimacy Enlist Intermediaries Develop Content
Resonate	Reactions to information when presented	Audience finds content offensive, poorly translated, boring, or emotionless	Develop Content Distort Existing Narratives
Persuade	Changes in attitudes, perceptions, and beliefs	The target audience does not accept the influencers argument/position	Distort Existing Narratives Amplify Supporting Information Denigrate Opposing Information Manipulate Information Flows
Motivate	Changes in behavior	Insufficient offline activity supporting influence actions Fear of retribution Barriers to action Lack of resources or will	All

6.3 Using the Campaign and Impact Scores

The campaign score provides a comparative measure for the quality of influence campaigns. The impact score measures the effect of an influence campaign on the target audience over time. For planners, policymakers, and operators involved in influence activities, these values are most useful in refining and adjusting a campaign to increase effectiveness. The influencer should add resources or apply additional effort to parts of the campaign with lower scores. Assessments on adversary campaigns help focus resources on detecting other campaign activities and point to the areas where a campaign is most likely to be effectively countered.

Assessors conduct two assessments when friendly and adversary campaigns target the same audience (aka counter-influence campaigns)—once to calculate the adversary's campaign and impact scores and a second time to determine the scores for the friendly campaign. A successful counter-influence campaign would see the adversary's scores decline and a corresponding (but not necessarily equivalent) increase in the friendly scores. The recommendations in Table 6-2Table 6-2. Table 6-2. provide the influencer options to improve an influence campaign based on campaign and impact scores.

Table 6-2. Recommendations Based on Campaign and Impact Scores

	Campaign Score High	Campaign Score Low
Impact Score Rising	Continue campaign activities until reaching the objective	Revise the component(s) of the campaign that is most responsible for the lower score
Impact Score Falling	Review quality of individual activities	Consider revising the entire campaign
Impact Score Unchanged	Allow more time for the campaign to be effective	Revise the component(s) of the campaign that is most responsible for the lower score

6.4 Data Sources for Assessments

Influence campaign assessment should incorporate all available, relevant data sources and integrate insights into operational decision making and evaluation. Data about people and their behaviors can now be mined from so many different traditional and non-traditional sources that a comprehensive list would be impossible in a paper of this length. Influencers must establish and monitor as many direct and indirect indicators as possible given the situation. Effective assessments require data collection that is focused and routine.

6.4.1 Audience Polling and Surveys

Traditional influence assessment focused on polling, surveys, and interviews of the target audience to discern attitudes, perceptions, and beliefs that could be precursors to behavior changes. These are viable sources, and many commercial firms offer such data as a service. Direct observation of the target audience and their behavior is the most valid measure of campaign effectiveness but may be hard to discern. It provides minimal interim analytic capability to explain why the target audience is, or is not, behaving as desired.

6.4.2 Social Media

Over the last decade, social media's growth has revolutionized the way individuals interact and industries conduct business. Individuals produce data at an unprecedented rate by interacting, sharing, and consuming content through social media. Understanding and processing this new type of data to glean actionable patterns presents challenges and opportunities for interdisciplinary research, novel algorithms, and tool development. Social media mining is an emerging field that can provide much-needed insight into the target audience. Social media mining represents, analyzes, and extracts actionable patterns from social media data.[58] When mining social media data, it remains important to focus on the target audience's desired behaviors and treat carefully "vanity" metrics such as likes, which, at best, indicate the degree of resonance but are not often the desired behavioral change itself. When users actively interact with the information on social media to show their attitude toward a behavior through commenting or sharing, this can be significant, especially if they do so by lending their credibility to the message, promulgating it across their social network.

Because social media platforms gain such huge profits by assisting their customers in delivering content to highly segmented and narrowly defined groups, they are incredibly protective of their algorithms and data. However, they share tremendous amounts of statistical data with those who pay for advertising or other sponsored content. Foreign social media providers can be especially tricky. Many have direct relationships with their governments, which may not be friendly toward the United States. Challenges remain for social media analysis, including sentiment detection, language changes, and the sheer volume of information. Advances in machine learning and big data analytics are making dramatic strides in social media analysis.

6.4.3 Intelligence

While there is an abundance of commercial providers of information, research, and polling to support marketing and other communications activities, few can penetrate the denied audiences or military formations that are often the targets of U.S. influence. All-source intelligence, clearly focused on gathering data about the information, target audiences, and behavioral indicators, is required in these cases. Signals Intelligence (SIGINT) is one of the intelligence disciplines traditionally underutilized by those conducting influence outside of the Intelligence Community. SIGINT is intelligence derived from foreign targets' electronic signals and systems, such as communications systems, radars, and weapons systems. SIGINT provides a vital window for our nation into foreign adversaries' capabilities, actions, and intentions.[59] Stronger connections between U.S. influencers and the SIGINT community will assist in collecting data required to assess influence.

6.4.4 Non-traditional Data Sources

As more of the world connects digitally, data available from non-traditional sources is increasing. These sources include shipping logs, traffic patterns, financial transactions, and other "digital footprints" left by the target audience. These often tangential indicators provide unique insight into target audience attitudes, beliefs, and behavior, and their vulnerabilities and idiosyncrasies.

---

[58] R. Zafarani, M. Ali Abbasi, and H. Liu, *Social Media Mining, an Introduction,* Cambridge University Press, 2014.

[59] "Signals Intelligence," NSA.gov, retrieved from https://www.nsa.gov/what-we-do/signals-intelligence/

7 Using SP!CE to Assist in Countering Adversary Influence

Upon detecting an adversary's influence campaign, many want to denounce them publicly and vigorously because they believe that the adversary will cease their malign behavior when publicly shamed. There are at least three reasons why simply *exposing* adversary influence is an ineffective strategy. First, publicly identifying influence content often increases the target audience's desire to seek it out and amplify its propagation. Second, research shows that information credibly attributed to a foreign government will propagate across multiple media if people think it agrees with their beliefs.[60] Finally, relying on "outing" disinformation can, at best, only achieve parity in information competition; it is impossible to win by declaring how badly your opponent is cheating, since there is no referee in world affairs. Increasing public awareness and education concerning influence campaigns is essential to build the target audience's resiliency against adversary influence efforts but is insufficient as a stand-alone activity in eliminating influence threats.

Reversing information flows, disrupting enabling activities, delivering alternative behaviors to the target audience, enhancing resilience within the target audience, threatening adversary objectives, and denying access to data sources is more effective than calling additional attention to adversary information campaigns.

7.1 Reverse Information Flows

Once an analyst identifies adversary information manipulation, reversing the adversary's intended flow of information derails their campaign. Where the adversary seeks to remove information, double its availability to the target audience. Where the adversary aims to create or add information, block it from reaching the target audience. Actions to reverse the flow of information create a direct attack on the adversary campaign once it is underway.

7.2 Disrupt Enabling Activities

Besides confrontation within an ongoing campaign, preventing the adversary from reaching the target audience can affect an adversary's campaign. In many instances, automated accounts, surreptitious access points, bots,[61] and troll farms[62] expand the adversary's reach. Disabling these capabilities reduces the effectiveness of the adversary campaign.

[60] S. Vosoughi, D. Roy, and S. Aral, "The spread of true and false news online," *Science*, vol. 359, pp. 1146–1151, 2018, doi:10.1126/ science.aap9559

[61] An internet bot is a specific kind of technology that interfaces with the global internet to provide different kinds of automations. Some of the more sophisticated bots such as spambots provide spam comments all over various blogs and other web venues. "Internet Bots," Technopedia.com, retrieved from https://www.techopedia.com/definition/24063/internet-bot

[62] "A troll farm or troll factory is an institutionalized group of internet trolls aimed to interfere in political opinions and decision-making." "Troll Farm," Wikipedia, retrieved from https://en.wikipedia.org/wiki/Troll_farm

7.3 Deliver Alternative Behaviors to the Target Audience

Using many of the same information pathways that the adversary employs, the United States can offer alternative behaviors to the target audience, employing what John Stuart Mill dubbed the "marketplace of ideas" to compete for the audience's behavior directly. [63]

7.4 Enhance Resilience Within the Target Audience

Once the adversary influence campaign begins to focus, an analyst can discern the campaign's target audience. Media literacy, critical thinking, and other resilience strategies can be shared directly with the target audience and focus attention to their media consumption patterns, ensuring they are less likely to acquiesce to the adversary's desires. Additionally, suppose an influence campaign is detected early in the influence chain. In that case, efforts to "inoculate" the target audience against adversary efforts warn them and arm them with accurate information to refute adversary information.

