REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
08/14/2023	Technical Report	

4. TITLE AND SUBTITLE
Structured Process for Information Campaign Enhancement (SP!CE) 2.1: An Analytic Framework, Knowledge Base, and Scoring Rubric for Operations in the Information Environment

5a. CONTRACT NUMBER
FA8702-23-C-0001

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Daniel R. Sixto; 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
SP!CE supports visualization, planning, assessment, and execution for conducting allied information operations and countering adversary campaigns. SP!CE comprises (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 ba

15. SUBJECT TERMS
Information Architectures; Communication; DISARM framework; adversary behavior; influence operation; framework; Adversarial Misinformation and Influence Tactics and Techniques (AMITT) framework; Structured Process for Information Campaign Enhancement (SP!CE); MITRE-FIU partnership

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE		92	Susan Carpenito
					19b. TELEPHONE NUMBER *(Include area code)* 781-271-7646

MITRE

MITRE PAPER

Structured Process for Information Campaign Enhancement (SP!CE) 2.1

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

Daniel R. Sixto
Paul S. Kim

May 2023

Approved for Public Release: Distribution Unlimited. Public Release Case Number 23-1986

McLean, VA

Approved By

Joe Ferraro	June 29, 2023
Cyber Division Chief Engineer, N140	Date
Michael Minter	June 29, 2023
Outcome Lead Cyber Command and Control & Effects, N142	Date

Abstract

The Structured Process for Information Campaign Enhancement (SP!CE) is a capability that supports strategic competition in the information environment for the U.S. Department of Defense, its partners, and allies. SP!CE supports visualization, planning, assessment, and execution for conducting allied information operations and countering adversary campaigns. SP!CE comprises (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) 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. 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. 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). 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. 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.

Acknowledgments

SP!CE owes much of its work to MITRE ATT&CK's foundational research. 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.[1]

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.

[1] 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 Plan Phase A-2
2.2.1 Determine Strategic End-State Tactic A-2
2.2.1.1 Review Existing Strategies and Policies A-2
2.2.1.2 Determine Strategic Objective A-3
2.2.1.3 Determine Operational Objectives A-3
2.2.1.4 Review Adversary Operation Strategy A-4
2.2.2 Study Target Audience (TA) Information Environment Tactic A-4
2.2.2.1 Reference Social Media Analytics A-4
2.2.2.2 Evaluate Media Surveys A-5
2.2.2.3 Apply Web Usage Analysis A-5
2.2.2.4 Assess Degree of Media Access A-5
2.2.2.5 Identify Trending Topics A-6
2.2.3 Study Social Landscape Tactic A-6
2.2.3.1 Reference Cultural Analysis A-6
2.2.3.2 Study Ongoing Target Audience (TA) Activities A-7
2.2.3.3 Identify Cognitive Biases A-8
2.2.3.4 Identify TA Adversaries A-9
2.2.3.5 Study Existing Narratives A-9
2.2.4 Select Operation Platforms Tactic A-10
2.2.4.1 Assess TA Platform Usage A-10
2.2.4.2 Assess Platform Usage Frequency A-10
2.2.4.3 Study Composition of Platform Content A-11
2.2.4.4 Assess Platform Utility A-11
2.2.5 Study Technical Landscape Tactic A-12
2.2.5.1 Identify Vulnerable Security Infrastructure A-12
2.2.5.2 Identify Data Voids A-12
2.2.5.3 Study Media System Landscape A-13
2.2.6 Develop Operational Approach Tactic A-13
2.2.6.1 Develop Master/Strategic Narrative A-13
2.2.6.2 Integrate Vulnerabilities into Narrative A-13

2.2.6.3 Review Postulations A-14
2.2.6.4 Mitigate Analytic Gaps A-14
2.3 Enable Phase A-15
2.3.1 Evaluate Resources Tactic A-15
2.3.1.1 Review Existing Messaging Strategies A-15
2.3.1.2 Identify Potential Campaign Constraints A-15
2.3.1.3 Collect Historical Content A-16
2.3.1.4 Review Existing Information-Related Capabilities (IRCs) A-16
2.3.2 Establish Information Assets and Intermediaries Tactic A-17
2.3.2.1 Create Online Entities A-17
2.3.2.2 Develop Offline Entities A-18
2.3.2.3 Establish Proxy Entities A-19
2.3.3 Emplace Sensors Tactic A-19
2.3.3.1 Observe Offline Behavior A-20
2.3.3.2 Observe Online Behavior A-20
2.3.3.3 Monitor Funding Flows A-21
2.3.3.4 Survey Public Opinion A-21
2.3.3.5 Employ Commercial Analytic Firms A-22
2.3.4 Cultivate Information Pathways Tactic A-22
2.3.4.1 Create Forums A-22
2.3.4.2 Infiltrate Existing Forums A-23
2.3.4.3 Establish Broadcast Services A-23
2.3.4.4 Prepare Fundraising Campaigns A-24
2.3.5 Develop Content Tactic A-24
2.3.5.1 Develop Human-Driven Media A-24
2.3.5.2 Create AI-Driven Media A-25
2.3.5.3 Tailor Content to Selected Platforms A-26
2.3.5.4 Launder Information A-26
2.3.6 Establish Legitimacy Tactic A-27
2.3.6.1 Co-Opt Trusted Sources A-27
2.3.6.2 Create Localized Content A-28
2.3.6.3 Curate Social Proof A-28
2.3.6.4 Leverage Existing Biases A-29
2.3.7 Enable Persistence Tactic A-29
2.3.7.1 Edit Existing Accounts A-29

2.3.7.2 Conceal Network Identity A-30
2.3.7.3 Conceal Sponsorship A-31
2.4 Engage Phase A-32
2.4.1 Persist in the Information Space Tactic A-32
2.4.1.1 Use Encrypted Networks A-32
2.4.1.2 Utilize Butterfly Attack A-32
2.4.1.3 Utilize Spamoflage A-33
2.4.1.4 Artificially Age Accounts A-33
2.4.1.5 Utilize Bulletproof Hosting A-34
2.4.1.6 Misattribute Activity A-34
2.4.1.7 Unattribute Activity A-35
2.4.1.8 Vary Type of Account Used A-35
2.4.1.9 Exploit Legal System A-35
2.4.2 Distort Existing Narratives Tactic A-36
2.4.2.1 Amplify Conspiracy Theories A-36
2.4.2.2 Reframe Context A-36
2.4.2.3 Use Malign Rhetoric A-37
2.4.2.4 Exploit Data Voids A-38
2.4.2.5 Post Provocative Content A-38
2.4.3 Deliver Content Tactic A-39
2.4.3.1 Receive Media Exposure A-39
2.4.3.2 Post on Platforms A-40
2.4.3.3 Leak Documents A-40
2.4.3.4 Microtargeting A-41
2.4.3.5 Utilize Social Media Management Software A-42
2.4.3.6 Target Purchased Ads A-42
2.4.4 Amplify Supporting Information (Maximize Exposure) Tactic A-43
2.4.4.1 Conduct Information Flooding A-43
2.4.4.2 Conduct Botnet Amplification A-44
2.4.4.3 Exploit Platform-Specific Features A-45
2.4.4.4 Conduct Cross-Posting A-45
2.4.4.5 Consistently Post Over Time A-46
2.4.4.6 Post at Hours Reflecting Highest Activity A-46
2.4.4.7 Leverage Platform Algorithm A-47
2.4.4.8 Automated Forwarding and Reposting A-47

