REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
10/5/2023	Technical Report	

4. TITLE AND SUBTITLE

Structured Process for Information Campaign Enhancement (SP!CE) 2.2

5a. CONTRACT NUMBER

FA8702-23-C-0001

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Daniel R. Sixto; Hannah Lettie; Paul S. Kim

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

The MITRE Corporation
7515 Colshire Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER

PRS-23-1986

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

United States Air Force (AFLCMC)

10. SPONSOR/MONITOR'S ACRONYM(S)

AFLCMC

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The Structured Process for Information Campaign Enhancement (SP!CE) 2.2 capability supports strategic competition in the information environment for the U.S. Department of Defense, its partners, and allies. SP!CE 2.2 makes several substantive adjustments to the SP!CE 2.1 framework's structure in efforts to support visualization, planning, assessment, and execution when conducting allied information operations and countering adversary campaigns.

15. SUBJECT TERMS

Social and Behavioral Sciences (General); SP!CE; adversary behavior; Structured Process for Information Campaign Enhancement; influence campaigns

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Susan Carpenito
				99	19b. TELEPHONE NUMBER *(Include area code)* 781-271-7646

MITRE

MITRE PAPER

Structured Process for Information Campaign Enhancement (SP!CE) 2.2

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

Daniel R. Sixto
Hannah Lettie
Paul S. Kim

August 2023

Approved for Public Release; Distribution Unlimited. Public Release Case Number 23-3191

This technical data was produced for the U. S. Government under Contract No. FA8702-19-C-0001, and is subject to the Rights in Technical Data-Noncommercial Items Clause DFARS 252.227-7013 (AUG 2023)

McLean, VA

Approved By

Joe Ferraro, Cyber Division Chief Engineer, N140	Date
Michael Minter, Cyber C2 & Effects Outcome Lead, N142	Date

Abstract

The Structured Process for Information Campaign Enhancement (SP!CE) 2.2 capability supports strategic competition in the information environment for the U.S. Department of Defense, its partners, and allies. SP!CE 2.2 makes several substantive adjustments to the SP!CE 2.1 framework's structure in efforts to support visualization, planning, assessment, and execution when conducting allied information operations and countering adversary campaigns. SP!CE comprises of (1) a framework defining the phases, tactics, and techniques of an influence operation, (2) a set of rating scales to support operators when assessing measures of performance for allied campaigns and modeling adversary behavior, and (3) a knowledge base of historical influence campaigns tagged to the framework that could support training and campaign modeling efforts. This specification defines the phases, tactics, and techniques of the framework, provides the rating scales for each technique, and describes the structure of the knowledge base.

This page intentionally left blank.

Executive Summary

The Structured Process for Information Campaign Enhancement (SP!CE) 2.2 specification updates the SP!CE framework's structure, content, and lexicon with the ultimate goal of enabling communication among analysts and operators in the information environment. SP!CE 2.2 incorporates a review of U.S. government sources outlining policy for operations in the information environment and integrates psychological behavior change models in multiple techniques.

The Structured Process for Information Campaign Enhancement (SP!CE) specification defines the phases, tactics, and techniques in the SP!CE framework, provides a set of rating scales to assess measures of performance for techniques in a specific campaign, and describes a knowledge base of historical influence campaigns tagged to the framework.[1] SP!CE provides U.S. government operators and analysts with a capability to enable visualization, planning, execution, and assessment tools to conduct allied influence operations and counter adversary campaigns. The SP!CE framework is structured to model tactics and techniques in an influence operation from the initial planning phase to execution. The SP!CE rating scales incorporate assessment throughout the framework and support operators when assessing measures of performance. The SP!CE knowledge base supports operators when visualizing campaigns with a corpus of historical influence operations tagged to the SP!CE framework

The SP!CE framework is structured by phase, tactic, and technique and covers each step from the early planning procedure before conducting an operation to its final assessment.[2] Each SP!CE framework phase represents a logical stage during an operation, tactics represent goals, and techniques represent methods to achieve goals outlined by tactics. Many techniques in the SP!CE framework contain multiple subtechniques outlining more detailed ways to use techniques.

Each technique in the SP!CE framework includes its own rating scale to assess measures of performance (MOPs).[3] SP!CE rating scales measure the level of investment an actor places into a technique. Ratings are measured on a scale of zero to three, where a rating of zero indicates that an actor did not use a technique during a campaign and a three indicates that a campaign conducted target audience analysis to effectively use a technique. The rating scale provides insights to operators when studying MOPs by outlining which steps an operation successfully completed.

The SP!CE knowledge base is a corpus of historical influence operations conducted by actors spanning states, private firms and individuals.[4] The knowledge base supports operators with case studies outlining the historical tradecraft of their adversaries for influence operations. Referencing the knowledge base when conducting allied influence operations helps operators prepare to counter any adversary responses to their campaigns.

[1] Sixto, D.R. and Kim, P.S (2023). "Structured Process for Influence Campaign Enhancement 2.1", PR 23-1986, The MITRE Corp.

[2] Ibid.

[3] Ibid.

[4] Ibid.

Acknowledgments

SP!CE owes much of its work to MITRE ATT&CK's foundational research.[5] ATT&CK is a "knowledge base of adversary tactics and techniques based on real-world observations" which laid the groundwork for practitioners to map, counter, and record adversary behavior to support cybersecurity resilience efforts. The SP!CE framework follows a similar mission to ATT&CK and documents adversary activities while informing responses to influence operations.

Following the establishment of a strategic partnership between the MITRE Corporation and Florida International University (FIU) in 2019, FIU has continuously shared its expertise while leading initatives developing and applying SP!CE to real-world scenarios. MITRE would like to offer its deepest gratitude to Dr. Mark Finlayson for leading the FIU effort and sharing its work with the wider community, Mr. Brian Fonseca for his efforts coordinating the MITRE-FIU partnership, and FIU students Claudia Perez Brito, Bryan Ruesca, Gabriella Berry, and Allen Mendes for driving work applying SP!CE to real-world scenarios and diligently supporting efforts to merge SP!CE with the Disinformation and Risk Management (DISARM) framework.

MITRE would also like to thank the DISARM foundation for its partnership with MITRE. The DISARM framework, formerly referred to as the Adversarial Misinformation and Influence Tactics and Techniques (AMITT) framework, is used to detect, counter, and document influence operations. In 2022, MITRE lent its expertise and merged SP!CE with AMITT to support the creation of the DISARM framework. Insights derived from this merge were incorporated into SP!CE version 2.0, the direct precursor to version 2.1.While the SP!CE framework will continue to independently serve the U.S. Department of Defense and its partners, MITRE plans to continue collaborating with DISARM to address the whole-of-society problem of cyber-enabled foreign influence and disinformation operations. For more information on the relationship between ATT&CK, AMITT, SP!CE, and DISARM, we refer the reader to the acknowledgements section of the SP!CE Specification version 1.0.[6]

Finally, MITRE would also like to extend its gratitude to Savina Koda, a former MITRE employee and FIU student responsible for research developing the original SP!CE framework, ratings, and knowledge base of case studies.

[5] MITRE Staff (2023). "MITRE ATT&CK", The MITRE Corp. Retrieved from https://attack.mitre.org/.

[6] Venhaus, J.M., Sixto, D.R., Koda, S., Fulk, M., Finlayson, M.A., Lopez Diaz, Z.A. (2021). "Structured Process for Influence Campaign Evaluation", Doc. MP210039, The MITRE Corp.

Table of Contents

1 Introduction 1-1
2 SP!CE Technique Descriptions and Ratings A-1
2.1 SP!CE Framework Structure A-1
2.2 Updates to SP!CE 2.2 ..... A-2
2.3 Plan Phase A-3
2.3.1 Determine Strategic End-State Tactic A-3
2.3.1.1 Review Existing Strategies and Policies A-3
2.3.1.2 Determine Strategic Objective A-3
2.3.1.3 Determine Desired Operational Outcomes A-4
2.3.1.4 Outline Operational Purpose A-4
2.3.1.5 Identify Relevant Information Activities A-5
2.3.1.6 Review Adversary Operation Strategy A-5
2.3.1.7 Identify Potential Target Audiences A-5
2.3.1.8 Identify Desired Level of Engagement A-6
2.3.2 Develop Operational Requirements A-7
2.3.2.1 Articulate Force Requirements A-7
2.3.2.2 Define Impact Indicators A-7
2.3.2.3 Establish Initial Assessment Criteria A-7
2.3.2.4 Review Postulations A-8
2.3.2.5 Mitigate Analytic Gaps A-8
2.3.2.6 Outline Operations Security Planning Guidance A-9
2.3.2.7 Develop Master/Strategic Narrative A-9
2.3.2.8 Integrate Vulnerabilities into Narrative A-9
2.3.2.9 Mitigate Potential Disruptors A-10
2.3.2.10 Identify Optimal Delivery Timeline A-10
2.4 Survey Phase A-11
2.4.1 Study Target Audience Information Environment A-11
2.4.1.1 Organize Situation Monitoring Requirements A-11
2.4.1.2 Reference Social Media Analytics A-11
2.4.1.3 Evaluate Media Surveys A-12
2.4.1.4 Apply Web Usage Analysis A-12
2.4.1.5 Assess Degree of Media Access A-12
2.4.1.6 Identify Trending Topics A-13

2.4.1.7 Identify Obstacles to Operation Success A-13
2.4.1.8 Study Competitors A-14
2.4.2 Study Social Landscape A-14
2.4.2.1 Reference Cultural Analysis A-14
2.4.2.2 Study Ongoing Target Audience Activities A-15
2.4.2.3 Identify Target Audience Incentives A-16
2.4.2.4 Identify Cognitive Predispositions A-17
2.4.2.5 Study Social Sentiment A-17
2.4.2.6 Study Existing Narratives A-18
2.4.2.7 Identify Social Vulnerabilities A-18
2.4.2.8 Identify Target Audience Proclivity to Change A-19
2.4.3 Select Operation Platforms A-19
2.4.3.1 Assess Target Audience Platform Usage A-19
2.4.3.2 Assess Target Audience Platform Usage Frequency A-20
2.4.3.3 Study Composition of Platform Content A-20
2.4.3.4 Assess Platform Utility A-20
2.4.4 Study Technical Landscape A-21
2.4.4.1 Identify Vulnerable Security Infrastructure A-21
2.4.4.2 Identify Data Voids A-21
2.4.4.3 Study Media System Landscape A-22
2.4.5 Emplace Sensors A-22
2.4.5.1 Observe Online Behavior A-22
2.4.5.2 Observe Offline Behavior A-23
2.4.5.3 Outline Collection Plan A-23
2.4.5.4 Pre-Test Products A-23
2.4.5.5 Monitor Funding Flows A-24
2.4.5.6 Survey Public Opinion A-24
2.4.5.7 Employ Commercial Analytic Firms A-25
2.5 Enable Phase A-25
2.5.1 Evaluate Resources A-25
2.5.1.1 Review Existing Messaging Strategies A-25
2.5.1.2 Identify Potential Campaign Constraints A-26
2.5.1.3 Collect Historical Content A-26
2.5.1.4 Review Existing Information-Related Capabilities (IRCs) A-26
2.5.1.5 Leverage Partners A-27

2.5.1.6 Review Logistics A-27
2.5.2 Establish Information Assets and Intermediaries A-28
2.5.2.1 Create Online Entities A-28
2.5.2.2 Develop Offline Entities A-28
2.5.2.3 Establish Proxy Entities A-29
2.5.2.4 Secure Dissemination Means A-29
2.5.3 Cultivate Information Pathways A-30
2.5.3.1 Create Forums A-30
2.5.3.2 Infiltrate Existing Forums A-30
2.5.3.3 Secure Off-Platform Production Capabilities A-30
2.5.3.4 Prepare Fundraising Campaigns A-31
2.5.4 Design and Develop Products A-31
2.5.4.1 Identify Product Types for Development A-31
2.5.4.2 Develop Human-Driven Media A-32
2.5.4.3 Create AI-Driven Media A-33
2.5.4.4 Present Desired Target Audience Actions A-34
2.5.4.5 Tailor Content to Selected Platforms A-34
2.5.4.6 Launder Information A-34
2.5.5 Establish Legitimacy A-35
2.5.5.1 Create Localized Content A-35
2.5.5.2 Co-opt Trusted Sources A-36
2.5.5.3 Curate Social Proof A-36
2.5.5.4 Leverage Existing Biases A-37
2.5.6 Enable Persistence A-37
2.5.6.1 Refine Initial Assessment Criteria A-37
2.5.6.2 Edit Existing Accounts A-38
2.5.6.3 Conceal Network Identity A-38
2.5.6.4 Conceal Sponsorship A-39
2.6 Engage Phase A-40
2.6.1 Persist in the Information Environment A-40
2.6.1.1 Use Encrypted Networks A-40
2.6.1.2 Infiltrate and Mimic Social Groups A-41
2.6.1.3 Disguise Spam Messages A-41
2.6.1.4 Artificially Age Accounts A-42
2.6.1.5 Utilize Lenient Hosting Services A-42

2.6.1.6 Misattribute Activity A-43
2.6.1.7 Unattribute Activity A-43
2.6.1.8 Vary Type of Account Used A-43
2.6.1.9 Exploit Legal System A-44
2.6.2 Distort Existing Narratives A-44
2.6.2.1 Amplify Conspiracy Theories A-44
2.6.2.2 Reframe Context A-45
2.6.2.3 Use Malign Rhetoric A-46
2.6.2.4 Exploit Data Voids A-46
2.6.2.5 Post Provocative Content A-47
2.6.3 Deliver Products A-48
2.6.3.1 Post on Platforms A-48
2.6.3.2 Receive Media Exposure A-48
2.6.3.3 Leak Documents A-49
2.6.3.4 Microtargeting A-50
2.6.3.5 Utilize Social Media Management Software A-50
2.6.3.6 Target Purchased Ads A-51
2.6.4 Amplify Supporting Information (Maximize Exposure) A-51
2.6.4.1 Distribute Products to Disseminating Entities A-51
2.6.4.2 Conduct Information Flooding A-52
2.6.4.3 Conduct Botnet Amplification A-53
2.6.4.4 Exploit Platform-Specific Features A-54
2.6.4.5 Conduct Cross-Posting A-54
2.6.4.6 Post Consistently Over Time A-55
2.6.4.7 Post at Hours Reflecting Highest Activity A-55
2.6.4.8 Leverage Platform Algorithm A-56
2.6.4.9 Automate Forwarding and Reposting A-56
2.6.4.10 Astroturfing ..... **Error! Bookmark not defined.**
2.6.4.11 Incentivize Sharing A-57
2.6.5 Disrupt Information Flow A-58
2.6.5.1 Block Content A-58
2.6.5.2 Bypass Content Blocking A-59
2.6.5.3 Destroy Information Generation Capabilities A-60
2.6.6 Denigrate Opposing Information A-60
2.6.6.1 Denigrate Believers of Opposing Narratives A-60

2.6.6.2 Report Opposing Content A-61
2.6.7 Drive Off-Platform Activity A-61
2.6.7.1 Drive to Alternative Platforms A-61
2.6.7.2 Drive to Physical Forums A-62
2.6.7.3 Call to Action A-62
2.6.7.4 Conduct Symbolic Action A-63
2.6.7.5 Conduct Physical Action A-64
2.6.7.6 Reach Mainstream Media Coverage A-64
2.6.7.7 Conduct Fundraising Campaigns A-65
2.6.7.8 Sell Merchandise A-65
2.6.8 Remove Evidence of Tactics A-66
2.6.8.1 Delete Account Activity A-66
2.6.8.2 Redirect URLs A-66
2.6.8.3 Delete URLs A-67
2.6.8.4 Remove Association from Content A-67
2.7 Assess Phase A-69
2.7.1 Assess Techniques A-69
2.7.1.1 Use Technique Ratings System A-69
2.7.1.2 Review Factors Affecting IO A-69
2.7.1.3 Map Operations in Information Environment to Framework A-69
2.7.1.4 Conduct Analysis of Alternatives A-69
2.7.2 Assess Key Performance Indicators (KPIs) A-70
2.7.2.1 Measure Operational Effects A-70
3 SP!CE Framework Matrix A-71
4 SP!CE Knowledge Base A-72
Glossary A-1
Appendix A Abbreviations A-1

List of Figures

Figure 1: Illustration of the SP!CE Framework Structure, showing the Plan and Survey phases with its underlying tactics and techniques..... A-2

Figure 2: SP!CE 2.2 Framework Matrix..... A-71

Figure 3: Techniques Tagged to the Knowledge Base on the current SP!CE Framework..... A-72

1 Introduction

The Structured Process for Information Campaign Enhancement (SP!CE) capability provides the U.S. government (USG) with a capability to map behavior, assess progress, execute, and develop strategies for operations in the information environment.[i] SP!CE consists of three tools: the framework, ratings scale, and knowledge base. SP!CE is accompanied by an interactive dashboard known as SP!CE Dash. The tool enables collaboration among USG operators when using SP!CE to plan and execute influence operations.

The SP!CE framework, ratings, and knowledge base respectively help operators map campaigns, assess progress, and identify relevant historical campaigns to inform courses of action. The SP!CE 2.2 framework builds on the SP!CE 1.0 and 2.1 frameworks to incorporate a more comprehensive collection of tactics and techniques relevant to influence operations.[ii] SP!CE tactics and techniques support operators when working on setting objectives, developing targets, and executing operations.

The SP!CE ratings system incorporates techniques when assessing measures of performance (MOPs).[iii] Each technique on the framework has a defined rating, ranging from 0-3, determined by the operator and supported by several data sources and techniques.

The SP!CE knowledge base presents a collection of historical adversary influence operations intended to inform operators of previous strategies, tactics, goals, and targeted audiences.[iv]

The SP!CE framework, its ratings, and the knowledge base all intend to optimize influence operations supporting integrated deterrence and managing strategic competition.[v] Specifically, the SP!CE capability is intended to add structure to the way information operations are conducted and assessed. The framework can guide decision-making without restricting analysis or neglecting nuance. SP!CE ratings present a general set of MOPs to guide assessment.[vi] Finally, the knowledge base lays the foundation for a corpus of operations mapped to a shareable format.

SP!CE supports integrated deterrence by providing operators and analysts with a set of tools to increase collaboration, coordinate operations, and inform their leadership's strategies.[vii] As competitors like Russia and China continue to conduct influence operations to disrupt, undermine, and deceive U.S. and allied audiences, the USG requires capabilities to streamline operation processes to substantively contribute to the whole of society problem of managing strategic competition.

2 SP!CE Technique Descriptions and Ratings

The SP!CE framework is structured as a hierarchy of phases, tactics, and techniques. Phases represent a general stage of an operation. For example, the "Plan" phase covers strategy development and target audience analysis. Tactics represent "what" an actor conducting operations may seek to achieve. Many tactics represent tactical goals that should be met in pursuit of strategic success. Finally, techniques represent "how" an actor may achieve a goal outlined by a tactic. Subtechniques often provide additional context to techniques by listing examples of how an actor may use a technique. For example, the "Develop Human-Driven Media" technique includes subtechniques like memes, text-based content, or misinfographics.[viii]

2.1 SP!CE Framework Structure

The SP!CE framework is structured into phases, tactics, techniques, and subtechniques. This structure enables operators to easily navigate through the framework's 23 tactics and over 150 techniques. The framework runs in sequential order and outlines techniques from the initial planning and goal-setting stages of an influence operation to the final measures of performance and effectiveness assessments while incorporating target audience analysis, forum creation, content delivery, and other stages in between.[ix]

SP!CE phases sit at the top of the framework structure and outline the five stages of an operation: plan, survey, enable, engage, and assess. Phases represent a definitive stage of an operation or campaign during which a large portion of the forces and capabilities are involved in similar or mutually supporting activities for a common purpose.[x] For example, the "Survey" phase includes tactics such as "Study Target Audience (TA) Information Environment", "Study Social Landscape", and "Study Technical Landscape" to support operators in the goal setting and target audience analysis processes while planning a campaign.

SP!CE tactics lie between phases and techniques and outline "what" an actor may seek to achieve. Tactics represent the employment and ordered arrangement of forces in relation to each other.[xi] The 23 tactics in SP!CE outline steps to take when developing strategy, organizing resources, engaging with the target audience, and assessing performance. Many SP!CE tactics are phrased as outcomes or behaviors. For example, the "Establish Legitimacy", "Disrupt Information Flow", and "Persist in the Information Space" tactics represent short-term goals that feed into a longer campaign.[xii]

SP!CE techniques lie under tactics and outline "how" an actor could achieve a goal outlined by a tactic.[xiii] Techniques refer to non-prescriptive ways or methods used to perform missions, functions, or tasks.[xiv] For example, the "Deliver Content" tactic contains specific techniques like "Post on Platforms", "Leak Documents", or "Microtargeting." Some campaigns may require a wider diversity of selected techniques than others and operation planners should draw on previous target audience analysis to select effective techniques. Many SP!CE techniques include subtechniques which list more specific methods to use a technique. Subtechniques represent more granular versions of techniques and provide further procedural detail when conducting an operation. For example, an operation using the "Create AI-Driven Media" technique may benefit from further exploration of the different forms of artificial intelligence driven content like deepfakes, cheapfakes, AI-generated text, and AI-generated images.[xv]

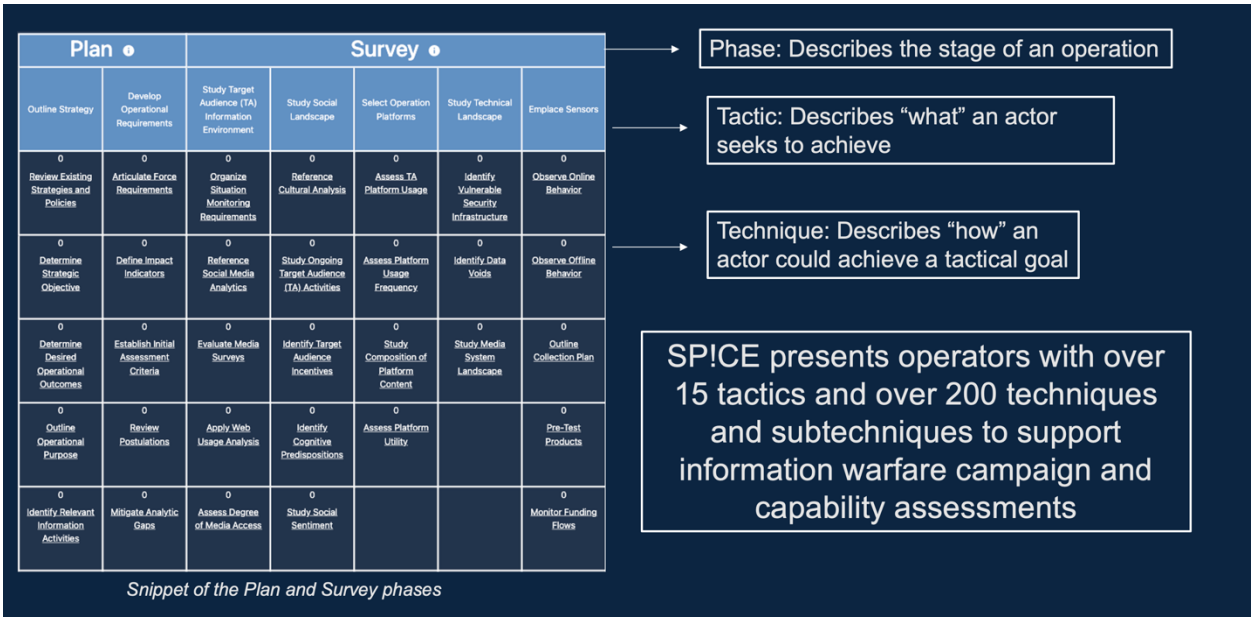

Figure 1: Illustration of the SP!CE Framework Structure, showing the Plan and Survey phases with its underlying tactics and techniques.

2.2 Updates in SP!CE 2.2

The SP!CE 2.2 specification incorporates several updates to the SP!CE framework's structure, content, and lexicon with the ultimate goal of enabling communication among analysts and operators in the information environment. Updates in SP!CE 2.2 resulted from feedback collected from a framework review conducted by current and former USG operators.

Incorporating DOD literature further aligned SP!CE to the USG's approach to operations in the information environment. A review of Department of Defense (DOD) literature on operations in the information environment, the psychological operations process, and military information support operations guided many of the edits to the SP!CE framework's phases, tactics, and techniques. One change, for example, resulted in the addition of a new "Survey" phase including many of the tactics and techniques associated with the target audience analysis process. Other techniques, such as "Identify Optimal Delivery Time" and "Present Desired Target Audience Actions", allow operators to study how and when to interact with the target audience before delivering products.

SP!CE 2.2 further incorporates insights from psychological behavior change models. In order to include more specific methods to communicate with target audiences, several techniques now reference relevant models that outline steps to approach target audience research and message delivery. The "Identify Obstacles to Operation Success" technique, for example, encourages operators to reference the Fogg Behavior Model when thinking about how individuals in the target audience will make decisions.

