NORWICH UNIVERSITY

2025 Richard S. Schultz '60 Symposium Fellow Research Report

Narrative Access and Maneuver Denial: Ethical Initiative in the Battle for Beliefs

By: Jayden LaVecchia

Narrative Access and Maneuver Denial: Ethical Initiative in the Battle for Beliefs

By: Jayden LaVecchia

Contents

NORWICH UNIVERSITY

Abstract

In the grand scheme of the Western world and democratic societies, misinformation has become all but a fact of life. The World Economic Forum has ranked it as the foremost threat the world is facing. Despite this focus, there is still an overly generalized view of offensive influence operations, leaving a distinct gap in understanding for defensive information warfare, or narrative defense. The general, catch-all defense is militant democracy, which restricts specific speech in the name of protecting other speech. However, militant democracy neglects a key fact of information warfare – the targeting of psychological weak points rather than the audience they reside in. This paper will synthesize a framework for understanding cognitive vulnerabilities by analyzing six historic offensive influence operations, focusing on their tactics, techniques, targets, and procedures. By targeting the flaws these operations exploit, this paper will propose the Narrative Access and Maneuver Denial (NAM-D) strategy for ethical and effective narrative defense.

Overview

This research proposal will operate in three phases: adversary analysis, cognitive vulnerability assessment, and cognitive red cell development. Phase one looks at existing, attributed influence operations targeting the United States and its allies launched by Russia, China, and Iran. By working through the three layers of the Information Environment (IE) as defined by Joint Publication 5-0, this phase will walk through tactics, techniques, and procedures (TTPs) along the DISARM Framework to develop a comprehensive view of historical information operations that seek to influence a target audience by exploiting cyberspace. These operations constitute CEIOs, or cyber-enabled information operations.

NATO's Cooperative Cyber Defense Center of Excellence refers to these as Information Cyber Operations. It defines them as "activities undertaken in cyberspace affecting the logical layer of cyberspace with the intention of influencing attitudes, behaviours, or decisions of target audiences." [1]

Phase two looks at the effects of these operations. It will discuss their success, or lack thereof, as well as residual effects. This phase will compare cross-operation tactics, techniques, and procedures and develop a cognitive vulnerability framework around them.

Phase three will tie it all together, drawing from the historical precedent in Phase One and scenarios in Phase Two. This phase will lay out the cognitive red cell composition and develop their workflow, culminating with the proposal of a proof of concept using Norwich University Applied Research Institute's DECIDE platform.

---

[1] Brangetto and Veenendaal, Influence Cyber Operations…

Phase I: Historical Analysis

Information Operations, while not universally known by this name, have been around as long as history can recall. In 1928, Edward Bernays introduced his book Propaganda, earning him the nickname of "Propaganda Master." Sun Tzu documented the strategy of military deception (MILDEC), a strategy codified in U.S. military doctrine today. From the Trojan Horse to the lead-up to D-Day, MILDEC has played a key role in history. Some scholars speculate that Jericho fell not because of Joshua's horn but because of a persistent influence operation that tore the city down from the inside out.[2]

A prime example of modern information warfare is OPERATION BOLO, a tactical victory from 1967 during the Vietnam War. The operation aimed to degrade North Vietnamese fighter capabilities in the face of restrictive rules of engagement and evolving North Vietnamese air tactics, which favored targeting bombers and only engaging when victory was inevitable. Col. Robin Olds and Capt. John "J.B." Stone of the 8th TFW exploited this trend, outfitting their F-4s with F-105 electronic warfare implements and adopting F-105 tactics to ambush North Vietnamese MiGs. In just 12 minutes, the 8th TFW destroyed 7 MiG-21s, half of the Vietnamese operational force, infiltrating their "OODA Loop." [3]

Recent History. In recent history, there has been a more significant trend away from direct information warfare, like Operations BOLO. Instead, it has been used as a shaping operation to influence a target audience in situations short of war. To a large extent, CEIO sits in what is typically considered the grey zone, a no-man's-land at the crossroads between peace and conflict. For an accurate counter-CEIO framework to function correctly, an understanding of modern operations is necessary. That said, this section will walk through a selection of attributed operations from the past 10-15 years, focusing on Russia, China, and Iran.