2.4.4.9 Astroturfing A-48
2.4.4.10 Incentivize Sharing A-49
2.4.5 Disrupt Information Flow Tactic A-49
2.4.5.1 Block Content A-49
2.4.5.2 Bypass Content Blocking A-50
2.4.5.3 Destroy Information Generation Capabilities A-51
2.4.6 Denigrate Opposing Information Tactic A-51
2.4.6.1 Denigrate Believers of Opposing Narratives A-51
2.4.6.2 Report Opposing Content A-52
2.4.7 Drive Off-Platform Activity Tactic A-53
2.4.7.1 Drive to Alternative Platforms A-53
2.4.7.2 Drive to Physical Forums A-54
2.4.7.3 Call to Action A-54
2.4.7.4 Conduct Symbolic Action A-55
2.4.7.5 Conduct Physical Action A-55
2.4.7.6 Reach Mainstream Media Coverage A-56
2.4.7.7 Conduct Fundraising Campaigns A-56
2.4.7.8 Sell Merchandise A-57
2.4.8 Remove Evidence of Tactics Tactic A-58
2.4.8.1 Delete Account Activity A-58
2.4.8.2 Redirect URLs A-58
2.4.8.3 Delete URLs A-59
2.4.8.4 Remove Association from Content A-59
2.5 Assess Phase A-60
2.5.1 Assess Techniques Tactic A-61
2.5.1.1 Use Technique Ratings System A-61
2.5.1.2 Review Factors Affecting IO A-61
2.5.1.3 Map Operations in Information Environment to Framework A-61
2.5.1.4 Conduct Analysis of Alternatives A-61
2.5.2 Assess Key Performance Indicators (KPIs) Tactic A-62
2.5.2.1 Measure Reach A-62
2.5.2.2 Measure Resonance A-62
2.5.2.3 Measure Support A-62
2.5.2.4 Measure Sentiment A-62
3 SP!CE Framework Matrix A-63

4 SP!CE Knowledge Base A-64
Glossary A-1
Appendix A Abbreviations A-1

List of Figures

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

Figure 2: SP!CE Framework Matrix A-63

Figure 3: Techniques Tagged to the Knowledge Base on the current SP!CE Framework A-64

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 influence operations. SP!CE consists of three tools: the framework, the ratings scale, and the knowledge base. SP!CE is accompanied by an interactive dashboard known as SP!CE Dash, a tool developed to enable collaboration among USG operators in relation to activities covered by SP!CE.

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 2.1 framework builds on the SP!CE 1.0 framework to incorporate a more comprehensive collection of tactics and techniques relevant to influence operations.[i] SP!CE tactics and techniques support operators when working on setting objectives, developing targets, and executing operations.

The updated SP!CE ratings system now incorporates techniques when assessing Measures of Performance (MOPs). Unlike version 1.0, each technique now 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.

The SP!CE framework, its ratings, and the knowledge base all intend to optimize influence operations supporting integrated deterrence and managing strategic competition. 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. 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. 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.[ii]

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.

SP!CE phases sit at the top of the framework structure and outline the four stages of an operation: plan, 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.[iii] For example, the plan phase includes tactics such as "Determine Strategic End-State", "Study Target Audience (TA) Information Environment", 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.[iv] 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 larger campaign.

SP!CE techniques lie under tactics and outline "how" an actor could achieve a goal outlined by a tactic. Techniques refer to non-prescriptive ways or methods used to perform missions, functions, or tasks.[v] 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.[vi]

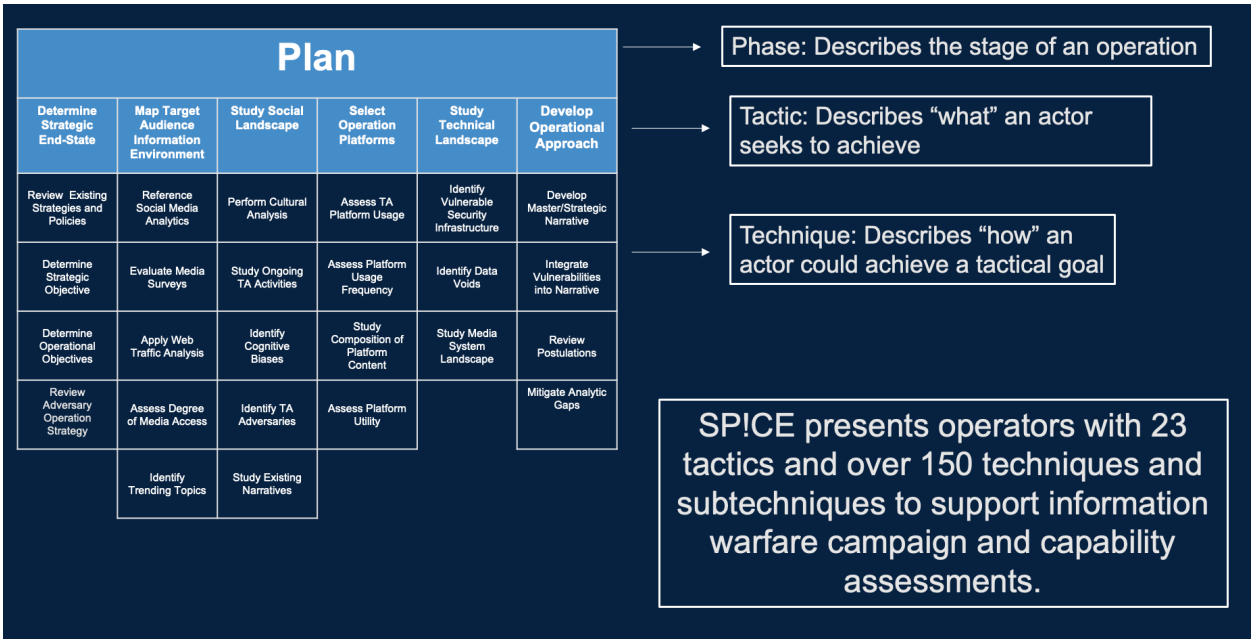

Figure 1: Illustration of the SP!CE Framework Structure, showing the Plan phase with its underlying tactics and techniques.

2.2 Plan Phase

The plan phase describes the stage of an operation where an actor outlines their strategic goals, performs target audience analysis, maps the information environment, and develops a general approach for operation conduct. Operators will set goals, conduct initial research, and develop strategy during the plan phase.

2.2.1 Determine Strategic End-State Tactic

Determining a strategic end-state identifies the intended result or impact of an influence operation. Identifying this end-state requires actors to review existing policies, identify potential outcomes, and comply with national strategies.

2.2.1.1 Review Existing Strategies and Policies

Sub-Techniques: Coordinate Multinational Information Operations, Review Rules of Engagement and Special Instructions, Comply to National Level Strategies[vii]

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

An influence operation should simultaneously adhere to national level policies to remain consistent with previously set goals. Successful operations should effectively identify avenues for efficient policy implementation.

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.

2.2.1.2 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

Department of Defense (DOD) doctrine defines strategy as a "prudent idea or set of ideas for employing the instruments of national power in a synchronized and integrated fashion to achieve theater, national, and/or multinational objectives."[viii] Decision-makers should develop clearly defined strategic objectives that fall under their respective agency missions and powers.

When determining a strategic objective, one outlines the overarching goals for 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).

2.2.1.3 Determine Operational Objectives

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 strategic success. Operational objectives often include actions taken to meet a strategic goal.

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.

2.2.1.4 Review Adversary Operation Strategy

Sub-Technique:

An influence operation may consult previously documented adversary operations to best understand commonly used tactics, techniques, and procedures. Understanding adversary strategies can help operators develop counters and minimize their adversary's potential influence. An actor should consult with interagency and international partners for additional perspectives and intelligence on an adversary's strategies.

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 tactics, reviews adversary material capabilities.
2. Operation fulfills two of three: reviews adversary strategic doctrine, identifies an adversary's previously documented tactics, reviews adversary material capabilities.
3. Operation fulfills three of three: reviews adversary strategic doctrine, identifies an adversary's previously documented tactics, reviews adversary material capabilities.