The specification additionally renamed certain techniques to avoid unnecessary jargon while making the framework's lexicon as intuitive and descriptive as possible. For example, the "Utilize Butterfly Attacks" technique was renamed to "Infiltrate and Mimic Social Groups." Renaming techniques loaded with jargon will increase the framework's navigability while diminishing the time required to familiarize oneself with certain techniques.

SP!CE 2.2 aims to increase communication among operators in the information environment. Incorporating changes that better reflect the policies that SP!CE's users abide by will improve the way operations are planned and executed. SP!CE 2.2's updates will also allow operators to effectively update their leadership on operation progress.

2.3 Plan Phase

2.3.1 Determine Strategic End-State Tactic

2.3.1.1 Review Existing Strategies and Policies

Sub-Techniques: Coordinate Multinational Operations, Review Rules of Engagement and Special Instructions, Comply to National-Level Strategies, Conduct Phasing, Review Authorizations, Review Unified Command Plan, Review Joint Strategic Capabilities Plan, Identify Relevant Commands and Force Structures

Examine existing national strategy, legislation, guidance from policymakers, external partnerships, and agreements to help determine an upcoming operation's objectives.

An operation in the information environment should also abide by national level policies to stay consistent with previously set goals. Successful operations should successfully identify relevant policies and find avenues for efficient implementation. Additionally, successful operations should translate national and theater-specific strategies into operational concepts.

Rating:

0. Operation does not review existing strategies and policies.
1. Operation reviews existing strategies and policies that are irrelevant and unimpactful to its determined goals.
2. Operation reviews relevant existing strategies and policies but fails to integrate them to its determined goals.
3. Operation reviews relevant existing strategies and policies and successfully integrates them with its determined goals.

2.3.1.2 Determine Strategic Objective

Sub-Techniques: Achieve Domestic Political Advantage, Undermine Public Health and Safety Attain Policy Change, Achieve Financial Gain, Promote an Alternative, Degrade Adversary Image, Achieve Geopolitical Advantage, Deter Aggression, Reach Policy Paralysis, Improve Actor Image, Prop up Local Government to Gain Influence

When determining a strategic objective, one outlines the overarching goals for all of an actor's associated entities to follow for the duration of an operation. A strategic objective identifies what an operation ultimately seeks to work towards while providing broad yet clear guidance to all related entities.

Rating:

0. Operation does not determine strategic objectives.
1. Operation achieves one of three criteria: sets a broad, clear, or malleable goal. e.g., to win a war. (broad, not clear nor malleable).
2. Operation achieves two of three criteria: sets a broad, clear, or malleable goal. e.g., to win a kinetic war against X country before a set date. (broad and clear, not malleable).
3. Operation achieves three of three criteria: sets a broad, clear, and malleable goal. e.g., to win a war against X country (broad, clear, malleable).

2.3.1.3 Determine Desired Operational Outcomes

Sub-Techniques: Manipulate Voting, Join a Movement, Encourage Fringe Behavior, Discredit Credible Sources, Muddy the Truth, Undermine Trust in Government/Candidates, Promote Narrative, Discourage Support, Inflame Emotions, Sow Confusion, Receive Recognition

An operation, after determining its strategic objectives, will outline tangible short-term goals to achieve in pursuit of the strategic goal. Successfully completing multiple operational objectives is more likely to yield operation success. Some operational objectives may include successfully evoking behaviors among the target audience.

Rating:

0. Operation does not determine operational objectives.
1. Operation selects erratic, incoherent, and irrelevant operational objectives.
2. Operation selects actionable and relevant operational objectives but communicates them incoherently.
3. Operation selects actionable, coherent, and relevant operational objectives.

2.3.1.4 Outline Operational Purpose

Sub-Techniques:

Outlining an operational purpose helps planners set priorities and later request relevant forces and capabilities for a campaign.[xvi] An operation's purpose refers to its desired end-state, effects on the target audience and types of capabilities used.

Rating:

0. Operation does not outline its operational purpose.
1. Operation outlines an unclear operational purpose that refers to vague or irrelevant required capabilities or strategic objectives.
2. Operation outlines an operational purpose that either clearly refers to required capabilities or strategic objectives.
3. Operation outlines a clear operational purpose that refers to its capabilities and strategic objectives.

2.3.1.5 Identify Relevant Information Activities

Sub-Techniques: Military Information Support Operations, Public Affairs, Information Operations, Defense Support to Public Diplomacy

After identifying goals and desired behaviors, an actor should identify different information-related activities that will help them achieve success in the information environment.[xvii] Information activities include general functions, capabilities, and tools that help actors formulate messaging for their intended audiences. For example, an overt campaign seeking to raise awareness to potentially dangerous weather may rely on public affairs, while an operation seeking to influence a target audience for geopolitical gains may refer to covert information operations.

Rating:

0. Operation does not identify relevant information activities.
1. Operation identifies irrelevant information activities that do not support operation goals or create relevant messaging for the target audience.
2. Operation identifies information activities that will either directly support operation goals or create relevant messaging for the target audience.
3. Operation identifies information activities that will directly support operation goals and create relevant messaging for the target audience.

2.3.1.6 Review Adversary Operation Strategy

Sub-Techniques: Study Adversary Decision-makers and Staff, Study Adversary Intelligence Systems, Study Adversary Intended Target Audiences, Outline Adversary Command Systems

An operation in the information environment may consult previously documented adversary operations to best understand commonly used tactics, techniques, and procedures. Understanding opposing strategies and tradecraft can help operators develop counters and minimize their adversary's potential for influence.

Rating:

0. Operation does not review adversary operation strategy.
1. Operation fulfills one of three: reviews adversary strategic doctrine, identifies an adversary's previously documented techniques, reviews adversary material capabilities.
2. Operation fulfills two of three: reviews adversary strategic doctrine, identifies an adversary's previously documented techniques, reviews adversary material capabilities.
3. Operation fulfills three of three: reviews adversary strategic doctrine, identifies an adversary's previously documented techniques, reviews adversary material capabilities.

2.3.1.7 Identify Potential Target Audiences

Sub-Techniques:

Before conducting a target audience analysis, an operation's leadership should identify multiple candidate populations to influence. These potential target audiences will provide planners and researchers with a starting point before prioritizing certain groups to conduct a deeper analysis on and identify strategies to influence them.

Rating:

0. Operation does not identify potential target audiences.
1. Operation leadership outlines multiple potential target audiences with direction for further analysis relevant to operation goals but not to organizational roles or material capabilities.
2. Operation leadership outlines multiple potential target audiences with direction for further analysis relevant to operation goals and organizational roles but not material capabilities.
3. Operation leadership outlines multiple potential target audiences with direction for further analysis relevant to operation goals, organizational roles, and material capabilities.

2.3.1.8 Identify Desired Level of Engagement

Sub-Techniques:

The desired level of engagement outlines how an operation will interact with its intended audience. Planners should derive the desired level of engagement by linking an operation's goals to an effective communication strategy. For example, an operation seeking to evacuate a population from their homes due to an incoming natural disaster should communicate as clearly and directly as possible.

When outlining a strategy delineating an operation's desired level of engagement, planners should consider a population's potential resistance to change by studying the type of material the audience may pay attention to, the value of forewarning a message, and their prior knowledge or experiences related to an issue.[xviii]

Rating:

0. The operation does not identify a desired level of engagement.
1. The operation identifies a desired level of engagement and fulfills one of three: outlines a level of engagement that will directly support operation strategic goals, outlines a level of engagement that appears receptive to potential target audiences, identifies a level of engagement that is relevant to desired operational outcomes.
2. The operation identifies a desired level of engagement and fulfills two of three: outlines a level of engagement that will directly support operation strategic goals, outlines a level of engagement that appears receptive to potential target audiences, identifies a level of engagement that is relevant to desired operational outcomes.
3. The operation identifies a desired level of engagement and fulfills three of three: outlines a level of engagement that will directly support operation strategic goals, outlines a level

of engagement that appears receptive to potential target audiences, identifies a level of engagement that is relevant to desired operational outcomes.

2.3.2 Develop Operational Requirements

2.3.2.1 Articulate Force Requirements

Sub-Techniques: Outline Manpower, Outline Training Requirements, Outline Technical Requirements

Planners should perform an initial assessment of the resources they will require to conduct operations in the information environment and articulate them to their leadership. This initial assessment will provide operators with a better picture of what objectives are attainable given the resources available to them. After articulating their required capabilities, planners may refine their initial objectives.

Rating:

0. Operation does not articulate force requirements.
1. Operation outlines vague requirements outlining two of three: resources, logistics, and training requirements.
2. Operation outlines specific requirements outlining two of three: resources, logistics, and training requirements.
3. Operation outlines specific requirements outlining three of three: resources, logistics, and training requirements.

2.3.2.2 Define Impact Indicators

Sub-Techniques:

Impact indicators refer to measures of effectiveness that highlight strategic success for an operation. For example, an operation in the information environment may want to alert a target audience to the outbreak of a dangerous virus like COVID-19 in their vicinity. One impact indicator in this operation monitors how many target audience members choose to quarantine.

Rating:

0. Operation does not define impact indicators.
1. Operation conducts a risk assessment and defines impact indicators that are unmeasurable or difficult to measure.
2. Operation conducts a risk assessment and defines clear impact indicators that are measurable with unavailable, but accessible, capabilities.
3. Operation conducts a risk assessment and defines clear impact indicators that are measurable given readily available capabilities.

2.3.2.3 Establish Initial Assessment Criteria

Sub-Techniques:

Assessment criteria refers to measurable outcomes that indicate change in behavior among a target audience. Defining initial assessment criteria helps operators define intelligence requirements and impact indicators to monitor throughout a campaign.[xix]

Rating:

0. Operation does not establish initial assessment criteria.
1. Operation establishes assessment criteria that fulfills one of three: contains measurable impact indicators, represents change in population behavior, accompanied with specific intelligence requirements.
2. Operation establishes assessment criteria that fulfills two of three: contains measurable impact indicators, represents change in population behavior, accompanied with specific intelligence requirements.
3. Operation establishes assessment criteria that fulfills three of three: contains measurable impact indicators, represents change in population behavior, accompanied with specific intelligence requirements.

2.3.2.4 Review Postulations

Sub-Techniques: Identify Assumed Facts, Identify Key Assumptions, Identify Campaign Constraints, Identify Campaign Ethical Restraints

Postulations refer to key assumptions relevant to an operation.[xx] As operators develop strategic narratives, they should carefully review their research into the TA's social and technical landscapes to probe for analytic gaps. Operators should also verify key assumptions in efforts to enhance the credibility of their narratives.

Rating:

0. Operation does not review postulations.
1. Operation reviews one of five: assumed facts, key assumptions, campaign constraints, campaign ethical restraints.
2. Operation reviews three of five: assumed facts, key assumptions, campaign constraints, campaign ethical restraints.
3. Operation Reviews five of five: assumed facts, key assumptions, campaign constraints, campaign ethical restraints.

2.3.2.5 Mitigate Analytic Gaps

Sub-Techniques:

Analytic gaps refer to unknown bits of information that prevent a full understanding of a subject. Operators should identify analytic gaps to ensure that campaign strategy is drafted with a more complete and refined understanding of a TA.

Rating:

0. Operation does not assess analytic gaps.
1. Operation identifies gaps but does not conduct further research on them or adapt campaign strategy.

2. Operation identifies analytic gaps, conducts further research into them, but ultimately does not adapt campaign strategy.
3. Operation identifies analytic gaps, conducts further research into them, and ultimately adapts campaign strategy to account for new findings.

2.3.2.6 Outline Operations Security Planning Guidance

Sub-Techniques:

Operations security refers to a "capability that identifies and controls critical information, indicators of friendly force actions attendant to military operations, and incorporates countermeasures to reduce the risk of an adversary exploiting vulnerabilities."[xxi] Maintaining strong operation security will prevent adversaries from exploiting vulnerabilities or existing strategies to their benefit.

Rating:

0. Operation does not outline operations security planning guidance.
1. Operation outlines operations security planning guidance for one of three entities: individuals, operations systems and capabilities, external partner relationships.
2. Operation outlines operations security planning guidance for two of three entities: individuals, operations systems and capabilities, external partner relationships.
3. Operation outlines operations security planning guidance for three of three entities: individuals, operations systems and capabilities, external partner relationships.

2.3.2.7 Develop Master/Strategic Narrative

Sub-Techniques: Develop Competing Narratives

An operation in the information environment should develop a primary strategic narrative from which sub-narratives extend, allowing the operation to maintain strategic clarity and develop coordinated content throughout the campaign.

Rating:

0. Operation does not develop a master/strategic narrative.
1. Operation develops an incoherent master/strategic narrative that is difficult for the TA to interpret or relate to.
2. Operation develops a coherent master/strategic narrative that is relevant to the TA but too narrow to adapt to changing circumstances.
3. Operation develops a coherent master/strategic narrative that is both relevant to the TA and adaptable.

2.3.2.8 Integrate Vulnerabilities into Narrative

Sub-Techniques: Integrate TA Adversaries into Narrative, Question Existing Institutions

Studying a target audience's social and technical landscapes helps integrate findings into strategic narratives. These findings demonstrate an operation's attention to detail to the TA's information environment and increase engagement over the long run.

Rating:

0. Operation does not integrate vulnerabilities into narratives.
1. Operation studies a TA's social and technical landscape but fails to integrate any findings into a master narrative.
2. Operation studies a TA's social and technical landscape to integrate irrelevant findings into a master narrative.
3. Operation studies a TA's social and technical landscape to integrate relevant findings into a master narrative.

2.3.2.9 Mitigate Potential Disruptors

Sub-Techniques: Review Competing Information, Review Uncontrollable Environmental Physical Factors, Review Uncontrollable Social Behaviors, Review Historical Disruptors to Operations

Disruptors refer to unexpected events that may prevent an operation from efficiently communicating with its target audience. Common disruptors may include weak civil infrastructure or popular opposing narratives. Identifying disruptors early in an operation enables operators to develop counter-narratives and prepare products that will reach and resonate with the target audience despite environmental barriers.

Rating:

0. Operation does not review and mitigate potential disruptors.
1. Operation reviews and mitigates potential disruptors by conducting one of three: mitigate structural disruptors in the information environment, mitigate social disruptors among the target audience, develop strategy for potential backlash.
2. Operation reviews and mitigates potential disruptors by conducting two of three: mitigate structural disruptors in the information environment, mitigate social disruptors among the target audience, develop strategy for potential backlash.
3. Operation reviews and mitigates potential disruptors by conducting three of three: mitigate structural disruptors in the information environment, mitigate social disruptors among the target audience, develop strategy for potential backlash.

2.3.2.10 Identify Optimal Delivery Timeline

Sub-Techniques: Identify Deadline to Observe Behavior Change, Identify Initial Product Delivery Date, Outline Logistics for Product Delivery Timeline

A proper product distribution plan should provide operators with clear yet malleable timeline for delivery. Delivery times will often change as a result of changing conditions in the information environment but should set a final deadline to observe behavior changes. This final deadline will often lie right before or after a major event like an offensive or election.

Rating:

0. Operation does not identify an optimal delivery time.
1. Operation identifies a delivery time and fulfills one of three criteria: sets an initial delivery time, sets a final deadline to observe behavior change in the target audience, keeps deadlines malleable to account for unexpected events.

2. Operation identifies a delivery time and fulfills two of three criteria: sets an initial delivery time, sets a final deadline to observe behavior change in the target audience, keeps deadlines malleable to account for unexpected events.
3. Operation identifies a delivery time and fulfills three of three criteria: sets an initial delivery time, sets a final deadline to observe behavior change in the target audience, keeps deadlines malleable to account for unexpected events.

2.4 Survey Phase

2.4.1 Study Target Audience Information Environment

2.4.1.1 Organize Situation Monitoring Requirements

Sub-Techniques: Order Intelligence Estimate, Conduct Background Studies, Multidiscipline Counterintelligence, Security Monitoring, Operational Feedback

Before performing a detailed target audience analysis, an operation should organize its resources to capture a general picture of the information environment using existing resources and capabilities. Situation monitoring requirements refer to the placement of resources in spaces that monitor ongoing activities or developments. When organizing situation monitoring requirements, operation planners should coordinate information requirements and formulate initial key performance indicators for assessment.

Rating:

0. Operation does not organize situation monitoring requirements.
1. Operation organizes minimal intelligence reporting and does not identify potential implementation actions.
2. Operation organizes intelligence reporting but does not identify potential implementation actions.
3. Operation organizes intelligence reporting and identifies potential implementation actions.

2.4.1.2 Reference Social Media Analytics

Sub-Techniques:

An operation in the information environment may use social media analytics to determine which factors will increase the operation content's exposure to its target audience on social media platforms including views, interactions, and sentiment relating to topics and content types. The operation may use the social media platform itself or utilize a third-party tool to collect the metrics.

Rating:

0. Operation does not monitor social media analytics.
1. Operation monitors one of three platform metrics: views, interactions, and sentiment.
2. Operation monitors two of three platform metrics: views, interactions, and sentiment.
3. Operation monitors three of three platform metrics: views, interactions, and sentiment.

2.4.1.3 Evaluate Media Surveys

Sub-Techniques:

An operation in the information environment may evaluate its own or third-party media surveys to determine what type of content appeals to its target audience. Media surveys may provide insight into an audience's political views, social class, general interests or other indicators used to tailor operation messaging to its target audience. Impactful media surveys should ask clear questions that the target audience would be interested in engaging with.

Rating:

0. Operation does not evaluate media surveys
1. Operation fulfills one of three: evaluates its own media surveys, evaluates third party surveys, crafts engaging media survey questions.
2. Operation fulfills two of three: evaluates its own media surveys, evaluates third party surveys, crafts engaging media survey questions.
3. Operation fulfills three of three: evaluates its own media surveys, evaluates third party surveys, crafts engaging media survey questions.

2.4.1.4 Apply Web Usage Analysis

Sub-Techniques:

An operation in the information environment may conduct web usage analysis to identify popular search engines, keywords, websites, and advertisements among its target audience. Web usage analysis monitors communications and interactions across webpages, providing operators insight into a target audience's interests.

Rating:

0. Operation does not conduct web traffic analysis.
1. Operation analyzes one of three: commonly searched keywords, individual website traffic, and popular content.
2. Operation analyzes two of three: commonly searched keywords, individual website traffic, and popular content types.
3. Operation analyzes three of three: commonly searched keywords, individual website traffic, and popular content types.

2.4.1.5 Assess Degree of Media Access

Sub-Techniques:

An operation in the information environment may survey a target audience's access to the internet and free media to determine which target audience members will more likely view operation content and on which platforms. An operation will likely face more difficulty targeting an information environment with heavy restrictions and media control than an environment with independent media, freedom of speech and of the press, and individual liberties.

Rating:

0. Operation does not survey the degree of media freedom.

1. Operation surveys one of three: state media regulations, private media regulations, and press freedom legislations.
2. Operation surveys two of three: state media regulations, private media regulations, and press freedom legislations.
3. Operation surveys three of three: state media regulations, private media regulations, and press freedom legislations.

2.4.1.6 Identify Trending Topics

Sub-Techniques: Identify Trending Hashtags, Monitor Media Developments

An operation in the information environment may study trending topics on social media platforms for later use in boosting operational content. Topics tend to grow and decline over time, but studying these patterns helps operators draw insights from the general trends and social tendencies of a population.

A hashtag refers to a word or phrase preceded by the hash symbol (#) on social media used to identify messages and posts relating to a specific topic.[xxii] All public posts that use the same hashtag are aggregated onto a centralized page dedicated to the word or phrase and sorted either chronologically or by popularity.

Rating:

0. Operation does not identify trending topics.
1. Operation identifies general trending topics that are irrelevant to the operation.
2. Operation identifies general trending topics that are slightly relevant to the operation.
3. Operation identifies trending topics that directly relate to the operation's topic of interest.

2.4.1.7 Identify Obstacles to Operation Success

Sub-Techniques: Identify Resource and Capability-related Obstacles, Identify Structural Obstacles in the Information Environment, Identify Cognitive Obstacles in the Target Audience

Obstacles to operation success threaten the achievement of operation goals and pose a threat to its assets.[xxiii] Evaluating the physical, digital, and social threats posed to an operation in the information environment helps guide planning and develop counters. According to the Fogg Behavior Model, individuals often make decisions based on their ability, motivation, and prompts to do so.[xxiv] Identifying obstacles to operation success could increase the probability of strategic success by making it easier for the target audience to participate and conduct certain behaviors. Other models, like Nudge Theory, recommends an indirect approach to asking the target audience questions without delivering orders.[xxv] Nudge Theory could help sway stubborn members of the target audience by not removing their freedom to make decisions.

Rating:

0. Operation does not identify obstacles to operation success.
1. Operation identifies one of three types of obstacles to operation success: resource-based obstacles, structural obstacles in the information environment, cognitive obstacles amongst the target audience.

2. Operation identifies two of three types of obstacles to operation success: resource-based obstacles, structural obstacles in the information environment, cognitive obstacles amongst the target audience.
3. Operation identifies three of three types of obstacles to operation success: resource-based obstacles, structural obstacles in the information environment, cognitive obstacles amongst the target audience.

2.4.1.8 Study Competitors

Sub-Techniques: Identify Adversary Goals, Discern Source of Power, Review Adversary Critical Capabilities

Competitors in the information environment directly challenge an operation with activities that prevent the achievement of its strategic goals. Identifying and studying competitors will prepare a campaign to efficiently counter competing narratives.

Rating:

0. Operation does not study competitors.
1. Operation studies competitors and fulfills one of three activities relevant to activities between the adversary and the target audience: identify adversary goals, review adversary capabilities, review major adversarial narratives.
2. Operation studies competitors and fulfills two of three activities relevant to activities between the adversary and the target audience: identify adversary goals, review adversary capabilities, review major adversarial narratives.
3. Operation studies competitors and fulfills three of three activities relevant to activities between the adversary and the target audience: identify adversary goals, review adversary capabilities, review major adversarial narratives.

2.4.2 Study Social Landscape

2.4.2.1 Reference Cultural Analysis

Sub-Techniques: Study Law, Study Customs, Study Religions, Study Demographics, Study Arts, Study Languages, Study Local Geography, Study Taboos, Study Venerated Figures, Study Myths, Survey Current Attitudes, Study Cultural Dynamics and Decision Making

An operation in the information environment may perform or reference a cultural analysis to better understand an audience's cultural tendencies and main characteristics. Cultural analysis may reference religion, migration patterns, geography, music and art, literature, symbols, law, customs, socioeconomic status, demographics, and other cultural identifying features.[xxvi]

Social dynamics play a key role in how a target audience may respond to external influences. For example, individualistic societies may require a more targeted approach compared to collectivist ones.[xxvii] Different cultural dynamics influence decision-making processes among populations. For example, the Chinese "face saving" culture emphasizes the "respect, pride, and dignity of an individual with regards to their 'position in society."[xxviii] Western cultures will be more utilitarian

and emphasize a 'cost-benefit approach' to difficult decisions by analyzing preferences at an individual instead of societal level.[xxix]

Rating:

0. Operation does not perform cultural analysis.
1. Operation surveys at least two of seven traits relevant to the target audience: local law, social customs, religions, demographics, arts and music, languages, symbols.
2. Operation surveys at least four of seven traits relevant to the target audience: local law, social customs, religions, demographics, arts and music, languages, symbols.
3. Operation surveys at least six of seven traits relevant to the target audience: local law, social customs, religions, demographics, arts and music, languages, symbols.

2.4.2.2 Study Ongoing Target Audience Activities

Sub-Techniques: Wedge Issues, Preexisting Prejudices, Breaking News Events, Active Crisis, Upcoming Election, Psychological Biases, Social Group Trauma, Existing Suspicions/Conspiracies, Existing/Emerging Movements, Media System Vulnerabilities Sentiment Analysis, Monitor News Cycle Analytics, Signals Intelligence, Political Cycle Topics, Potential Volume Burst/Social Events, Assess Attitude Strength

An operation in the information environment can best study ongoing TA activities by identifying relevant developments among the population. Studying cultural phenomena, existing conflicts, emerging trends, and the political landscape, for example, can help operators optimize the planning process. Planners should relate ongoing activities to the target audience's general attitude. Strong attitudes may predict the audience's propensity to behave a certain way in cases where individuals may feel a sense of self-importance, express knowledge of a certain subject, or directly experience something that inflames their emotions.[xxx]

Rating:

0. Operation does not study ongoing target audience activities.
1. Operation studies or identifies three of fifteen: Wedge Issues, Preexisting Prejudices, Breaking News Events, Active Crisis, Upcoming Election, Psychological Biases, Social Group Trauma, Existing Suspicions/Conspiracies, Existing/Emerging Movements, Media System Vulnerabilities, Sentiment Analysis, Monitor News Cycle Analytics, Signals Intelligence, Political Cycle Topics, Potential Volume Burst/Social Events.
2. Operation studies or identifies eight of fifteen: Wedge Issues, Preexisting Prejudices, Breaking News Events, Active Crisis, Upcoming Election, Psychological Biases, Social Group Trauma, Existing Suspicions/Conspiracies, Existing/Emerging Movements, Media System Vulnerabilities, Sentiment Analysis, Monitor News Cycle Analytics, Signals Intelligence, Political Cycle Topics, Potential Volume Burst/Social Events.
3. Operation studies or identifies twelve of fifteen: Wedge Issues, Preexisting Prejudices, Breaking News Events, Active Crisis, Upcoming Election, Psychological Biases, Social Group Trauma, Existing Suspicions/Conspiracies, Existing/Emerging Movements, Media System Vulnerabilities, Sentiment Analysis, Monitor News Cycle Analytics, Signals Intelligence, Political Cycle Topics, Potential Volume Burst/Social Events.