7.5 Threaten Objectives

Threatening the adversary's objectives requires the most comprehensive understanding of their campaign, as many of the activities may conceal a larger purpose. U.S. influencers and policymakers armed with this level of knowledge can use other elements of national power beyond information to threaten those objectives. Such an approach has the advantage of avoiding playing to potential adversary strengths in the information domain and countering adversary activity in an environment advantageous to the United States. For example, adversary actions may appear to increase ethnic tensions between two groups and provoke violence. However, their ultimate objective may be to degrade the country's industrial production where those two ethnic groups compose most factory workers. Their purpose has little to do with ethnicity and more to do with increasing adversary market share and raising their exports' value. Economic sanctions and bans on their exports of goods may prove more effective at stopping the ethnic rabble-rousing than directly engaging either target audience.

7.6 Deny Access to Data Sources

Because successful influence campaigns rely heavily on knowledge about the target audience, the information environment, and important issues, adversaries increasingly rely on data created for legitimate purposes. Social media platforms regularly provide data about their users to advertisers and political parties. Denying this data to foreign governments bent on malicious manipulation of the information environment hinders their ability to mount an influence campaign effectively.

[63] "The marketplace of ideas is a rationale for freedom of expression based on an analogy to the economic concept of a free market. The marketplace of ideas holds that the truth will emerge from the competition of ideas in free, transparent public discourse and concludes that ideas and ideologies will be culled according to their superiority or inferiority and widespread acceptance among the population… The marketplace of ideas metaphor is founded in the philosophy of John Milton in his work Areopagitica in 1644 and also John Stuart Mill in his book On Liberty in 1859." "Marketplace of ideas," Wikipedia, retrieved from https://en.wikipedia.org/wiki/Marketplace_of_ideas

8 Recommendations for Implementation

MITRE offers the following recommendations for those interested in implementing the SP!CE™ methodology for evaluating an influence campaign.

- **Dedicate resources to assessments.** Comprehensive assessments require dedicated resources to perform. A multidisciplinary team with access to a wide variety of data sources will enhance the quality of assessments.
- **Separate assessors from performers.** Too often, assessing the effects of an influence campaign is relegated to the influence operators themselves. Besides the "grading their own work" issues that this creates, influencers are not trained, equipped, or resourced to both conduct and assess their activities. Intelligence professionals who understand adversary intentions, data scientists, social scientists, digital forensic analysts, and other specialized skills should form the heart of an independent assessment team.
- **Do not limit assessments to only those activities under your control.** The target audience takes in all the information in its environment, not just what the campaign offers. Consider other actions from the visual indicators to others' actions on the information environment when conducting an assessment.
- **Build survey instruments and data queries to address components of the assessment framework specifically.** The enemy of useful data is a vague collection plan. Data gathering must be as focused and as targeted as any other form of earnest endeavor.
- **Apply the assessment framework to earlier campaigns where the outcome is known and there is sufficient data.** Retrospective analysis of previous campaigns will generate lessons learned, give the assessment team opportunities to practice with the framework, and validate and refine evaluation criteria.
- **Initiate assessment at receipt of mission for new campaigns.** Continuous assessment of any activity or operation is critical to a successful mission. Influence campaigns are no different. The assessment team must fully understand the objectives and activities planned to develop their data requirements and task collection assets.
- **Incorporate assessment reports into your organizational schedule (battle rhythm).** Influence campaigns are a fundamental part of nation-state activities globally, and the explosion of influence mechanisms is unlikely to abate. Influence campaigning and regular assessment of influence activity must be kept in the mainstream of an organization's routine.

9 Conclusion

This paper outlines a framework to measure the efficacy of influence activities. This framework focuses on core aspects of influence operations. It applies to assessing both adversary campaigns and U.S. influence operations. It emphasizes the importance of assessing individual acts of information manipulation and analyzing the planning and enabling activities necessary for successful influence. Analyzing each group of engagement activities based on its effect on the audience and its penetration level into the information environment yields a better view of the impact of portions of the campaign than relying on a single metric. It can lead to a better understanding of adversary campaigns and quicker adjustments in U.S. campaigns to maximize their effects.

More than ever, influence is a team sport. In today's information environment, most individuals have unprecedented, continuous access to information. No matter how well crafted, no single act will change the outcome when the target audience consumes information from many sources. To fully manipulate the flow of information requires the technical ability to affect the information itself and the cultural and psychological skills to create impactful, nuanced, and appropriate content. Economic pressure, diplomatic efforts, and military force's presence or threat contribute to influencing without being centrally administered or controlled. Successful influence requires telling the full story in words, pictures, and actions timed to reinforce the effect continuously.

Today's media environment, especially social media, is similar to market capitalism in the heyday of the robber barons and the Mafia. Unfair practices erode the marketplace of ideas. This does not mean that any government or any social media platform should be the arbiter of truth for a society—far from it. Fair competition in the marketplace of ideas regulates practices, not content.

The modern information environment and the intensity of global competition between the three most powerful nation-states focus on the three states' key strategic narratives and objectives.

- Russia offers that *America is dangerously unstable and fickle, encouraging Europe to seek comfort and security in the arms of Mother Russia*.
- China contends that the *Chinese way of life and its people are superior and must be shielded from outside influence. From Beijing's perspective, any measure necessary to bring their economic dominance in line with their cultural superiority is acceptable.*
- The United States has yet to clearly define its stance, so the authors of this paper would like to offer the following:

  You cannot censor or sensor your way to victory. The right of free people to choose liberty is so important that we will destroy barriers to information flow to oppressed people. The marketplace of ideas must survive. There is no problem that America cannot invent its way out of. We remain steadfast in our belief that transparency is the enemy of tyranny.

Whether with that approach or another, we should endeavor to assess our progress and our adversaries' actions constantly and carefully as we continue to strive to secure our nation and our way of life.

10 Bibliography

Ajzen, I. The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, vol. 50, pp. 179-211, 1991.

Albarracin, D. J., Blair, T., and Zanna, M. P. (*The Handbook of Attitudes*. Lawrence Erlbaum Associates, 2005.

Alliance for Securing Democracy. *Linking Values and Strategy: How Democracies Can Offset Autocratic Advances.* Alliance for Securing Democracy, 2020. https://securingdemocracy.gmfus.org/wp-content/uploads/2020/10/Linking-Values-and-Strategy.pdf

Andrade, R. O., and Yoo, S. G. (2019). "Cognitive security: A comprehensive study of cognitive science in cybersecurity." *Journal of Information Security and Applications*, vol. 48, 102352. 10.1016/j.jisa.2019.06.008

Barrett, P. M. "Tackling Domestic Disinformation: What the Social Media Companies Need to Do." States News Service. Apr. 3, 2019. https://issuu.com/nyusterncenterforbusinessandhumanri/docs/nyu_domestic_disinformation_digital?e=31640827/68184927

Blair, M. H. "An Empirical Investigation of Advertising Wearin and Wearout." *Journal of Advertising Research,* vol. 40, no. 6, pp. 95-100, 2000. 10.2501/JAR-40-6-95-100

Bodine-Baron, E., Helmus, T. C., Radin, A., and Treyger, E. *Countering Russian social media influence*. RAND Corporation, 2018.

Bondarenko, I. "Tools of Explicit Propaganda: Cognitive Underpinnings." *Open Journal of Modern Linguistics,* vol. 10, no. 1, pp. 23-48, 2020. 10.4236/ojml.2020.101003

Bowe, A. *China's Overseas United Front Work: Background, and Implications for the United States.* US-China Economic and Security Review Commission, 2018.