2.2.2 Study Target Audience (TA) Information Environment Tactic

Actors study their target audience's information environment to best understand which tools, strategies, and procedures may effectively achieve campaign goals. When studying the target audience's information environment, actors may review social media analytics, study web traffic activity, and identify trending topics.[ix]

2.2.2.1 Reference Social Media Analytics

Sub-Techniques:

An influence operation 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.[x] The operation may use a social media platform or utilize a third-party tool to collect relevant 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.

2.2.2.2 Evaluate Media Surveys

Sub-Techniques:

An influence operation 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 ask clear questions that garner the target audience's interest.

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.

2.2.2.3 Apply Web Usage Analysis

Sub-Techniques:

An influence operation 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.[xi]

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.

2.2.2.4 Assess Degree of Media Access

Sub-Techniques:

An influence operation 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 challenges targeting an information environment with heavy restrictions on the press than an environment with independent media, freedom of speech, 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.

2.2.2.5 Identify Trending Topics

Sub-Techniques: Identify Trending Hashtags, Monitor Media Developments

An influence operation may study trending topics on social and print 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 general trends and social tendencies of a population. For example, understanding what types of developments will evoke stronger responses from a target audience could provide operators with valuable information for narrative development.

- A hashtag refers to a word or phrase preceded by the hash symbol (#) on social media used to filter messages and posts relating to a specific topic.[xii] All public posts that use the same hashtag are commonly 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.

2.2.3 Study Social Landscape Tactic

Understanding an audience's social landscape helps actors relate content to their intended viewership. By performing cultural analysis, studying ongoing activities, and understanding existing trends, narratives, and social intricacies, an actor may optimize the reach of an operation.

2.2.3.1 Reference Cultural Analysis

Sub-Techniques: Study Law, Study Customs, Study Religions, Study Demographics, Study Arts, Study Languages, Study Local Geography

An influence operation 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.[xiii]

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.

2.2.3.2 Study Ongoing Target Audience (TA) 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

An influence operation 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.

- A wedge issue is a divisive political issue, usually concerning a social phenomenon, that divides individuals along a defined line.[xiv] An influence operation may exploit wedge issues by intentionally polarizing the public along the wedge issue line and encouraging opposition between factions.[xv]
- Preexisting prejudices refer to preconceived racial, religious, demographic, or social biases to further polarize a TA from the rest of the public.[xvi]
- An influence operation may use the chaos and confusion surrounding an active crisis to promote operation content. Active crises include violent events, natural disasters, public health phenomena, and other situations that incite panic.
- Information operations may identify psychological weaknesses, or targetable cognitive biases, using information.[xvii] A report prepared for the Strategic Multilayer Assessment Integrating Information in Joint Operations identifies several common psychological weaknesses that an influence operation may target in its operational narratives and strategy, including mere exposure effect and authority bias.[xviii]
- Social group trauma refers to the negative psychological effects endured by an entire population as a result of a single event.[xix]
- Media system weaknesses may include existing biases among media agencies, vulnerability to false news agencies on social media, or existing distrust of traditional media sources. An existing distrust among the public in the media system's credibility holds high potential for exploitation by an influence operation when establishing alternative news agencies to spread operation content.
- Sentiment analysis refers to an examination of how a TA feels about a topic.[xx] In the planning stage, sentiment analysis provides a baseline from which an influence operation can measure changes in audience perception. Sentiment analysis can use basic "vanity metrics" such as likes or more advanced aspect-aware sentiment analysis tools.

- An influence operation may review the target audience's local news to better tailor operation narratives to local activities and mimic the local language and writing style. Local news is often trusted more by a target audience due to its ties to the local community.[xxi]
- Signals intelligence, or SIGINT, refers to data collected from communication between two entities, including timestamps, locations, file sizes, and other information that gives the collecting party insight into the conversations.[xxii] An influence operation may use SIGINT to tailor operation content to the TA's time zone or to map network connections between TA individuals and organizations.
- Political cycle topics refer to issues that the TA regularly debates during an election season.[xxiii] For example, immigration, healthcare, and gun policy are often political cycle topics in the United States.[xxiv]
- Potential volume bursts and social events refer to holidays, political meetings, or festivals that hold potential for social or political mobilization, potentially creating an uptick, or volume burst, in online activity.[xxv]

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.

2.2.3.3 Identify Cognitive Biases

Sub-Techniques:

According to *Simply Psychology*, a cognitive bias is a subconscious error in thinking that leads individuals to misinterpret information from their surrounding environment.[xxvi] Identifying cognitive biases 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.

Rating:

0. Operation does not identify cognitive biases.

1. The operation conducts or identifies one of three: identify cognitive biases that are observed among the target audience, cognitive biases that are construable from ongoing target audience developments, identify biases and integrate them into an operation's context or narrative.
2. The operation conducts or identifies two of three: identify cognitive biases that are observed among the target audience, cognitive biases that are construable from ongoing target audience developments, identify biases and integrate them into an operation's context or narrative.
3. The operation conducts or identifies three of three: identify cognitive biases that are observed among the target audience, cognitive biases that are construable from ongoing target audience developments, identify biases and integrate them into an operation's context or narrative.

2.2.3.4 Identify TA Adversaries

Sub-Techniques:

An operation could identify individuals, groups, or ideas that rankle a target audience. Criticizing adversaries in operation narratives could inflame emotions among a population and damage the adversary's credibility.

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.

2.2.3.5 Study Existing Narratives

Sub-Techniques:

An operation may survey the information space to study existing narratives with the goal of integrating existing trends, developments, and topics relevant 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 fortify the campaign's master narratives.

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.

2.2.4 Select Operation Platforms Tactic

Platforms serve as a conduit to the information space. Successful operations identify popular platforms among the target audience and tailor their messaging to that platform's requirements and features.

2.2.4.1 Assess TA Platform Usage

Sub-Techniques: Analyze External Viewership, Assess Nielsen 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.

- An external viewership analysis employs tools to collect data on TAs and understand the type of content they're most receptive to.[xxvii] These tools often conduct cross-channel viewership analysis, study behavioral data, and monitor other consumer indicators.[xxviii]
- Nielsen ratings represent the primary source of television ratings to track program viewership.[xxix]
- Operators may survey existing social media communities to better gauge TA stances on certain topics and to understand the online community's culture.

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.

2.2.4.2 Assess Platform Usage Frequency

Sub-Techniques:

Studying platform usage frequency surveys emerging technologies and trends in the information space. Understanding which platforms are growing and declining in popularity provides vital intelligence for operators to effectively deliver 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.

2.2.4.3 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.

2.2.4.4 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.

2.2.5 Study Technical Landscape Tactic

Technical landscape analysis studies security infrastructure, identifies data voids, and finds other exploitable vulnerabilities in the cyber-realm. The technical landscape constitutes a wide range of networks from simple news websites to complex social media platforms.

2.2.5.1 Identify Vulnerable Security Infrastructure

Sub-Techniques:

An influence operation may identify weak security infrastructure to later bypass security controls and compromise accounts, use malware, or take other actions to achieve 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.[xxx]

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.

2.2.5.2 Identify Data Voids

Sub-Techniques:

Data voids refer to a lack of coverage regarding a breaking news event or general topic.[xxxi] The lack of coverage on a topic presents opportunities for operators to amplify content discussing the subject and frame the issue for the TA. Data voids are hard to detect and relatively harmless until exploited by an entity aiming to quickly proliferate false or misleading information on relatively undiscussed topics. In the plan phase, an influence operation may identify data voids for later exploitation in the operation. Data voids could be exploited using search engine optimization techniques.