2.4.2.3 Identify Target Audience Incentives

Sub-Techniques: Positive Reinforcement, Negative Reinforcement, Social Reinforcement Material Reinforcement

Incentives refer to factors motivating the target audience to behave a certain way. The U.S. Military Information Support Operations Process refers to four primary types of incentives: positive reinforcement, negative reinforcement, social reinforcement, and material reinforcement.[xxxi] When approaching incentives, planners should consider reaching the best possible outcome by mitigating potential secondary outcomes after a target audience conducts a behavior. Secondary outcomes refer to consequences that directly result from the target audience behaving a certain way. For example, security patrols may increase as a direct result of a rebel group's attacks. Some behavior models, such as Maurer's model on "resistance to change", recommend direct and clear engagement with the target audience that clearly communicate the benefits that will arise from behaving a certain way.[xxxii]

Positive reinforcement refers to instances where the target audience engages in a behavior in order to receive something desirable. Desirable outcomes may include food, money, justice, liberty, or praise from peers.

Negative reinforcement refers to instances where the target audience engages in a behavior to avoid a negative outcome. Negative outcomes may include injury, death, defeat in a conflict, social ostracism, or reprisal.

Social reinforcement refers to positive and negative reinforcement that stems from a target audience's cultural environment. Societal reinforcers include physical non-physical, and verbal affirmations or gestures that indicate either acceptance or rejection in society.

Material reinforcers involve desirable tangible objects that motivate individuals to perform certain behaviors. Some material reinforcers may include money, land, or material possessions like cars or clothes.

The Fogg Behavior Model outlines three categories of motivation that may incentivize certain behaviors among the target audience: sensation, anticipation, and belonging.[xxxiii] Sensation refers to physical feelings like pleasure or pain. Anticipation refers to hope and fear. Belonging refers to instances where an individual is either accepted into or ostracized from a society.

Rating:

0. Operation does not identify target audience incentives.
1. Operation identifies target audience incentives and fulfills one of three: identifies positive or negative reinforcements, identifies social or material reinforcements, identifies and mitigates potential negative secondary outcomes.
2. Operation identifies target audience incentives and fulfills two of three: identifies positive or negative reinforcements, identifies social or material reinforcements, identifies and mitigates potential negative secondary outcomes.

3. Operation identifies target audience incentives and fulfills three of three: identifies positive or negative reinforcements, identifies social or material reinforcements, identifies and mitigates potential negative secondary outcomes.

2.4.2.4 Identify Cognitive Predispositions

Sub-Techniques: Identify Group Attitude Polarization, Identify Cognitive Dissonance Causes

A cognitive predisposition, or bias, is an error in judgement that leads individuals to misinterpret information from their surrounding environment.[xxxiv] Identifying cognitive predispositions helps place the target audience in a highly emotional state while incentivizing engagement with operation content. In a highly emotional state, the target audience may be more susceptible to calls for action and less likely to think rationally.

When approaching cognitive predispositions, operators should assess whether the target audience has the knowledge and skills to make a behavior change.[xxxv] This involves an understanding of whether they may want to make the change, whether their environment is conducive to it, and understanding what barriers may be preventing the behavior change.

Attitude polarization, an effect of confirmation bias, refers to increasing disagreement among a population as different parties consider contradictory evidence towards an issue.[xxxvi]

Cognitive dissonance refers to an individual's refusal to change their mind when "doing so will result in inconsistent beliefs or attitudes that are inconsistent with prior behavior."[xxxvii] Planners should be wary of sources of cognitive dissonance among a target audience and take measures to avoid eliciting such responses.

Rating:

0. Operation does not identify cognitive predispositions.
1. The operation conducts or identifies one of three: identify cognitive predisposition that are observed among the target audience, cognitive predisposition that are construable from ongoing target audience developments, identify predisposition and integrate them into an operation's context or narrative.
2. The operation conducts or identifies two of three: identify cognitive predisposition that are observed among the target audience, cognitive predisposition that are construable from ongoing target audience developments, identify predisposition and integrate them into an operation's context or narrative.
3. The operation conducts or identifies three of three: identify cognitive predisposition that are observed among the target audience, cognitive predisposition that are construable from ongoing target audience developments, identify predisposition and integrate them into an operation's context or narrative.

2.4.2.5 Study Social Sentiment

Sub-Techniques: Identify TA Adversaries, Assess Local Government Power

An operation could identify individuals, groups, or ideas that do not resonate with or rankle a target audience. Adversaries could be integrated into operation narratives to inflame emotions among a population.

Rating:

0. Operation does not identify TA adversaries.
1. Operation identifies one of three: adversary individuals, groups, ideas.
2. Operation identifies two of three: adversary individuals, groups, ideas.
3. Operation identifies three of three: adversary individuals, groups, ideas.

2.4.2.6 Study Existing Narratives

Sub-Techniques: Identify Key Issues, Identify TA Rewards, Study Historical Sources of Influence

An operation may survey the information space to study existing narratives with the goal of integrating existing trends, developments, and topics of interest to the target audience into a broader campaign. Understanding existing narratives provides operators with key insights as to what catches a target audience's attention and could support the development of stronger campaign master narratives.

Historical sources of influence refer to actors that have conducted operations attempting to change target audience behaviors. Audiences that have been historically targeted will likely stay grounded to their beliefs and may grow more resilient to operations in the information environment.

Rating:

0. Operation does not study existing narratives.
1. Operation studies historical narratives with no direct relevance to a campaign.
2. Operation studies ongoing narratives but fails to integrate them to the campaign's narratives.
3. Operation studies ongoing narratives and integrates them into relevant campaign narratives.

2.4.2.7 Identify Social Vulnerabilities

Sub-Techniques: Motives, Psychographics, Psychological Characteristics, Demographics, Gender, Religion, Symbols, Loyalties

Vulnerabilities refer to pre-existing societal divisions among a target audience. Some common vulnerabilities may arise from differences in demographics, religion, or competing loyalties to different political factions.

Rating:

0. Operation does not identify vulnerabilities.
1. Operation identifies vulnerabilities but fails to integrate them into the operation's products or dissemination techniques.

2. Operation identifies vulnerabilities but only integrates them into either the operation's products or dissemination techniques.
3. Operation identifies vulnerabilities and integrates them into the operation's products and dissemination techniques.

2.4.2.8 Identify Target Audience Proclivity to Change

Sub-Techniques: Identify Target Audience Proclivity to Relapse Behaviors

Analyzing a target audience's social and cultural history, their current information environment, and incentives will help planners understand their propensity to changing behaviors. After a behavior change has occurred, some operations should monitor the target audience and mitigate the risk of relapses in behavior. Mitigating relapses in behavior will improve an operation's long-term influence.

Behavior change models like the Fogg Behavior Model could help planners study an individual's motivation, ability, and prompts in their environment to encourage changes in behavior.[xxxviii]

Rating:

0. Operation does not identify the target audience's proclivity to change.
1. The operation analyzes one of three before assessing the target audience's proclivity to change: the target audience's social and cultural history, the target audience's information environment, potential target audience incentives.
2. The operation analyzes two of three before assessing the target audience's proclivity to change: the target audience's social and cultural history, the target audience's information environment, potential target audience incentives.
3. The operation analyzes three of three before assessing the target audience's proclivity to change: the target audience's social and cultural history, the target audience's information environment, potential target audience incentives.

2.4.3 Select Operation Platforms

2.4.3.1 Assess Target Audience Platform Usage

Sub-Techniques: Analyze External Viewership, Assess Nielson Ratings, Survey Existing Social Media Communities

Surveying and assessing the most popular platforms among a target audience provides insights that directly support a campaign’s reach. Platform types also provide insight to the type of content that the target audience may be more attracted to.

Rating:

0. Operation does not assess TA platform usage.
1. Operation satisfies one of three: survey existing platforms and technologies, review media and platform regulations, study platform user demographics.
2. Operation satisfies two of three: survey existing platforms and technologies, review media and platform regulations, study platform user demographics.
3. Operation satisfies three of three: survey existing platforms and technologies, review media and platform regulations, study platform user demographics.

2.4.3.2 Assess Target Audience Platform Usage Frequency

Sub-Techniques:

Studying platform usage frequency informs operators on emerging technologies and trends in the information space. Understanding which platforms are growing and declining provides vital intelligence for operators to effectively publish and amplify their content.

Rating:

0. Operation does not assess TA platform usage.
1. Operation satisfies one of three: study platform user growth patterns, study active users over a set period, selects most popular platforms among the TA for operation use.
2. Operation satisfies two of three: study platform user growth patterns, study active users over a set period, selects most popular platforms among the TA for operation use.
3. Operation satisfies three of three: study platform user growth patterns, study active users over a set period, selects most popular platforms among the TA for operation use.

2.4.3.3 Study Composition of Platform Content

Sub-Techniques:

Studying the composition of platform content entails analysis of a platform's structure and features to optimize campaign success. For example, studying a video-based platform would require operators to understand the video length, active audiences, and characteristics of popular creators.

Rating:

0. Operation does not study the composition of platform content.
1. Operation satisfies one of three: studies supported content types (video, image, text, audio), popular content types on a platform, tailors narratives, content development, and messaging strategy to support popular content types.
2. Operation satisfies two of three: studies supported content types (video, image, text, audio), popular content types on a platform, tailors narratives, content development, and messaging strategy to support popular content types.
3. Operation satisfies three of three: studies supported content types (video, image, text, audio), popular content types on a platform, tailors narratives, content development, and messaging strategy to support popular content types.

2.4.3.4 Assess Platform Utility

Sub-Techniques: Analyze Platform Algorithm, Review Required Registration Information, Review Platform Terms of Service

Studying a platform's utility involves analysis of a platform's reach, popularity, and regulation. Understanding these features helps operators select the friendliest platforms for their campaign's content.

Rating:

0. Operation does not assess a platform's utility.

1. Operation assesses one of three: platform regulation, target audience presence, and supported content types.
2. Operation assesses two of three: platform regulation, target audience presence, and supported content types.
3. Operation assesses three of three: platform regulation, target audience presence, and supported content types.

2.4.4 Study Technical Landscape

2.4.4.1 Identify Vulnerable Security Infrastructure

Sub-Techniques:

An operation in the information environment may identify weak security infrastructure to later bypass security controls and compromise accounts, use malware, or take other actions that facilitate the operation's objectives. An operation may target users or organizations with weak cyber hygiene or a lack of basic security guidelines a network or host maintains to protect itself from attacks.[xxxix]

Rating:

0. Operation does not identify vulnerable security infrastructure.
1. Operation identifies weak but unexploitable security infrastructure.
2. Operation identifies weak and exploitable security infrastructure that would not advance operation objectives.
3. Operation identifies weak and exploitable security infrastructure that would advance operation objectives.

2.4.4.2 Identify Data Voids

Sub-Techniques:

Data voids refer to a lack of coverage regarding a breaking news event or general topic.[xl] The lack of coverage on a topic presents opportunities for operators to amplify content discussing the subject and frame the issue. Data voids are hard to detect and relatively harmless until exploited by an entity aiming to quickly proliferate false or misleading information during a phenomenon that causes a high number of individuals to query the term or phrase. In the Plan phase, an operation in the information environment may identify data voids for later exploitation in the operation.

Rating:

0. Operation does not identify data voids.
1. Operation identifies data voids on search engines or platforms with little to no target audience engagement. E.g., operation targeting individuals in China identify a data void on Google, which users cannot access behind the Great Firewall.
2. Operation identifies data voids on topics not related to operation narratives on search engines or platforms with limited target audience engagement. E.g., operation aiming to discredit COVID-19 vaccine efficacy identifies data voids on terms not directly related to public health.

3. Operation identifies data voids on topics related to operation narratives on search engines or platforms with high target audience engagement.

2.4.4.3 Study Media System Landscape

Sub-Techniques:

Studying the media system's landscape refers to performing a holistic analysis of legal, social, and political influences on a population's information environment. This analysis may include assessment of press freedoms, the openness of forums, and freedoms of speech and expression. Media system landscape assessment may also review existing tensions, potential for conflict, and sentiment.

Rating:

0. Operation does not study the media system's landscape.
1. Operation studies one of three: legal, political, social influences on the information environment.
2. Operation studies two of three: legal, political, social influences on the information environment.
3. Operation studies three of three: legal, political, social influences on the information environment.

2.4.5 Emplace Sensors

2.4.5.1 Observe Online Behavior

Sub-Techniques:

Monitoring online developments among a target audience provides insight to emerging trends, topics of discussion, and events that may influence the physical world. An operation may observe online behavior through social media, forums, local online news feeds, and open data sources.

Rating:

0. Operation does not observe online behavior.
1. Operation achieves one of three when observing online behavior: periodically monitor online developments relevant to the operation, adapts existing narratives to accommodate changing circumstances, draws insights from multiple information sources to monitor developments.
2. Operation achieves one of three when observing online behavior: periodically monitor online developments relevant to the operation, adapts existing narratives to accommodate changing circumstances, draws insights from multiple information sources to monitor developments.
3. Operation achieves one of three when observing online behavior: periodically monitor online developments relevant to the operation, adapts existing narratives to accommodate changing circumstances, draws insights from multiple information sources to monitor developments.

2.4.5.2 Observe Offline Behavior

Sub-Techniques: Follow Local News and Developments

While enabling resources to engage with a target audience, operators should consistently observe offline behavior, such as local news developments to adapt operation strategy whenever necessary. As a result of observing offline behavior, a campaign stays relevant, engaging, and intriguing to a target audience.

Rating:

0. Operation does not observe offline behavior.
1. Operation conducts one of three when observing offline behavior: periodically monitor developments relevant to the operation, adapts existing narratives to accommodate changing situations, pulls from multiple information sources to monitor developments.
2. Operation conducts two of three when observing offline behavior: periodically monitor developments relevant to the operation, adapts existing narratives to accommodate changing situations, pulls from multiple information sources to monitor developments.
3. Operation conducts three of three when observing offline behavior: periodically monitor developments relevant to the operation, adapts existing narratives to accommodate changing situations, pulls from multiple information sources to monitor developments.

2.4.5.3 Outline Collection Plan

Sub-Techniques: Define Key Areas of Interest for Collection, Allocate Intelligence, Surveillance, and Reconnaissance Related Assets

Collection plans refer to strategies to gather information on a target audience to continuously measure operation performance. A collection plan enables operators to identify measures of effectiveness by allocating resources to specifically monitor changes in target audience behavior. Throughout an operation, operators may alter their initial collection plan to better capture target audience activities.

Rating:

0. Operation does not outline a collection plan.
1. Operation outlines a collection plan that fulfills one of three: the plan is malleable, the plan leverages existing assets and partners, the plan allocates resources that will measure changes in behavior.
2. Operation outlines a collection plan that fulfills two of three: the plan is malleable, the plan leverages existing assets and partners, the plan allocates resources that will measure changes in behavior.
3. Operation outlines a collection plan that fulfills three of three: the plan is malleable, the plan leverages existing assets and partners, the plan allocates resources that will measure changes in behavior.

2.4.5.4 Pre-Test Products

Sub-Techniques: Sample Populations for Testing, Evaluate Target Audience Initial Response

Pre-testing products involves the evaluation of whether products will have their desired effect on the target audience by measuring their understanding and acceptance of products.[xli] Before launching an operation in the information environment, operators should pretest their content with a sample target audience before distributing products to an entire audience. Pretesting enables operators to understand whether the message will be received as intended.

Rating:

0. Operation does not pre-test products.
1. Operation completes one of three: pretests products with a sample population, documents target audience responses to products, and assesses target audience responses to operation messaging.
2. Operation completes two of three: pretests products with a sample population, documents target audience responses to products, and assesses target audience responses to operation messaging.
3. Operation completes three of three: pretests products with a sample population, documents target audience responses to products, and assesses target audience responses to operation messaging.

2.4.5.5 Monitor Funding Flows

Sub-Techniques: Use Malware, Install Cookies, Track Devices

Monitoring funding flows assesses the passage of money between organizations to identify the source of resources between external entities. An operation in the information environment may monitor funding flows to determine vulnerabilities in external organization resources or map networks between publicly unaffiliated groups.

Rating:

0. Operation does not monitor funding flows.
1. Operation makes clear efforts to identify sources but fails to identify smaller sources of funding or track the larger network resource flows.
2. Operation identifies smaller sources of funding but does not identify the larger network of resource flow.
3. Operation monitors key sources of funding and identifies vulnerabilities in the resource flow.

2.4.5.6 Survey Public Opinion

Sub-Techniques: Use Poll/Survey Data, Use Targeted Poll/Ads

Operations in the information environment gauge public opinion with targeted polls and surveys. An operation in the information environment may conduct its own polls or use existing poll data to record information on target audience attitudes and opinions regarding operation topics. An operation requiring detailed data may similarly conduct surveys or use existing survey data, which provide more detailed audience response data. An operation may use the data to tailor narratives to existing audience beliefs, biases, or knowledge gaps.

Rating:

0. Operation does not survey public opinion.

1. Operation uses third-party polls/survey data.
2. Operation conducts its own polls/surveys.
3. Operation both uses third-party poll/survey data and conducts its own polls/surveys.

2.4.5.7 Employ Commercial Analytic Firms

Sub-Techniques:

Commercial analytic firms collect data on target audience activities and evaluate the data to detect trends, such as content receiving high click-rates. An operation in the information environment may employ commercial analytic firms to facilitate external collection on its target audience to complicate attribution efforts and better tailor the content to audience's preferences.

Rating:

0. Operation does not employ commercial analytic firms.
1. Operation's commercial analytic firms accomplish one of three: firm obfuscates affiliation with operation sources, firm is familiar with the target audience's information environment, firm has access to relevant target audience data.
2. Operation's commercial analytic firms accomplish two of three: firm obfuscates affiliation with operation sources, firm is familiar with the target audience's information environment, firm has access to relevant target audience data.
3. Operation's commercial analytic firms accomplish three of three: firm obfuscates affiliation with operation sources, firm is familiar with the target audience's information environment, firm has access to relevant target audience data.

2.5 Enable Phase

2.5.1 Evaluate Resources

2.5.1.1 Review Existing Messaging Strategies

Sub-Techniques: Review Existing or Ongoing Operations

Operators may review messaging strategies from previous campaigns to assess best practices and lessons learned to inform future operations. Adapting historical strategies to new operations helps operators optimize their capacity for influence and saves time. A review of previous messaging strategies may survey narratives, target audience analysis methods, amplification methods, platforms used, and other features.

Rating:

0. Operation does not review existing messaging strategies.
1. Operation reviews one of three: previous narratives, target audience analysis methods, message delivery techniques.
2. Operation reviews two of three: previous narratives, target audience analysis methods, message delivery techniques.
3. Operation reviews three of three: previous narratives, target audience analysis methods, message delivery techniques

2.5.1.2 Identify Potential Campaign Constraints

Sub-Techniques: Identify Information Constraints, Identify Physical Constraints

An operation may use previous work identifying analytic gaps, messaging strategies, and target audience analysis to pinpoint constraints. Understanding campaign limitations prepares operators by identifying inaccessible information spaces, unreachable audiences, weak narratives, and other vulnerabilities that can damage the operation's conviction.

Rating:

0. Operation does not identify potential campaign constraints.
1. Operation identifies campaign constraints in one of three spheres: information environment (I.e. social media platforms, forums, and other mediums of communication), message resonance, campaign resources (funding, assets, etc.).
2. Operation identifies campaign constraints in two of three spheres: information environment (I.e. social media platforms, forums, and other mediums of communication), message resonance, campaign resources (funding, assets, etc.).
3. Operation identifies campaign constraints in three of three spheres: information environment (I.e. social media platforms, forums, and other mediums of communication), message resonance, campaign resources (funding, assets, etc.).

2.5.1.3 Collect Historical Content

Sub-Techniques: Collect from Internet Caches, Collect Successful Posts from Previous Operations

An operation may collect archived historical content to spur engagement. Operations often mix campaign content with unrelated content intended to boost viewership. For example, some operations will post previously viral videos to boost views and interactions.

Rating:

0. Operation does not collect historical content.
1. Operation completes one of three with collected historical content: collects previously viral content, collects content interesting to the target audience, collects content applicable to a platform (e.g. sharing videos on YouTube).
2. Operation completes two of three with collected historical content: collects previously viral content, collects content interesting to the target audience, collects content applicable to a platform (e.g. sharing videos on YouTube).
3. Operation completes three of three with collected historical content: collects previously viral content, collects content interesting to the target audience, collects content applicable to a platform (e.g. sharing videos on YouTube).

2.5.1.4 Review Existing Information-Related Capabilities (IRCs)

Sub-Techniques: Issue Military Information Support Operations (MISO) Studies Production Program, Review Enabling Capabilities, Review Service and Organizational Capabilities, Review Message Traffic Archive, Review Previous Study Collections, Public Affairs, Military Deception, Computer Network Operations, Operations Security

According to JP 1-02, an Information-Related Capabilities (IRCs) represent "tools, techniques, or activities employed within a dimension of the information environment that can be used to create effects and operationally desirable conditions."[xlii] Some IRCs may include electronic warfare, intelligence, and public affairs. Essentially, IRCs are tools that enable activities in the information environment.

Rating:

0. Operation does not review existing information-related capabilities.
1. Operation reviews IRCs for one of three: relevance to operation, technical feasibility for IRC use, and potential for IRC effect on a target audience.
2. Operation reviews IRCs for two of three: relevance to operation, technical feasibility for IRC use, and potential for IRC effect on a target audience.
3. Operation reviews IRCs for three of three: relevance to operation, technical feasibility for IRC use, and potential for IRC effect on a target audience.

2.5.1.5 Leverage Partners

Sub-Techniques: Leverage International Partners, Leverage Interagency Partners, Leverage Commercial Vendors

As an operation seeks to better understand and more efficiently reach its intended audience, actors should interact with interagency and multinational partners for additional perspectives, resources, and direction. Leveraging partners adds value to a campaign's credibility and could mitigate previously identified analytic gaps.

Rating:

0. Operation does not leverage partners.
1. Operation leverages existing partners for one of three: product development capabilities, product delivery capabilities, gaining additional perspectives for target audience analysis.
2. Operation leverages existing partners for two of three: product development capabilities, product delivery capabilities, gaining additional perspectives for target audience analysis.
3. Operation leverages existing partners for three of three: product development capabilities, product delivery capabilities, gaining additional perspectives for target audience analysis.

2.5.1.6 Review Logistics

Sub-Techniques: Commercial Contracting, Review Supplies, Review Disseminating Agents

A logistics review involves the evaluation of resources, tools, capabilities, relationships, and timelines relevant to an operation. Executing a clear campaign requires strong communication of roles and responsibilities among operators and their partner organizations.

Rating:

0. Operation does not review logistics.
1. Operation reviews and sets a logistics plan that fulfills one of three: organizes capabilities and resources, organizes staff preparedness, sets clear goals and deadlines for product delivery.

2. Operation reviews and sets a logistics plan that fulfills two of three: organizes capabilities and resources, organizes staff preparedness, sets clear goals and deadlines for product delivery.
3. Operation reviews and sets a logistics plan that fulfills two of three: organizes capabilities and resources, organizes staff preparedness, sets clear goals and deadlines for product delivery.

2.5.2 Establish Information Assets and Intermediaries

2.5.2.1 Create Online Entities

Sub-Techniques: Create Anonymous Accounts, Create Sock Puppet Accounts, Create Cyborg Accounts, Develop Troll Accounts, Compromise Existing Accounts, Repurpose Existing Accounts, Create Bot Accounts (Amplifier Bots, Hacker Bots, Spammer Bots, Impersonator Bots)

Online entities account for all cyber-enabled entities that are capable of influencing a target audience. Most online entities influence their target audiences through social media platforms by exploiting platform-specific features to effectively reach a population. For example, bots are commonly used on Twitter and have been used to amplify disinformation.[xliii]

Rating:

0. Operation does not create any online entities.
1. Operation performs one of three when creating online entities: develops entities on relevant platforms, develops entities that are more likely to avoid platform detection, develop entities that directly support operation goals.
2. Operation performs two of three when creating online entities: develops entities on relevant platforms, develops entities that are more likely to avoid platform detection, develop entities that directly support operation goals.
3. Operation performs three of three when creating online entities: develops entities on relevant platforms, develops entities that are more likely to avoid platform detection, develop entities that directly support operation goals.

2.5.2.2 Develop Offline Entities

Sub-Techniques: Fund Cultural Ambassadors, Create a Television Station, Create a Radio Station

Offline entities account for all physical entities that are capable of influencing a target audience. Offline entities involve all forms of influence beyond the cyber-realm or internet and may include radio, television, posters, and influential individuals.