Bradshaw, S., and Howard, P. N. *The Global Disinformation Order: 2019 Global inventory of organized social media manipulation.* Oxford, UK: Computational Propaganda Research Project, 2019. https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf

Brady, A. *Magic weapons: China's political influence activities under Xi Jinping.* Washington, DC: Wilson Center, 2017. hhttps://www.wilsoncenter.org/sites/default/files/media/documents/article/magic_weapons.pdf

Brandt, J., and Taussig, T. *The Kremlin's disinformation playbook goes to Beijing.* Washington, DC: Brookings, 2020. https://www.brookings.edu/blog/order-from-chaos/2020/05/19/the-kremlins-disinformation-playbook-goes-to-beijing/

Brooking, E. T., and Kianpour, S. (*Iranian Digital Influence Efforts: Guerrilla Broadcasting for the Twenty-First Century.* Atlantic Council, 2020. https://www.atlanticcouncil.org/wp-content/uploads/2020/02/IRAN-DIGITAL.pdf

Bucklin, R. E., and Hoban, P. R. *Marketing Models for Internet Advertising. Handbook of Marketing Decision Models,* pp. 431-462. Springer International Publishing, 2017. 10.1007/978-3-319-56941-3_14

Committee to Protect Journalists. *One Country, One Censor: How China undermines media freedom in Hong Kong and Taiwan.* 2019. https://cpj.org/?p=36113

Cook, S. *Beijing's Global Megaphone: The Expansion of Chinese Communist Party Media Influence since 2017*. Washington, DC: Freedom House, 2020. https://freedomhouse.org/sites/default/files/2020-02/01152020_SR_China_Global_Megaphone_with_Recommendations_PDF.pdf

Diresta, R., and Grossman, S. *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014-2019.* Stanford Internet Observatory, 2019. https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/potemkin-pages-personas-sio-wp.pdf

Donovan, J., and Friedberg, B. *Source hacking: media manipulation in practice.* Data & Society Research Institute, 2019. Retrieved from Informit Analysis and Policy Observatory (APO), https://search.informit.org/documentSummary;res=APO;dn=257046

FireEye, Inc. *Suspected Iranian Influence Operation Leveraging Inauthentic News Sites and Social Media Aimed at U.S., U.K., Other Audiences.* Milpitas, CA, 2018. https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-FireEye-Iranian-IO.pdf

Fuchs, C. "Propaganda 2.0: Herman and Chomsky's Propaganda Model in the Age of the Internet, Big Data and Social Media." In J. Pedro-Carañana, D. Broudy, and J. Klaehn, Eds., *The Propaganda Model Today*. University of Westminster Press, 2018, pp. 71-92.

Global Engagement Center. *GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem; 2020 ASI 7008-84.* Washington, DC: U.S. Department of State, 2020. https://statistical.proquest.com/statisticalinsight/result/pqpresultpage.previewtitle?docType=PQSI&titleUri=/content/2020/7008-84.xml

Hafez, M. M. "Rationality, Culture, and Structure in the Making of Suicide Bombers: A Preliminary Theoretical Synthesis and Illustrative Case Study." *Studies in Conflict and Terrorism,* vol. 29, no. 2, 2006, pp. 165-185. 10.1080/10576100500496964

Hanson, F., O'Connor, S., Walker, M., and Courtois, L. *Hacking Democracies*. .Australian Strategic Policy Institute, 2019. https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2019-05/Hacking%20democracies_0.pdf?.RKLLc8uKm1wobfWH1VvC.C88xGWYY29

Helmus, T. C. et al. . *Russian Social Media Influence*. RAND Corporation, 2018

Insikt Group. "Beyond Hybrid War: How China Exploits Social Media to Sway American Opinion." *Recorded Future*, 2019. https://go.recordedfuture.com/hubfs/reports/cta-2019-0306.pdf

Insikt Group. "Chinese Influence Operations Evolve in Campaigns Targeting Taiwanese Elections, Hong Kong Protests." *Recorded Future*, 2020. https://go.recordedfuture.com/hubfs/reports/cta-2020-0429.pdf

Joint Chiefs of Staff. *Insights and Best Practices Focus Paper: Communication Strategy and Synchronization.* Suffolk, VA, 2016. https://www.jcs.mil/Portals/36/Documents/Doctrine/fp/comm_strategy_and_sync_fp.pdf

Joint Chiefs of Staff. *Joint Concept for Integrated Campaigning.* Washington, DC, 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concept_integrated_campaign.pdf?ver=2018-03-28-102833-257

Joint Chiefs of Staff. *Joint Concept for Operating in the Information Environment*. Washington, DC, 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf

Joint Chiefs of Staff. *JP 3-12: Cyberspace Operations.* Washington, DC,2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

Joint Chiefs of Staff. *Joint Doctrine Note 1-19: Competition Continuum.* Washington, DC, 2019. https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn1_19.pdf

Joint Chiefs of Staff. *Joint Planning.* Washington, DC, 2020. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp5_0.pdf?ver=ztDG06paGvpQRrLxThNZUw%3d%3d

Jones, J., Kuehl, D. T., Burgess, D., and Rochte, R. "Strategic Communication and the Combatant Commander." *Joint Force Quarterly*, vol. 55, no. 4, pp.104-109, 2009. https://ndupress.ndu.edu/portals/68/Documents/jfq/jfq-55.pdf

Kenney, C., Bergmann, M., and Lamond, J. *Understanding and Combating Russian and Chinese Influence Operations.* Washington, DC: Center for American Progress, 2019. https://www.americanprogress.org/issues/security/reports/2019/02/28/466669/understanding-combating-russian-chinese-influence-operations/

Kent, T. *Striking Back*. The Jamestown Foundation, 2020

King, S. B. "Military social influence in the global information environment: A civilian primer." *Analyses of Social Issues and Public Policy (ASAP)*, vol. 11, pp. 1-26, 2011. 10.1111/j.1530-2415.2010.01214.x.

Kofman, M., Migacheva, K., Nichiporuk, B., Radin, A., Tkacheva, O., and Oberholtzer, J.. *Lessons from Russia's operations in Crimea and Eastern Ukraine.* RAND Corporation, 2017

Lamb, C. J. *Review of Psychological Operations Lessons Learned from Recent Operational Experience.* 2005.http://www.dtic.mil/docs/citations/ADA445151

Laswell, H. D. "The Theory of Political Propaganda." *The American Political Science Review,* vol. 21, no. 3, pp. 627-631, 1927

Leont'ev, A. N. *Activity, Consciousness, and Personality*. Prentice-Hall, 1978.

Levy, J. S. "Deterrence and Coercive Diplomacy: The Contributions of Alexander George." *Political Psychology,* vol. 29, no. 4, pp. 537-552, 2008. 10.1111/j.1467-9221.2008.00648.x

Libicki, M. C. "The Convergence of Information Warfare." *Strategic Studies Quarterly: SSQ,* vol. 11, no. 1, pp. 49-65, 2017. https://www.jstor.org/stable/26271590

Liu, J. H. "Neo-Confucian epistemology and Chinese philosophy: Practical postulates for actioning psychology as a human science." *Asian Journal of Social Psychology,* vol. 20, no. 2, pp. 137-149, 2017. 10.1111/ajsp.12168

Mazarr, M. J., Casey, A., Demus, A., Harold, S. W., Beauchamp-Mustafaga, N., and Sladden, J. *Hostile Social Manipulation: Present Realities and Emerging Trends*. RAND Corporation, 2019.

McCorkindale, T. *2020 IPR Disinformation in Society Report.* Institute for Public Relations, 2020. https://instituteforpr.org/wp-content/uploads/Disinformation-In-Society-2020-v6-min-1.pdf

Mill, J. S. *On Liberty*. G&D Media, 1859

Mozur, P., and Stevenson, A. "Chinese Cyberattack Hits Telegram, App Used by Hong Kong Protesters." *The New York Times,* June 13, 2019. https://global.factiva.com/en/du/article.asp?accessionno=NYTFEED020190613ef6d002s1

Ngai, E. W. T., Moon, K. K., Lam, S. S., Chin, E. S. K., and Tao, S. S. C. "Social media models, technologies, and applications." *Industrial Management + Data Systems*, vol. 115, no. 5, pp. 769-802, 2015. 10.1108/IMDS-03-2015-0075

Nimmo, B., Eib, C. S., and Ronzaud, L. *Operation Naval Gazing*. Milpitas, CA: Graphika, 2020. https://public-assets.graphika.com/reports/graphika_report_naval_gazing.pdf

Nimmo, B., Eib, C. S., and Tamora, L. *Cross-Platform Spam Network Targeted Hong Kong Protests.* Graphika, 2019. https://public-assets.graphika.com/reports/graphika_report_spamouflage.pdf

Nimmo, B., Francois, C., Eib, C. S., and Ronzaud, L. *Return of the (Spamouflage) Dragon.* Milpitas, CA: Graphika, 2020. https://public-assets.graphika.com/reports/Graphika_Report_Spamouflage_Returns.pdf

Nimmo, B., Francois, C., Eib, C. S., Ronzaud, L., and Carter, J. *GRU and the Minions.* New York, NY: Graphika, 2020. https://public-assets.graphika.com/reports/graphika_report_gru_minions.pdf

Nimmo, B., et al. *Infektion*. Graphika, 2020. https://secondaryinfektion.org/downloads/secondary-infektion-report.pdf