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.

2.2.5.3 Study Media System Landscape

Sub-Techniques:

Studying the media system's landscape refers to completing a holistic analysis of the 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.

2.2.6 Develop Operational Approach Tactic

After studying the target audience's social and technical landscapes, actors should use their findings to craft narratives. Narratives lay the foundation of any successful campaign, bringing a single coordinated message to the target audience to serve the actor's purpose. Successful narratives should be broad, adaptable to changing circumstances and postulations, and relevant to its intended audience.

2.2.6.1 Develop Master/Strategic Narrative

Sub-Techniques: Develop Competing Narratives

An influence operation will 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.

2.2.6.2 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.

2.2.6.3 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. As operators develop strategic narratives, they should carefully review their research into the TA's social and technical landscapes and identify analytic gaps. Operators should verify key assumptions in efforts to enhance the credibility of their narratives and diminish risks associated with a faulty narrative.

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.

2.2.6.4 Mitigate Analytic Gaps

Sub-Techniques:

Analytic gaps refer to unknown information that prevents a full understanding of a subject. Operators 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 Enable Phase

The enable phase involves the development of resources and assets for operation use. Once an actor sets their operation's goals, the enable phase outlines steps to establish information assets, find information pathways, develop content, and identify methods to persist in the information space.

2.3.1 Evaluate Resources Tactic

Assessing what tools are available to planners is essential to an operation's ability to avoid miscoordination and maintain consistency.

2.3.1.1 Review Existing Messaging Strategies

Sub-Techniques:

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 optimize the capacity for influence while saving time. A review of previous messaging strategies may survey narratives, target audience analysis methods, amplification methods, platforms used, and other features. Operators could also review previous adversary messaging strategies to devise countermeasures.

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.

2.3.1.2 Identify Potential Campaign Constraints

Sub-Techniques:

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.).

2.3.1.3 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.

- A cache is a "special storage space for temporary files that makes a device, browser, or app run faster and more efficiently."[xxxii] Internet caches and archives contain information that may have been removed from a website.

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).

2.3.1.4 Review Existing Information-Related Capabilities (IRCs)

Sub-Techniques:

According to Joint Publication 3-13, an Information-Related Capability (IRC) is a "tool, technique, or activity employed within a dimension of the information environment that can be used to achieve a specific end."[xxxiii] Some IRCs and their elements may include electronic warfare, computer network operations, psychological operations, military deception, 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.

2.3.2 Establish Information Assets and Intermediaries Tactic

When an operation establishes information assets, they create the fundamental infrastructure on which their campaign relies on. Assets include online entities such as bots, user-accounts, or troll accounts and offline entities such as radio, billboards, or television stations.

2.3.2.1 Create Online Entities

Sub-Techniques: Create Anonymous Accounts, Create Sockpuppet 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 can influence a target audience. Online entities often influence their target audiences through social media platforms by exploiting platform-specific features to effectively reach them. For example, bots are commonly used on Twitter and have been used to amplify disinformation.[xxxiv]

- Anonymous accounts or anonymous users refer to users that access network resources without providing a username or password.[xxxv] An influence operation may use anonymous accounts to spread content without direct attribution to the operation.
- Sockpuppet accounts refer to falsified accounts that either promote the influence operation's own material or deceive a TA.[xxxvi] Individuals who control sockpuppet accounts also man at least one other user account. Sockpuppet accounts help legitimize operation narratives by providing an appearance of external support for the material and discrediting opponents of the operation.
- Cyborg accounts refer to partly manned, partly automated social media accounts.[xxxvii] Cyborg accounts primarily act as bots, but a human operator periodically takes control of the account to engage with real social media users by responding to comments and posting original content. Influence operations may use cyborg accounts to reduce the amount of direct human input required to maintain a regular account but increase the apparent legitimacy of the cyborg account by occasionally breaking its bot-like behavior with human interaction.
- Classic trolls refer to regular people who troll for personal reasons, such as attention-seeking or boredom. Classic trolls may advance operation narratives by coincidence but are not directly affiliated with any larger operation.[xxxviii] Conversely, hybrid trolls act on behalf of another institution, such as a state or financial organization, and post content with a specific ideological goal.[xxxix] Hybrid trolls may be highly advanced and institutionalized or less organized and work for a single individual.

- Bots refer to autonomous internet users that interact with systems or other users while imitating traditional human behavior.[xl] Bots use a variety of tools to stay active without direct human operation, including artificial intelligence and big data analytics. For example, an individual may program a Twitter bot to retweet a tweet every time it contains a certain keyword or hashtag. An influence operation may use bots to increase its exposure and artificially promote its content across the internet without dedicating additional time or human resources.
- Amplifier bots promote operation content through reposts, shares, and likes to increase the content's online popularity.[xli] Hacker bots are traditionally covert bots running on computer scripts that rarely engage with users and work primarily as agents of larger cyberattacks, such as a Distributed Denial of Service attacks.[xlii] Spammer bots are programmed to post content on social media or in comment sections, usually as a supplementary tool.[xliii] Impersonator bots pose as real people by mimicking human behavior, complicating their detection.[xliv]

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.

2.3.2.2 Develop Offline Entities

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

Offline entities account for all physical entities that can influence a target audience. Offline entities involve all forms of influence beyond the cyber-realm or internet and may include radio, television, posters, and public speeches.

- Cultural ambassadors refer to individuals that represent a population for foreign audiences. Cultural ambassadors may support influence operation objectives by creating a favorable or unfavorable perceptions of their representative population.

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.

2.3.2.3 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.

- Sympathetic users and unwitting agents promote operation narratives and provide credibility to an operation while removing association between themselves and the operation's planners. Sympathetic users may include local spokespeople, celebrities, subject matter experts, and social media influencers.

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.

2.3.3 Emplace Sensors Tactic

Sensors help an operation assess ongoing progress and improve resource allocation. They can track public opinion, identify rising trends, and perform analytics to provide timely and actionable performance intelligence to operation planners.

2.3.3.1 Observe Offline Behavior

Sub-Techniques: Follow Local News and Developments

While developing 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 may stay relevant and engaging 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.

2.3.3.2 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.

2.3.3.3 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 influence operation may monitor funding flows to determine vulnerabilities in external organization resources or map networks between publicly unaffiliated groups.

Malware refers to software designed to damage or gain access to a computer system.[xlv] Some types of malware include spyware, which gathers information about a target, adware, which disguises itself as a legitimate application and displays unwanted advertisements on a victim's computer, and a trojan, which disguises itself as a legitimate application to fool users to download damaging software.[xlvi]

Cookies refer to files that store browsing data regarding a user's activity on a web server.[xlvii] An influence operation may install cookies onto target devices to gather information on target audience activity and interests.

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.

2.3.3.4 Survey Public Opinion

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

Influence operations gauge public opinion with targeted polls and surveys. An influence operation 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.

2.3.3.5 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 engagement.[xlviii] An influence operation 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.

2.3.4 Cultivate Information Pathways Tactic

An information pathway is a venue of discussion on an active platform. Cultivating pathways reaches the target audience and exposes them to operation content. Operations may create or infiltrate forums, establish broadcast services, or prepare fundraising campaigns to attract and retain an engaged audience.

2.3.4.1 Create Forums

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

An influence operation 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.

- An echo chamber refers to an internet subgroup, often along ideological lines, where individuals only engage with "others with which they are already in agreement."[xlix]
- An operation may create echo chambers by matching existing groups, or aggregating individuals into a single target audience based on politics, values, demographics, and other characteristics to recommend other groups to join based on these interests.[l]

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 the following criteria: create a page, periodically create a group, update pages and groups to appear legitimate and attract followers or members.