Rating:

0. Operation does not create any offline entities.
1. Operation performs one of three when developing offline entities: creates entities that will reach target audience, ensures entities will sustainably maintain TA engagement, creates entities that directly support operation narratives.

2. Operation performs two of three when developing offline entities: creates entities that will reach target audience, ensures entities will sustainably maintain TA engagement, creates entities that directly support operation narratives.
3. Operation performs three of three when developing offline entities: creates entities that will reach target audience, ensures entities will sustainably maintain TA engagement, creates entities that directly support operation narratives.

2.5.2.3 Establish Proxy Entities

Sub-Techniques: Recruit/Train/Promote Sympathetic Users, Cultivate Unwitting Agents, Create Organizations, Hire External Individuals or Organizations, Create a Content Farm, Co-Opt Existing Influencers, Create Fake Influencers, Create Organizations, Pay Users for Account Access

Proxy entities amplify operation content while avoiding direct affiliation with an operation's planners. Proxy entities obfuscate evidence that can attribute an operation to an actor. Proxies may guard their affiliation to an operation by removing digital footprints, concealing funding sources, and practicing strict operational security.

Rating:

0. Operation does not establish proxy entities.
1. Proxy entities achieve one of three: are not directly affiliated to an operation's source, a proxy entity's removal from a platform will not compromise a larger operation, proxy-developed content appears genuine.
2. Proxy entities achieve two of three: are not directly affiliated to an operation's source, a proxy entity's removal from a platform will not compromise a larger operation, proxy-developed content appears genuine.
3. Proxy entities achieve three of three: are not directly affiliated to an operation's source, a proxy entity's removal from a platform will not compromise a larger operation, proxy-developed content appears genuine.

2.5.2.4 Secure Dissemination Means

Sub-Techniques: Secure Assets, Secure Delivery Methods, Secure Products

An operation should connect assets, products, and dissemination capabilities with each other to facilitate efficient product delivery. Linking different entities and clearly detailing their roles enables operation planners to later prepare for executing an operation.

Rating:

0. The operation does not secure dissemination means.
1. Operation fulfills one of three to secure dissemination means: prepares information-related capabilities, connects products to assets, outlines delivery timelines for assets.
2. Operation fulfills two of three to secure dissemination means: prepares information-related capabilities, connects products to assets, outlines delivery timelines for assets.
3. Operation fulfills three of three to secure dissemination means: prepares information-related capabilities, connects products to assets, outlines delivery timelines for assets.

2.5.3 Cultivate Information Pathways

2.5.3.1 Create Forums

Sub-Techniques: Create Pages and Groups, Create Online Forums (Reddit, 4chan, 8kun, etc.), Create Group Chats, Create Newsletters, Create Websites, Create Echo Chambers, Match Existing Groups

An operation in the information environment may create fake and authentic forums to provide a platform to coordinate its information assets. Forums often legitimize an operation by creating a false sense of community and popular support for the operation.

Rating:

0. Operation does not create pages or groups.
1. Operation completes one of three criteria: create a page, create a group, periodically update pages and groups to appear legitimate and attract followers or members.
2. Operation completes two of three criteria: create a page, create a group, periodically update pages and groups to appear legitimate and attract followers or members.
3. Operation completes all of the following criteria: create a page, periodically create a group, update pages and groups to appear legitimate and attract followers or members.

2.5.3.2 Infiltrate Existing Forums

Sub-Techniques: Co-Opt Grassroots Groups

An operation in the information environment may infiltrate existing forums that align with operation narratives and objectives to reach its target audience without having to form and coordinate its own groups. Operations may also infiltrate existing forums to disrupt communities of individuals with opposing operation narratives. Existing networks may include social media groups, video channel subscribers, newsletter subscribers, news outlets.

Rating:

0. Operation does not infiltrate existing networks.
1. Operation infiltrates an inactive network and can only read archived messages for additional target audience research.
2. Operation infiltrates an existing network that is active but cannot actively post its content to the network's members.
3. Operation infiltrates an existing network that is active and can actively post its content to the network's members.

2.5.3.3 Secure Off-Platform Production Capabilities

Sub-Techniques: Contract Local Media Sources

Off-platform production capabilities refer to organizations that publish news stories on current events, sports, entertainment, and other topics. An operation in the information environment may establish or contract broadcast services such as subscription options and curated newsletters to promote operation narratives to its target audience. An operation may completely falsify news outlets or base outlets on legitimate entities. News outlets may utilize different forms of

communication including internet, radio, and television. Newsletters are periodic, usually subscription-based reports delivered physically or electronically that outline information or news to an audience with a specific interest in the content.[xliv] An operation in the information environment may create newsletters to proliferate personalized and curated content to its target audience.

Rating:

0. Operation does not secure off-platform production capabilities.
1. Operation secures off-platform production capabilities on platforms that are irrelevant to the target audience, makes poor efforts to establish legitimacy, and posts irrelevant content.
2. Operation secures off-platform production capabilities on relevant platforms for the target audience but fails to establish legitimacy and posts slightly irrelevant content.
3. Operation applies target audience analysis to secure off-platform production capabilities on the target audience's most active platforms to post relevant content to maintain legitimacy among the target audience.

2.5.3.4 Prepare Fundraising Campaigns

Sub-Techniques: Newsletters

Fundraising campaigns refer to an operation in the information environment's systematic effort to seek financial support for a charity, cause, or other enterprise using online activities that further promote operation information pathways while raising a profit. An operation in the information environment may prepare fundraising campaigns by determining where to host the fundraiser, employing personnel to staff the fundraiser, and creating operation-aligned messaging to market the fundraiser.

Rating:

0. Operation does not prepare fundraising campaigns.
1. Operation achieves one of three: determines where to host the fundraiser, employs personnel to staff the fundraiser, and creates operation-aligned messaging to support the fundraiser.
2. Operation achieves two of three: determines where to host the fundraiser, employs personnel to staff the fundraiser, and creates operation-aligned messaging to support the fundraiser.
3. Operation achieves three of three: determines where to host the fundraiser, employs personnel to staff the fundraiser, and creates operation-aligned messaging to support the fundraiser.

2.5.4 Design and Develop Products

2.5.4.1 Identify Product Types for Development

Sub-Techniques: Audio-Based Products, Text-Based Products, Visual-Based Products, Audio-Visual-Based Products, Physical Products

Identifying product types for development refers to the leveraging of previous target audience analysis to select appropriate forms of content to disseminate to a target audience based on

accessibility, resonance, and engagement. When selecting between audio, visual, audio-visual, and other types of products, planners should consider the target audience's information environment and infrastructure before selecting product types.

Rating:

0. Operation does not identify product types for development.
1. Operation achieves one of three: identifies product types accessible to the target audience, identifies product types that will resonate with the target audience, and identifies product types that will engage with the target audience.
2. Operation achieves two of three: identifies product types accessible to the target audience, identifies product types that will resonate with the target audience, and identifies product types that will engage with the target audience.
3. Operation achieves three of three: identifies product types accessible to the target audience, identifies product types that will resonate with the target audience, and identifies product types that will engage with the target audience.

2.5.4.2 Develop Human-Driven Media

Sub-Techniques: Memes, Evidence Collage, Infographics, Text-Based Content, Fake/Distorted Quotes, Forged Documents, False Research

Human-driven media refers to content created with minimal automation capabilities. An influence operation may develop human-driven media to support operation narratives through various media types including written texts, visual depictions, or soundbites.

- Memes are units of culture that spread through the diffusion of ideas, usually pictures, videos, or gifs on the internet.[xlv] An influence operation may use memes to deliver content in a simple, digestible, and entertaining way. Internet memes often increase their exposure for a certain period due to trends potentially granting operations a window of time to deliver content more effectively.
- An evidence collage is a compilation of screenshots and text into a single shareable document, usually in image format to persuade or convince a target audience.[xlvi] A misinfographic is an infographic with false or misleading information.[xlvii] It may also refer to a forged infographic using watermarks and branding from a legitimate organization.
- An influence operation may use fake or distorted quotes, especially from political figures or other celebrities, to advance operation narratives. Quotes may falsely depict support for the operation's objective, frame opposition in a negative light, or aim to further a conspiracy. Text-based content include articles or written social media posts.
- An operation may forge documents to advance narratives with fake support or "proof" include falsified legal, professional, and academic credentials, fake emails, texts, and other communications, inauthentic political documents and press releases.
- False research includes fake political reports, statistical analyses, pseudo-scientific conclusions, and other false, misleading, or unproven research. An operation may use false research to further conspiracy theories, increase operation legitimacy or add pseudo-scientific justifications to operation narratives.

Rating:

0. Operation creates less than three types of human-driven media.
1. Operation creates three of nine types of content: memes, evidence collage, (mis)infographics, articles, quotes, pictures, video, leaked or forged documents, research.
2. Operation creates five of nine types of content: memes, evidence collage, (mis)infographics, articles, quotes, pictures, video, leaked or forged documents, research.
3. Operation creates seven of nine types of content: memes, evidence collage, (mis)infographics, articles, quotes, pictures, video, leaked or forged documents, research.

2.5.4.3 Create AI-Driven Media

Sub-Techniques: Deepfakes, Cheapfakes, AI-Generated Profile Pictures (Generative Adversarial Networks), Autonomous Text Generation (Readfakes)

AI-driven media refers to media produced, manipulated, or altered using automatic tools, including artificial intelligence and algorithms.[xlviii] An influence operation may use AI-driven media to quickly produce and proliferate content with minimum human input. AI-driven media may also facilitate a liar's dividend in which actors facing accusations based off audio or video recording can deflect the blame by claiming the media is automated and inauthentic.[xlix]

- Deepfakes refer to AI-generated falsified photos, videos, or soundbites.[l] An influence operation may use deepfakes to depict an inauthentic situation by synthetically recreating an individual's face, body, voice, and physical gestures.
- Cheapfakes utilize less sophisticated measures of altering an image or video, for example, slowing, speeding, or cutting footage to create a false context surrounding an image or event.[li]
- AI-generated profile pictures use artificial intelligence to create a false image depicting a person's headshot. AI-Generated Profile Pictures often depict individuals who do not exist and use Generative Adversarial Networks (GAN) to create fake individuals.[lii] GANs take multiple images and compile them to create new, original images of nonexistent individuals while simultaneously attempting to detect which images are fake. As a result, the program can create strikingly real headshots at a rapid pace.
- Readfakes refer to synthetic text composed by computers using text-generating AI technology.[liii]
- Autonomous generation refers to content created by a bot without human input, also known as bot-created content generation. Autonomous generation represents the next step in automation after language generation and may lead to automated journalism. An influence operation may use read fakes or autonomous generation to quickly develop and distribute content to the target audience.

Rating:

0. Operation does not create AI-driven media.
1. Operation creates AI-driven media that is easily detectable as inorganic by platform monitoring services and external investigations.
2. Operation creates AI-driven media that may be detectable by some platform monitoring services and external investigations but effectively communicates operation narratives and avoids initial detection.

3. Operation creates AI-driven media that is nearly indistinguishable from organic media and effectively communicates operation narratives.

2.5.4.4 Present Desired Target Audience Actions

Sub-Techniques: Ask to Exhibit a Behavior, Ask to Refrain from Action, Ask to Encourage Cooperation, Ask to Exercise Caution

Some operation products should communicate the behaviors it wishes a target audience to exhibit. Products may ask target audience members to refrain from joining a movement, to vote in an upcoming election, surrender during open conflict, or other behaviors. Clearly communicating desired behaviors among a target audience could shelter them from potentially unsafe or risky conditions.

Rating:

0. Operation does not present desired target audience actions.
1. Operation references target audience analysis to develop unclear messaging that does not resonate with the target audience.
2. Operation references target audience analysis to develop messaging but fails to directly communicates desired actions on products.
3. Operation references target audience analysis to develop clear messaging and directly communicates desired actions on products.

2.5.4.5 Tailor Content to Selected Platforms

Sub-Techniques: Match Content Posted with Platform Supported Content-Types, Create Hashtag(s)/Hashtag Group(s), Purchase Advertisements

Tailoring content to a selected platform refers to the preparation of content to best fit a platform's structure and amplification algorithms. For example, an operation that uses Instagram to reach its target audience may benefit from using reels instead of pictures because reels have a higher likelihood of being amplified by the platform's algorithm.

Rating:

0. Operation does not tailor content to selected platforms.
1. Operation creates content that is supported by selected platforms but is not conducive to sharing on the platform or by the target audience.
2. Operation creates content that is supported by selected platforms but is not conducive to sharing or amplification on the platform.
3. Operation creates content that is supported by selected platforms and is conducive to sharing or amplification on the platform by the target audience.

2.5.4.6 Launder Information

Sub-Techniques:

Laundered information refers to the amplification of a message while concealing its source. Operators may seek to launder information to increase a narrative's reach while concealing the state-backed actor that developed it. Information laundering can take many forms including

plagiarized content, misquotes, misrepresentations, and the use of proxies to conceal sponsorship.

Rating:

0. Operation does not launder information.
1. Operation achieves one of three when laundering information: conceals operation sponsorship, bypasses plagiarism detectors, appears original.
2. Operation achieves two of three when laundering information: conceals operation sponsorship, bypasses plagiarism detectors, appears original.
3. Operation achieves three of three when laundering information: conceals operation sponsorship, bypasses plagiarism detectors, appears original.

2.5.5 Establish Legitimacy

2.5.5.1 Create Localized Content

Sub-Techniques: Utilize Social Framing, Create Age-Specific Content

Localized content refers to content that appeals to a specific community of individuals often in defined geographic areas. An operation may create localized content using local languages and dialects to resonate with its target audience and blend in with other local news and social media. Localized content may help an operation increase legitimacy, avoid detection, and complicate external attribution.

- Social framing alters the way a subject is presented to a social group to elicit a specific response or reaction. According to Erving Goffman's framing theory, individuals interpret their environment based on their personal primary framework, an abstract point-of-view that is unique to their natural and social experiences.[liv] An influence operation may reframe its narratives to appeal to the target audience framework using familiar stories, myths, or legends, traditions, rituals, or ceremonies, slogans or catchphrases, metaphors, and comparisons.
- Age-specific content refers to information tailored towards a certain age-bracket with the intent of increasing audience interaction among networks of individuals within that age-bracket. An influence operation may create age-specific content by developing narratives that align with the interests of a certain age bracket, such as promoting narratives on Medicare to appeal to U.S. audiences over 65 years old.

Rating:

0. Operation does not create localized content.
1. Operation creates localized content that meets one of three criteria: uses local language, aligns with local narratives, and uses local outlets for dissemination.
2. Operation creates localized content that meets two of three criteria: uses local language, aligns with local narratives, and uses local outlets for dissemination.
3. Operation creates localized content that meets three of three criteria: uses local language, aligns with local narratives, and uses local outlets for dissemination.

2.5.5.2 Co-opt Trusted Sources

Sub-Techniques: Utilize Academic/Pseudoscientific Justifications, Prepare Assets Impersonating Legitimate Entities, Typosquatting, Use Web-Scraped Content, Local Spokespeople, Celebrities, Subject Matter Experts, Social Media Influencers, Impersonate Legitimate Entities

When an operation co-opts trusted sources, they will compromise a reputable individual or organization to shift their perspective or amplify operation narratives. Compromised sources are often bribed, misled, or influenced in a malign manner to support an operation.

- Academic/Pseudoscientific justifications refer to instances where an actor misrepresents, misuses, or creates false research to prove a point related to an operation's narrative. Pseudoscientific research often incorrectly attributes findings to being based on the scientific method when they're not.[lv]
- Typosquatting refers to the intentional registration of a domain name that incorporates typographical variants of the target domain name in order to deceive visitors.[lvi]
- Web scraping refers to the use of bots to gather data from a website.[lvii] An influence operation may use web-scraped content to replicate or repurpose existing materials.

Rating:

0. Operation does not co-opt trusted sources.
1. Operation co-opts sources that have little credibility and receive little exposure to the target audience.
2. Operation co-opts sources with either high credibility or exposure to the target audience.
3. Operation co-opts sources with both high credibility and exposure to the target audience.

2.5.5.3 Curate Social Proof

Sub-Techniques: Apply Social Learning Theory

Social proof refers to the phenomenon in which individuals follow the actions of the masses.[lviii] People will more likely mimic the behavior of a large group even if they do not agree with the actions if they perceive the others as more knowledgeable or if they want to "fit in." An influence operation may use social proofing to establish legitimacy through numbers and popularity.

Curated Social Proof occurs when individuals overestimate the number of people supporting one side of a debate and therefore side with this perspective, even though it lacks the perceived amount of support.[lix]

Social Learning Theory "explains human behavior in terms of a continuous reciprocal interaction among cognitive, behavioral, and environmental determinants."[lx] Individuals are both driven from personal forces and learn to adopt behaviors by observing others in their social environment. This mix of environmental influences and personal factors forges an individual's perspective and helps them make decisions based on what their perceived options are.

Rating:

0. Operation does not exploit social proof.
1. Operation attempts to mimic popular social trends but fails to appear authentic to the target audience.
2. Operation mimics popular social trends in a way that convinces few members of the target audience but integrates the trend with the operation.
3. Operation uses previous target audience analysis to identify ongoing social trends and embed them with their operation.

2.5.5.4 Leverage Existing Biases

Sub-Techniques: Study Assimilation Bias, Study Confirmation Bias

An operation in the information environment may create products that support the target audience's existing beliefs and biases to increase its legitimacy by reinforcing assimilation and confirmation bias. [lxi]

Rating:

0. Operation does not leverage existing biases.
1. Operation attempts to leverage existing biases but fails to relate its content to the target audience.
2. Operation successfully leverages biases identified in the previous phases, but only uses it for one of the following reasons: reinforcing content, reinforcing narratives, or reinforcing the legitimacy of the operation.
3. Operation successfully leverages existing biases identified in the previous phases, using them to reinforce content, narratives, and the legitimacy of the operation in a manner that directly relates to the target audience.

2.5.6 Enable Persistence

2.5.6.1 Refine Initial Assessment Criteria

Sub-Techniques:

Refining initial assessment criteria provides critical feedback to operators to enable the longevity and success of an operation. When refining initial impact indicators, operators should redefine impact indicators, if necessary, and outline any new intelligence requirements for collection. Operators should capture quirks or nuances observed while assessing early product deliveries to the target audience.

Rating:

0. Operation does not refine initial assessment criteria.
1. Operation achieves one of three: evaluates insights from initial assessment results, outlines new intelligence requirements for collection, clearly defines trends outlining changes in behavior.

2. Operation achieves two of three: evaluates insights from initial assessment results, outlines new intelligence requirements for collection, clearly defines trends outlining changes in behavior.
3. Operation achieves three of three: evaluates insights from initial assessment results, outlines new intelligence requirements for collection, clearly defines trends outlining changes in behavior.

2.5.6.2 Edit Existing Accounts

Sub-Techniques: Anonymize Accounts, Use Pseudonyms, Change Account Names, Launder Accounts

When an operation edits existing accounts, it attempts to bypass content moderation algorithms by changing key identifiable account features. Operators may anonymize accounts, use pseudonyms, or launder accounts to obfuscate operation asset sources.

- An operation may use pseudonyms, or fake names, to mask the identity of operation accounts, publish anonymous content, or otherwise use falsified personas to conceal identity of the operation. An operation may coordinate pseudonyms across multiple platforms, for example, by writing an article under a pseudonym and then posting a link to the article on social media on an account with the same falsified name.
- Account laundering occurs when an influence operation acquires control of previously legitimate online accounts from third parties through sale or exchange and often in contravention of terms of use. Influence operations use laundered accounts to reach target audience members from an existing information channel and complicate attribution.

Rating:

0. Operation does not edit existing accounts.
1. Operation edits existing accounts in one of three ways: to make operation accounts indistinguishable from non-operation accounts, edit identifiable account features to appear authentic, bypass account moderation features.
2. Operation edits existing accounts in two of three ways: to make operation accounts indistinguishable from non-operation accounts, edit identifiable account features to appear authentic, bypass account moderation features.
3. Operation edits existing accounts in three of three ways: to make operation accounts indistinguishable from non-operation accounts, edit identifiable account features to appear authentic, bypass account moderation features.

2.5.6.3 Conceal Network Identity

Sub-Techniques: Use Anonymizers, Use a Virtual Private Network (VPN), Use Compromised Intermediate Servers, Use Proxies, Mask Location of Accounts, Avoid Grammatical Errors

An operation that hopes to avoid detection needs to take multiple steps to conceal its identity. Obfuscating patterns of activity, using anonymizers, hiding locations, and using proper grammar

helps an operation avoid detection and account removal. Proper network concealment allows an operation to continue influencing the information space without regulation.

Unlike concealing sponsorship, concealing network identity denies the existence of any sort of organization. To conceal network identity, an operation may use:

- An anonymizer, or an anonymous proxy, to hide private information on the user's behalf by either not logging the information or refusing requests to reveal the information to adversaries.[lxii]
- A Virtual Private Network (VPN) to provide an encrypted Internet connection from a device to a network.[lxiii] VPNs help anonymize activity by changing the device's Internet Protocol (IP) address, which provides network and location information.
- Compromised intermediate servers, or exploited or hacked servers that can obscure network communications over the server.[lxiv]
- Proxies include people, companies, and organizations that work on behalf of an influence operation.[lxv] An operation may use previously funded proxies to outsource work to various locations, complicating attribution and further disguising the network.

Influence operations may use a variety of techniques to mask the location of their social media accounts to complicate attribution and conceal evidence of foreign interference. Operation accounts may set their location to a false place, often the location of the target audience, and post in the region's language. For example, accounts may post in English for U.S. audiences, Arabic for Middle Eastern audiences, and Spanish for Latin American audiences. Accounts may also post according to the time zone of the target audience location to maintain an appearance of living in the correct area and avoid posting in the middle of the night, a common indicator of foreign accounts.

Additionally, foreign operation assets may avoid posting content that requires written text in a foreign language. For example, a Russian asset that is not fluent in English may post memes or images without a description on Instagram, ensuring that the platform's algorithm or the target audience do not detect the network's identity via language errors.

Rating:

0. Operation does not conceal network identity.
1. Operation does not conceal the existence of a coordinated organization but partially conceals sponsorship so that only the high-level identity of the sponsor is identifiable.
2. Operation does not conceal the existence of a coordinated organization but does successfully conceals sponsorship to mislead or obscure the sponsor behind the operation.
3. Operation successfully conceals network identity so that no external entity could recognize the existence of a coordinated organization.

2.5.6.4 Conceal Sponsorship

Sub-Techniques: Proxies, Cut-Outs

Concealing sponsorship aims to mislead or obscure the identity of an operation's sponsor rather than entity publicly running the operation. Operations that conceal sponsorship may maintain visible falsified groups, news outlets, non-profits, or other organizations, but seek to mislead or obscure the identity sponsoring, funding, or otherwise supporting these entities.

- Proxies include people, companies, and organizations that work for the influence operation.[lxvi] An influence operation may use previously funded proxies to outsource work to various locations, complicating attribution and further disguising the network.
- Cut-outs represent intermediaries that facilitate communication between two entities in a clandestine operation.[lxvii] In the context of an influence operation, proxies use cut-outs to hide sponsorship or involvement.

Rating:

0. Operation does not conceal sponsorship.
1. Operation minimally conceals sponsorship but leaves a digital footprint that reveals a granular aspect of the sponsor's identity.
2. Operation partially conceals sponsorship so that only the high-level identity of the sponsor is identifiable.
3. Operation successfully conceals sponsorship so that no aspect of the sponsor's identity is identifiable.

2.6 Engage Phase

Once an actor has prepared their resources and is ready to interact with the target audience, the engage phase outlines steps to deliver and amplify content. The engage phase uses resources developed in the enable phase to achieve the operation's previously set goals in the plan phase.

2.6.1 Persist in the Information Environment

2.6.1.1 Use Encrypted Networks

Sub-Techniques: Obfuscate Source Code

Encryption converts plaintext to ciphertext with a cryptographic algorithm.[lxviii] Encrypted networks provide influence operations a semi-protected platform to promote operation content without immediate exposure to authorities or the public. Examples of encrypted networks include WhatsApp, Signal, and LINE.

Rating:

0. Operation does not use encrypted networks.
1. Operation uses networks with weak encryption algorithms.
2. Operation uses networks that collect metadata and other forms of user activity without recording private conversations.
3. Operation uses encrypted networks or platforms that do not collect data or track any form of user activity.

2.6.1.2 Infiltrate and Mimic Social Groups

Sub-Techniques:

Group mimicry, known colloquially as a butterfly attack, occurs when an actor infiltrates a social space and pretends to be a member of a certain social group, usually a group that struggles for representation. An operation in the information environment may mimic a group to insert controversial statements into the discourse, encourage the spread of operation content, or promote harassment among group members. Unlike astroturfing, group mimicry aims to infiltrate and discredit existing grassroots movements, organizations, and media campaigns.

Rating:

0. Operation does not utilize group mimicry.
1. Operation achieves one of three: integrates into the target group, inserts engagement-inducing statements into the discourse, and promotes engagement and interaction among group members.
2. Operation achieves two of three: integrates into the target group, inserts engagement-inducing statements into the discourse, and promotes engagement and interaction among group members.
3. Operation achieves three of three: integrates into the target group, inserts engagement-inducing statements into the discourse, and promotes engagement and interaction among group members.