Russia

Ghostwriter. Ghostwriter is a primarily Russian operation that employs thousands of fake accounts across various microblogging and social media platforms. The target audience for Ghostwriter was Russian-speaking minority communities in NATO countries, especially the former states of the Soviet Union. Ghostwriter has been operating since early 2016, but dodged identification until 2020. Google's Mandiant intelligence made the initial discovery using pattern recognition.[4] The cyber assets behind Ghostwriter were attached to a Belarusian group called UNC1151, which harvested passwords and spread malware in support of Ghostwriter's use of compromised social media accounts.[5]

Secondary Infektion. Secondary Infektion is a Russian influence operation that functions more organically than Ghostwriter, relying on forged accounts over compromised ones. The Atlantic Council's Digital Forensics Research Laboratory (DFRLab) made the initial attribution and noted a four-phase fingerprint. Each narrative starts as a believable claim, turns into a meme, cascades through algorithm manipulation, and then goes mainstream through state-run traditional media. Specific attribution labels include incorrect transliterations (cultural mismatch), mistranslations, and account age compared to history.[6]

---

[2] Andrew, The Secret World: *A History of Intelligence*, 22.

[3] https://www.nationalmuseum.af.mil/Visit/Museum-Exhibits/Fact-Sheets/Display/Article/196006/operation-bolo/

[4] Foster et al, Ghostwriter Update, 2021.

[5] Insikt Group, *Ghostwriter in the Shell*, 2022.

[6] Aleksejeva et al, OPERATION "SECONDARY INFEKTION", 2019.

China

Dragonbridge. Dragonbridge, more commonly called Spamouflage, is a Chinese operation heavily reliant upon spam. Dragonbridge was first noted in the United States in 2019 by Graphika. Google's Mandiant later reported an increase in political narratives from assets linked to Dragonbridge in 2022. The operation primarily targets Western countries, aiming to discredit them and replace them with Chinese alternatives. This action usually hides behind spam accounts, hence the name spamouflage. The operation has also targeted non-Western entities close to China, such as Taiwan and Hong Kong. Key hallmarks of Dragonbridge are AI-generated video and audio posted particularly around X (formerly Twitter); however, TTPs are continually evolving.[7] [8]

Glassbridge. Glassbridge is another Chinese operation that focuses more on fake news sites. Before its attribution as Glassbridge, one of its sub-campaigns was called HaiEnergy due to its attribution to Shanghai Haixun Technology Co., Ltd (上海海讯社科技有限公司). HaiEnergy was later revealed as one part of a larger picture, integrating three other Chinese PR firms operating as hosting services for fake news media.[9] [10] The operation usually imitates names from authentic media sources, such as Milano Moda or Fashion Milan, as a means of concealment. The key attribution, however, was the hosting platform for these news sites. Canada's Citizen Lab traced the servers that hosted these sites to three IP addresses attributed to Xinhai. Glassbridge hides its political content not simply in local content but also in low-quality spam content, similar to Dragonbridge. Published content is typically Chinese state propaganda, conspiracy theories, and targeted ad hominem attacks. A key example of this is Yan Limeng, a PRC dissident in the U.S., whom these sham pundits targeted and smeared alongside authentic media.[11]

Iran

Cotton Sandstorm. Cotton Sandstorm is an advanced persistent threat responsible for multiple operations, primarily targeting Israel, its allies, and any Western forces in the Middle East and North Africa (MENA). Cotton Sandstorm operations typically occur in three phases: reconnaissance, exploitation, and cascade. Cotton Sandstorm starts by discovering vulnerabilities in a target, often critical infrastructure. When targeting social media users, operations typically use open-source assets to gain access through password decryption. The exploitation phase frequently targets user logs or voter profiles. The group then uses these assets to publicize their breaches in an often-exaggerated fashion. The key Modus Operandi of Cotton Sandstorm operations is impersonation for intimidation, such as in the 2020 case, where Cotton Sandstorm impersonated Proud Boys to pressure or suppress votes.[12] [13]

---

[7] Mandiant, 2021.

[8] Cheng et ak, *Spamouflage Outbreak*, 2021.

[9] Serabian and Zafra, 2022.

[10] Molter, 2024.

[11] Alberto Fittarelli, 2024

[12] Watts, *Rinse and Repeat*, 2023.

[13] Bing and Vicens, *Iranian Hacker Group…*, 2024.