O'Connor, S., Hanson, F., Currey, E., and Beattie, T. *Cyber-enabled foreign interference in elections and referendums.* Australian Strategic Policy Institute, 2020. https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-10/Cyber%20enabled%20foreign%20interference.pdf?_7RoySKD0mc9GkMEIZ45NkXLtIK2wOyj=

Pamment, J. *The EU's Role in Fighting Disinformation: Crafting a Disinformation Framework.* Washington, DC: Carnegie Endowment for International Peace, 2020. https://carnegieendowment.org/files/Pamment_-_Crafting_Disinformation_1.pdf

Pamment, J., Nothhaft, H., Agardh-Twetman, H., and Fjällhed, A. *Countering Information Influence Activities: The State of the Art version 1.4*. 2018. https://lup.lub.lu.se/record/825192b8-9274-4371-b33d-2b11baa5d5ae

Petty, R. E., and Cacioppo, J. T. *The Elaboration Likelihood Model of Persuasion. Advances in Experimental Social Psychology*. Elsevier Science & Technology, 1986, pp. 123-205. 10.1016/S0065-2601(08)60214-2

Polyakova, A., and Fried, D. *Democratic defense against disinformation 2.0.* Atlantic Council, 2019. Retrieved from Informit Analysis and Policy Observatory (APO) https://search.informit.org/documentSummary;res=APO;dn=242041

Rajtmajer, S., and Susser, D. "Automated Influence and the Challenge of Cognitive Security." HoTSoS: ACM Symposium on Hot Topics in the Science of Security, forthcoming

Roonemaa, H., and Springe, I. “This is How Russian Propaganda Actually Works in the 21st Century.” BuzzFeed News, Aug. 31, 2018. https://www.buzzfeednews.com/article/holgerroonemaa/russia-propaganda-baltics-baltnews

Ross, B., Pilz, L., Cabrera, B., Brachten, F., Neubaum, G., and Stieglitz, S. “Are social bots a real threat? An agent-based model of the spiral of silence to analyse the impact of manipulative actors in social networks.” *European Journal of Information Systems,* vol. 28, no. 4, pp. 394-412, 2019. 10.1080/0960085X.2018.1560920

Schneier, B. *Toward an Information Operations Kill Chain*. LAWFARE, 2019. https://www.lawfareblog.com/toward-information-operations-kill-chain#

Searight, A. *Countering China’s Influence Activities: Lessons from Australia.* Center for Strategic and International Studies, 2020. Retrieved from Informit Analysis and Policy Observatory (APO). https://search.informit.org/documentSummary;res=APO;dn=307243

Shanker, T., and Hertling, M. “The military-media relationship: a dysfunctional marriage?” *Military Review,* vol. 89, no. 2, Sept. 1, 2009. https://search.proquest.com/docview/225300542

Singer, J. D. “Inter-National Influence: A Formal Model.” *The American Political Science Review,* vol. 57, no. 2, pp. 420-430, 1963. https://www.jstor.org/stable/1952832

Thomas, E., Thompson, N., and Wanless, A. *The Challenges of Countering Influence Operations*. Carnegie Endowment for International Peace – Papers, June 10, 2020. https://search.proquest.com/docview/2411102737

Tirpak, J. A. “Find, Fix, Track, Target, Engage, Assess.” *Air Force Magazine,* July 1, 2000. https://www.airforcemag.com/article/0700find/

U.S. Department of Justice. *Report of the Attorney General’s Cyber-Digital Task Force.* Washington, DC, 2018. https://www.justice.gov/archives/ag/page/file/1076696/download

U.S. Senate. *Report of the Select Committee on Intelligence, United States Senate on Russian Active Measures Campaigns, and Interference in the 2016 U.S. Election. Volume 2: Russia’s Use of Social Media with Additional Views.* Washington, DC, 2020. https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures

Vosoughi, S., Roy, D., and Aral, S. “The spread of true and false news online.” *Science* (American Association for the Advancement of Science), vol. 359, no. 6380, pp. 1146-1151, 2018. 10.1126/science.aap9559

Wanless, A., and Pamment, J. “How Do You Define a Problem Like Influence?” *Journal of Information Warfare,* vol. 18, no. 3, pp. 1-14, 2019. https://www.jstor.org/stable/26894679

Wardle, C., and Derakhshan, H. *Information Disorder: Toward an interdisciplinary framework for research and policy making.* Council of Europe, 2017. https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

Yaveroglu, I., and Donthu, N. (2008). "Advertising Repetition and Placement Issues in On-Line Environments." *Journal of Advertising,* vol. 37, no. 2, pp. 31-44, 2008. 10.2753/JOA0091-3367370203

Zafarani, R., Abbasi, M. A., and Liu, H. *Social Media Mining, an Introduction.* Cambridge University Press, 2014. 10.1017/CBO9781139088510ss. 10.1017/CBO9781139088510

Appendix A Evaluating Friendly Information Campaign Conduct

Table A-1. Evaluation Criteria for Friendly Influence Campaigns – Plan Phase

Determine Strategic Objectives	**Low:** Objective is clearly defined and achievable. (1) **Medium:** Objective is consistent with others operating in the information space. (2) **High:** Objective is shared and agreed upon by all parties involved in affecting the information environment. (5)
Determine Desired Behaviors	**Low:** Desired behavior selected. (1) **Medium:** Desired behavior fulfills a sizable portion of accomplishing objective. (2) **High:** Desired behavior directly accomplishes objective. (5)
Identify and Analyze Target Audience	**Low:** Target audience (TA) is demographically homogeneous. (1) **Medium:** Audience is the largest stakeholder in the behavior. (2) **High**: Audience is the only one that can perform the behavior. (5)
Map TA Information Environment	**Low:** The TA culture, bias, and predisposition are known. (1) **Medium:** Information conduits with the highest level of interaction are documented. (2) **High:** All routes of information input are known. (5)
Identify Social & Technical Vulnerabilities	**Low:** Academic study of the target audience complete; various aspects of language, culture, and history provide expectations of behavior patterns. (1) **Medium:** Direct evaluation of the target audience is completed through survey, social media analysis, or other measurement instrument. (2) **High:** Measurement instrument directly relevant to desired behavior and barriers to its execution are employed prior to campaign initiation. (5)
Select Platforms	**Low:** Platforms selected represent less than 40% of the TA's Information Environment map. (1) **Medium:** Platforms selected represent between 40% and 80% of the TA's Information Environment map. (2) **High:** Platforms selected represent greater than 80% of the TA's Information Environment map. (5)
Identify & Understand Ongoing TA Activities	**Low:** Influence activity appears authentic to casual observers (grammar, idiom, and content). (1) **Medium:** Influence activity appears to be single topic focused. (2) **High:** Influence activity presented across a broad range of topics consistent with ongoing conversations. (5)
Develop Operational Approach	**Low:** Plan is developed independent of other plans within the organization's control. (1) **Medium:** Plan is developed in conjunction with other plans within the organization's control. (2) **High:** Plan is developed in cooperation with other plans within and outside of the organization's control (whole of government). (5)
Evaluate Resources	**Low:** Planners know and understand the resource limitations. (1) **Medium:** Sufficient resources are available and in place to execute the campaign. (2) **High:** Sufficient resources are available and in place to execute the campaign AND additional resources are available to extend or expand as required. (5)

Table A-2. Evaluation Criteria for Friendly Influence Campaigns – Enable Phase

Establish Information Assets (Direct Control)	**Low:** Influence assets are present on information pathways that are used by the target audience. (1) **Medium:** Influence assets are present on information pathways that are trusted by the target audience. (2) **High:** Influence assets are present on information pathways that are considered authoritative by the target audience. (5)
Emplace Sensors	**Low:** Influence assets are present on information pathways and monitoring conversations. (1) **Medium:** Autonomous monitoring yields real time data streams. (2) **High:** Autonomous monitoring yields real time data streams AND sufficient analytic capability is available to detect changes in topic or sentiment. (5)
Establish Legitimacy	**Low:** Influence activity appears authentic to casual observers (grammar, idiom, and content). (1) **Medium:** Influence assets are present on information pathways and communicating information with the TA without significant negative response. (2) **High:** U.S.-controlled or -aligned information is sufficiently credible that members of the target audience reuse it. (5)
Cultivate Information Pathways	**Low:** Influence activities can be conducted on multiple information pathways. (1) **Medium:** Influence activities are coordinated in both their content and timing across most information pathways to the target audience. (2) **High:** Target audience receives information on one controlled pathway and seeks confirmation/validation from another. (5)
Enlist Intermediaries (Indirect Control)	**Low:** Target audience receives information directly from friendly information assets ONLY. (1) **Medium:** Key communicators within the target audience are identified and engaged. (2) **High:** Key communicators and prominent media influencers reliably amplify information. (5)
Develop Content	**Low:** Content appears authentic to target audience (grammar, idiom, and tone). (1) **Medium:** Friendly content and other content is rarely identified as fake. (2) **High:** Friendly content is usually attributed to members of the target audience or other trusted source. (5)
Persist in the Information Space	**Low:** Information assets must be regularly reconstituted. (1) **Medium:** Information assets are established at campaign initiation. (2) **High:** Information assets operated without detection in the TA's information environment prior to the information campaign's initiation. (5)