2.6.1.3 Disguise Spam Messages

Sub-Techniques:

Disguising spam messages, also known as spamoflage, refers to the practice of disguising spam messages as legitimate.[lxix] Spam refers to the use of electronic messaging systems to deliver unsolicited messages in bulk.[lxx] Simple methods of spamoflage include replacing letters with numbers to fool keyword-based email spam filters, for example, 'Congr4tu1at10n5, y0u'v3 b33n s3l3ct3d f0r a fr33 iPhone!'. Spamoflage may extend to more complex techniques such as modifying the grammar or word choice of the language, casting messages as images which spam detectors cannot automatically read, or encapsulating messages in password protected attachments, such as .pdf or .zip files. Operations in the information environment may use spamoflage to avoid spam filtering systems and increase the likelihood of the target audience receiving operation messaging.

Rating:

0. Operation does not disguise spam messages.
1. Operation is unable to avoid spam filtering systems and does not release messaging that encourages direct target audience interactions.
2. Operation avoids most spam filtering systems but does not release messaging that encourages direct target audience interactions.
3. Operation almost completely avoids spam filtering systems and develops messaging that encourages direct target audience interactions.

2.6.1.4 Artificially Age Accounts

Sub-Techniques: Establish Sleeper Sites

An artificially aged account refers to an account manipulated to appear older than it is. An influence operation may artificially age accounts to disguise an account's recent date of creation or inconsistencies in a persona. Artificially aging accounts usually occurs at account creation since attempts to falsely manipulate an account's age after its activation are more easily detectable.

Rating:

0. Operation does not artificially age accounts.
1. Operation fulfills one of three: posts operation content over time to create a false timeline, posts content unrelated to operation narratives to avoid platform detection, maintains minimum activity to avoid account deletion by a platform.
2. Operation fulfills two of three: posts operation content over time to create a false timeline, posts content unrelated to operation narratives to avoid platform detection, maintains minimum activity to avoid account deletion by a platform.
3. Operation fulfills three of three: posts operation content over time to create a false timeline, posts content unrelated to operation narratives to avoid platform detection, maintains minimum activity to avoid account deletion by a platform.

2.6.1.5 Utilize Lenient Hosting Services

Sub-Techniques:

Hosting refers to services through which storage and computing resources are provided to an individual or organization for the accommodation and maintenance of one or more websites and related services.[lxxi] Services may include web hosting, file sharing, and email distribution.

Bulletproof hosting, or lenient hosting services, refers to services provided by an entity, such as a domain hosting or web hosting firm, that allows its customer considerable freedom in use of the service.[lxxii] An operation in the information environment may utilize lenient hosting services to uphold suspicious, illegal, or disruptive operation activities that stricter hosting services would limit, report, or suspend.

Rating:

0. Operation does not utilize lenient hosting services.
1. Operation uses services that heavily monitor user activity for suspicious behavior and collects explicit user data (e.g., photos, message text, etc.).
2. Operation uses services that slightly monitors user activity for suspicious behavior and collects user metadata.
3. Operation uses services that allow for almost complete freedom in user activity without monitoring or reporting suspicious behavior.

2.6.1.6 Misattribute Activity

Sub-Techniques:

Misattributed activity refers to incorrectly attributed operation activity. For example, a state-sponsored influence operation may conduct operation activity in a way that mimics another state so that external entities misattribute activity to the incorrect state. An operation may misattribute their activities to complicate attribution, avoid detection, or frame an adversary for negative behavior.

Rating:

0. Operation does not misattribute activity.
1. Operation fulfills one of three: uses false attributions, creates false evidence to support the misattribution, and amplifies false attribution messaging.
2. Operation fulfills two of three: uses false attributions, creates false evidence to support the misattribution, and amplifies false attribution messaging.
3. Operation fulfills three of three: uses false attributions, creates false evidence to support the misattribution, and amplifies false attribution messaging.

2.6.1.7 Unattribute Activity

Sub-Techniques:

Unattributed activity refers to undetected or activity not attributed to an actor. For example, an influence operation may post anonymously on social media and avoid taking credit for operation activities. Operations may unattribute activity to complicate attribution or avoid detection.

Rating:

0. Operation does not unattribute activity.
1. Operation fulfills one of three: publishes content anonymously, conceals ties between information assets, and conceals network location (e.g., uses a VPN).
2. Operation fulfills two of three: publishes content anonymously, conceals ties between information assets, and conceals network location (e.g., uses a VPN).
3. Operation fulfills three of three: publishes content anonymously, conceals ties between information assets, and conceals network location (e.g., uses a VPN).

2.6.1.8 Vary Type of Account Used

Sub-Techniques:

An operation in the information environment may mix its use of information assets to avoid content removals and bans on selected platforms. Varying the type of account used may help an operation avoid platform detection algorithms by increasing the appearance of an organic movement rather than a coordinated operation. Different account types will vary on the account's autonomy, the platforms they operate on, and the type of content the account posts.

Rating:

0. Operation does not vary type of account used.
1. Operation varies one of three: account autonomy (e.g., manned or unmanned), account platform, and account content type (e.g., photo, video text, etc.).
2. Operation varies two of three: account autonomy (e.g., manned or unmanned), account platform, and account content type (e.g., photo, video text, etc.).
3. Operation varies three of three: account autonomy (e.g., manned or unmanned), account platform, and account content type (e.g., photo, video text, etc.).

2.6.1.9 Exploit Legal System

Sub-Techniques: Exploit Terms and Conditions

Exploiting terms and conditions refers to an instance where an actor vigorously researches a platform's terms of use and carefully crafts a campaign strategy that influences a target audience under the bounds of the platform's conditions. Actors that successfully exploit the terms and conditions will bypass content blocking and maximize campaign reach.

Rating:

0. Operation does not exploit terms and conditions.
1. Operation studies terms and conditions but fails to exploit it in campaign strategy.
2. Operation studies terms and conditions, identifies vulnerabilities and loopholes, and integrates them into the campaign's strategy to avoid detection for a limited time.
3. Operation studies terms and conditions, identifies vulnerabilities and loopholes, and integrates them into the campaign's strategy without detection.

2.6.2 Distort Existing Narratives

2.6.2.1 Amplify Conspiracy Theories

Sub-Techniques: Amplify Original Conspiracy Theories, Amplify Existing Conspiracy Theories, Adapt Existing Conspiracy Theories

An operation in the information environment may create and amplify its own conspiracy theories to support operation objectives using falsely manipulated situations. Conspiracy theories may attract attention to operation assets or narratives, erode trust in public institutions or figures, or sow doubt about operation adversaries.

An operation in the information environment may amplify existing conspiracy theories that align with its narratives to support operation objectives using falsely manipulated situations. Conspiracy theories may attract attention to operation assets or narratives, erode trust in public institutions or figures, or sow doubt about operation adversaries.

Rating:

0. Operation does not amplify original conspiracy theories.

1. Operation amplifies conspiracies that fulfill one of three: are believable to the target audience, opportunistically present real situations out of context, use false or distorted evidence to prove the conspiracy theory.
2. Operation amplifies conspiracies that fulfill two of three: are believable to the target audience, opportunistically present real situations out of context, use false or distorted evidence to prove the conspiracy theory.
3. Operation amplifies original conspiracies that fulfill three of three: are believable to the target audience, opportunistically present real situations out of context, use false or distorted evidence to prove the conspiracy theory.

2.6.2.2 Reframe Context

Sub-Techniques: Viral Sloganeering, Distort Facts, Misattribute Others' Actions

Reframing context refers to removing an event from its surrounding context to distort its intended meaning. Rather than deny that an event occurred, reframing context frames an event in a manner that may lead the target audience to draw a different conclusion about its intentions.

- Viral sloganeering refers to the use of short, catchy phrases to facilitate message delivery, for example, the "lock her up" catchphrase directed at presidential candidate Hillary Clinton during the 2016 election.[lxxiii] Creators of viral slogans often purposefully conceal their identity so that the phrase reaches external audiences and mainstream discourse.
- Distorting facts refers to manipulating the basis of truthful events, reports, or occurrences to support operation narratives. Operations may distort facts by omitting factual information, adding falsified information, or otherwise presenting facts in a falsified context. An influence operation may distort facts to increase the acceptance or persuasiveness of its narrative which the facts would otherwise contradict or undermine.
- Misattributing others' actions refers to misrepresenting, misquoting, or distorting the actions of an unaffiliated individual, organization, or actor. An influence operation may misattribute others' actions to mislead the target audience, sow confusion, or frame the actor in a bad light.

Rating:

0. Operation does not reframe context.
1. Operation achieves one of three: recontextualizes a real event, supports recontextualization with supplemental content, and relates recontextualization to operation narratives.
2. Operation achieves two of three: recontextualizes a real event, supports recontextualization with supplemental content, and relates recontextualization to operation narratives.
3. Operation achieves three of three: recontextualizes a real event, supports recontextualization with supplemental content, and relates recontextualization to operation narratives.

2.6.2.3 Use Malign Rhetoric

Sub-Techniques: Practice Attitude Inoculation, Disrupt Target Audience's Confidence

Malign rhetoric refers to discourse that exploits the often-fragmented nature of conversations in the modern public sphere, especially on social media, to sow confusion in the information space and discourage reasonable discussion.[lxxiv] Malign rhetoric includes the use of logical fallacies, name-calling, and other rhetorical practices that distract from practical discourse.

Attitude inoculation refers to the act of giving a target audience practice at resisting easily refutable arguments.[lxxv] As a result, the target audience may naturally adopt and defend certain arguments over time. Attitude inoculation takes an indirect approach to behavior change by providing subtle counters to certain arguments instead of directly telling a population why they should support a statement. Introducing subtle counterarguments to a target audience will alert them to the idea that a statement or narrative is fragile and requires defending.

Rating:

0. Operation does not use malign rhetoric.
1. Operation's conducts one of three when using malign rhetoric: use malign rhetoric to amplify operation narratives, uses logical fallacies that the target audience finds convincing, delegitimizes opposing narratives.
2. Operation's conducts two of three when using malign rhetoric: use malign rhetoric to amplify operation narratives, uses logical fallacies that the target audience finds convincing, delegitimizes opposing narratives.
3. Operation's conducts three of three when using malign rhetoric: use malign rhetoric to amplify operation narratives, uses logical fallacies that the target audience finds convincing, delegitimizes opposing narratives.

2.6.2.4 Exploit Data Voids

Sub-Techniques:

A data void is a word or phrase that results in little, manipulated, or low-quality search engine data.[lxxvi] Data voids are hard to detect and relatively harmless until exploited by an influence operation aiming to quickly proliferate false or misleading information during a phenomenon that causes a high number of individuals to query the term or phrase. In the engage phase, an influence operation may exploit previously identified data voids (see: Identify Social and Technical Vulnerabilities) to promote content via search engine queries.

A 2019 report by Michael Golebiewski identifies five types of data voids:

(1) "Breaking news" data voids occur when a keyword gains popularity during a short period of time, allowing an influence operation to publish false content before legitimate news outlets have an opportunity to publish relevant information.

(2) An influence operation may create a "strategic new terms" data void by creating their own terms and publishing information online before promoting their keyword to the target audience.
(3) An influence operation may publish content on "outdated terms" that have decreased in popularity, capitalizing on most search engines' preferences for recency.
(4) "Fragmented concepts" data voids separate connections between similar ideas, isolating segment queries to distinct search engine results.
(5) An influence operation may use "problematic queries" that previously resulted in disturbing or inappropriate content to promote misinformation until mainstream media recontextualizes the term.[lxxvii]

Rating:
0. Operation does not exploit data voids.
1. Operation exploits data voids on topics with little to no target audience engagement.
2. Operation exploits data voids on topics not related to operation narratives on forums with limited target audience engagement.
3. Operation exploits data voids on topics related to operation narratives on forums with high target audience engagement.

2.6.2.5 Post Provocative Content

Sub-Techniques: Sh*tposting, Post Clickbait Content, Elicit Emotional Response

Provocative content refers to content designed to attract attention or evoke a specific reaction from the target audience. Provocative content may include sh*tposting or off-topic, misleading, or offensive content posted to online forums designed to derail the conversation, provoke other participants, or confuse the message.

- Provocative content may also include clickbait content, or content whose main purpose is to encourage users to click on a certain post, link, or headline.[lxxviii] An influence operation may post provocative content to promote its messaging on platforms whose algorithms prioritize user engagement, attract attention to its content using inflammatory language, or otherwise increase operation content exposure to the target audience.

Rating:
0. Operation does not exploit data voids.
1. Operation exploits data voids on topics with little to no target audience engagement.
2. Operation exploits data voids on topics not related to operation narratives on search engines with limited target audience engagement.
3. Operation exploits data voids on topics related to operation narratives on search engines with high target audience engagement.

2.6.3 Deliver Products

2.6.3.1 Post on Platforms

Sub-Techniques: Post on Internet Social Media, Post in Physical Forums, Direct Posting, Radio and TV Broadcasts, Aerial Leaflet Drops, Loudspeaker Transmissions, Handbills or Brochures, Face-to-Face Communication, Written Direct Letters

An operation can directly amplify its messaging by posting content on platforms frequented by a target audience. Content delivery is an integral campaign step that provides operators the opportunity to amplify their messaging and connect with the target audience.

Direct posting refers to a method of posting content via a one-way messaging service, where the recipient cannot directly respond to the poster's messaging. An operation in the information environment may post directly to promote operation narratives to the target audience without allowing opportunities for fact-checking or disagreement, creating a false sense of support for the narrative.

A social media post refers to any social media status update, photo, or video, or an item shared on a blog or forum.[lxxix] An operation in the information environment may post to social media to promote operation narratives to its target audience while exploiting factors of social media use that facilitate content virality, including information overload, the limited time users spend on each post while scrolling through platform timelines, and platform algorithms that prioritize views and engagement.[lxxx]

Rating:

0. Operation does not post content directly.
1. Operation achieves one of three: posts content on platforms that obfuscate attribution, moderates engagement and interactions from the target audience, and cross-posts operation-related content from other channels or sources.
2. Operation achieves two of three: posts content on platforms that obfuscate attribution, moderates engagement and interactions from the target audience, and cross-posts operation-related content from other channels or sources.
3. Operation achieves three of three: posts content on platforms that obfuscate attribution, moderates engagement and interactions from the target audience, and cross-posts operation-related content from other channels or sources.

2.6.3.2 Receive Media Exposure

Sub-Techniques: Earn Media Recognition, Purchase Media Recognition, Purchase Advertisements, Advertise on Selected Platforms

Receiving media exposure involves an operation's acknowledgement, whether it be praise or criticism, on media channels seemingly unaffiliated with the operation. Media exposure varies from earned media to paid media.

- Earned media consists of content and conversation around a brand or product that originates externally through relationship building, brand recognition, endorsements, and

other methods that garner a following.[lxxxi] For example, a state-sponsored influence operation may appeal to patriotism in its foreign nationals to convince them to publish operation content on their personal channels.
- Paid media refers to media that an operation purchases with currency rather than brand recognition or another form of indirect payment.[lxxxii] An operation may purchase traditional media to reach its target audience through established channels including TV, radio, and newspaper.

Rating:
0. Operation does not receive media exposure.
1. Operation achieves one of six: earns media without spending operation funds, earns media that exposes content to the target audience, obscures ties between the earned media and the operation to avoid attribution, purchases media that exposes content to target audience members at peak viewing times, tailors the content to the target audience without violating marketing standards, and purchases traditional media on at least two different channels or mediums.
2. Operation achieves three of six: earns media without spending operation funds, earns media that exposes content to the target audience, obscures ties between the earned media and the operation to avoid attribution, purchases media that exposes content to target audience members at peak viewing times, tailors the content to the target audience without violating marketing standards, and purchases traditional media on at least two different channels or mediums.
3. Operation achieves five of six: earns media without spending operation funds, earns media that exposes content to the target audience, obscures ties between the earned media and the operation to avoid attribution, purchases media that exposes content to target audience members at peak viewing times, tailors the content to the target audience without violating marketing standards, and purchases traditional media on at least two different channels or mediums.

2.6.3.3 Leak Documents

Sub-Techniques: Leak False Documents, Leak Authentic Documents, Demonstrate Document Authenticity, Retrieve, but don't Leak Documents

Leaking documents refers to releasing documents containing sensitive or private information. An operation in the information environment may leak authentic or falsified documents to discredit or undermine an adversary, expose hidden information that supports operation narratives, or otherwise bring attention to the operation's relevant topics.

Rating:
0. Operation does not leak authentic documents.
1. Operation leaks documents that contain previously known or publicly released information that does not relate to operation narratives.
2. Operation leaks documents that contain new, supposedly private, but unconvincing information that does not relate to operation narratives.
3. Operation leaks documents that contain new, private, and compelling information that supports operation narratives.

2.6.3.4 Microtargeting

Sub-Techniques: Curate Content, Curate Content for a Fee, Trading Up the Chain, Exploit Small Platforms

Microtargeting refers to a marketing strategy that uses large amounts of data collected from social media accounts and online activity to create highly specific content for a target audience.[lxxxiii] Microtargeted ads narrow their focus to a specific group of individuals with similar views. For example, a regular political ad may target conservative voters, while a microtargeted ad will focus in on specific factions within the Republican Party, such as conservative voters in Ohio who oppose a state-specific gun law or Hispanic registered Republicans in Miami who oppose county-specific climate change legislation. Microtargeting may incorporate data spanning different rhetorical strategies like morality, religion, and personal attacks collected from sources beyond social media.[lxxxiv]

- Curated content refers to a collection of content, such as news articles, images, videos, or other media, specifically assembled for the target audience. Curated content for a fee refers to personalized content collections that a user pays to access. An influence operation may curate content to personalize operation narratives to the target audience, potentially raising revenue in the process if the target audience pays for access.
- Trading up the chain refers to posting content to smaller online communities and platforms so that larger online communities and platforms will reference and further amplify the content.[lxxxv] Influence operations may aim for its content to trade up the chain during times of confusion, such as during a breaking news event, when facts remain unclear and authentic news outlets search for relevant reporting on smaller platforms.

Rating:

0. Operation does not use microtargeting.
1. Operation microtargets the audience based on two of five: location, demographics, political affiliation, economic status, and psychographic data.
2. Operation microtargets the audience based on three/four of five: location, demographics, political affiliation, economic status, and psychographic data.
3. Operation microtargets the audience based on five of five: location, demographics, political affiliation, economic status, and psychographic data.

2.6.3.5 Utilize Social Media Management Software

Sub-Techniques:

Social media management software (SMMS) allows a single user to simultaneously manage multiple different social media accounts.[lxxxvi] An influence operation may use SMMS to post to multiple channels simultaneously, conduct comparative analysis of posts on different platforms, or gather general analytics from posts on multiple channels. Analysts could detect the use of social media management software by studying Twitter web clients.

Rating:

0. Operation does not utilize social media management software.

1. Operation uses social media management software to achieve one of three: post to multiple channels simultaneously, conduct comparative analysis of posts on different platforms, and gather interaction metrics from multiple channels.
2. Operation uses social media management software to achieve two of three: post to multiple channels simultaneously, conduct comparative analysis of posts on different platforms, and gather interaction metrics from multiple channels.
3. Operation uses social media management software to achieve three of three: post to multiple channels simultaneously, conduct comparative analysis of posts on different platforms, and gather interaction metrics from multiple channels.

2.6.3.6 Target Purchased Ads

Sub-Techniques:

Targeting purchased ads refers to paying a platform or organization to direct operation advertising toward the entire target audience or specific members of the target audience. An influence operation may target purchased ads to ensure that its content reaches the intended audience. Unpublished ads, or dark ads refer to ads that only appear to a single user based on their personal algorithm and preferences, limiting opportunities for platform monitoring services and external investigators to identify and track operation activities as they appear exclusively to a single user.[lxxxvii]

Rating:

0. Operation does not target purchased ads.
1. Operation attempts to target a general target audience but fails to receive content exposure on active platforms.
2. Operation pays platform to display ads to specific target audience members based on collected analytics but does not obscure the relationship between operators and platforms to avoid attribution.
3. Operation pays platform to display ads to specific target audience members based on collected analytics and obscures the relationship between operators and platforms to avoid attribution.

2.6.4 Amplify Supporting Information (Maximize Exposure)

2.6.4.1 Distribute Products to Disseminating Entities

Sub-Techniques: Air Transport, Ground Transport, Digitally Secure Means, Domestic or Multinational Transportation, Home Nation Assets, Nationalized Enterprises, Commercial Vendors, Non-Governmental Organizations

An operation should distribute its previously developed products to relevant disseminating entities to uphold timeliness and maximize reach. Distributing products refers to the identification of relevant organizations, agencies, partners, systems, and individuals with the capacity to share content with the target audience.

Rating:

0. Operation does not distribute products to disseminating entities.

1. Operation distributes products either in an untimely manner or to irrelevant entities.
2. Operation distributes products in a timely manner to entities unfamiliar with how to effectively distribute them.
3. Operation distributes products to relevant entities familiar with how to distribute them in a timely manner.

2.6.4.2 Conduct Information Flooding

Sub-Techniques: Aggressive Post Interaction, Information Pollution, Negative Information Flooding, Swarming, Cheerleading for Distraction, Manufactured Volume Bursts, Swiftboating, Post Duplicate Messages

Information flooding refers to the repetitive promotion of a common message over a network to reinforce an operation-aligned message to the audience.[lxxxviii] An influence operation may flood platforms with content that supports operation narratives to overwhelm opposing narratives, create a false sense of support for operation narratives, or otherwise increase content exposure to the target audience.

- Aggressive post interaction refers to the continuous liking, commenting, and sharing on content to either amplify or discredit it. An influence operation may support information flooding with aggressive post interaction to further promote content to the target audience and create a false sense of support for operation narratives.
- Information pollution refers to a specific form of information flooding that contaminates the information environment with incomplete, inconsistent, or irrelevant content.[lxxxix] An influence operation may use information pollution to confuse the target audience, discredit adversary narratives, or crowd out opposing content.
- Negative information flooding refers to the infiltration of adversarial information spaces to flood the channel with the same, operation-aligned message.
- Swarming refers to the coordinated use of accounts to overwhelm the information space with operation content.[xc] Unlike information flooding, swarming centers exclusively around a specific event or actor rather than a general narrative. Swarming relies on "horizontal communication" between information assets rather than a top-down, vertical command-and-control approach.[xci]
- Cheerleading for distraction refers to posting unrelated positive content, including patriotic, grateful, encouraging, and motivational sentiments, to distract the public from an issue and change the subject of reporting in traditional and online.[xcii]
- Manufactured bursts refer to coordinated increases in social media activity, usually surrounding a specific event.[xciii] An influence operation may manufacture bursts of social media activity to either draw attention to or distract from narratives around the event.
- Swiftboating refers to a form of swarming through smear attacks on an individual actor before a decisive event, such as an election, leaving little time for the target to respond.[xciv] An influence operation may use swiftboating to overwhelm the information space with its content, burying adversary responses and allowing the operation to frame the narrative around the actor with limited interference. The term 'swiftboating' dates back to the 2004 U.S. election, when former Vietnam veterans and prisoners of war falsely claimed that presidential candidate John Kerry 'distorted material facts' related to his 'conduct' during the war. The organization responsible for the claims, Swift Vets and POWs for Truth, contributed to a shift in public opinion against Kerry.

Rating:

0. Operation does not conduct information flooding.
1. Operation achieves one of three: floods sufficient content to crowd out opposing narratives with noise, persistently interacts with opposing narratives while amplifying operation narratives, and floods content in a manner that the media and non-operation sources perceive as authentic.
2. Operation achieves two of three: floods sufficient content to crowd out opposing narratives with noise, persistently interacts with opposing narratives while amplifying operation narratives, and floods content in a manner that the media and non-operation sources perceive as authentic.
3. Operation achieves three of three: floods sufficient content to crowd out opposing narratives with noise, persistently interacts with opposing narratives while amplifying operation narratives, and floods content in a manner that the media and non-operation sources perceive as authentic.

2.6.4.3 Conduct Automated Amplification

Sub-Techniques: In-Network Amplification, Bandwagoning, Botsharing

Automated amplification, also known as botnet amplification, refers to the use of a network of automated or cyborg accounts in a coordinated fashion to promote a defined group of users by aggregating and reposting content originally posted by seed users.[xcv] An influence operation may conduct botnet amplification to artificially promote operation content to the target audience.

In-network amplification utilizes the existing accounts within an influence operation to amplify the posts made by other accounts within that network, allowing an operation to capitalize on its existing social media assets rather than create brand-new accounts.[xcvi]

Bandwagoning refers to instances in influence operations where users are incentivized to believe a statement or narrative because a majority of the population appears to support it.

Rating:

0. Operation does not conduct automated amplification.
1. Operation achieves one of three: creates echo chambers with operation and target-audience accounts, uses automated amplification to infiltrate existing communities with operation-related content and narratives, and botnet account activity avoids detection by platforms.
2. Operation achieves two of three: creates echo chambers with operation and target-audience accounts, uses automated amplification to infiltrate existing communities with operation-related content and narratives, and botnet account activity avoids detection by platforms.
3. Operation achieves three of three: creates echo chambers with operation and target-audience accounts, uses automated amplification to infiltrate existing communities with operation-related content and narratives, and botnet account activity avoids detection by platforms.