"Likes for Lorestan." "Likes for Lorestan," unlike any of the above, is an Iranian campaign hyper-targeting opposition leaders in the Iranian province of Lorestan. This campaign directly links to the Iranian Revolutionary Guard Corps (IRGC) and Ministry of Intelligence and Security (MOIS). Additionally, "Likes for Lorestan" has been a truly persistent campaign, with activity attributed to it as early as 2011. The campaign primarily targets the dissident group Mojahedin-e-Khalq (MEK). This pro-Western and Trump-supported dissident group could serve as a replacement in the event of an Iranian regime change. This campaign is embedded in the local Lorestan culture and propagates pro-government narratives. These accounts are typically sham media outlets and impersonation accounts. Such accounts propagate narratives that promote tourism in Lorestan, discredit and attack the MEK, and support the current government. These accounts also have a peripheral link to the Seraj Cyberspace Organization (SCO) and the Nejat Society, both of which link to the IRGC and MOIS, respectively.[14] [15]

Figure 1: Activity Overlaps

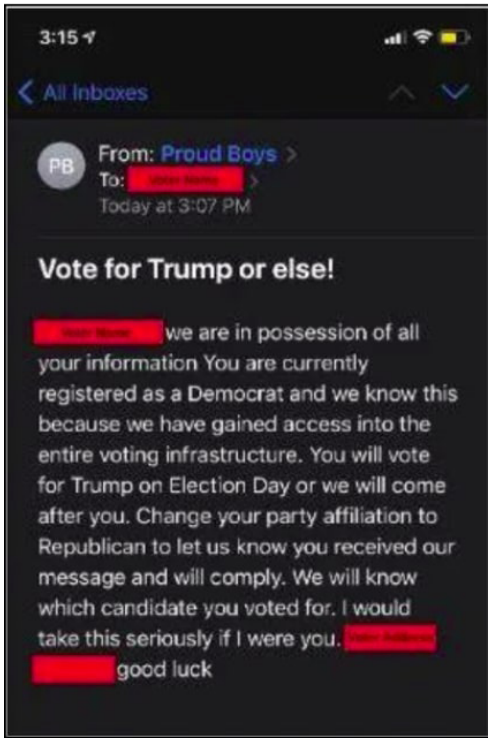
Major Observed Activity	Tactic	Target
Poisoning the well (propagating misinformation)	Social Media Algorithm Exploitation; bot accounts; echo chambers	Target Audience; Polarization; Availability Bias; Confirmation Bias
Localized Internet traffic	Compromising Infrastructure; Coopting local servers/addresses; local language media	Conventional Media; Non-social media users; Information Overload
Impersonation	Coopting Political or Cultural figures; Account Compromise	Polarization; Political Audiences; Tourist/Visiting Populations
Discrediting	Account Compromise; Smearing; Attacking; Counter-Narratives	Significant Political Figures/Parties; Celebrities; Major News Accounts; Pundit Accounts

[14] Chandra et al, *Likes for Lorestan*, 2021.

[15] Dehghan, *Who is the Iranian group…*, 2018.

Phase II: Cognitive Vulnerabilities and their Exploitation

Methodology. Before developing the Cognitive Vulnerability Framework (CVF), an analysis of the three primary countries of interest provided data to a complex understanding of the Information Environment surrounding each country, its operational complexes, and its direct and indirect links to the U.S. and its allies. A current state diagram was developed from this data, which served as a contextual basis for the CVF.



A case study from the larger campaigns helps develop an understanding of these cognitive vulnerabilities. This case study is directly linked to Cotton Sandstorm and pertains to the legal recording of the Iranian interference in the 2020 U.S. election.

Case Study: Proud Boys in a Sandstorm. During the 2020 election, registered democrats in Florida and Alaska received an email from an address purportedly tied to the Proud Boys, an alt-right violent extremist group primarily found in the U.S.[16] These emails claimed to be able to track how specific individuals voted and threatened violence in the face of non-compliance.

Cotton Sandstorm leveraged a network breach of Estonian textbook publisher Koolibri[.]ee, using emails with grammatically incorrect English and sender addresses (like vhost43553f0@avalik[.]koolibri[.]ee) to their advantage.[17]

In an October 2024 threat intelligence report, Microsoft Threat Analysis Center reiterated a previous finding that the corporate shell of Cotton Sandstorm, Emennet Pasargad, was linked to the operation. The report references *United States of America V. Seyyed Mohammad Hosein Mousa Mazemi and Sajjad Kashian* in the United States District Court, Southern District of New York.