Table A-3. Evaluation Criteria for Friendly Influence Campaigns – Engage Phase

Distort Existing Narratives	**Low:** Existing narratives remain prominent in the information space and are rarely questioned. (1) **Medium:** Target audience expresses doubt, mistrust, or confusion about existing narratives. (2) **High:** Target audience expresses strong emotional reactions to existing narratives. (5)
Command and Control Information Assets	**Low:** Information assets accept direction from information campaign leaders. (1) **Medium:** Influence campaign planners and commanders are aware of changes in the information environment as they occur. (2) **High:** Information assets respond in a timely and coordinated fashion to changes in the information environment. (5)
Deliver Content (Add Information)	**Low:** Majority of content consumed by the TA is negative toward the desired behavior produced by adversaries. (1) **Medium:** Target audience sees friendly and adversary content in equal measures. (2) **High:** Majority of the content consumed by the target audience supports the desired behavior AND friendly content is regularly consumed. (5)
Manipulate Information Flows	**Low:** Target audience has limited sources of information. (1) **Medium:** Information consumed by the audience is generally biased toward the behavior. (2) **High:** Most information consumed by the audience actively reinforces the behavior. (5)
Amplify Supporting Information (Maximize Exposure)	**Low:** Friendly content is only amplified by friendly information assets. (1) **Medium:** Friendly content is available on multiple platforms regularly and occasionally supported by the target audience. (2) **High:** Target audience amplifies supporting information without prompting from friendly information assets. (5)
Denigrate Opposing Information	**Low:** Opposing information is occasionally criticized by friendly information. (1) **Medium:** Opposing content is regularly criticized by friendly information AND occasionally by the target audience. (2) **High:** Target audience criticizes opposing information without prompting from friendly information assets. (5)
Drive Offline Activity	**Low:** Friendly information assets advocate for offline activity that supports the desired behavior. (1) **Medium:** Target audience advocates for offline activity that supports the desired behavior. (2) **High:** Target audience engages in offline activity that supports the desired behavior. (5)
Remove Evidence of the Campaign	**Low:** Friendly information assets directly attributed to the campaign remain in the information environment. (1) **Medium:** All information assets and connections to the information campaign are removed from the information environment. (2) **High:** Friendly information assets remain in the information environment operating without popular knowledge of their participation in the information campaign. (5)

Appendix B Evaluating Adversary Information Campaign Conduct

Table B-1. Evaluation Criteria for Adversary Influence Campaigns – Plan Phase

Determine Strategic Objectives	**Low:** Understandable connection between influence activities and adversary interests. (1) **Medium:** Specific adversary interest is identified that corresponds to the behavior elicited in influence activities. (2) **High:** Direct confirmation from the adversary of the intent of their influence. (5)
Determine Desired Behaviors	**Low:** Adversary information includes a generic call to action. (1) **Medium:** Information presented directs a specific behavior. (2) **High:** Adversary confirms its intent to generate a specific behavior. (5)
Identify and Analyze Target Audience	**Low:** Adversary activity is only available to a known segment of the population. (1) **Medium:** Adversary activities are directed toward an identifiable audience. (2) **High:** Direct confirmation from the adversary of the target audience. (5)
Map TA Information Environment	**Low:** Adversary activity is only available to some segments of the population. (1) **Medium:** More than 50% of the information conduits in use are known. (2) **High:** All information conduits are known and monitored. (5)
Identify Social & Technical Vulnerabilities	**Low:** Evidence that an adversary is conducting general research about U.S./allied audiences. (1) **Medium:** Adversary is using polling or other instruments to survey the attitudes of a segment of the population. (2) **High:** Direct confirmation that an adversary is gathering information from a specific group that they want to influence. (5)
Select Platforms	**Low:** Adversary presence is detected on a single platform. (1) **Medium:** Adversary presence is detected on multiple platforms. (2) **High:** Adversary presence is detected on multiple platforms AND the connections/relationships between platform activities is recognized. (5)
Identify & Understand Ongoing TA Activities	**Low:** Adversary activity appears inauthentic to casual observers (grammar, idiom, and content). (1) **Medium:** Adversary activity appears to be single topic focused. (2) **High:** Adversary activity observed across a broad range of topics consistent with ongoing conversations. (5)
Develop Operational Approach	**Low:** Adversary activities are episodic and may conflict with one another. (1) **Medium:** Adversary activities appear complementary in both timing and message. (2) **High:** Direct confirmation of a coordinated adversary campaign. (5)
Evaluate Resources	**Low:** Adversary activities appear limited by available resources. (1) **Medium:** No evidence of adversary resource shortages. (2) **High:** Direct confirmation of adversary resource levels. (5)

Table B-2. Evaluation Criteria for Adversary Influence Campaigns – Enable Phase

Establish Information Assets (Direct Control)	**Low:** Adversary presence is known to exist in information pathways. (1) **Medium:** Adversary has some ability to manipulate information on a pathway to the target audience. (2) **High:** Adversary fully controls information along a pathway used by the target audience. (5)
Emplace Sensors	**Low:** No adversary monitoring or sensors are detected. (1) **Medium:** Adversary monitoring is identified on TA's information pathways. (2) **High:** Direct confirmation from the adversary of sensor emplacement. (5)
Establish Legitimacy	**Low:** Adversary-controlled or -aligned presence in target information environment. (1) **Medium:** Adversary-controlled or -aligned information can remain in the information environment. (2) **High:** Adversary-controlled or -aligned information is sufficiently credible that members of the target audience reuse it. (5)
Cultivate Information Pathways	**Low:** Adversary activities appear on multiple information pathways. (1) **Medium:** Adversary activity is complementary between pathways. (2) **High:** Adversary information activities are coordinated in both their content and timing across most information pathways to the target audience. (5)
Enlist Intermediaries (Indirect Control)	**Low:** Target audience receives information directly from adversary information assets ONLY. (1) **Medium:** Adversary engages key communicators within the target audience. (2) **High:** Key communicators and prominent media influencers reliably amplify adversary information. (5)
Develop Content	**Low:** Content appears authentic to target audience (grammar, idiom,and tone). (1) **Medium:** Adversary content is rarely identified as fake. (2) **High:** Adversary content is usually attributed to members of the target audience or other trusted sources. (5)
Persist in the Information Space	**Low:** Adversary information assets are quickly identified and removed from platforms. (1) **Medium:** Adversary information assets are identified but remain on platforms. (2) **High:** Adversary information assets operate without detection in the TA's information environment. (5)

Table B-3. Evaluation Criteria for Adversary Influence Campaigns – Engage Phase

Distort Existing Narratives	**Low:** Existing narratives remain prominent in the information space and are rarely questioned. (1) **Medium:** Target audience expresses doubt, mistrust, or confusion about existing narratives. (2) **High:** Target audience expresses strong emotional reactions to existing narratives. (5)
Command and Control Information Assets	**Low:** Information assets accept direction from information campaign leaders. (1) **Medium:** Influence campaign planners and commanders are aware of changes in the information environment as they occur. (2) **High:** Information assets respond in a timely and coordinated fashion to changes in the information environment. (5)
Deliver Content (Add Information)	**Low:** Majority of content consumed by the TA is negative toward the desired behavior. (1) **Medium:** Target audience sees friendly and adversary content in equal measures. (2) **High:** Majority of the content consumed by the target audience supports the desired behavior AND adversary content is regularly consumed. (5)
Manipulate Information Flows	**Low:** Target audience has limited sources of information. (1) **Medium:** Information consumed by the audience is generally biased toward the behavior. (2) **High:** Most information consumed by the audience actively reinforces the behavior. (5)
Amplify Supporting Information (Maximize Exposure)	**Low:** Adversary content is only amplified by adversary information assets. (1) **Medium:** Adversary content is available on multiple platforms regularly and occasionally supported by the target audience. (2) **High:** Target audience amplifies supporting information without prompting from adversary information assets. (5)
Denigrate Opposing Information	**Low:** Opposing information is occasionally criticized by adversary information. (1) **Medium:** Opposing content is regularly criticized by adversary information AND occasionally by the target audience. (2) **High:** Target audience criticizes opposing information without prompting from adversary information assets. (5)
Drive Offline Activity	**Low:** Adversary information assets advocate for offline activity that supports the desired behavior. (1) **Medium:** Target audience advocates for offline activity that supports the desired behavior. (2) **High:** Target audience engages in offline activity that supports the desired behavior. (5)
Remove Evidence of the Campaign	**Low:** Adversary information assets and activities directly attributed to the campaign remain in the information environment. (1) **Medium:** All information assets and connections to the information campaign are removed from the information environment. (2) **High:** Adversary information assets remain in the information environment, operating without popular knowledge of their participation in the information campaign. (5)