2.6.4.4 Exploit Platform-Specific Features

Sub-Techniques: Use Hashtag(s)/Hashtag Groups, Co-Opted Hashtag(s), Original Hashtag(s), Private Messaging, Share Memes (Viral Sloganeering)

After analyzing a platform's strengths and limitations, operators should assess which types of content tend to receive greater exposure on that forum. As a result, they could share memes, use hashtags, and integrate other techniques into their operation strategy to increase reach.

- A private message refers to an exchange that only its sender and recipient can access. An influence operation may tailor private messages to its target audience or potential intermediaries such as journalists, activists, and public figures, to increase the appearance of authenticity and likelihood that the message will resonate with the recipient. An operation may use private messaging to reinforce operation messaging directly to target audience members without external viewership, limiting opportunities for platform monitoring systems or external investigators to identify and track operation activities.
- A hashtag refers to a word or phrase preceded by the hash symbol (#) on social media used to identify messages and posts relating to a specific topic. A hashtag group occurs when a message developer places several hashtags at the end of a message, allowing a single post to appear in multiple searches. All public posts that use the same hashtag are aggregated onto a centralized page dedicated to the word or phrase and sorted either chronologically or by popularity. An influence operation may create original hashtag(s) and/or hashtag groups in preparation to boost operation content on social media.
- Viral sloganeering refers to the use of short, catchy phrases to facilitate message delivery.[xcvii] Creators of viral slogans often purposefully conceal their identity so that the phrase reaches external audiences and mainstream discourse.

Rating:

0. Operation does not exploit platform-specific features.
1. Operation attempts to exploit platform-specific features, but formats content in ways that don't complement social media algorithms or platform-conducive post structure (e.g., not using a hashtag on Twitter or not using reels on Instagram).
2. Operation partially exploits platform-specific features by formatting content in either ways that complement social media algorithms or platform-conducive post structure.
3. Operation successfully exploits platform-specific features by formatting content in ways that complement social media algorithms and platform-conducive post structure.

2.6.4.5 Conduct Cross-Posting

Sub-Techniques:

Cross-posting refers to posting the same message to multiple internet discussions, social media platforms or accounts, or news groups at one time.[xcviii] An influence operation may post content online in multiple communities and platforms to increase the chances of exposing content to the target audience.

Rating:

0. Operation does not cross-post.

1. Operation cross-posts content on multiple platforms in one of three ways: posts content on platforms with high potential for target audience engagement, posts content tailored for sharing on multiple platforms, coordinates messaging across multiple platforms.
2. Operation cross-posts content on multiple platforms in two of three ways: posts content on platforms with high potential for target audience engagement, posts content tailored for sharing on multiple platforms, coordinates messaging across multiple platforms.
3. Operation cross-posts content on multiple platforms in three of three ways: posts content on platforms with high potential for target audience engagement, posts content tailored for sharing on multiple platforms, coordinates messaging across multiple platforms.

2.6.4.6 Post Consistently Over Time

Sub-Techniques:

Posting consistently over time refers to an operation's uninterrupted publication of content over an extended period. In an erratic information environment, operators should consistently publish content to ensure that operation narratives retain their influence and relevance. Different topics often grow and decline over time in popularity, but successful operations know to consistently post and adapt narratives to account for rising developments. What constitutes as consistent posting may vary depending on an operation's goals and its information environment.

Rating:

0. Operation does not post consistently over time.
1. Operation posts in an irregular but semi-consistent pattern that sometimes reaches the target audience.
2. Operation posts consistently but does not adapt messaging in response to external developments.
3. Operation posts consistently and incorporates external developments into narratives.

2.6.4.7 Post at Hours Reflecting Highest Activity

Sub-Techniques:

Posting at hours reflecting highest activity refers to posting content when the target audience will most likely view and engage with the content depending on the time zone or user habits. An operation in the information environment may post content at hours reflecting highest activity to increase content exposure to the target audience.

Rating:

0. Operation does not post at hours reflecting highest activity.
1. Operation uses previous target audience analysis to achieve one of the following: post at hours of highest target audience activity on a platform, post at times immediately after a breaking news event, tailor posts to a specific time of day.
2. Operation uses previous target audience analysis to achieve two of the following: post at hours of highest target audience activity on a platform, post at times immediately after a breaking news event, tailor posts to a specific time of day.

3. Operation uses previous target audience analysis to achieve all the following criteria: post at hours of highest target audience activity on a platform, post at times immediately after a breaking news event, tailor posts to a specific time of day.

2.6.4.8 Leverage Platform Algorithm

Sub-Techniques: Keyword Squatting

Manipulating a platform algorithm refers to conducting activity on a platform in a way that intentionally targets its underlying algorithm. After analyzing a platform's algorithm (see: Select Operation Platforms Tactic), an influence operation may use a platform in a way that increases its content exposure, avoids content removal, or otherwise benefits the operation's strategy. For example, an influence operation may use bots to amplify its posts so that the platform's algorithm recognizes engagement with operation content and further promotes the content on user feeds.

- Keyword squatting refers to the creation of online content, such as websites, articles, or social media accounts, around a specific search engine-optimized term to overwhelm the search results of that term.[xcix] An influence may keyword squat to increase content exposure to target audience members who query the exploited term in a search engine and manipulate the narrative around the term.

Rating:

0. Operation does not leverage platform algorithm.
1. Operation leverages platform algorithm to achieve one of three: maximize content exposure on target audience timelines, avoid content removal by platform monitoring services, create an echo chamber reinforcing operation narratives to the target audience.
2. Operation leverages platform algorithm to achieve two of three: maximize content exposure on target audience timelines, avoid content removal by platform monitoring services, create an echo chamber reinforcing operation narratives to the target audience.
3. Operation leverages platform algorithm to achieve three of three: maximize content exposure on target audience timelines, avoid content removal by platform monitoring services, create an echo chamber reinforcing operation narratives to the target audience.

2.6.4.9 Automate Forwarding and Reposting

Sub-Techniques:

Automated forwarding and reposting refers to the proliferation of operation content using automated means, such as artificial intelligence or social media bots. An operation in the information environment may use automated activity to increase content exposure without dedicating resources such as personnel and time to forward and repost content.

Rating:

0. Operation does not automate forwarding and reposting.

1. Operation automates forwarding and reposting to achieve one of three: mimics human behavior to avoid detection by platform monitoring services and external investigators, automates posts at hours of high activity and engagement, automates posts on platforms with exposure to the target audience.
2. Operation automates forwarding and reposting to achieve two of three: mimics human behavior to avoid detection by platform monitoring services and external investigators, automates posts at hours of high activity and engagement, automates posts on platforms with exposure to the target audience.
3. Operation automates forwarding and reposting to achieve three of three: mimics human behavior to avoid detection by platform monitoring services and external investigators, automates posts at hours of high activity and engagement, automates posts on platforms with exposure to the target audience.

2.6.4.10 Conceal Grassroots Movement Sponsorship

Sub-Techniques:

Concealing grassroots movement sponsorship, also known as astroturfing, occurs when an influence operation disguises itself as a grassroots movement or organization that supports operation narratives.[c] Unlike group mimicry, astroturfing aims to increase the appearance of popular support for the operation cause without infiltrating existing groups to discredit their objectives.

Rating:

0. Operation does not use astroturfing.
1. Operation achieves one of three: poses as movements that support operation narratives, uses information assets to create a false sense of support for the movement, and uses symbols, slogans, or other coordinated messaging to increase the movement's appearance of authenticity.
2. Operation achieves two of three: poses as movements that support operation narratives, uses information assets to create a false sense of support for the movement, and uses symbols, slogans, or other coordinated messaging to increase the movement's appearance of authenticity.
3. Operation achieves three of three: poses as movements that support operation narratives, uses information assets to create a false sense of support for the movement, and uses symbols, slogans, or other coordinated messaging to increase the movement's appearance of authenticity.

2.6.4.11 Incentivize Sharing

Sub-Techniques:

Incentivizing content sharing refers to actions that encourage users to share content themselves, reducing the need for the operation itself to post and promote its own content. An influence operation may incentivize content sharing by:

- Directly encouraging sharing on its content (i.e., "repost if you agree").
- Posting content on platforms that allow for direct forwarding and reposting.
- Posting content tailored for sharing on multiple platforms (i.e., articles with embedded links to share on social media).
- Posting content that inflames emotions (i.e. articles with sensational or outrageous titles).

Rating:

0. Operation does not incentivize sharing.
1. Operation conducts one of three: encourages sharing directly on its content, posts content on platforms that allow for direct reposting or forwarding, posts content tailored for sharing on multiple platforms.
2. Operation conducts two of three: encourages sharing directly on its content, posts content on platforms that allow for direct reposting or forwarding, posts content tailored for sharing on multiple platforms.
3. Operation conducts three of three: encourages sharing directly on its content, posts content on platforms that allow for direct reposting or forwarding, posts content tailored for sharing on multiple platforms.

2.6.5 Disrupt Information Flow

2.6.5.1 Block Content

Sub-Techniques: Delete Opposing Content, IP or Packet-Based Blocking, Deep Inspection-Based Blocking, URL-Based Blocking, Platform-Based Blocking, DNS-Based Blocking, DDOS Attack

Content blocking refers to actions taken to restrict internet access or render certain areas of the internet inaccessible.[ci] An influence operation may restrict content based on both network and content attributes. Types of content blocking include:

- IP or packet-based blocking restricts the network itself and filters traffic based on IP addresses or other network identifiers, such as TCP/IP port numbers.[cii] IP or packet-based blocking require the operation to have complete control over the user's network connection and will not restrict content from users using a Virtual Private Network (VPN) or Content Delivery Network (CDN).
- Deep packet inspection-based blocking restricts content based on the content itself, patterns, or application types.[ciii] Deep packet inspection-based blocking may filter traffic based on keywords, traffic characteristics, filenames, or other attributes and requires high cost and levels of access to a user's network. Deep packet filtering may fail to filter encrypted traffic and multimedia files, such as videos.
- URL-based blocking restricts content by intercepting web (HTTP) traffic and comparing the URL to a local database or online service.[civ] URL-based blocking requires the operation to have control over the user's connection to the internet and may fail to block embedded, complicated, or frequently altered links.
- Platform-based blocking requires the assistance of the platform owner, such as a search engine, and restricts access to certain sites on the platform itself.[cv] Platform-based

blocking is rarely effective as it only restricts pointers to the content on the platform, leaving the content accessible on other part of the internet.
- Domain Name System, or DNS-based blocking, uses a specialized DNS resolver to restrict content based on DNS queries.[cvi] DNS-based blocking requires the operation to have complete control over the user's network connection.
- A Distributed Denial of Service (DDOS) attack attempts to disrupt the services of a network or service temporarily or indefinitely by overwhelming the target with requests and traffic.[cvii] An influence operation may conduct a DDOS attack against either opposing information sources to limit their ability to distribute conflicting content or target audience members to limit their ability to receive conflicting content.

Rating:

0. Operation does not block content.
1. Operation employs platform-based content blocking mechanisms to restrict content on the targeted platforms.
2. Operation employs either content-aware or network-based content blocking mechanisms to restrict content based on its messaging or its source.
3. Operation employs both content-aware and network-based content blocking mechanisms to restrict content based on its messaging and its source.

2.6.5.2 Bypass Content Blocking

Sub-Techniques:

Bypassing content blocking refers to actions taken to circumvent network security measures that prevent users from accessing certain servers, resources, or other online spheres. An influence operation may bypass content blocking to amplify its content on internet-restricted areas. Common strategies for bypassing content blocking include:[cviii]

- Altering IP addresses to avoid IP filtering.
- Using a Virtual Private Network (VPN) to avoid IP filtering.
- Using a Content Delivery Network (CDN) to avoid IP filtering.
- Enabling encryption to bypass packet inspection blocking.
- Manipulating text to avoid filtering by keywords.
- Posting content on multiple platforms to avoid platform-specific removals.
- Using local facilities or modified DNS servers to avoid DNS filtering.

Rating:

0. Operation does not bypass content blocking.
1. Operation bypasses either content-aware or network-based content blocking for a portion of the operation.
2. Operation bypasses either content-aware or network-based content blocking for the entirety of the operation.
3. Operation bypasses both content-aware and network-based content blocking for the entirety of the operation.

2.6.5.3 Destroy Information Generation Capabilities

Sub-Techniques:

Destroying information generation capabilities refers to actions taken to limit, degrade, or otherwise incapacitate an actor's ability to generate conflicting information. An operation in the information environment may destroy an actor's information generation capabilities by physically dismantling the information infrastructure, disconnecting resources needed for information generation, or redirecting information generation personnel. An operation may destroy an adversary's information generation capabilities to limit conflicting content exposure to the target audience and crowd the information space with its own narratives.

Rating:

0. Operation does not destroy information generation capabilities.
1. Operation achieves one of three: destroys adversary information generation capabilities for the duration of the operation, destroys information generation capabilities without attribution, and promotes its own operational content in information spaces in which the adversary's capabilities have been incapacitated.
2. Operation achieves two of three: destroys adversary information generation capabilities for the duration of the operation, destroys information generation capabilities without attribution, and promotes its own operational content in information spaces in which the adversary's capabilities have been incapacitated.
3. Operation achieves three of three: destroys adversary information generation capabilities for the duration of the operation, destroys information generation capabilities without attribution, and promotes its own operational content in information spaces in which the adversary's capabilities have been incapacitated.

2.6.6 Denigrate Opposing Information

2.6.6.1 Denigrate Believers of Opposing Narratives

Sub-Techniques: Doxing, Exploit Cancel Culture, Harass/Discredit Journalists

Denigrating believers of opposing narratives refers to the use of intimidation techniques, including cyberbullying and doxing, to discourage opponents from voicing their dissent. An influence operation may threaten or harass believers of the opposing narratives to deter individuals from posting or proliferating conflicting content.

- Doxing refers to online harassment in which individuals publicly release private information about another individual, including names, addresses, employment information, pictures, family members, and other sensitive information.[cix] An influence operation may dox its opposition to encourage individuals aligned with operation narratives to harass the doxed individuals themselves or otherwise discourage the doxed individuals from posting or proliferating conflicting content.
- Cancel culture refers to the ostracism of an individual or group from society for conducting actions deemed unacceptable by said society.[cx]

Rating:

0. Operation does not denigrate believers of the opposing narrative.

1. Operation achieves one of three: identifies individuals that both believe and proliferate conflicting content, tailor threats and harassment techniques to the individual, and provide the individuals with alternative, pro-operation narratives to review and disseminate.
2. Operation achieves two of three: identifies individuals that both believe and proliferate conflicting content, tailor threats and harassment techniques to the individual, and provide the individuals with alternative, pro-operation narratives to review and disseminate.
3. Operation achieves three of three: identifies individuals that both believe and proliferate conflicting content, tailor threats and harassment techniques to the individual, and provide the individuals with alternative, pro-operation narratives to review and disseminate.

2.6.6.2 Report Opposing Content

Sub-Techniques: Leverage Copyright Regulations, Mass-Report Opposing Content, Mass-Dislike Opposing Content

Reporting opposing content refers to notifying and providing an instance of a violation of a platform's guidelines and policies for conduct on the platform. In addition to simply reporting the content, an operation may leverage copyright regulations to trick social media and web platforms into removing opposing content by manipulating the content to appear in violation of copyright laws. Reporting opposing content facilitates the suppression of contradictory information and allows operation narratives to take priority in the information space.

Rating:

0. Operation does not report opposing content.
1. Operation achieves one of three: reports content on platforms that deactivate or suspend accounts for violating its terms of service, encourages its target audience to report content on adversarial accounts, and presents its own content as an alternative to the reported content.
2. Operation achieves two of three: reports content on platforms that deactivate or suspend accounts for violating its terms of service, encourages its target audience to report content on adversarial accounts, and presents its own content as an alternative to the reported content.
3. Operation achieves three of three: reports content on platforms that deactivate or suspend accounts for violating its terms of service, encourages its target audience to report content on adversarial accounts, and presents its own content as an alternative to the reported content.

2.6.7 Drive Off-Platform Activity

2.6.7.1 Drive to Alternative Platforms

Sub-Techniques:

Rerouting to alternative platforms refers to encouraging users to move from the platform on which they initially viewed operation content and engage with content on alternate information

channels, including separate social media channels and inauthentic websites. An operation may drive to alternative platforms to diversify its information channels and ensure the target audience knows where to access operation content if the initial platform suspends, flags, or otherwise removes the original operation assets and content.

Rating:

0. Operation does not reroute to alternative platforms.
1. Operation achieves one of three: embeds links to alternative platforms within original content posts, coordinates content across platforms for consistent messaging, and encourages users to subscribe, follow, or otherwise bookmark each individual channel to continue consuming messaging.
2. Operation achieves two of three: embeds links to alternative platforms within original content posts, coordinates content across platforms for consistent messaging, and encourages users to subscribe, follow, or otherwise bookmark each individual channel to continue consuming messaging.
3. Operation achieves three of three: embeds links to alternative platforms within original content posts, coordinates content across platforms for consistent messaging, and encourages users to subscribe, follow, or otherwise bookmark each individual channel to continue consuming messaging.

2.6.7.2 Drive to Physical Forums

Sub-Techniques: Organize Rallies/Protests, Radio, Newspapers, Billboards

Driving to physical forums refers to encouraging users to leave the platform on which they initially viewed operation content and engage in the physical information space. Physical forums may include operation-aligned rallies or protests, radio, newspaper, or billboards. An operation in the information environment may drive to physical forums to diversify its information channels and facilitate spaces where the target audience can engage with both operation content and like-minded individuals offline.

Rating:

0. Operation does not drive to physical forums.
1. Operation achieves one of three: drives to physical forums that the target audience can easily access (e.g., bulletins in the target audience's geographic area), promotes physical activities on online information channels to maximize participation/attendance, and coordinates online and offline content for consistent messaging.
2. Operation achieves two of three: drives to physical forums that the target audience can easily access (e.g., bulletins in the target audience's geographic area), promotes physical activities on online information channels to maximize participation/attendance, and coordinates online and offline content for consistent messaging.
3. Operation achieves three of three: drives to physical forums that the target audience can easily access (e.g., bulletins in the target audience's geographic area), promotes physical activities on online information channels to maximize participation/attendance, and coordinates online and offline content for consistent messaging.

2.6.7.3 Call to Action

Sub-Techniques:

A call to action refers to an instruction in the form of a speech, piece of writing, or other composition that encourages people to physically react to a development.[cxi] An influence operation may use a call to action to motivate its target audience to take specific actions that support operation objectives, for example, encouraging the target audience to "get out and vote" for its preferred candidate.

Rating:

0. Operation does not call to action.
1. Operation achieves one of three: calls for an action that directly supports its determined desired behavior(s) for the target audience, calls for a specific action that the target audience can practically complete (e.g., voting for a candidate), and supports the call to action with content that justifies the instruction.
2. Operation achieves two of three: calls for an action that directly supports its determined desired behavior(s) for the target audience, calls for a specific action that the target audience can practically complete (e.g., voting for a candidate), and supports the call to action with content that justifies the instruction.
3. Operation achieves three of three: calls for an action that directly supports its determined desired behavior(s) for the target audience, calls for a specific action that the target audience can practically complete (e.g., voting for a candidate), and supports the call to action with content that justifies the instruction.

2.6.7.4 Conduct Symbolic Action

Sub-Techniques: Potemkin Village of Evidence

Symbolic action refers to activities specifically intended to advance an operation's narrative by signaling something to the audience.[cxii] For example, a military parade supporting a state's narrative of military superiority. An influence operation may use symbolic action to create situations supporting operation narratives in the physical information space.

A Potemkin Village of evidence refers to an operation's wide use of doctored or falsified content, evidence, or support for operation narratives.[cxiii] An operation may use a Potemkin Village to shift perceptions to external audiences, deceiving others into thinking that there is truth in what is presented.

Rating:

0. Operation does not conduct symbolic action.
1. Operation achieves one of three: promotes symbolic action in advance of the activity to maximize participation/attendance, supports symbolic action with additional content explaining or justifying the action, times symbolic action to support operation narratives or objectives (e.g., conducts a rally supporting a candidate directly before an election).
2. Operation achieves two of three: promotes symbolic action in advance of the activity to maximize participation/attendance, supports symbolic action with additional content explaining or justifying the action, times symbolic action to support operation narratives or objectives (e.g., conducts a rally supporting a candidate directly before an election).

3. Operation achieves three of three: promotes symbolic action in advance of the activity to maximize participation/attendance, supports symbolic action with additional content explaining or justifying the action, times symbolic action to support operation narratives or objectives (e.g., conducts a rally supporting a candidate directly before an election).

2.6.7.5 Conduct Physical Action

Sub-Techniques:

Physical action occurs when an influence operation convinces individuals to act in the physical realm. An influence operation may pay for physical action to create specific situations and frame them in a way that supports operation narratives, for example, paying a group of people to burn a car to later post an image of the burning car and frame it as an action of protest. Physical violence refers to the use of force to injure, abuse, damage, or destroy.[cxiv] An influence operation may conduct physical violence to discourage opponents from promoting conflicting content or draw attention to operation narratives using shock value.

Rating:

0. Operation does not conduct physical action.
1. Operation achieves one of three: conducts physical action that directly supports operation narratives, obscures ties between the operation and intermediaries, and supports physical action with content explaining or justifying the action (does not require the operation to take responsibility).
2. Operation achieves two of three: conducts physical action that directly supports operation narratives, obscures ties between the operation and intermediaries, and supports physical action with content explaining or justifying the action (does not require the operation to take responsibility).
3. Operation achieves three of three: conducts physical action that directly supports operation narratives, obscures ties between the operation and intermediaries, and supports physical action with content explaining or justifying the action (does not require the operation to take responsibility).

2.6.7.6 Reach Mainstream Media Coverage

Sub-Techniques: Incentivize Real Reporting on the Story

Reaching mainstream media coverage occurs when conventional media outlets cover operation narratives or cite operation materials as sources. An operation in the information environment may incentivize real reporting on a story by paying journalists to cover operation narratives or the narratives may reach mainstream media incidentally, for example, by going "viral" on social media.

Rating:

0. Operation does not reach mainstream media coverage.
1. Operation achieves one of three: reaches mainstream media coverage on outlets that the target audience consumes, receives positive mainstream media coverage, and sources media coverage in later content to add legitimacy to operation messaging.

2. Operation achieves two of three: reaches mainstream media coverage on outlets that the target audience consumes, receives positive mainstream media coverage, and sources media coverage in later content to add legitimacy to operation messaging.
3. Operation achieves three of three: reaches mainstream media coverage on outlets that the target audience consumes, receives positive mainstream media coverage, and sources media coverage in later content to add legitimacy to operation messaging.

2.6.7.7 Conduct Fundraising Campaigns

Sub-Techniques: Crowdfunding, Individual Donations, Sell Merchandise

Fundraising campaigns refer to an influence operation's systematic effort to seek financial support for a charity, cause, or other enterprise using online activities that further promote operation information pathways while raising a profit. Many influence operations have engaged in crowdfunding services on platforms including Tipee, Patreon, and GoFundMe.[cxv] Crowdfunding involves efforts where a group of people donate funds to a cause. An operation may use its previously prepared fundraising campaigns to promote operational messaging while raising money to support its activities.

Rating:

0. Operation does not conduct fundraising campaigns.
1. Operation achieves one of three: promotes the fundraiser on multiple existing information channels, incorporates operation messaging into fundraising materials and activities, and raises a profit from the fundraising campaign.
2. Operation achieves two of three: promotes the fundraiser on multiple existing information channels, incorporates operation messaging into fundraising materials and activities, and raises a profit from the fundraising campaign.
3. Operation achieves three of three: promotes the fundraiser on multiple existing information channels, incorporates operation messaging into fundraising materials and activities, and raises a profit from the fundraising campaign.

2.6.7.8 Sell Merchandise

Sub-Techniques:

Selling merchandise refers to the sale of often branded items to the target audience. An operation in the information environment may sell merchandise to raise funds and promote its messaging in the physical information space, for example, by selling t-shirts with operational messaging displayed on the fabric.

Rating:

0. Operation does not sell merchandise.
1. Operation achieves one of three: obfuscates links between merchandise and operation funding sources, incorporates operation messaging and slogans into merchandise, and sells merchandise tailored to target audience consumer tendencies (e.g., selling hoodies in cold climates and baseball caps in warm climates).
2. Operation achieves two of three: obfuscates links between merchandise and operation funding sources, incorporates operation messaging and slogans into merchandise, and

sells merchandise tailored to target audience consumer tendencies (e.g., selling hoodies in cold climates and baseball caps in warm climates).
3. Operation achieves three of three: obfuscates links between merchandise and operation funding sources, incorporates operation messaging and slogans into merchandise, and sells merchandise tailored to target audience consumer tendencies (e.g., selling hoodies in cold climates and baseball caps in warm climates).