The Voter Intimidation and Influence Campaign (VIIC) seems to have also operated in Oklahoma and New York, targeting democratic voters. The operation exploited an 11-state voter information website, leaking over 100,000 instances of voter information. The VIIC also targeted Facebook and email to spread false election messages to influential Republicans, the 2020 Trump Campaign, and the media. These messages claimed Democrats planned to exploit "serious security vulnerabilities" to alter mail-in ballots and register non-existent voters. The VIIC ultimately attempted media manipulation, with Seyyed compromising an undisclosed media corporation's content management system, aiming to disseminate false narratives. Seyyed and Sajjad unsuccessfully tried to regain access post-election with outdated credentials.[18] [19]

---

[16] Gringlas, *Voters in Florida…*

[17] Owen and Francheschi-Bicchierai, *'Proud Boys' Emails Threatening…*

[18] Sweetman, *'Vote for Trump or Else'…*

[19] *UNITED STATES OF AMERICA V. SEYYED MOHAMMAD HOSEIN MOUSA KAZEMI AND SAJJAD KASHIAN.*

Analysis

This case study provides a larger insight into targeting and effective cognitive vulnerabilities. The VIIC was specifically chosen due to its insight into the specific cognitive vulnerabilities through which it approaches the target audience. Generally, these vulnerabilities fall into one of two broad categories: psychological and sociocultural. Psychological vulnerabilities can be considered the zero-days of cognitive vulnerabilities, existing as blind spots in the minds of every individual. Sociocultural vulnerabilities are those that are more acquired, stemming from group identities, social norms, and shared history.

To a large extent, the VIIC focused very heavily on exploiting both types of vulnerabilities. The VIIC operation directly weaponizes political polarization to influence election outcomes in the United States. Polarization also served as an obfuscation measure. The VIIC utilized the pre-existing political climate and the cognitive vulnerabilities accompanying it to spread its impact. The narrative spread in a manner that exploited emotions such as fear by co-opting institutional beliefs and the history surrounding the Proud Boys.

However, while polarization is far from the only cognitive vulnerability exploited, it provides the perfect study for understanding the interdependence of psychological and sociocultural vulnerabilities in cognitive vulnerability exploitation. Polarization is frequently used as an exploitation because it inherently combines groupthink and shared identity with emotions, bias, and, to a lesser extent, information saturation.

Phase III: Addressing Cognitive Vulnerabilities

Critical thinking is a crucial, yet flawed, solution to cognitive vulnerabilities. The U.S. education system needs to teach diverse thought, but education has historically failed against, and even bolstered, autocracy (e.g., Nazi Germany). Former KGB agent Yuri Bezmenov highlighted education as a prime target for Soviet anti-Western efforts, further disqualifying it as the sole counter-influence strategy. The slow implementation of national education standards also poses a problem, as generative and agentic AI could revolutionize adversarial influence tactics before critical thinking initiatives take hold.[20] [21]

Against Censorship. Censorship, in whole or in part, is out of the question. Perception and reality are the key reasons here. On the perception front, any inkling of censorship will create a political environment that discredits counter-influence efforts and creates fertile ground for hostile narratives, effectively killing the effort in its tracks. Censorship also provides narrative fuel, leaving the aforementioned political polarization hybrid vulnerability wide open for exploitation.

These perceptual bases are rooted in reality, enshrined in the U.S. Constitution. Sitting in the Bill of Rights as the First Amendment: "Congress shall make no law… abridging the freedom of speech." [22] While there are court-based restrictions and laws passed that amend specific types of speech, the vast majority of speech and information by proxy is still protected.

---

[20] Taken from the statements by Dr. Travis Morris, NU Peace and War Center Director, 2 June 2025.