Appendix C Impact Calculations for a Notional Influence Campaign

This appendix shows how to calculate the impact of competing campaigns using SP!CE™. The scenario aims to demonstrate the impact of scoring principles as straightforwardly as possible. Nation-states have used all of the information actions in the notional example in actual influence campaigns. The techniques selected are representative of real campaigns, not an exhaustive list. As an illustrative example, the scenario provides SP!CE™ users a better understanding of the methodology; it is not intended as a policy prescription or recommendation for future activities outside of the evaluation methodology.

C.1 Scenario

- **Situation:**

  Country X, a notional country, is historically aligned with one of the United States' peer competitors. Country X borders neither the United States nor the peer competitor, so U.S. involvement with Country X is not likely to escalate into open conflict. The assessment team is using SP!CE™ to advise a U.S. geographic combatant commander who conducts operations regarding Country X in concert with the other U.S. government departments and agencies under the auspices of the combatant command's theater engagement campaign.

- **Strategic Objective:**

  The United States seeks economic benefits by increasing trade with Country X. Central to the success of U.S. economic aspirations is the signing of a U.S.–X trade agreement known as the USXTA.

- **Target Audience:**

  There are 100 academics and members of think tanks who frequently publish on national security and trade policy within country X. As a target audience, they are more educated and more aware of international politics than the average citizen of the country. They have influential ties to the government, as many of them have previously served as Country X government officials. Their writings have the power to sway public policy.

- **Desired Behavior:**

  The target audience writes and publishes articles and research reports advocating closer relations with the United States and supporting the proposed trade agreement.

C.2 Target Audience Information Environment

The assessment team produces an audience-specific information map to display the sources of information the target audience primarily uses and trusts. The information environment map, which is specific to the target audience, forms the cognitive terrain on which the battle of ideas occurs. Each identified information pathway to the target audience serves to either add new information or reduce information flow in service of the campaign's objectives. The assessment team produced the target audience's information environment map depicted in Figure C-1. The boxes around portions of the audience show what percentage of the audience gets information from a particular source. For example, 35 percent of the audience follows Sam Politician on

Twitter. Anything added into Sam's Twitter feed would, therefore, reach 35 percent of the audience. The combatant command (CCMD) website is owned and operated by the U.S. geographic CCMD. 8Kuhn is a fringe blogging network know for lax terms of service where multiple conspiracy theories have emerged. Newsotheday.com is an independent news and information website hosted in Country X whose editorial slant has always been against the United States.

Many audience members have multiple information sources. For purposes of the example, each information source is equally weighted in terms of target audience trust and acceptance. In practice, each could be weighted to reflect their standing with the audience members. The large box around the entire audience reflects that all audience members will see any physical actions that affect the whole country.

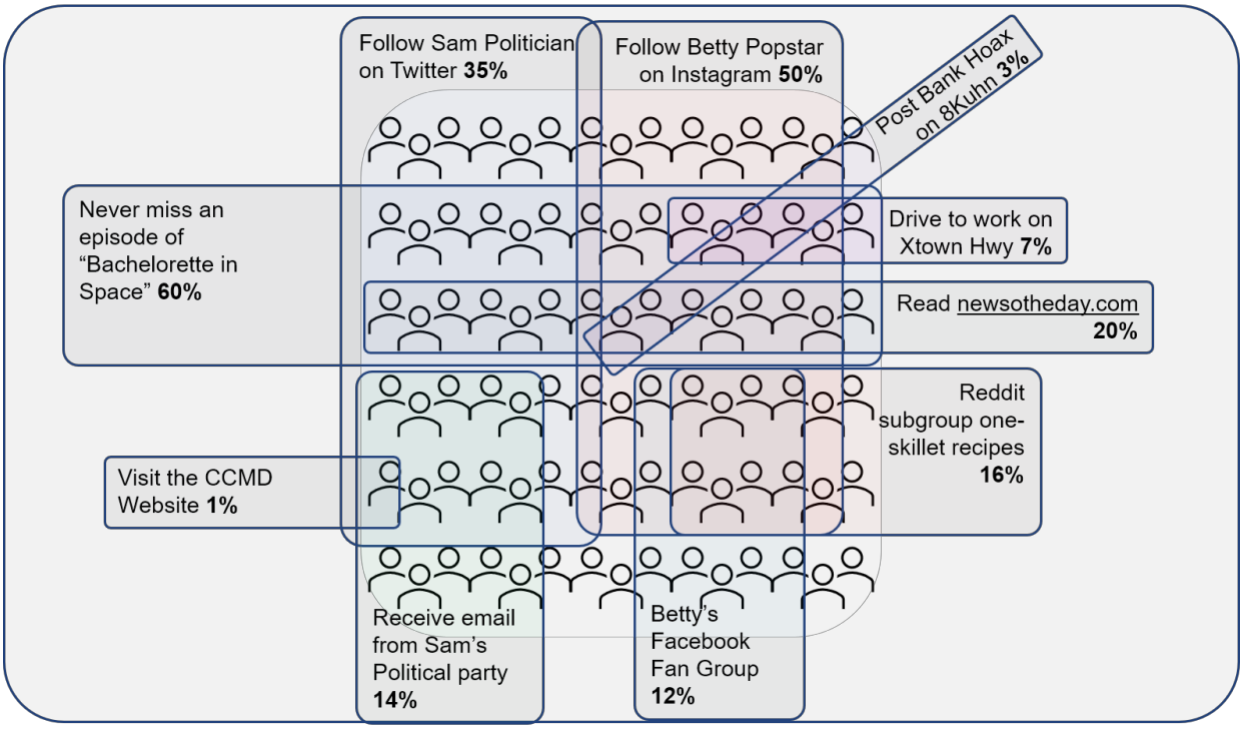

Figure C-1. Target Audience's Information Environment

C.3 Target Audience – Behavior Baseline

In the month before the information campaign, nine members of the target audience published articles supporting the USXTA. Eighteen target audience members published articles opposing the USXTA. The remaining 73 members of the target audience did not publish any articles. These numbers form the baseline behavior against which the assessment team can compare the results at the end of the first reporting period.

C.4 Information Actions

The United States and its peer adversary initiate information campaigns. Throughout the example, the term "friendly" denotes the U.S. government, including all of the actions that it either conducts or directs. The peer competitor country is called "enemy." The friendly and enemy influence campaigns include the following actions:

C.4.1 Friendly Actions

- Friendly influence operators produce a series of public service announcements (PSAs) and purchase placement of the PSAs during the "Bachelorette in Space" program twice per week.
- The CCMD public affairs office publishes positive stories about the United States daily on the CCMD website.
- Friendly cyber operations forces deplatform[64] the accounts promulgating the Bank Hoax thread on 8Kuhn.
- Friendly cyber forces redirect internet users attempting to access newsotheday.com to the CCMD website.[65]
- The White House expresses public support for Sam Politician, a vocal advocate for the USXTA.
- Sam Politician and Betty Popstar each receive private messages from friendly senior officials to encourage their support for the USXTA.

C.4.2 Enemy Actions

- Enemy cyber forces hack into the email accounts of Sam Politician's party. The enemy creates forged emails with evidence of political corruption in the party before leaking all of the emails, genuine and forged, publicly.
- Using the forged emails as evidence, country X security forces arrest the Deputy Minister of Trade, charging him with corruption and fraud.
- Enemy operators pay a local firm to erect a billboard on the Xtown Highway that calls U.S. relations with Country X "Plantation Economics."
- The enemy covertly exercises editorial control of newsotheday.com, ensuring that it retains an anti-U.S. bias.
- At the enemy government's invitation, Betty Popstar visits the enemy capital and shares pictures with her followers.
- Sock Puppet[66] followers of Sam Politician post the Bank Hoax narrative where Sam's legitimate followers will all see it.