2.3.4.2 Infiltrate Existing Forums

Sub-Techniques: Co-Opt Grassroots Groups

An influence operation may penetrate 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, and 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.

2.3.4.3 Establish Broadcast Services

Sub-Techniques:

Broadcast services refer to organizations that publish news stories on current events, sports, entertainment, and other topics. An influence operation may establish 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.[li] An influence operation may create newsletters to proliferate personalized and curated content to its target audience.

Rating:

0. Operation does not establish any broadcast services.
1. Operation establishes broadcast services on platforms that are irrelevant to the target audience, makes poor efforts to establish legitimacy, and posts irrelevant content.

2. Operation establishes broadcast services on relevant platforms for the target audience but fails to establish legitimacy and posts slightly irrelevant content.
3. Operation applies target audience analysis to create broadcast services on the target audience's most active platforms to post relevant content to maintain legitimacy among the target audience.

2.3.4.4 Prepare Fundraising Campaigns

Sub-Techniques: Newsletters

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. An influence operation 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.

2.3.5 Develop Content Tactic

An operation's content often varies in form and message but is the culmination of an operation's research on platforms and their target audience. Successful content is attention-grabbing, entertaining, and persuasive to the target audience.

2.3.5.1 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.[lii] 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.[liii] A misinfographic is an infographic with false or misleading information.[liv] 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.

2.3.5.2 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.[lv] 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.[lvi]

- Deepfakes refer to AI-generated falsified photos, videos, or soundbites.[lvii] 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.[lviii]
- 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.[lix] 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.[lx]
- 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.

2.3.5.3 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.

2.3.5.4 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.

2.3.6 Establish Legitimacy Tactic

A target audience's continued engagement with an operation is reliant on the operation's ability to establish legitimacy. When developing content, actors should ensure that their information is both engaging and believable to their target audience.

2.3.6.1 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.[lxi]
- Typosquatting refers to the intentional registration of a domain name that incorporates typographical variants of the target domain name in order to deceive visitors.[lxii]
- Web scraping refers to the use of bots to gather data from a website.[lxiii] 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.

2.3.6.2 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.[lxiv] 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.

2.3.6.3 Curate Social Proof

Sub-Techniques:

Social proof refers to the phenomenon in which individuals follow the actions of the masses.[lxv] 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.[lxvi]

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.

2.3.6.4 Leverage Existing Biases

Sub-Techniques:

An influence operation may create content that supports the target audience's existing beliefs and biases to increase its legitimacy by reinforcing preexisting beliefs and facilitating confirmation bias.[lxvii]

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.

2.3.7 Enable Persistence Tactic

While enabling an operation, operators should prepare for roadblocks and unexpected content removals. Enabling persistence prevents these roadblocks from completely shuttering a campaign's impact.

2.3.7.1 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.

2.3.7.2 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.[lxviii]
- A Virtual Private Network (VPN) to provide an encrypted Internet connection from a device to a network.[lxix] 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.[lxx]
- Proxies include people, companies, and organizations that work on behalf of an influence operation.[lxxi] 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.

2.3.7.3 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.[lxxii] 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.[lxxiii] 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.

2.4 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.

2.4.1 Persist in the Information Space Tactic

The "Persist in the Information Space" tactic covers different methods that could help an actor avoid detection and attribution.

2.4.1.1 Use Encrypted Networks

Sub-Techniques: Obfuscate Source Code

Encryption converts plaintext to ciphertext with a cryptographic algorithm.[lxxiv] 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.

2.4.1.2 Utilize Butterfly Attack

Sub-Techniques:

Butterfly attacks occur when operators pretend to be members of a certain social group, usually a group that struggles for representation.[lxxv] An influence operation 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, butterfly attacks aim to infiltrate and discredit existing grassroots movements, organizations, and media campaigns.

Rating:

0. Operation does not utilize butterfly attacks.
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.

2.4.1.3 Utilize Spamoflage

Sub-Techniques:

Spamoflage refers to the practice of disguising spam messages as legitimate.[lxxvi] Spam refers to the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.[lxxvii]

Simple methods of spamoflage include replacing letters with numbers to fool keyword-based email spam filters, for example, 'you've w0n our jackp0t!'. 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. Influence operations may use spamoflage to avoid spam filtering systems and increase the likelihood of the target audience receiving operation messaging.

Rating:

0. Operation does not utilize spamoflage.
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.

2.4.1.4 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.

2.4.1.5 Utilize Bulletproof Hosting

Sub-Techniques:

Hosting refers to a computer that is attached to a subnetwork and uses the services provided by the hosting subnetwork.[lxxviii]

Bulletproof Hosting refers to 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.[lxxix] An influence operation may utilize bulletproof hosting to maintain continuity of service for suspicious, illegal, or disruptive operation activities that stricter hosting services would limit, report, or suspend.

Rating:

0. Operation does not utilize bulletproof hosting.
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.

2.4.1.6 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.

2.4.1.7 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).

2.4.1.8 Vary Type of Account Used

Sub-Techniques:

An influence operation 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.).

2.4.1.9 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.

2.4.2 Distort Existing Narratives Tactic

An actor may distort, misrepresent, or intentionally manipulate an opposing narrative in efforts to maximize their own exposure and credibility. Given that a target audience uses platforms for a limited period of time each day, actors should recognize that a strong and popular narrative is critical to operation success.

2.4.2.1 Amplify Conspiracy Theories

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

An influence operation may create and amplify its own or existing conspiracy theories to support operation objectives with manipulated situations. Conspiracy theories may attract attention to operation assets or narratives, erode trust in public institutions or figures, or sow doubts about operation adversaries. Conspiracy theories often assert that a secret of great importance is being withheld from the general public.[lxxx]

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.

2.4.2.2 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.[lxxxi] 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.

2.4.2.3 Use Malign Rhetoric

Sub-Techniques:

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.[lxxxii] Malign rhetoric includes the use of logical fallacies, name-calling, and other rhetorical practices that distract from practical discourse. Malign rhetoric is often used in forums tailored to debate.

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 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.
3. 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.

2.4.2.4 Exploit Data Voids

Sub-Techniques:

A data void is a word or phrase that results in little, manipulated, or low-quality search engine data.[lxxxiii] 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.[lxxxiv]

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.

2.4.2.5 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.[lxxxv] 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.

2.4.3 Deliver Content Tactic

Content delivery involves posting, publishing, or releasing operation content to the target audience. Effective content delivery is timely, relevant, and engaging.

2.4.3.1 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.[lxxxvi] 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.[lxxxvii] 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.

2.4.3.2 Post on Platforms

Sub-Techniques: Post on Social Media, Post in Physical Forums, Direct Posting

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.

- A social media post refers to any social media status update, photo, or video, or an item shared on a blog or forum.[lxxxviii] An influence operation may post to social media to promote operation narratives to its target audience while exploiting features 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.
- 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 influence operation 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.

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.

2.4.3.3 Leak Documents

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

Leaking documents refers to releasing materials containing sensitive or private information. An influence operation may leak authentic or falsified documents to discredit or undermine an adversary, expose hidden information that supports operation narratives, or 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.

2.4.3.4 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.[lxxxix] 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.[xc]

- 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.[xci] 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.

2.4.3.5 Utilize Social Media Management Software

Sub-Techniques:

Social media management software (SMMS) allows a single user to simultaneously manage multiple different social media accounts.[xcii] 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.

2.4.3.6 Target Purchased Ads

Sub-Techniques: Unpublished page posts

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.[xciii]

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.

2.4.4 Amplify Supporting Information (Maximize Exposure) Tactic

Amplification methods share previously delivered content to maximize the reach of operation material on a platform.