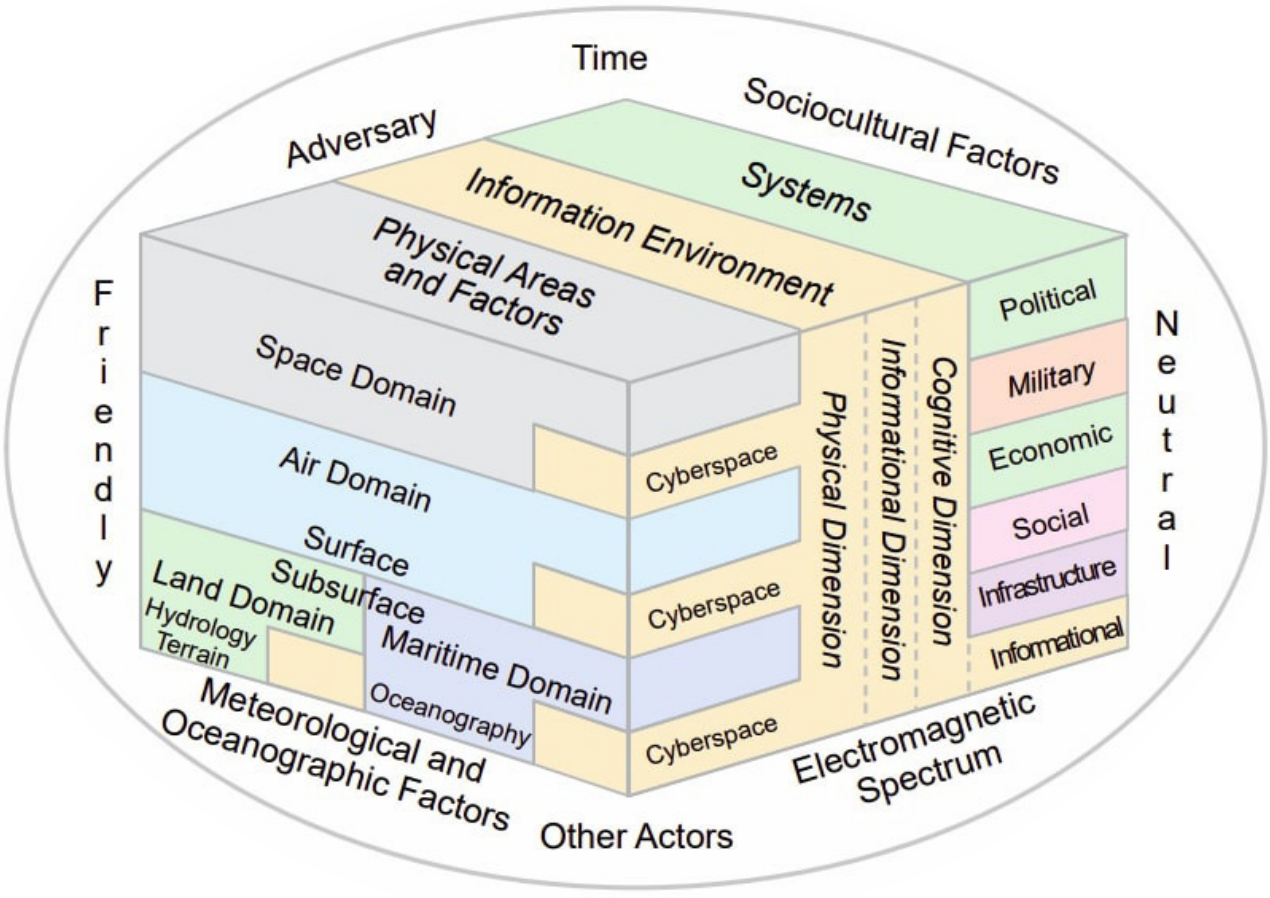
[21] https://bezmenov.neocities.org/

[22] https://www.law.cornell.edu/constitution/first_amendment

Information Environment. As a contextual basis, the course of action that follows is an active defense in the information environment. The information environment, according to Joint Publication 5-0 (JP 5-0), is a subset of the operational environment that contains the physical, datalogical, and personal layers. The physical layer constitutes the physical connections that maintain the flow of information. The datalogical layer pertains to information itself while in transit. The personal layer pertains to the individual processing of information by people.

Figure 2: Wholistic View of the Operational Environment (JP 5-0)

Narrative Access and Maneuver Denial. Narrative Access and Maneuver Denial (NAM-D) is a pre-emptive and active narrative defense strategy based on research into cognitive vulnerabilities, similar to Google Jigsaw's "prebunking." Unlike prebunking, which requires a narrative to propagate and be detected before intervention, NAM-D uses Information Environment Development (IEDev) to control narrative fuel and deny adversarial access to information as a tool and an environment.[23]



[23] Harjani, T. et al (2022). A Practical Guide to Prebunking Misinformation.

NAM-D views information as both an environment and a weapon, seeking to shape the information environment by addressing cognitive vulnerabilities through adversary emulation, thereby limiting adversaries' ability to influence American "Hearts and Minds." Drawing from cybersecurity practices like penetration testing and red teaming, NAM-D anticipates adversarial campaigns, narratives, and TTPs by examining past and current events. A team of experts analyzes these ideas, develops cultural competency in adversarial areas, and executes IEDev to deny enemies access to information as a weapon and an environment.