2.6.8 Remove Evidence of Tactics

2.6.8.1 Delete Account Activity

Sub-Techniques: Delete Accounts

Deleting accounts and account activity occurs when an operation in the information environment removes its online social media assets, including social media accounts, posts, likes, comments, and other online artifacts. An operation in the information environment may delete its accounts and account activity to complicate attribution or remove online documentation that the operation ever occurred.

Rating:

0. Operation does not delete accounts/account activity.
1. Operation achieves one of four: unfollows, unlikes, and unshares operation content on its information assets, removes attribution indicators (e.g., watermarks, names, etc.) from operation content, refrains from further engagement with operation content (applies to platforms that store data for a certain period before actual deletion), and deletes accounts from the platforms they operated in.
2. Operation achieves two of four: unfollows, unlikes, and unshares operation content on its information assets, removes attribution indicators (e.g., watermarks, names, etc.) from operation content, refrains from further engagement with operation content (applies to platforms that store data for a certain period before actual deletion), and deletes accounts from the platforms they operated in.
3. Operation achieves three of four: unfollows, unlikes, and unshares operation content on its information assets, removes attribution indicators (e.g., watermarks, names, etc.) from operation content, refrains from further engagement with operation content (applies to platforms that store data for a certain period before actual deletion), and deletes accounts from the platforms they operated in.

2.6.8.2 Redirect URLs

Sub-Techniques: 301 Redirect, 302 Redirect, Meta Refresh

An influence operation may redirect its falsified or typosquatted URLs to legitimate websites to increase the operation's appearance of legitimacy, complicate attribution, and avoid detection. The three primary types of URL redirects include:[cxvi]

- A 301 redirect which permanently redirects one URL to another by implementing the redirect in both the webpage and the server. 301 redirects are especially difficult to identify because they are recognized and indexed by search engines.

- A 302 redirect is a temporary redirect that is primarily used when the website owner plans to return to the original URL in the future.
- A Meta Refresh advises the user that they are being redirected to another website by displaying a page notifying that the original URL has been moved and giving the user time to exit out of the page.

Rating:

0. Operation does not redirect URLs.
1. Operation achieves one of three: uses a redirection method that does not require the permission of a third-party website or platform, uses a redirection method recognized and indexed by search engines (e.g., 301 redirect), and removes links to the redirected URL on remaining operation content.
2. Operation achieves two of three: uses a redirection method that does not require the permission of a third-party website or platform, uses a redirection method recognized and indexed by search engines (e.g., 301 redirect), and removes links to the redirected URL on remaining operation content.
3. Operation achieves three of three: uses a redirection method that does not require the permission of a third-party website or platform, uses a redirection method recognized and indexed by search engines (e.g., 301 redirect), and removes links to the redirected URL on remaining operation content.

2.6.8.3 Delete URLs

Sub-Techniques:

URL deletion occurs when an operation completely removes its website registration, rendering the URL inaccessible. An operation in the information environment may delete its accounts and account activity to complicate attribution or remove online documentation that the operation ever occurred.

Rating:

0. Operation does not delete URLs.
1. Operation achieves one of three: follows the correct URL deletion instructions from its website registration, removes links to the deleted URL on remaining operation content, and web archives remove URLs and webpage evidence.
2. Operation achieves two of three: follows the correct URL deletion instructions from its website registration, removes links to the deleted URL on remaining operation content, and web archives remove URLs and webpage evidence.
3. Operation achieves three of three: follows the correct URL deletion instructions from its website registration, removes links to the deleted URL on remaining operation content, and web archives remove URLs and webpage evidence.

2.6.8.4 Remove Association from Content

Sub-Techniques: Distance Reputable Individuals, Remove Post Origins, Remove Physical Infrastructure, Relinquish Control of Hijacked Assets

Removing association from content occurs when an operation in the information environment actively separates itself from its own content. An operation in the information environment may

break association with content by unfollowing, unliking, or unsharing its content, removing attribution from its content, or otherwise taking actions that distance the operation from its messaging. An operation in the information environment may break association with its content to complicate attribution or regain credibility for a new operation.

Distancing reputable individuals from the operation occurs when enlisted individuals, such as celebrities or subject matter experts, actively disengage themselves from operation activities and messaging. Individuals may distance themselves from the operation by deleting old posts or statements, unfollowing operation information assets, or otherwise detaching themselves from the operation's timeline. An operation in the information environment may want reputable individuals to distance themselves from the operation to reduce operation exposure, particularly if the operation aims to remove all evidence.

Removing post origins refers to the elimination of evidence that indicates the initial source of operation content, often to complicate attribution. An operation in the information environment may remove post origins by deleting watermarks, renaming files, or removing embedded links in its content.

Removing physical infrastructure occurs when an operation in the information environment eliminates tangible evidence of the operation, including buildings that served as headquarters or offices, printing equipment, or broadcast infrastructure. An operation in the information environment may remove physical infrastructure to complicate attribution and remove offline indicators that the operation ever occurred.

Relinquishing control of hijacked assets refers to the surrendering of previously acquired information assets including compromised accounts, websites, or personnel. An operation in the information environment may relinquish control of hijacked assets to complicate attribution and avoid responsibility for compromised assets, such as accounts that social media companies have identified as falsified. Operations may release the assets directly to their original owners or release control generally, leaving them available for others to possess.

Rating:

0. Operation does not break association with content.
1. Operation achieves one of three: unfollows, unlikes, and unshares content while distancing influencers from operation content on its information assets, removes post origins, and refrains from further engagement with operation content.
2. Operation achieves two of three: unfollows, unlikes, and unshares content while distancing influencers from operation content on its information assets, removes post origins, and refrains from further engagement with operation content.
3. Operation achieves three of three: unfollows, unlikes, and unshares content while distancing influencers from operation content on its information assets, removes post origins, and refrains from further engagement with operation content.

2.7 Assess Phase

2.7.1 Assess Techniques

2.7.1.1 Use Technique Ratings System

Sub-Techniques:

Operators may use the SP!CE ratings capability to assess how operations prepare, distribute, and maintain consistent messaging. Each technique on the SP!CE knowledge base contains a rating scale that ranges from zero to three. An assigned rating of zero on a specific technique indicates that it wasn't used in the operation. A score of three indicates proper use of the technique to reach a target audience.

Analysts mapping adversary operations and assessing friendly operations may use the ratings system to quantify each operation's degree of preparation across the first three phases of the SP!CE knowledge base. When comparing blue and red operations, a higher cumulative ratings score may indicate an operation's superior preparation and message-tailoring, which may correlate with higher success in the information space. Rating individual blue-team techniques and mapping them to the SP!CE knowledge base supports countermeasures and informs courses of action to counter adversary operations.

2.7.1.2 Review Factors Affecting Operations in the Information Environment

Sub-Techniques:

When an operator reviews factors affecting operations in the information environment, they study the strategic, environmental, and technological barriers to operation success. Reviewing these factors helps operators assess priorities, understand limitations, and mitigate failure before campaign execution.

2.7.1.3 Map Operations in Information Environment to Framework

Sub-Techniques:

Mapping influence operations to SP!CE refers to the identification and attribution of technique usage to an actor. After completing a full analysis of an operation, analysts could study the operation's strategy and compare it to blue operations. Insights drawn from campaign mapping procedures could inform the refinement of existing strategies and open doors to responses or mitigations.

2.7.1.4 Conduct Analysis of Alternatives

Sub-Techniques:

An analysis of alternatives refers to the study of different approaches that may be taken to reach an objective. The Office of Aerospace Studies describes analysis of alternatives as follows:[cxvii]

- “An analytical comparison or evaluation of proposed approaches to meet an objective. An analysis of alternatives can be applied to anything—from a large military acquisition decision to a decision between two products. The formal or informal process involves identifying key decision factors, such as life cycle operations, support, training, and sustainment costs, risk, effectiveness, and assessing each alternative with respect to these factors. An analysis of alternatives is an analytical comparison of the operational effectiveness, cost, and risks of proposed materiel solutions to gaps and shortfalls in operational capability. Such analyses document the rationale for identifying/recommending a preferred solution or solutions to the identified shortfall. Threat changes, deficiencies, obsolescence of existing systems, or advances in technology can trigger an analysis of alternatives.”

2.7.2 Assess Key Performance Indicators (KPIs)

2.7.2.1 Measure Operational Effects

Sub-Techniques: Assess Setting, Assess Frequency, Assess Intensity, Assess Rate, Assess Time

Operational effects should be 'specific, measurable, and observable data' documenting the target audience's behavior. The assessment criteria for an operation should focus on a target audience's behaviors relevant to desired outcomes. Assessment criteria is sometimes updated to reflect developments in the information environment. For example, a certain candidate may drop out of a race against an incumbent, but if a campaign's goal is to not re-elect the incumbent, the assessment criteria could shift to votes for other candidates.

Rating:

0. The operation does not measure operational effects.
1. The operation's assessment criteria fulfills one of three: outlines specific elements for assessment, prepares tools to measure behavior change, updates assessment criteria where necessary.
2. The operation's assessment criteria fulfills two of three: outlines specific elements for assessment, prepares tools to measure behavior change, updates assessment criteria where necessary.
3. The operation's assessment criteria fulfills three of three: outlines specific elements for assessment, prepares tools to measure behavior change, updates assessment criteria where necessary.

3 SP!CE Framework Matrix

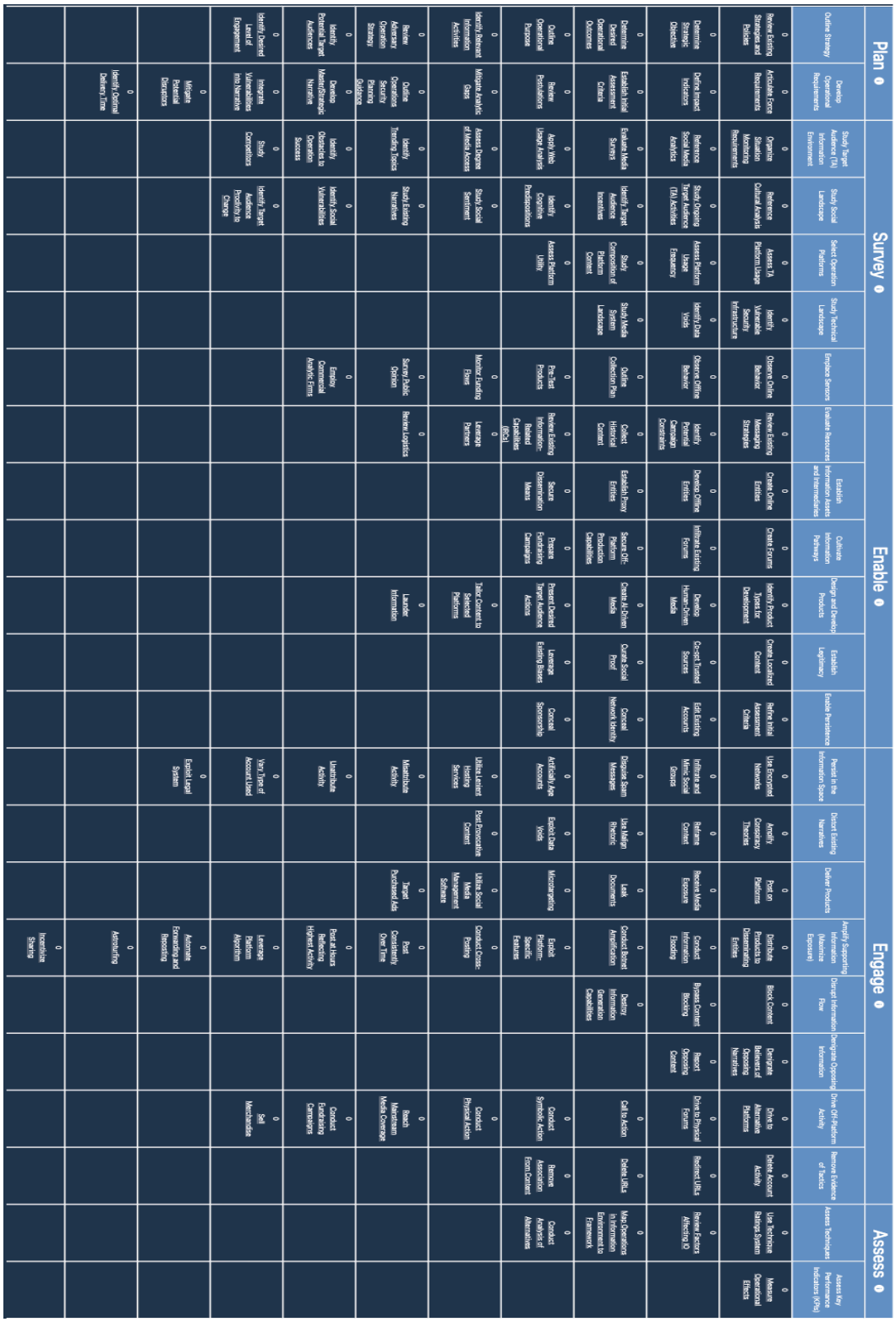

Figure 2: SP!CE 2.2 Framework Matrix

4 SP!CE Knowledge Base

The SP!CE knowledge base, accessible through SP!CE Dash, presents operators with a corpus of historical influence operations conducted by actors spanning states, private firms and individuals. Each case study in the knowledge base is mapped to the SP!CE framework by techniques used and attributed to a specific actor. As the knowledge base accumulates case studies over time, the tool will provide operators with information detailing certain actors' common strategies, tradecraft, and desired outcomes from influence operations. Providing users with access to the strategies employed by their adversaries will help educate the DOD in influence operations, improve information resilience, increase informational power, and provide context for future campaigns.

A successful integrated deterrence strategy requires the DOD to rely on communication between its interagency partners and allies. The knowledge base sets a foundation for information sharing amongst practitioners and will facilitate an improved understanding in the community of how adversaries attempt to influence targeted audiences. Additionally, the capability delivers insights for campaign analysis methodology to help optimize existing assessment and target audience analysis capabilities.

The SP!CE 2.2 specification does not outline the knowledge base detail due to the tool's size. As Figure 3 illustrates, the knowledge base documents the use of 49 techniques across 80 openly sourced case studies. The knowledge base's case studies were manually collected, studied, and tagged but future versions will integrate methods to automate the case study collection and tagging process.

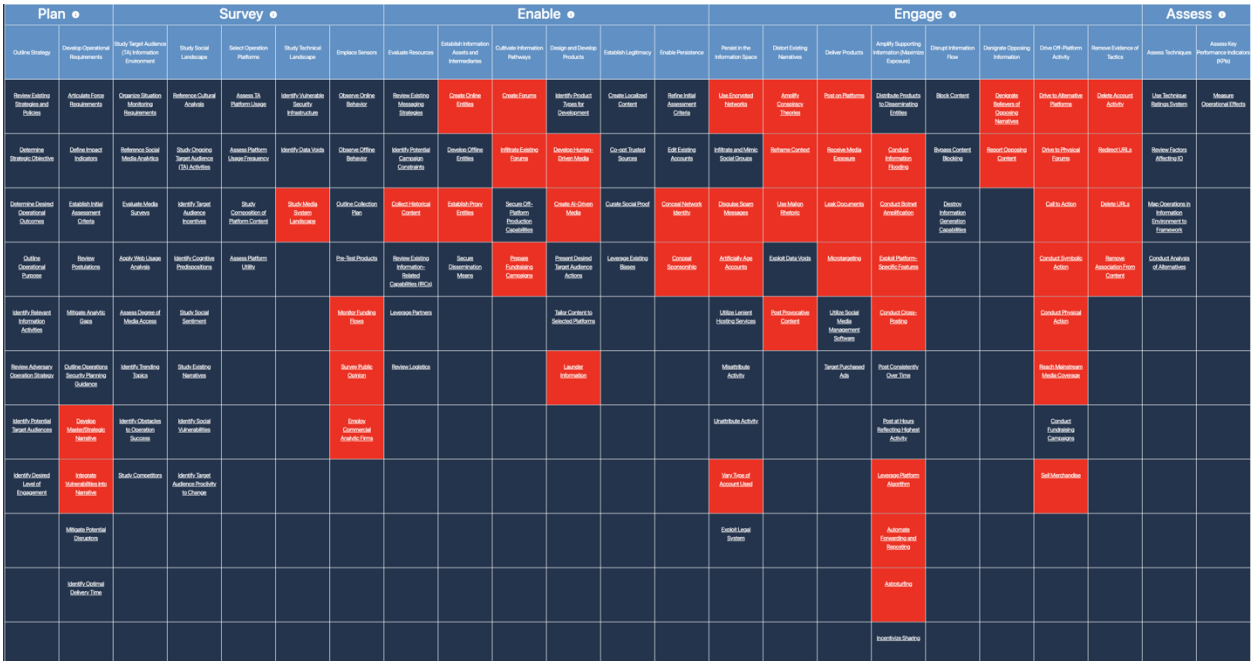

Figure 3: Techniques Tagged to the Knowledge Base on the current SP!CE Framework

Glossary

Term	Definition
AI-Driven Media	Media or content created using automation capabilities with minimal human input.
Astroturfing	The strategy by which established, politically motivated groups impersonate grassroots activist movements for political gain.[cxviii]
Bulletproof Hosting	Services provided by an entity, such as a domain hosting or web hosting firm, that allows its customer considerable leniency in use of the service.[cxix]
Butterfly Attack	When imposters mimic the patterns of behavior of a social group.[cxx]
Content Delivery Network	A network of servers that is geographically dispersed to enable faster web performance by locating copies of web content closer to users or facilitating delivery of dynamic content.[cxxi]
Deep Fake	The use of "deep" or machine learning to hybridize or generate human bodies and faces.[cxxii]
Distributed Denial of Service Attack	When legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor.[cxxiii]
Dox	The act of publishing on the internet private or identifying information about a specific individual, usually with malicious intent.[cxxiv]
Generative Adversarial Network	A model that can create new data instances that resemble training data. The system creates new data in which a generator creates data and a discriminator determines whether that created data is valid or invalid.[cxxv]
Human-Driven Media	Media or content created using minimal automation capabilities.
Hypertext Transfer Protocol	A standard method for communication between clients and Web servers.[cxxvi]
Influence Operation	See *Information Operation*.
Information Environment	The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. (JP 3-13)[cxxvii]
Information Operation	The integrated employment, during military operations, of information-related capabilities in concert with other

Term	Definition
	lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. (JP 3-13)[cxxviii]
Information-related capability	A tool, technique, or activity employed within a dimension of the information environment that can be used to create effects and operationally desirable conditions.
Internet Protocol	The standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks.[cxxix]
Key Performance Indicator	A measure gauging campaign performance.
Keyword Squatting	Creating online content around a specific search-engine-optimized term so as to determine the search results of that term.[cxxx]
Master Narrative	The overarching story that underpins an information operation that major geopolitical goals.
Measure of Effectiveness	A criterion used to assess changes in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect.[cxxxi]
Measure of Performance	A criterion used to assess friendly actions that is tied to measuring task accomplishment.[cxxxii]
Meme	Units of culture that spread through the diffusion of ideas, usually pictures, videos, or gifs on the internet.[cxxxiii]
Operation in the Information Environment	See *Information Operation.*
Phase	A definitive stage of an operation or campaign during which a large portion of the forces and capabilities are involved in similar or mutually supporting activities for a common purpose.[cxxxiv]
Social Media Management Software	Software that allows a single user to simultaneously manage multiple social media accounts.[cxxxv]
Spamoflage	A combination of "spam" and "camouflage" referring to tactics used by spammers where they replace certain letters with numbers to fool email spam filters.[cxxxvi]
Strategic Competition	A persistent and long-term struggle that occurs between two or more adversaries seeking to pursue incompatible interests without necessarily engaging in armed conflict with each other.

Term	Definition
Strategic Narrative	See *Master Narrative*
Structured Process for Information Campaign Enhancement	A capability developed to support U.S. government operators in planning, conducting, and assessing influence operations.
Subtechnique	Standard, detailed steps that prescribe how to perform specific tasks.[cxxxvii]
Tactic	The employment and ordered arrangement of forces in relation to each other.[cxxxviii]
Target Audience	An individual or group selected for influence.
Target Audience Analysis	The process of identifying and studying a campaign's intended audience.
Technique	Non-prescriptive ways or methods used to perform missions, functions, or tasks.[cxxxix]
Trading Up the Chain	The process of getting a story from a small, local, or niche platform or media outlet to a more popular, national news service.[cxl]
Typosquatting	The intentional registration of a domain name that incorporates typographical variants of the target domain name in order to deceive visitors.[cxli]
Viral Sloganeering	Creating short, catchy phrases intended to deliver persuasive, disruptive messaging.[cxlii]
Virtual Private Network	A virtual network built on top of existing networks that can provide a secure communications mechanism for data and IP information transmitted between networks.[cxliii]

Appendix A Abbreviations

Acronym	Term
AI	Artificial Intelligence
AMITT	Adversarial Misinformation and Influence Tactics and Techniques
CDN	Content Delivery Network
DDOS	Distributed Denial of Service
DISARM	Disinformation and Risk Management
DOD	Department of Defense
GAN	Generative Adversarial Network
HTTP	Hypertext Transfer Protocol
IE	Information Environment
IP	Internet Protocol
IRC	Information-Related Capability
IW	Information Warfare
KPI	Key Performance Indicator
MOE	Measures of Effectiveness
MOP	Measures of Performance
OIE	Operation in the Information Environment
PRC	People's Republic of China
SMMS	Social Media Management Software
SP!CE	Structured Process for Information Campaign Enhancement
TA	Target Audience
USG	United States Government
VPN	Virtual Private Network

References

[i] Sixto, D.R. and Kim, P.S (2023). "Structured Process for Influence Campaign Enhancement 2.1", PR 23-1986, The MITRE Corp.

[ii] Venhaus, J.M., Sixto, D.R., Koda, S., Fulk, M., Finlayson, M.A., Lopez Diaz, Z.A. (2021). "Structured Process for Influence Campaign Evaluation", Doc. MP210039, The MITRE Corp.; Sixto, D.R., Kim, Paul S.. (2023) "Structured Process for Information Campaign Enhancement (SP!CE) 2.1", PR_23-1986, The MITRE Corp.

[iii] Ibid.

[iv] Ibid.

[v] Ibid.

[vi] Ibid.

[vii] Ibid.

[viii] Donovan, J. et al (2020). *The Media Manipulation Casebook 1.0*. Harvard Kennedy School Shorenstein Center on Media, Politics, and Public Policy. Retrieved from https://mediamanipulation.org/sites/default/files/media-files/code-book-v1-26Oct20.pdf; Donovan, J. et al. (n.d.). Misinfographics. *Media Manipulation Casebook*. Retrieved May 15, 2023 from https://mediamanipulation.org/definitions/misinfographics; Sixto, D.R. and Kim, P.S (2023). "Structured Process for Influence Campaign Enhancement 2.1", PR 23-1986, The MITRE Corp.

[ix] Sixto, D.R. and Kim, P.S (2023). "Structured Process for Influence Campaign Enhancement 2.1", PR 23-1986, The MITRE Corp.

[x] Joint Chiefs of Staff Washington United States. (2017). *Department of Defense Dictionary of Military and Associated Terms*. United States Department of Defense Staff. https://apps.dtic.mil/sti/pdfs/AD1029823.pdf

[xi] Joint Chiefs of Staff Washington United States. (2017). *Department of Defense Dictionary of Military and Associated Terms*. United States Department of Defense Staff. https://apps.dtic.mil/sti/pdfs/AD1029823.pdf

[xii] Sixto, D.R. and Kim, P.S (2023). "Structured Process for Influence Campaign Enhancement 2.1", PR 23-1986, The MITRE Corp.

[xiii] Sixto, D.R. and Kim, P.S (2023). "Structured Process for Influence Campaign Enhancement 2.1", PR 23-1986, The MITRE Corp.

[xiv] Joint Chiefs of Staff Washington United States. (2017). *Department of Defense Dictionary of Military and Associated Terms*. United States Department of Defense Staff. https://apps.dtic.mil/sti/pdfs/AD1029823.pdf

[xv] Woodbury, R. (2021). The Rise of Synthetic Media & Digital Creators. *Digital Native*. Retrieved from https://digitalnative.substack.com/p/the-rise-of-synthetic-media-and-digital

[xvi] Department of Defense Staff. *Military Information Support Operations*. Retrieved from https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1C1_JP_3-13-2.pdf

[xvii] Department of Defense Staff. *Military Information Support Operations*. Retrieved from https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1C1_JP_3-13-2.pdf

[xviii] Tormala, Z. and Richard E. Petty. (2004). "Resisting Persuasion and Attitude Certainty: A Meta-Cognitive Analysis." In E. S. Knowles and J. Linn, *Resistance and Persuasion* (pp. 65-82). Lawrence Erlbaum Associates. Retrieved from https://perpus.univpancasila.ac.id/repository/EBUPT180158.pdf#page=71

[xix] Department of Defense Staff. (2014). *Military Information Support Operations in the Military Decisionmaking Process*. Retrieved from https://armypubs.army.mil/ProductMaps/PubForm/Details_Printer.aspx?PUB_ID=104206.