2.4.4.1 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.[xciv] 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.[xcv] 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.[xcvi] 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.[xcvii]
- 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.[xcviii]
- Manufactured bursts refer to coordinated increases in social media activity, usually surrounding a specific event.[xcix] 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.[c] 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.

2.4.4.2 Conduct Botnet Amplification

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

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.[ci] 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.[cii]

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 botnet amplification.
1. Operation achieves one of three: creates echo chambers with operation and target-audience accounts, uses botnet 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 botnet 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 botnet amplification to infiltrate existing communities with operation-related content and narratives, and botnet account activity avoids detection by platforms.

2.4.4.3 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.[ciii] 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.[civ] 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.

2.4.4.4 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.[cv] 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.

2.4.4.5 Consistently Post 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 consistently post 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.

2.4.4.6 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 content depending on the time zone or user habits. An influence operation 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.

2.4.4.7 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.[cvi] 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.

2.4.4.8 Automated Forwarding and Reposting

Sub-Techniques:

Automated forwarding and reposting refer to the proliferation of operation content using automated means, such as artificial intelligence or social media bots. An influence operation 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.

2.4.4.9 Astroturfing

Sub-Techniques:

Astroturfing occurs when an influence operation disguises itself as grassroots movement or organization that supports operation narratives.[cvii] Unlike butterfly attacks, 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.

2.4.4.10 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.

2.4.5 Disrupt Information Flow Tactic

An operation may seek to suppress opposing viewpoints from reaching the target audience when they wish to maximize their content's exposure and minimize their adversary's influence. To accomplish this, a campaign can block content or bypass existing barriers.

2.4.5.1 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.[cviii] 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.[cix] 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.[cx] 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.[cxi] 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.[cxii] 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.[cxiii] 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.[cxiv] 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.

2.4.5.2 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:[cxv]

- 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.

2.4.5.3 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 influence operation 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.

2.4.6 Denigrate Opposing Information Tactic

In order to maximize the credibility of an operation's master narrative, operators must be prepared to effectively criticize opposing information. Successful denigration of adversary narratives will counter an opposing operation's influence over the long run.

2.4.6.1 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.[cxvi] 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.[cxvii]

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.

2.4.6.2 Report Opposing Content

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

Reporting opposing content refers to notifying and providing a platform with an instance of a violation of their guidelines and conduct policies. 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.

2.4.7 Drive Off-Platform Activity Tactic

After reaching a target audience, certain operations may seek to drive users to use platforms directly run or hosted by an operation's perpetrators. As a result, content delivery is streamlined and directly sent to members of the target audience. Off-platform activity also involves physical activity, which can serve as an indicator of campaign impact.

2.4.7.1 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 to 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.

2.4.7.2 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 influence operation 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.

2.4.7.3 Call to Action

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

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.[cxviii] 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.

2.4.7.4 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.[cxix] 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.[cxx] 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).

2.4.7.5 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.[cxxi] 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).

2.4.7.6 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 influence operation may incentivize real reporting on a story by paying journalists to cover operation narratives or having them reach mainstream media organically. 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.

2.4.7.7 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.[cxxii] 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 funding 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.

2.4.7.8 Sell Merchandise

Sub-Techniques:

Selling merchandise refers to the sale of often branded items to the target audience. An influence operation 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).

2.4.8 Remove Evidence of Tactics Tactic

After conducting an operation, some campaigns may need to cover their digital footprint. Removing evidence of tactics distances operation planners from attribution and enables them to conduct more covert operations in the future.

2.4.8.1 Delete Account Activity

Sub-Techniques: Delete Accounts

Deleting accounts and account activity occurs when an influence operation removes its online social media assets, including social media accounts, posts, likes, comments, and other online artifacts. An influence operation may delete its accounts and account activity to complicate attribution or remove online evidence 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.

2.4.8.2 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:[cxxiii]

- 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.

2.4.8.3 Delete URLs

Sub-Techniques:

URL deletion occurs when an influence operation completely removes its website registration, rendering the URL inaccessible. An influence operation 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.

2.4.8.4 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 influence operation actively separates itself from its own content. An influence operation 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 influence operation 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 influence operation 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 influence operation may remove post origins by deleting watermarks, renaming files, or removing embedded links in its content.
- Removing physical infrastructure occurs when an influence operation eliminates tangible evidence of the operation, including buildings that served as headquarters or offices, printing equipment, or broadcast infrastructure. An influence operation 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 influence operation 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.

2.5 Assess Phase

Even though the assess phase sits at the far-right of the framework, users should refer to the phase during and after conducting an operation. A campaign periodically reviews its progress as

an operation progresses and after it concludes. The assess phase outlines methods to measure technique impact during an operation.

2.5.1 Assess Techniques Tactic

Techniques can be individually assessed using the SP!CE technique ratings system and by mapping the operation to the framework. Users could then compare how competing operations strategize and engage with a single target audience. This procedure also informs courses of action and responses to adversary operations.

2.5.1.1 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.

2.5.1.2 Review Factors Affecting IO

Sub-Techniques:

When an operator reviews factors affecting IO, 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.

2.5.1.3 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.

2.5.1.4 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:[cxxiv]

- "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."

2.5.2 Assess Key Performance Indicators (KPIs) Tactic

Key Performance Indicators help analysts gauge campaign progress. Indicators can be reviewed as an operation is being conducted and used to alter strategy or adapt to changing circumstances.

2.5.2.1 Measure Reach

Sub-Techniques:

An operation's measurement of its campaign reach refers to the measurement of target audience exposure to operation content.

2.5.2.2 Measure Resonance

Sub-Techniques:

An operation's measurement of its campaign reach refers to the measurement of target audience approval or disapproval of operation-affiliated content.

2.5.2.3 Measure Support

Sub-Techniques:

An operation's measurement of its campaign reach refers to the measurement of target audience's level of persuasion by operation-aligned content.

2.5.2.4 Measure Sentiment

Sub-Techniques:

An operation's measurement of its campaign reach refers to the measurement of a target audience's emotions regarding operation narratives.