Cognitive Red Cell (CRC). NAM-D's primary tactical unit, the Cognitive Red Cell (CRC), aims to hijack a target audience's (TA) OODA loop's observation phase to control their orientation. A CRC has four mission packages: targeting, cognitive action, physical action, and information action. Targeting selects the TA and assists with dissemination. Cognitive action exploits TA vulnerabilities and obfuscates adversarial actions, while its targeting team understands the adversary's and TA's background. Physical action focuses on infrastructure impacting operations (sites, communication, data flow, critical infrastructure). Information action handles content development and dissemination (algorithm/SEO manipulation, OODA loop injection, network intrusion, local cognitive security). All packages share the goal of IEDev. Appendix B shows a complete CRC.

CRC Workflow. In practice, this workflow stays contained to a specific time frame set by the operation leader. In the private world, this may be an active disaster-response simulation that happens in the background of a typical workday or week. Companies and governments should use this form of cognitive penetration testing to simultaneously test response capability and diagnose cognitive vulnerabilities, a term from the cybersecurity world. In general, the CRC workflow should run as such:

Target Audience Analysis. The first operational step is TA analysis. Given a specific adversary, the CRC tasked with mimicking them will look at a specified goal and assign a target audience for their operation. The TA will vary depending on various target factors, desired impacts, and threat actor history. Flexibility and authenticity should take precedence.

Narrative Development. With the TA established, the CRC develops a key narrative, narrative-aligned content, and avenues of dissemination. The key narrative will depend heavily upon the desired end state, but will generally exist in one of two fashions: destabilizing and bolstering. Destabilizing narratives aim to destabilize an opposing power, and bolstering narratives seek to build an adversary's reputation and influence. Narrative-aligned content serves as a tactical layer for the development, propagation, and evolution of the narrative(s). The content itself, for maximum effectiveness, should exploit both psychological and sociocultural cognitive vulnerabilities.

For all intents and purposes, content generation is the most open-ended step, relying on either organic or AI-generated material in text, image, video, audio, and other emerging formats. As AI video and audio generation improve, the potential for content will only increase. Avenues of Dissemination and Cascading boil down to niche microblogs and various types of media, including alternative, social, and traditional or state-controlled media.

Dissemination and Cascading. Once the key narrative, content, and avenues of dissemination are established, their propagation should begin. This propagation should initially be tested in a sector of the TA, with consistent monitoring for successful content or content that needs revision. Revisions should be developed, implemented, and retested. In order to test content and dissemination, the CRC should establish measures of effectiveness and measures of performance to test against, from which the CRC can identify a cascade point.

Repetition. As the CRC identifies the most effective means of dissemination and cascading, they should adapt the operation as necessary to maximize the effect. However, that means that until they can effectively pivot to an evolution of the narrative, they will require repetition of the testing phase. From this point, the CRC repeats a continuous cycle of testing, cascading, and adapting until the desired end state is achieved or wholly out of reach.

Reporting. In the final step of the wargame, the CRC should produce a report noting the specifics of the game and provide it to the entity targeted. This report should include: specific cognitive vulnerabilities targeted and discovered, the effectiveness of the targeting, avenues of dissemination and cascading, specific narratives and content, and a map of whatever revisions the CRC made.

The general NAM-D workflow is very similar to penetration testing or red teaming workflow, or a general operations timeline, for that matter. For the sake of containment, a general NAM-D operation should operate using a CRC in a wargame format, operating off a system similar to Norwich University Applied Research Institute's DECIDE platform. Alternatively, an AI system likely operating a Large Language Model (LLM) trained to mimic the target asset's capabilities could be utilized.

Figure 3: CRC Workflow

Conclusion: Taking Back the Initiative

Beyond the research used to develop this research, various subject-matter experts also helped develop both the Cognitive Vulnerability Framework and Heuristic Narrative Security outline. This report consulted professionals from Special Operations Command and psychological operations,[24] [25] information warfare and cybersecurity, [26] and psychology[27] in the development and modification of the NAM-D strategy. Their expertise is also currently helping develop and procure a proof of concept, outlined below.

Unfortunately, this project does not have the means or timeframe to assemble 20-odd subject-matter experts to test this CRC theory or the defense against it. However, Norwich University Applied Research Institute operates a disaster response simulation platform called DECIDE, or the Distributed Environment for Critical Infrastructure Decision-making Exercises. Admittedly, DECIDE primarily targets cyberattacks against critical infrastructure; however, as described above, cyberspace is an inseparable domain of CEIOs. Proof of concept may be developed by adjusting scenario injections around real-world command and control exploits or narrative attacks provided by a CRC, or simply providing those injects through the moderator.