---

[64] Deplatforming, also known as no-platforming, is the removal of individuals or groups from a platform, preventing them from using the platform's services even if they try to create new accounts. It is frequently used to prevent someone holding views regarded as unacceptable or offensive from contributing to a forum or debate, especially by blocking them on a particular website.

[65] When a web browser attempts to open a Uniform Resource Locator (URL) that has been redirected, a page with a different URL is opened.

[66] A sock puppet or sockpuppet is an online identity used for purposes of deception. The term, a reference to the manipulation of a simple hand puppet made from a sock, originally referred to a false identity assumed by a member of an internet community who spoke to, or about, themselves while pretending to be another person. The use of the term has expanded to include other misleading uses of online identities, such as those created to praise, defend, or support a person or organization, to manipulate public opinion, or to circumvent restrictions, such as viewing a social media account that they are blocked from, or suspension or an outright ban from a website. A significant difference between the use of a pseudonym and the creation of a sockpuppet is that the sockpuppet poses as an independent third-party unaffiliated with the main account operator. Sockpuppets are unwelcome in many online communities and forums.

C.5 Response and Indicators

Throughout the first month of the influence campaign, the assessment team monitors the emplaced sensors and other intelligence sources to gather data to conduct their assessment. At the end of the assessment period, the team has compiled the following list of responses and indicators:

- Hackers deface the CCMD Website with anti-U.S. slogans and images. The command's cybersecurity team restores the site in 24 hours.
- A story about the leaked party emails revealing that Deputy Minister of Trade takes bribes appears on newsotheday.com. Several party emails link to the article.
- The CCMD website gets three positive and two negative comments likely originating from the target audience.
- "Bachelorette in Space" remains the target audience's most popular show, with 60 percent tuning in each week.
- On the 8Kuhn site, Bank Hoax posters post, on average, three times per day.
- After being removed from 8Kuhn, Bank Hoax promulgators re-emerge 14 days later on Yamdex.zx.
- After two days, newsotheday.com discovers that users are redirected, but it takes another three days to remove the exploit that caused it.
- Newsotheday.com publishes eight stories saying that U.S. companies are exploiting local workers for poverty wages.
- A picture of Betty Popstar and the enemy Prime Minister dancing becomes a meme, and new versions appear daily for two days.
- Ten percent of Sam Politician's legitimate Twitter followers retweet the Bank Hoax.
- Unknown vandals, possibly working as friendly agents, set the Xtown Highway billboard ablaze three weeks after it appears. The fire destroys the billboard, and commuters can see the charred remains from the highway.
- Sam Politician reposts the White House message of support and includes it in his weekly email to the party.
- Twenty-three percent of the target audience's online activity includes one or more of the following keywords: (trade+agreement, USXTA, US+Trade, or US+X+Economy).
- When members of the target audience encounter friendly-produced or sponsored content:
    - 4% responded positively.
    - 2.5% amplified (shared with supporting comment).
    - 1% responded negatively.
    - 0.5% amplified negative response.
- When members of the target audience encounter enemy-produced or sponsored content:
    - 1.5% responded positively.

    - 0.5% amplified (shared with supporting comment).
    - 3% responded negatively.
    - 1.75% amplified negative response.
- The assessment team commissions a survey of the target audience to measure their attitudes about the USXTA. The results show:
    - 13% support USXTA.
    - 19% oppose USXTA.
    - 68% are undecided.
- During the assessment period, the target audience publishes 11 articles.
- Four articles support the USXTA; seven oppose the USXTA.

C.6 Impact Score Calculations

At the end of the first month of the influence campaign, the assessment team uses the data gleaned from the responses and indicators to calculate both friendly and enemy impact scores. The team calculates the Penetrate score (P), the Isolate score (I), the Activate score (A), the Resonate score (R), the Persuade score (S), and the Motivate score (M) using the formulas in Section 6.2 of this paper. Once the assessment team calculates the six element scores, they calculate the Overall Impact score (*K*). The assessment period is a 30-day month.

C.6.1 Friendly Impact Score Calculations

C.6.1.1 Penetrate (P)

$$\%\ watching\ Bachelorette(\#PSAs\ shown)$$

$$+\ \%\ reading\ CCMD\ website(\#days\ website\ available)$$

$$+\ (\%\ following\ Sam\ on\ Twitter + \%\ receiving\ party\ emails)(\#posts\ or\ emails\ about\ White\ House\ support)$$

$$+\ \%\ viewing\ billboard(\#days\ billboard\ burned\ or\ unrepaired)$$

$$\div \text{"\#channels in info map"}$$

$$\therefore \textbf{Penetration (P)} = \frac{0.6(8)+0.01(29)+(0.35+0.14)(1)+0.07(8)}{10} = \mathbf{61.4\%}$$

C.6.1.2 Isolate (I)

$$\%\ viewing\ 8\text{Kuhn}(\%days\ successfully\ deplatformed)$$

$$+\ \%\ viewing\ newsotheday.com(\%\ days\ offline)$$

$$+\ \%\ viewing\ billboard(\%\ days\ billboard\ unreadable)$$

$$\div \text{"\#channels in info map"}$$

$$\therefore \textbf{Isolate (I)} = \frac{0.03(0.5)+0.2(0.167)+0.07(0.333)}{10} = \mathbf{0.71\%}$$

C.6.1.3 Activate (A)

$\%\ TA\ activity\ with\ keywords = (trade + agreement\ or\ USXTA\ or\ US + Trade, or\ US + X + Economy)$

∴ Activate (A) = 23.0%

C.6.1.4 Resonate (R)

$(\#\ Positive\ responses\ to\ content$

$+\#\ Positive\ amplifications)$

$-(\#\ Negative\ responses\ to\ content$

$+ Negative\ amplifications)$

$\div\ Total\ responses$

∴ Resonate (R) $= \frac{(4+2.5)-(1+.05)}{100} =$ 5.5%

C.6.1.5 Persuade (S)

$\%\ responding\ positively\ to\ survey\ at\ end\ of\ month - \%\ responding\ positively\ at\ baseline$

∴ Persuade (S) $= 0.13 - 0.09 =$ 4.0%

C.6.1.6 Motivate (M)

$$\frac{\#\ positive\ articles\ this\ month}{Total\ articles\ this\ month} - \frac{\#\ positive\ articles\ at\ baseline}{total\ articles\ at\ baseline}$$

∴ Motivate (M) $= \frac{4}{11} - \frac{9}{27} =$ 3.0%

C.6.1.7 Impact Score (K)

Impact (K) $= \frac{P+I+A+R+S+5(M)}{10} = \frac{0.614+0.071+0.23+0.055+0.04+5(0.03)}{10} =$ <u>11.6%</u>

C.6.2 Enemy Impact Score Calculations

C.6.2.1 Penetrate (P)

$\%\ reading\ CCMD\ website(\#days\ website\ defaced)$

$+ (\%\ following\ Sam\ on\ Twitter$

$+\ \%\ receiving\ party\ emails)(\#posts\ or\ email\ about\ corrupt\ official)$

$+$ % viewing *8*Chan(#days *platform available)(#posts per day)*

$+\ \%\ viewing\ newsotheday(\#stories\ about\ low\ wages)$

$+$ (% *following Betty on Instagram + % in Betty's Facebook fan group)(#memes)*

$+ (\%\ following\ Sam\ on\ Twitter)(\#Bank\ Hoax\ retweets)$

$+\ \%\ viewing\ billboard(\#days\ billboard\ burned\ or\ unrepaired\ )$

$\div\ \#channels\ in\ info\ map$

∴ Penetration (P) $= \frac{0.01(1)+(0.20+0.14)1+(0.03)(15)(3)+0.20(8)+(0.50+0.12)(2)+(0.35)(10)+.07(22)}{10} =$ 95.9%

C.6.2.2 Isolate (I)

$+ \%\ viewing\ CCMD\ website(\%\ days\ website\ unreadable)$

$\div \#channels\ in\ info\ map$

$\therefore$ Isolate (I) $= \frac{0.01(0.0333)}{10} =$ **0.003%**

C.6.2.3 Activate (A)

$\%\ TA\ activity\ with\ keywords = (trade +\ agreement\ or\ USXTA\ or\ US + Trade,\ or\ US + X + Economy)$

$\therefore$ Activate (A) $=$ **23.0%**

C.6.2.4 Resonate (R)