3 SP!CE Framework Matrix

Plan						Enable							Engage								Assess	
Determine Strategic End-State	Study Target Audience (TA) Information Environment	Study Social Landscape	Select Operation Platforms	Study Technical Landscape	Develop Operational Approach	Evaluate Resources	Establish Information Assets and Intermediaries	Emplace Sensors	Cultivate Information Pathways	Develop Content	Establish Legitimacy	Enable Persistence	Persist in the Information Space	Distort Existing Narratives	Deliver Content	Amplify Supporting Information (Maximize Exposure)	Disrupt Information Flow	Denigrate Opposing Information	Drive Off-Platform Activity	Remove Evidence of Tactics	Assess Techniques	Assess Key Performance Indicators (KPIs)
0 Review Existing Strategies and Policies	0 Reference Social Media Analytics	0 Reference Cultural Analysis	0 Assess TA Platform Usage	0 Identify Vulnerable Security Infrastructure	0 Develop Master/Strategic Narrative	0 Review Existing Messaging Strategies	0 Create Online Entities	0 Observe Offline Behavior	0 Create Forums	0 Develop Human-Driven Media	0 Co-opt Trusted Sources	0 Edit Existing Accounts	0 Use Encrypted Networks	0 Amplify Conspiracy Theories	0 Receive Media Exposure	0 Conduct Information Flooding	0 Block Content	0 Denigrate Believers of Opposing Narratives	0 Drive to Alternative Platforms	0 Delete Account Activity	0 Use Technique Ratings System	0 Measure Reach
0 Determine Strategic Objective	0 Evaluate Media Surveys	0 Study Ongoing TA Activities	0 Assess Platform Usage Frequency	0 Identify Data Voids	0 Integrate Vulnerabilities into Narrative	0 Identify Potential Campaign Constraints	0 Develop Offline Entities	0 Observe Online Behavior	0 Infiltrate Existing Forums	0 Create AI-Driven Media	0 Create Localized Content	0 Conceal Network Identity	0 Utilize Butterfly Attack	0 Reframe Context	0 Post on Platforms	0 Conduct Botnet Amplification	0 Bypass Content Blocking	0 Report Opposing Content	0 Drive to Physical Forums	0 Redirect URLs	0 Review Factors Affecting IO	0 Measure Resonance
0 Determine Operational Objectives	0 Apply Web Usage Analysis	0 Identify Cognitive Biases	0 Study Composition of Platform Content	0 Study Media System Landscape	0 Review Postulations	0 Collect Historical Content	0 Establish Proxy Entities	0 Monitor Funding Flows	0 Establish Broadcast Services	0 Tailor Content to Selected Platforms	0 Curate Social Proof	0 Conceal Sponsorship	0 Utilize Spamoflauge	0 Use Malign Rhetoric	0 Leak Documents	0 Exploit Platform-Specific Features	0 Destroy Information Generation Capabilities		0 Call to Action	0 Delete URLs	0 Map Operations in Information Environment to Framework	0 Measure Support
0 Review Adversary Operation Strategy	0 Assess Degree of Media Access	0 Identify TA Adversaries	0 Assess Platform Utility		0 Mitigate Analytic Gaps	0 Review Existing Information-Related Capabilities (IRCs)		0 Survey Public Opinion	0 Prepare Fundraising Campaigns	0 Launder Information	0 Leverage Existing Biases		0 Artificially Age Accounts	0 Exploit Data Voids	0 Microtargeting	0 Conduct Cross-Posting			0 Conduct Symbolic Action	0 Remove Association From Content	0 Conduct Analysis of Alternatives	0 Measure Sentiment
	0 Identify Trending Topics	0 Study Existing Narratives						0 Employ Commercial Analytic Firms					0 Utilize Bulletproof Hosting	0 Post Provocative Content	0 Utilize Social Media Management Software	0 Consistently Post Over Time			0 Conduct Physical Action			
													0 Misattribute Activity		0 Target Purchased Ads	0 Post at Hours Reflecting Highest Activity			0 Reach Mainstream Media Coverage			
													0 Unattribute Activity			0 Leverage Platform Algorithm			0 Conduct Fundraising Campaigns			
													0 Vary Type of Account Used			0 Automated Forwarding and Reposting			0 Sell Merchandise			
													0 Exploit Legal System			0 Astroturfing						
																0 Incentivize Sharing						

Figure 2: SP!CE 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 2.1 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.

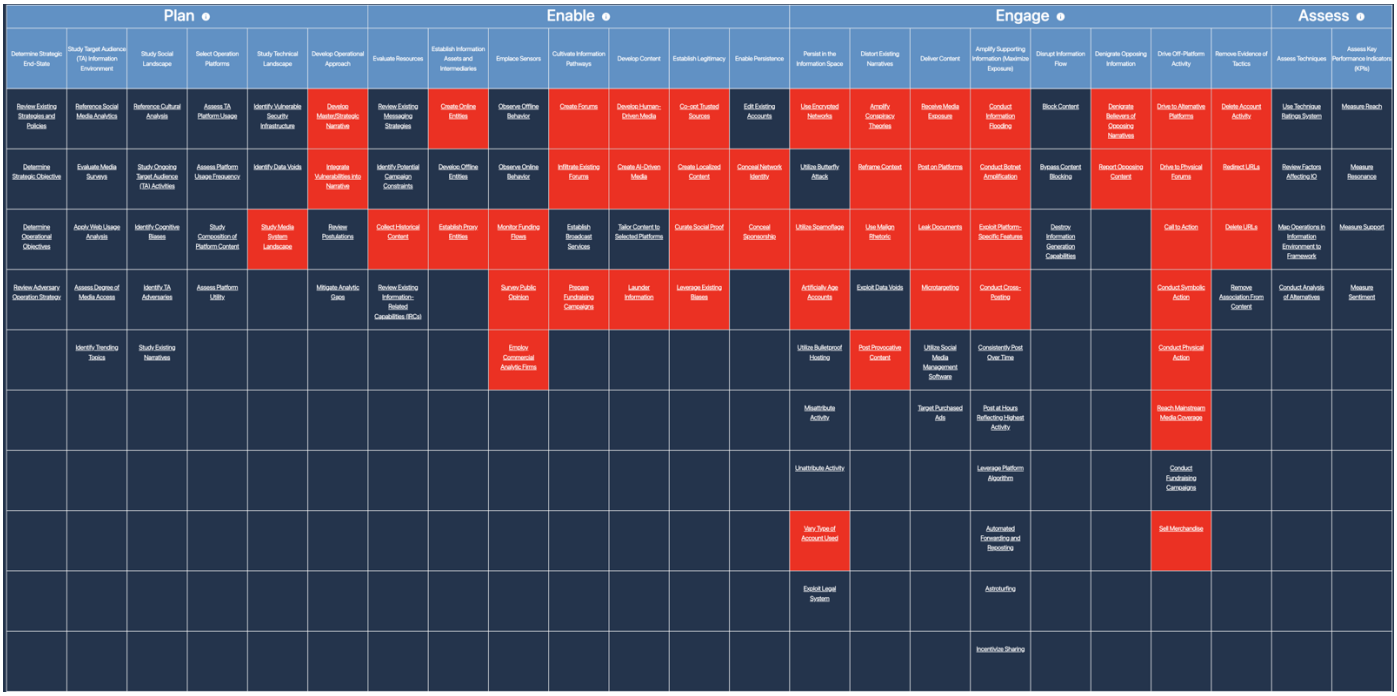

Figure 3: Techniques Tagged to the Knowledge Base on the current SP!CE Framework

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.[cxxv]
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.[cxxvi]
Butterfly Attack	When imposters mimic the patterns of behavior of a social group.[cxxvii]
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.[cxxviii]
Deep Fake	The use of "deep" or machine learning to hybridize or generate human bodies and faces.[cxxix]
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.[cxxx]
Dox	The act of publishing on the internet private or identifying information about a specific individual, usually with malicious intent.[cxxxi]
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.[cxxxii]
Human-Driven Media	Media or content created using minimal automation capabilities.
Hypertext Transfer Protocol	A standard method for communication between clients and Web servers.[cxxxiii]
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)[cxxxiv]
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)[cxxxv]
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.[cxxxvi]
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.[cxxxvii]
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.[cxxxviii]
Measure of Performance	A criterion used to assess friendly actions that is tied to measuring task accomplishment.[cxxxix]
Meme	Units of culture that spread through the diffusion of ideas, usually pictures, videos, or gifs on the internet.[cxl]
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.[cxli]
Social Media Management Software	Software that allows a single user to simultaneously manage multiple social media accounts.[cxlii]
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.[cxliii]
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.
Strategic Narrative	See *Master Narrative*

Term	Definition
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.[cxliv]
Tactic	The employment and ordered arrangement of forces in relation to each other.[cxlv]
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.[cxlvi]
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.[cxlvii]
Typosquatting	The intentional registration of a domain name that incorporates typographical variants of the target domain name in order to deceive visitors.[cxlviii]
Viral Sloganeering	Creating short, catchy phrases intended to deliver persuasive, disruptive messaging.[cxlix]
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.[cl]

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
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] 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.