In the future, NAM-D also has the potential for an AI application for prediction, prevention, and denial. However, this is too far down the line for consideration. For the time being, the primary focus is on using DECIDE for a proof of concept. Following this, future possibilities will be evaluated and pursued.

Annex A: Objectives Overlap Diagram

Tactic	Technique	Ghostwriter	Secondary Infektion	Dragonbridge	Glassbridge	Cotton Sandstorm	Likes for Lorestan
	Plan Objectives						
	Defame						
	Intimidate						
	Spread Hate						
	Boost Reputation						
	Cultivate Support for Ally						
	Cultivate Support for Initiative						
	Defend Reputation						
Cause Harm	Energize Support						
	Increase Prestige						
	Justify Action						
	Recruit Members						
	Degrade Adversary						
	Dismay						
Cultivate Support	Discredit Credile Source						
	Deter						
	Discourage						
	Silence						
	Distort						
	Distract						
Dismiss	Divide						
	Facilitate State Propaganda						
Disuade from Acting	Extort						
	Generate Ad Revenue						
Facilitate State Propaganda	Manipuate Stocks						
Distract	Raise Funds						
Divide	Scam						
Fascilitate State Propaganda	Sell Under False Pretenses						
	Compel						
	Encourage						
	Prevoke						
Motivate to Act	Polarize						
	Smear						
	Subvert						
	Thwart						

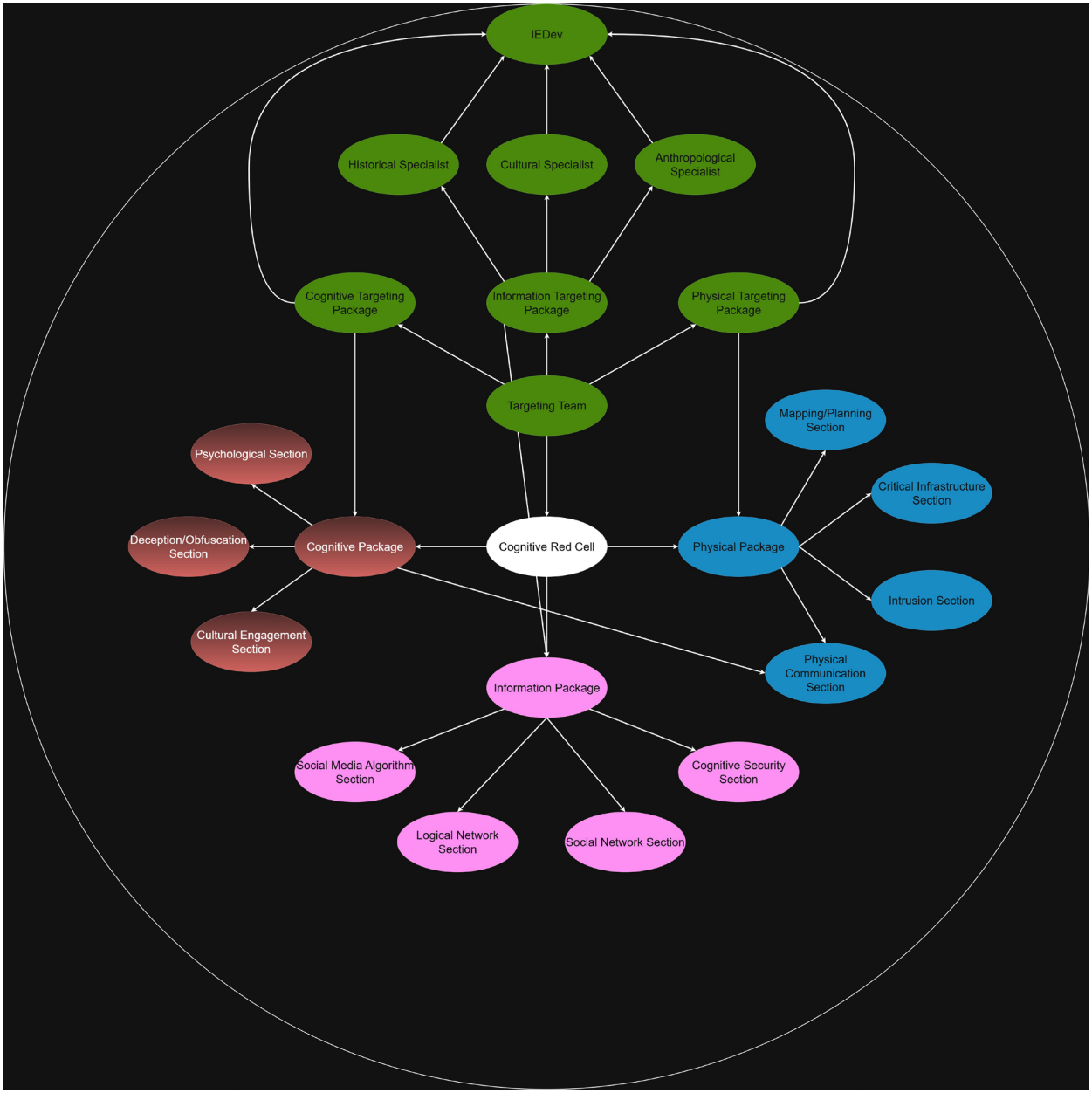
[24] Interview, COL Curt Boyd (ret.), US SOCOM, USASOC, 3 July 2025.