[xx] Department of Defense Staff (2014). *Information Operations*. Retrieved from https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf

[xxi] Department of Defense Staff. *Military Information Support Operations*. Retrieved from https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1C1_JP_3-13-2.pdf

[xxii] Myslewski, R. (2014). 'Hashtag' added to the OED – but # isn't a hash, pound, nor number sign. *The Register*. Retrieved from https://www.theregister.com/2014/06/13/hashtag_added_to_the_oed/

[xxiii] Department of Defense Staff. *Military Information Support Operations*. Retrieved from https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1C1_JP_3-13-2.pdf

[xxiv] Toxboe, A. Making the Fogg Behavior Model actionable. *UI* Patterns. Retrieved from https://ui-patterns.com/blog/making-the-fogg-behavior-model-actionable

[xxv] Tahir, U. (2020, January 18). Nudge Theory in Change Management. *CMI*. https://changemanagementinsight.com/nudge-theory-in-change-management/

[xxvi] Bustillo, D. (2019). Taylor's Definition of Culture. *IDOCPUB*. Retrieved from https://idoc.pub/documents/taylors-definition-of-culture-546g02j0p9n8

[xxvii] Tse, David K. et al. (1988). Does Culture Matter? A Cross-Cultural Study of Executives' Choice, Decisiveness, and Risk Adjustment in International Marketing. *Journal of Marketing*, Vol. 52, No. 4, 81-95. Retrieved from https://www.jstor.org/stable/pdf/1251635.pdf.

[xxviii] Ibid.

[xxix] Tse, David K. et al. (1988). Does Culture Matter? A Cross-Cultural Study of Executives' Choice, Decisiveness, and Risk Adjustment in International Marketing. *Journal of Marketing*, Vol. 52, No. 4, 81-95. Retrieved from https://www.jstor.org/stable/pdf/1251635.pdf.

[xxx] Conner, M. et al. (2022). "Testing predictors of attitude strength as determinants of attitude stability and attitude-behaviour relationships: A multi-behaviour study." *European Journal of Social Psychology*, 52, pp. 656-668. DOI: 10.1002/ejsp.2844.

[xxxi] Department of Defense Staff. (2014). *Military Information Support Operations in the Military Decisionmaking Process*. Retrieved from https://armypubs.army.mil/ProductMaps/PubForm/Details_Printer.aspx?PUB_ID=104206.

[xxxii] Maurer, R. (2021, July 5). Resistance to Change | Why it Matters and What to Do About It? Rick Maurer. https://rickmaurer.com/articles/resistance-to-change-why-it-matters/

[xxxiii] Toxboe, A. Making the Fogg Behavior Model actionable. *UI* Patterns. Retrieved from https://ui-patterns.com/blog/making-the-fogg-behavior-model-actionable

[xxxiv] Ellis, G. (2018). So, What Are Cognitive Biases?. In: Ellis, G. (eds) Cognitive Biases in Visualizations. Springer, Cham. https://doi.org/10.1007/978-3-319-95831-6_1

[xxxv] *The COM-B Model for Behavior Change*. (n.d.). The Decision Lab. Retrieved August 29, 2023, from https://thedecisionlab.com/reference-guide/organizational-behavior/the-com-b-model-for-behavior-change

[xxxvi] Miller, Arthur G. et al. (1993). "The attitude polarization phenomenon: Role of response measure, attitude extremity, and behavioral consequences of reported attitude change." *Journal of Personality and Social Psychology*, Vol 64(4), pp. 561-574. Retrieved from https://psycnet.apa.org/buy/1993-25568-001

[xxxvii] Petty, R. E., Tormala, Z. L., & Rucker, D. D. (2004). Resisting persuasion by counterarguing: An attitude strength perspective. In J. T. Jost, M. R. Banaji, & D. A. Prentice (Eds.), Perspectivism in social psychology: The yin and yang of scientific progress (pp. 37–51). American Psychological Association. https://doi.org/10.1037/10750-004

[xxxviii] Toxboe, A. Making the Fogg Behavior Model actionable. UI Patterns. Retrieved from https://ui-patterns.com/blog/making-the-fogg-behavior-model-actionable

[xxxix] Redseal staff. (n.d.). Cyber Hygiene with Redseal. *Redseal*. Retrieved May 17, 2023 from https://www.redseal.net/cyber-hygiene/.

[xl] Golebiewski M. and Danah Boyd. (2019). Data Voids – Where Missing Data Can Easily Be Exploited. *Data & Society*. Retrieved from https://datasociety.net/library/data-voids

[xli] Department of Defense Staff. (2014). *Military Information Support Operations in the Military Decisionmaking Process*. Retrieved from https://armypubs.army.mil/ProductMaps/PubForm/Details_Printer.aspx?PUB_ID=104206.

[xlii] Joint Chiefs of Staff Washington United States. (2006). *Joint Publication 3-13, Information Operations*. United States Department of Defense Staff. Retrieved from https://www.globalsecurity.org/intell/library/policy/dod/joint/jp3_13_2006.pdf

[xliii] Harding, L. (2021). Chinese bots had key role in debunked ballot video shared by Eric Trump. *The* Guardian. Retrieved from https://www.theguardian.com/world/2021/jan/27/chinese-bots-eric-trump-ballot-votes-viral-video

[xliv] Merriam-Webster. (n.d.). Newsletter. In Merriam-Webster.com dictionary. Retrieved May 18, 2023, from https://www.merriam-webster.com/dictionary/newsletter

[xlv] Donovan, J. et al (2020). *The Media Manipulation Casebook 1.0*. Harvard Kennedy School Shorenstein Center on Media, Politics, and Public Policy. Retrieved from https://mediamanipulation.org/sites/default/files/media-files/code-book-v1-26Oct20.pdf

[xlvi] Donovan, J. et al. (n.d.). Evidence Collages. *Media Manipulation Casebook*. Retrieved May 15, 2023 from https://mediamanipulation.org/definitions/evidence-collages

[xlvii] Donovan, J. et al. (n.d.). Misinfographics. *Media Manipulation Casebook*. Retrieved May 15, 2023 from https://mediamanipulation.org/definitions/misinfographics

[xlviii] Woodbury, R. (2021). The Rise of Synthetic Media & Digital Creators. *Digital Native*. Retrieved from https://digitalnative.substack.com/p/the-rise-of-synthetic-media-and-digital

[xlix] Engler, Alex. (2019). Fighting deepfakes when detection fails. *Brookings Institution*. Retrieved from https://www.brookings.edu/research/fighting-deepfakes-when-detection-fails/

[l] Burt, T. and Eric Horvitz. (2020). New Steps to Combat Disinformation. *Microsoft On the Issues*. Retrieved from https://blogs.microsoft.com/on-the-issues/2020/09/01/disinformation-deepfakes-newsguard-video-authenticator/

[li] Donovan, J, et al. (n.d.) Cheap Fake. *Media Manipulation Casebook*. Retrieved May 17, 2023 from https://mediamanipulation.org/definitions/cheap-fake

[lii] Hill, Kashmir and Jeremy White. (2020). Designed to Deceive: Do These People Look Real to You?. *The New York Times*. Retrieved from https://www.nytimes.com/interactive/2020/11/21/science/artificial-intelligence-fake-people-faces.html

[liii] Murphy, H. (2020). The new AI tools spreading fake news in politics and business. *Financial Times*. Retrieved from https://www.ft.com/content/55a39e92-8357-11ea-b872-8db45d5f6714

[liv] Arowolo, S. (2017). Understanding Framing Theory. *Research Gate*. Retrieved from https://www.researchgate.net/publication/317841096_UNDERSTANDING_FRAMING_THEORY

[lv] Bell, S. (2013). *A Dictionary of Forensic Science*. Oxford University Press.

[lvi] Donovan, J. et al. (n.d.). Typosquatting. Media Manipulation Casebook. Retrieved May 15, 2023 from https://mediamanipulation.org/definitions/typosquatting

[lvii] Fortinet Staff. (n.d.). What is Web Scraping? How Do Scrapers Work? Fortinet. Retrieved from https://www.fortinet.com/resources/cyberglossary/web-scraping

[lviii] West, C. (2021). Social proof: How to use psychology in digital marketing. *Sproutsocial*. Retrieved from https://sproutsocial.com/insights/social-proof/

[lix] Pamment, J. et al. (2018). *Countering Information Influence Activities*. Swedish Civil Contingencies Agency. Retrieved from https://www.msb.se/RibData/Filer/pdf/28697.pdf

[lx] Latham, Gary P. and Lise M. Saari. (1979). "Application of social-learning theory to training supervisors through behavorial modeling.", *Journal of Applied Psychology* Vol 64(3), pp. 239-246. Retrieved from https://psycnet.apa.org/buy/1980-28986-001

[lxi] FS Staff. (n.d.). Confirmation Bias And the Power of Disconfirming Evidence. *FS*. Retrieved May 17, 2023 from https://fs.blog/confirmation-bias/.

[lxii] Shirey, R. (2007). Anonymizer. In *Internet Security Glossary* (Version 2). Retrieved from https://datatracker.ietf.org/doc/html/rfc4949

[lxiii] Cisco Staff. (n.d.). What is a VPN? – Virtual Private Network. *Cisco*. Retrieved May 17, 2023 from https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html

[lxiv] Media Temple Staff. (n.d.). Working with a Hacked or Compromised Server. *Media Temple*. Retrieved from https://mediatemple.net/community/products/dv/204644550/working-with-a-hacked-or-compromised-server

[lxv] Shirey, R. (2007). Proxy. In *Internet Security Glossary* (Version 2). Retrieved from https://datatracker.ietf.org/doc/html/rfc4949

[lxvi] Merriam-Webster. (n.d.). Proxy. In Merriam-Webster.com dictionary. Retrieved June 28, 2023, from https://www.merriam-webster.com/dictionary/proxy

[lxvii] Merriam-Webster. (n.d.). Cutout. In Merriam-Webster.com dictionary. Retrieved June 28, 2023, from https://www.merriam-webster.com/dictionary/cutout

[lxviii] Joint Chiefs of Staff Washington United States. (2017). *Department of Defense Dictionary of Military and Associated Terms*. United States Department of Defense Staff. https://apps.dtic.mil/sti/pdfs/AD1029823.pdf

[lxix] Collins Dictionary Staff. (2012). Spamoflage. *Collins Dictionary*. Retrieved from https://www.collinsdictionary.com/us/submission/1005/Spamouflage

[lxx] Joint Chiefs of Staff Washington United States. (2017). *Department of Defense Dictionary of Military and Associated Terms*. United States Department of Defense Staff. https://apps.dtic.mil/sti/pdfs/AD1029823.pdf

[lxxi] Shirey, R. (2007). Hosting. In *Internet Security Glossary* (Version 2). Retrieved from https://datatracker.ietf.org/doc/html/rfc4949

[lxxii] Norton LifeLock Staff. (n.d.). What is Bulletproof Hosting?. *Norton*. Retrieved May 15, 2023 from https://us.norton.com/blog/emerging-threats/what-is-bulletproof-hosting#

[lxxiii] Donovan, J. et al. (n.d.). Viral Sloganeering. *Media Manipulation Casebook*. Retrieved June 28, 2023 from https://mediamanipulation.org/definitions/viral-sloganeering

[lxxiv] Pamment, J. et al. (2018). *Countering Information Influence Activities*. Swedish Civil Contingencies Agency. Retrieved from https://www.msb.se/RibData/Filer/pdf/28697.pdf

[lxxv] Petty, R. E., Tormala, Z. L., & Rucker, D. D. (2004). Resisting persuasion by counterarguing: An attitude strength perspective. In J. T. Jost, M. R. Banaji, & D. A. Prentice (Eds.), Perspectivism in social psychology: The yin and yang of scientific progress (pp. 37–51). American Psychological Association. https://doi.org/10.1037/10750-004

[lxxvi] Golebiewski M. and Danah Boyd. (2019). Data Voids – Where Missing Data Can Easily Be Exploited. *Data & Society*. Retrieved from https://datasociety.net/library/data-voids

[lxxvii] Golebiewski M. and Danah Boyd. (2019). Data Voids – Where Missing Data Can Easily Be Exploited. *Data & Society*. Retrieved from https://datasociety.net/wp-content/uploads/2019/11/Data-Voids-2.0-Final.pdf

[lxxviii] Chen, Y. et al. (2015). Misleading Online Content: Recognizing Clickbait as "False News." *Research Gate*. Retrieved from https://www.researchgate.net/profile/Victoria-Rubin/publication/283721117_Misleading_Online_Content_Recognizing_Clickbait_as_False_News/links/5644c4b108ae54697fb813d1/Misleading-Online-Content-Recognizing-Clickbait-as-False-News.pdf

[lxxix] Hootsuite Staff. (n.d.). Post. *Dictionary of Social Media Terms*. Retrieved from https://blog.hootsuite.com/social-media-definitions/post/

[lxxx] Mukerjee, Madhursee. (2017). "How Fake News Goes Viral – Here's the Math." *Scientific American*. Retrieved from https://www.scientificamerican.com/article/how-fake-news-goes-viral-mdash-heres-the-math/

[lxxxi] Smith, K. (2016). How to Measure Paid, Owned, and Earned Media. *Brandwatch*. Retrieved from https://www.brandwatch.com/blog/define-measure-paid-owned-earned-media/.

[lxxxii] Ibid.

[lxxxiii] Hamilton, Isobel. (2020). Easily overblown, little-understood, and dangerous: Why new need to understand political microtargeting. *Insider*. Retrieved from https://www.businessinsider.com/microtargeting-efficacy-overblown-still-dangerous-2020-10

[lxxxiv] Tappin, B. M., Wittenberg, C., Hewitt, L., berinsky, a., & Rand, D. G. (2022, November 7). Quantifying the Potential Persuasive Returns to Political Microtargeting. https://doi.org/10.31234/osf.io/dhg6k

[lxxxv] Holiday, R. (2014). Trading Up The Chain: Mainstream Media Takes Cues from Blogosphere. *Observer*. Retrieved from https://observer.com/2014/04/mainstream-media-takes-cues-from-blogosphere/

[lxxxvi] Cooke, A. (2013). The Buyers Guide for Social Media Management Software. Trustradius. Retrieved from https://media.trustradius.com/downloads/smmsguide.pdf

[lxxxvii] Pamment, J. et al. (2018). *Countering Information Influence Activities*. Swedish Civil Contingencies Agency. Retrieved from https://www.msb.se/RibData/Filer/pdf/28697.pdf

[lxxxviii] Innes, M. (2021). Fogging and Flooding: Countering Extremist Mis/Disinformation After Terror Attacks. *Global Network on Extremism & Technology*. Retrieved from https://gnet-research.org/2021/11/08/fogging-and-flooding-countering-extremist-mis-disinformation-after-terror-attacks/

[lxxxix] Orman, L. (2015). Fighting Information Pollution with Decision Support Systems. *Taylor & Francis Online*. Retrieved from https://www.tandfonline.com/doi/abs/10.1080/07421222.1984.11517704

[xc] Faggard, D. (2013). Social Swarming. *Air University Military Review*. Retrieved from https://www.airuniversity.af.edu/Portals/10/AFCSLC/resources/faggard.pdf

[xci] Faggard, D. (2013). Social Swarming. *Air University Military Review*. Retrieved from https://www.airuniversity.af.edu/Portals/10/AFCSLC/resources/faggard.pdf

[xcii] King, G. et al. (2017). How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument. *American Political Science Review*. Retrieved from https://gking.harvard.edu/files/gking/files/how_the_chinese_government_fabricates_social_media_posts_for_strategic_distraction_not_engaged_argument.pdf

[xciii] Ibid.

[xciv] Pamment, J. et al. (2018). Countering Information Influence Activities. Swedish Civil Contingencies Agency. Retrieved from https://www.msb.se/RibData/Filer/pdf/28697.pdf

[xcv] Bastos, M. (2017). The Brexit Botnet and User-Generated Hyperpartisan News. *Social Science Computer Review*. Retrieved from https://journals.sagepub.com/doi/pdf/10.1177/0894439317734157

[xcvi] The Graphika Team. (2020). *IRA in Ghana: Double Deceit*. Graphika. Retrieved from https://public-assets.graphika.com/reports/graphika_report_ira_in_ghana_double_deceit.pdf

[xcvii] Donovan, J. et al. (n.d.). Viral Sloganeering. *Media Manipulation Casebook*. Retrieved June 28, 2023 from https://mediamanipulation.org/definitions/viral-sloganeering

[xcviii] Cambridge Dictionary. (n.d.). Cross-posting. In *Cambridge Dictionary*. Retrieved May 17, 2023 from https://dictionary.cambridge.org/us/dictionary/english/cross-posting

[xcix] Donovan, J. et al. (n.d.). Keyword Squatting. *Media Manipulation Casebook*. Retrieved May 15, 2023 from https://mediamanipulation.org/definitions/keyword-squatting

[c] Donovan, J. et al. (n.d.). Astroturfing. *Media Manipulation Casebook*. Retrieved May 15, 2023 from https://mediamanipulation.org/definitions/astroturfing

[ci] Internet Society Staff. (2017). Internet Society Perspectives on internet Content Blocking: An Overview. *Internet Society*. Retrieved from https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/

[cii] Ibid.

[ciii] Internet Society Staff. (2017). Internet Society Perspectives on internet Content Blocking: An Overview. *Internet Society*. Retrieved from https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/

[civ] Ibid.

[cv] Internet Society Staff. (2017). Internet Society Perspectives on internet Content Blocking: An Overview. *Internet Society*. Retrieved from https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/

[cvi] Ibid.

[cvii] Cybersecurity and Infrastructure Security Agency Staff. (2021). Understanding Denial-of-Service Attacks. Cybersecurity and Infrastructure Security Agency. Retrieved from https://www.cisa.gov/news-events/news/understanding-denial-service-attacks

[cviii] Internet Society Staff. (2017). Internet Society Perspectives on internet Content Blocking: An Overview. *Internet Society*. Retrieved from https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/

[cix] Donovan, J. et al. (n.d.). Dox. *Media Manipulation Casebook*. Retrieved May 15, 2023 from https://mediamanipulation.org/definitions/dox

[cx] Merriam-Webster. (n.d.). Cancel Culture. In Merriam-Webster.com dictionary. Retrieved June 28, 2023, from https://www.merriam-webster.com/dictionary/cancel%20culture

[cxi] Merriam-Webster. (n.d.). Called into action. In Merriam-Webster.com dictionary. Retrieved May 18, 2023, from https://www.merriam-webster.com/dictionary/called%20into%20action

[cxii] United Kingdom Government Communication Service. (2021). *RESIST 2 Counter Disinformation Toolkit*. United Kingdom Government Communication Service. Retrieved from https://gcs.civilservice.gov.uk/publications/resist-2-counter-disinformation-toolkit/

[cxiii] Merriam Webster Dictionary. (2023). Potemkin village. In *Merriam Webster*. Retrieved from https://www.merriam-webster.com/dictionary/Potemkin%20village

[cxiv] Merriam Webster Dictionary. (2023). violence. In *Merriam Webster*. Retrieved from https://www.merriam-webster.com/dictionary/violence

[cxv] Alaphillippe, A. (2021). Disinformation is evolving to move under the radar. *Brookings Institute Tech Stream*. Retrieved from https://www.brookings.edu/techstream/disinformation-is-evolving-to-move-under-the-radar/

[cxvi] Hicks, K. (2020). 3 Ways to Redirect a Website URL. *HostGator*. Retrieved from https://www.hostgator.com/blog/ways-redirect-website-url/

[cxvii] Office of Aerospace Studies. (2008). Analysis of Alternatives (AoA) Handbook. Office of Aerospace Studies. Retrieved from https://www.acqnotes.com/Attachments/Analysis%20of%20Alternative%20(AoA)%20Handbook%20July%202008.pdf

[cxviii] Donovan, J. et al. (n.d.). Astroturfing. *Media Manipulation Casebook*. Retrieved May 15, 2023 from https://mediamanipulation.org/definitions/astroturfing

[cxix] Norton LifeLock Staff. (n.d.). What is Bulletproof Hosting?. *Norton*. Retrieved May 15, 2023 from https://us.norton.com/blog/emerging-threats/what-is-bulletproof-hosting#

[cxx] Donovan, J. et al. (n.d.). Butterfly Attack. *Media Manipulation Casebook*. Retrieved May 15, 2023 from https://mediamanipulation.org/definitions/butterfly-attack

[cxxi] International Business Machines (IBM). (n.d.). "What is a content delivery network (CDN)?" *International Business Machines (IBM) Topics*. Retrieved May 15, 2023 from https://www.ibm.com/topics/content-delivery-networks

[cxxii] Donovan, J. et al. (n.d.). Deep Fake. *Media Manipulation Casebook*. Retrieved May 15, 2023 from https://mediamanipulation.org/definitions/deep-fake

[cxxiii] Cybersecurity and Infrastructure Security Agency Staff. (2021). Understanding Denial-of-Service Attacks. Cybersecurity and Infrastructure Security Agency. Retrieved from https://www.cisa.gov/news-events/news/understanding-denial-service-attacks

[cxxiv] Donovan, J. et al. (n.d.). Dox. *Media Manipulation Casebook*. Retrieved May 15, 2023 from https://mediamanipulation.org/definitions/dox

[cxxv] Google Staff. (n.d.). Generative Adversarial Network. *Machine Learning Glossary*. Google. Retrieved May 15, 2023 from https://developers.google.com/machine-learning/glossary#generative_adversarial_network

[cxxvi] National Institute of Standards and Technology. (n.d.). HTTP. *National institute of Standards and Technology Computer Security Resource Center*. Retrieved May 15, 2023 from https://csrc.nist.gov/glossary/term/http

[cxxvii] Joint Chiefs of Staff Washington United States. (2017). *Department of Defense Dictionary of Military and Associated Terms*. United States Department of Defense Staff. https://apps.dtic.mil/sti/pdfs/AD1029823.pdf

[cxxviii] Joint Chiefs of Staff Washington United States. (2017). *Department of Defense Dictionary of Military and Associated Terms*. United States Department of Defense Staff. https://apps.dtic.mil/sti/pdfs/AD1029823.pdf

[cxxix] National Institute of Standards and Technology. Internet Protocol. *National institute of Standards and Technology Computer Security Resource Center*. Retrieved May 15, 2023 from https://csrc.nist.gov/glossary/term/internet_protocol

[cxxx] Donovan, J. et al. (n.d.). Keyword Squatting. *Media Manipulation Casebook*. Retrieved May 15, 2023 from https://mediamanipulation.org/definitions/keyword-squatting

[cxxxi] Joint Chiefs of Staff Washington United States. (2017). *Department of Defense Dictionary of Military and Associated Terms*. United States Department of Defense Staff. https://apps.dtic.mil/sti/pdfs/AD1029823.pdf

[cxxxii] Joint Chiefs of Staff Washington United States. (2017). *Department of Defense Dictionary of Military and Associated Terms*. United States Department of Defense Staff. https://apps.dtic.mil/sti/pdfs/AD1029823.pdf

[cxxxiii] Donovan, J. et al (2020). *The Media Manipulation Casebook 1.0*. Harvard Kennedy School Shorenstein Center on Media, Politics, and Public Policy. Retrieved from https://mediamanipulation.org/sites/default/files/media-files/code-book-v1-26Oct20.pdf

[cxxxiv] Joint Chiefs of Staff Washington United States. (2017). *Department of Defense Dictionary of Military and Associated Terms*. United States Department of Defense Staff. https://apps.dtic.mil/sti/pdfs/AD1029823.pdf

[cxxxv] Cooke, A. (2013). The Buyers Guide for Social Media Management Software. *Trustradius*. Retrieved from https://media.trustradius.com/downloads/smmsguide.pdf

[cxxxvi] Collins Dictionary Staff. (2012). Spamoflage. *Collins Dictionary*. Retrieved from https://www.collinsdictionary.com/us/submission/1005/Spamouflage

[cxxxvii] Joint Chiefs of Staff Washington United States. (2017). *Department of Defense Dictionary of Military and Associated Terms*. United States Department of Defense Staff. https://apps.dtic.mil/sti/pdfs/AD1029823.pdf

[cxxxviii] Joint Chiefs of Staff Washington United States. (2017). *Department of Defense Dictionary of Military and Associated Terms*. United States Department of Defense Staff. https://apps.dtic.mil/sti/pdfs/AD1029823.pdf

[cxxxix] Joint Chiefs of Staff Washington United States. (2017). *Department of Defense Dictionary of Military and Associated Terms*. United States Department of Defense Staff. https://apps.dtic.mil/sti/pdfs/AD1029823.pdf

[cxl] Donovan, J. et al. (n.d.). Trading up the Chain. *Media Manipulation Casebook*. Retrieved May 15, 2023 from https://mediamanipulation.org/definitions/trading-chain

[cxli] Donovan, J. et al. (n.d.). Typosquatting. *Media Manipulation Casebook*. Retrieved May 15, 2023 from https://mediamanipulation.org/definitions/typosquatting

[cxlii] Donovan, J. et al. (n.d.). Viral Sloganeering. *Media Manipulation Casebook*. Retrieved May 15, 2023 from https://mediamanipulation.org/definitions/viral-sloganeering

[cxliii] National Institute of Standards and Technology. (n.d.). Virtual Private Network. *National institute of*