[ii] 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

[iii] 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

[iv] 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

[v] 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

[vi] 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

[vii] 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

[viii] Joint Chiefs of Staff Washington United States. (2019). *Joint Doctrine Note 2-19, Strategy*. United States Department of Defense Staff. Retrieved from https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn2_19.pdf?ver=2019-12-20-093655-890

[ix] U.S. General Services Administration Staff. Web Analytics Basics. *usability.gov*. Retrieved from https://www.usability.gov/what-and-why/web-analytics.html

[x] Olafson, K. 19 Social Media KPIs You Should Be Tracking. *Hootsuite*. Retrieved from https://blog.hootsuite.com/social-media-kpis-key-performance-indicators/

[xi] U.S. General Services Administration Staff. Web Analytics Basics. *usability.gov*. Retrieved from https://www.usability.gov/what-and-why/web-analytics.html

[xii] 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

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

[xiv] Fredel M. Wiant. (2002). Exploiting factional discourse: Wedge issues in contemporary American political campaigns, Southern Communication Journal. 67:3, 276-289, DOI: 10.1080/10417940209373236

[xv] Ibid.

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

[xvii] Polansky, Sabrina and Tom Rieger. (2020). Cognitive Biases: Causes, Effects, and Implications for Effective Messaging. Strategic Multilayer Assessment Integrating Information in Joint Operations (IIJO). Retrieved from https://nsiteam.com/cognitive-biases-causes-effects-and-implications-for-effective-messaging/

[xviii] Ibid.

[xix] Hirschberger Gilad. (2018). Collective Trauma and the Social Construction of Meaning. Frontiers in Psychology, Volume 9, DOI: 10.3389/fpsyg.2018.01441

[xx] Microsoft Dynamics 365 Staff. (n.d.). What is sentiment analysis? Microsoft Dynamics 365. Retrieved from https://dynamics.microsoft.com/en-us/ai/customer-insights/what-is-sentiment-analysis/

[xxi] Sands, J. (2019). Local news is more trusted than national news – but that could change. Knight Foundation. Retrieved from https://knightfoundation.org/articles/local-news-is-more-trusted-than-national-news-but-that-could-change/

[xxii] Bliley Technologies. (2017). What is SIGINT and How is it Used in Electronic Warfare? Bliley Technologies. Retrieved from https://blog.bliley.com/sigint-electronic-warfare

[xxiii] Pew Research Center Staff (2020). Important issues in the 2020 election. Pew Research Center. Retrieved from https://www.pewresearch.org/politics/2020/08/13/important-issues-in-the-2020-election/

[xxiv] Ibid.

[xxv] King, G., Pan, J., and Roberts, M. (2017). How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument. American Political Science Review, 111(3), 484-501. doi:10.1017/S0003055417000144

[xxvi] Ruhl, C. (2023). What is Cognitive Bias. *Simply Psychology*. Retrieved from https://www.simplypsychology.org/cognitive-bias.html#definition/

[xxvii] Jindal, V. (2022). A New Era of Advertising Measurement: Cross-Channel Viewership Analytics. *DMN News*. Retrieved from https://www.dmnews.com/a-new-era-of-advertising-measurement-cross-channel-viewership-analytics/

[xxviii] Ibid.

[xxix] Kirst, S. (2015). What Are Nielsen Ratings And how Are They Calculated? *Forbes*. Retrieved from https://www.forbes.com/sites/seamuskirst/2015/12/18/what-are-nielsen-ratings-and-how-are-they-calculated/?sh=3c295a7b56e0

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

[xxxi] 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

[xxxii] Johnson, D. (2020). What is a cache? A complete guide to caches and their important uses on your computer, phone, and other devices. *Business Insider*. Retrieved from https://www.businessinsider.com/guides/tech/what-is-cache

[xxxiii] 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

[xxxiv] 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

[xxxv] BBC Staff. (2021). Social Media: Should people be allowed to be anonymous online? *British Broadcasting Corporation*. Retrieved from https://www.bbc.co.uk/newsround/56114122

[xxxvi] Kats, D. (2020). Identifying Sockpuppet Accounts on Social Media Platforms. *Norton Lifelock Blogs*. Retrieved from https://www.nortonlifelock.com/blogs/norton-labs/identifying-sockpuppet-accounts-social-media

[xxxvii] Associated Press. (2020). Cyborgs, Trolls and Bots: A Guide to Online Misinformation. *Voice of America News*. Retrieved from https://www.voanews.com/a/silicon-valley-technology_cyborgs-trolls-and-bots-guide-online-misinformation/6183912.html

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

[xxxix] Ibid.

[xl] Department of Homeland Security Staff. (2018). Social Media Bots Overview. Department of Homeland Security Office of Cyber and Infrastructure Analysis. Retrieved from https://niccs.cisa.gov/sites/default/files/documents/pdf/ncsam_socialmediabotsoverview_508.pdf?trackDocs=ncsam_socialmediabotsoverview_508.pdf

[xli] Wright, J. and Olabode Anise. (2018). Anatomy of Twitter Bots: Amplification Bots. *Duo*. Retrieved from https://duo.com/labs/research/anatomy-of-twitter-bots-amplification-bots

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

[xliii] Ibid.

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

[xlv] Department of Homeland Security Staff. Malware Tip Card. Department of Homeland Security Office of Cyber and Infrastructure Analysis. Retrieved from https://www.cisa.gov/sites/default/files/publications/Malware_1.pdf

[xlvi] Department of Homeland Security Staff. Malware Tip Card. Department of Homeland Security Office of Cyber and Infrastructure Analysis. Retrieved from https://www.cisa.gov/sites/default/files/publications/Malware_1.pdf

[xlvii] Stouffer, C. (2022). Computer cookies: A definition + how cookies work in 2023. Norton Blogs. Retrieved from https://us.norton.com/blog/privacy/what-are-cookies

[xlviii] Davenport, T. (2006). Competing on Analytics. *Harvard Business Review*. Retrieved from https://hbr.org/2006/01/competing-on-analytics

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

[l] Youfang, L. et al. (2022). Dynamically aggregating individuals' social influence and interest evolution for group recommendations, Information Sciences, Volume 614, Pages 223-239, https://doi.org/10.1016/j.ins.2022.09.058.

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

[lii] 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

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

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

[lv] 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

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

[lvii] 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/

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

[lix] 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

[lx] 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

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

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

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

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

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

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

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

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

[lxix] 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

[lxx] 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

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

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

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

[lxxiv] 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

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

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

[lxxvii] 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

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

[lxxix] 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#

[lxxx] Merriam-Webster. (n.d.). Conspiracy Theory. In Merriam-Webster.com dictionary. Retrieved June 28, 2023, from https://www.merriam-webster.com/dictionary/conspiracy%20theory

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

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

[lxxxiii] 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

[lxxxiv] 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

[lxxxv] 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

[lxxxvi] 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/.

[lxxxvii] Ibid.

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

[lxxxix] 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

[xc] 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

[xci] 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/

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

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

[xciv] 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/

[xcv] 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

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

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

[xcviii] 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

[xcix] Ibid.

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

[ci] 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

[cii] 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

[ciii] Zoria, Y. (2019). MH17 crash days: Russian trolls generated over 100K tweets, at least 65K to blame Ukraine. *Euromaidan Press*. Retrieved from https://euromaidanpress.com/2019/06/26/mh17-crash-days-russian-trolls-generated-over-100k-tweets-at-least-65k-to-blame-ukraine/

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

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

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

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

[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] Ibid.

[cx] 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/

[cxi] Ibid.

[cxii] 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/

[cxiii] Ibid.

[cxiv] 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

[cxv] 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/

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

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

[cxviii] 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

[cxix] 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/

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

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

[cxxii] 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/

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

[cxxiv] 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

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

[cxxvi] 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#

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

[cxxviii] 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

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

[cxxx] 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

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

[cxxxii] 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

[cxxxiii] 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

[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] 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

[cxxxvi] 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

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

[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 (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

[cxli] 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

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

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

[cxliv] 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

[cxlv] 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

[cxlvi] 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

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

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

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

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