$(\#\ Positive\ responses\ to\ content$

$+\#\ Positive\ amplifications)$

$-(\#\ Negative\ responses\ to\ content$

$+Negative\ amplifications)$

$\div Total\ responses$

$\therefore$ Resonate (R) $= \frac{(1.5+.5)-(3+1.75)}{100} =$ **-2.75%**

C.6.2.5 Persuade (S)

$\%\ responding\ positively\ to\ survey\ at\ end\ of\ month\ -\ \%\ responding\ positively\ at\ baseline$

$\therefore$ Persuade (S) $= 0.19 - 0.18 =$ **1.0%**

C.6.2.6 Motivate (M)

$$\frac{\#\ positive\ articles\ this\ month}{Total\ articles\ this\ month} - \frac{\#\ positive\ articles\ at\ baseline}{total\ articles\ at\ baseline}$$

$\therefore$ Motivate (M) $= \frac{7}{11} - \frac{18}{27} =$ **-3.0%**

C.6.2.7 Impact Score (K)

Impact (K) $= \frac{P+I+A+R+S+5(M)}{10} = \frac{0.959+0.00003+0.23+(-0.0275)+0.01+5(-0.03)}{10} =$ **10.2%**

C.7 Portraying and Interpreting the Impact Scores

The art and science of data visualization are well beyond the scope of this paper. The examples in this section demonstrate how to interpret the scores and connect them to specific recommendations based on the SP!CE™ framework.

C.7.1 Interpreting the Penetrate, Isolate, and Activate Scores

The three dials in Figure C-2 have a red needle for the enemy score and a green needle for the friendly score. The range on these dials goes from 0 to 100 percent. These three metrics aim to achieve as close to 100 percent as possible and deny one's opponent a high score, making both the absolute score and the distance between the needles noteworthy.

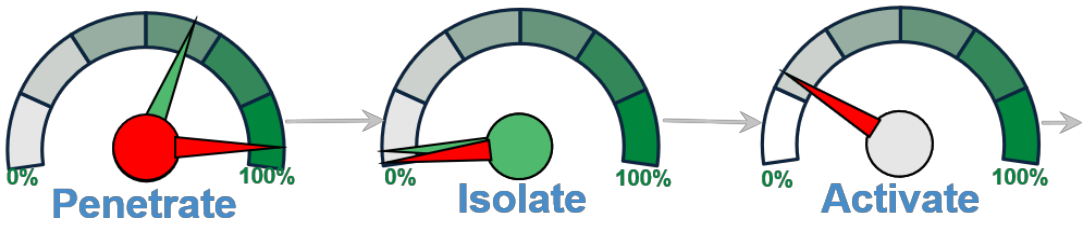

Figure C-2. Penetrate, Isolate, and Activate Score Indicators

While both the friendly and the enemy campaigns penetrated most of the target audience, the enemy score was significantly higher. Friendly influencers should revisit the "Cultivate Information Pathways," "Select Platforms," "Deliver Content," and "Amplify Supporting Information" tactics and techniques in the SP!CE™ framework and adjust the campaign to raise their Penetrate score.

Another way to reduce the enemy's ability to penetrate the audience is to raise the friendly isolate score. In this example, both the friendly and enemy influence campaigns had very low isolate scores. Higher isolate scores primarily result from successfully using the techniques under the "Manipulate Information Flows" tactic in the SP!CE™ framework. The wide margin between the penetrate scores overshadows the slight advantage that the friendly campaign has in its isolate score, so the friendly assessment team should conclude that their campaign failed to isolate the target audience.

Since both the enemy and friendly campaigns target the same audience for competing objectives, their activate scores are identical. Twenty-three percent of the target audience shows interest in the USXTA topic. The techniques listed under the "Establish Legitimacy," "Enlist Intermediaries," and "Develop Content" tactics in the SP!CE™ framework have the most significant impact on the activate score, so the assessment team should recommend changes in those portions of the campaign.

C.7.2 Interpreting the Resonate, Persuade, and Motivate Scores

The three dials in Figure C-3 have a red needle for the enemy score and a green needle for the friendly score. Unlike the previous dials, the range on these three dials goes from -15 percent to +15 percent because the scores can be either positive or negative.

Figure C-3. Resonate, Persuade, and Motivate Score Indicators

The negative enemy resonate score points to a potential weakness in the enemy's campaign. The most likely proximate causes of negative resonate scores are the enemy's failure to execute the "Establish Legitimacy" and "Develop Content" tactics correctly in the SP!CE™ framework or friendly efforts under the "Denigrate Opposing Information" tactic in the SP!CE™ framework.

The assessment team recommends to the commander that efforts to denigrate enemy information increase to exploit this opportunity. The positive resonate score for the friendly campaign indicates that the target audience generally accepts the information presented; therefore, the assessment team recommends maintaining the current thematic approach.

Although both enemy and friendly persuade scores are positive, the higher friendly score indicates that attitudes about the USXTA are shifting slightly in favor of the friendly position. Since this is only the first month of the campaign, and the scores are relatively close, the persuade score should be closely tracked in the future to see if the positive trend continues.

The motivate score is the most significant of the impact score elements because it measures the target audience's behavior, which is the *raison d' être* for the influence campaign. Although this month saw more negative USXTA articles (seven) than positive ones (four), the change in the percentage of positive articles from the initial baseline (nine positive and 18 negative) is encouraging. Since the friendly motivate score is positive and the enemy score is negative, the assessment team concludes that the campaign is an overall success.

C.7.3 Interpreting the Overall Impact Scores

The campaign score provides a comparative measure for the quality of influence campaigns. The impact score measures the effect of an influence campaign on the target audience over time. For planners, policymakers, and operators involved in influence activities, these values are most useful in refining and adjusting a campaign to increase effectiveness. The influencer should add resources or apply additional effort to parts of the campaign with lower scores. Assessments on adversary campaigns help focus resources on detecting other campaign activities and point to the areas where a campaign is most likely to be effectively countered.

In this example, the friendly impact score is 11.6 percent. The enemy score was 10.2 percent, indicating that the friendly campaign has a slightly greater impact on the target audience than the enemy campaign. The higher impact score, combined with the positive motivate score, should give the commander hope that the campaign is working. The assessment team's top three recommendations to increase friendly success are:

- Increase information actions in the "Manipulate Information Flows" tactic in the SP!CE™ framework to further isolate the target audience from opposing information and lower enemy information penetration.
- Increase information actions in the "Denigrate Opposing Information" tactic in the SP!CE™ framework to exploit the enemy's negative resonate score and discourage the target audience from considering enemy information.
- Sustain information actions in the "Develop Content" and "Deliver Content" tactics in the SP!CE™ framework as the target audience is generally positive towards this information, and it is persuasive.

C.8 Tracking Impact over Time

Meaningful and sustainable change in a target audience is a long-term process, and it is essential to track progress throughout the campaign and assess at regular intervals. This example provided a single assessment at the end of the first month of a campaign. The next step is to use this assessment results as the baseline for the next month's assessment. After several months and campaign adjustments, trends in the impact score should emerge that are more meaningful than a single assessment alone. The assessment team should maintain consistency in data sources and

collection to ensure that month-to-month comparisons are valid as rigorous adherence to the SP!CE™ methodology produces the most useful results.

Appendix D Current SP!CE™ Framework

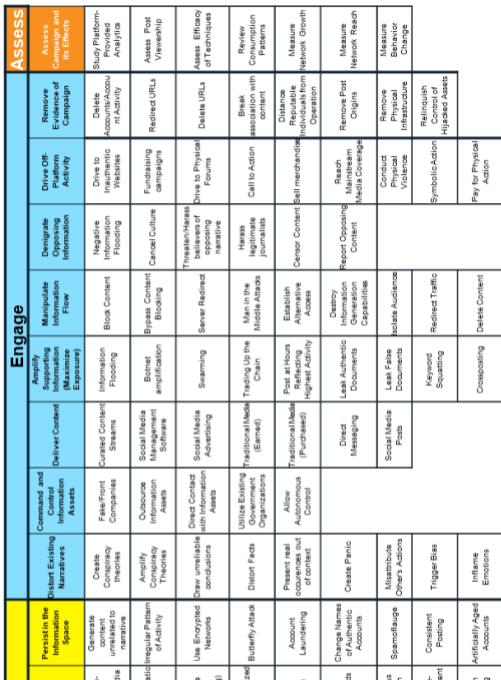

Figure D-1. SP!CE™ Framework as of March 19, 2021