[25] Interview, SFC Michael Ortiz, US SOCOM, USASOC, 3 July 2025.

[26] Interview, Shawn Lane, 3-124 Information Operations Battalion, VTARNG, 31 July 2025.

[27] Interview, Dr. Presley McGarry, Peace and War Center, Norwich University.

Annex B: CRC Composition



References

Aleksejeva, Nika , et al. “Operation Secondary Infektion.” Atlantic Council, 22 June 2019, www.atlanticcouncil.org/in-depth-research-reports/report/operation- secondary-infektion/.

Andrew, Christopher. *The Secret World: A History of Intelligence*. London, Penguin Books, 2019.

Bing, Christopher, and A.J. Vicens. 2024. “Iranian Hacker Group Aims at US Election Websites and Media before Vote, Microsoft Says.” Reuters. October 23, 2024. https://www.reuters.com/technology/cybersecurity/iranian-hacker-group-focuses-us-election-websites-media-ahead-vote-microsoft-2024-10-23/.

Brangetto, P., & Veenendaal, M. (2016). “Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations.” https://ccdcoe.org/uploads/2018/10/Art-08-Influence-Cyber-Operations-The-Use-of-Cyberattacks-in-Support-of-Influence-Operations.pdfggeutte

Cook, Sarah. 2019. “China Central Television: A Long-Standing Weapon in Beijing’s Arsenal of Repression.” Thediplomat.com. September 25, 2019. https://thediplomat.com/2019/09/china-central-television-a-long-standing-weapon-in-beijings-arsenal-of-repression/.

Dehghan, Saeed Kamali. 2018. “Who Is the Iranian Group Targeted by Bombers and Beloved of Trump Allies?” The Guardian. The Guardian. July 2, 2018. https://www.theguardian.com/world/2018/jul/02/iran-mek-cult-terrorist-trump-allies-john-bolton-rudy-giuliani.

Fittarelli, Alberto. 2024. “PAPERWALL: Chinese Websites Posing as Local News Outlets Target Global Audiences with Pro-Beijing Content - the Citizen Lab.” The Citizen Lab. February 7, 2024. https://citizenlab.ca/2024/02/paperwall-chinese-websites-posing-as-local-news-outlets-with-pro-beijing-content/.

Gillett, Francesca. 2025. “German Spy Agency ‘Believed Covid Likely Started in Lab.’” Bbc.com. BBC News. March 13, 2025. https://www.bbc.com/news/articles/cz7vypq31z7o.

Google Threat Intelligence Group. 2024. “Seeing through a GLASSBRIDGE: Understanding the Digital Marketing Ecosystem Spreading Pro-PRC Influence Operations.” Google Cloud Blog. Google Cloud. November 22, 2024. https://cloud.google.com/blog/topics/threat-intelligence/glassbridge-pro-prc-influence-operations.

Greig, Jonathan. 2024. “Google Takes down Fake News Sites, Wire Services Run by Chinese Influence Operation.” The Record. Recorded Future. November 22, 2024. https://therecord.media/google-fake-news-china-outlets.

Insikt Group. 2022. “CYBER THREAT ANALYSIS Ghostwriter in the Shell: Expanding on Mandiant’ S Attribution of UNC1151 to Belarus.” Recorded Future.

Janofsky, Adam. 2023. “Pro-China Information Campaign Used Fake Websites to Spread Propaganda: Mandiant.” The Record. Recorded Future. January 11, 2023. https://therecord.media/pro-china-information-campaign-used-fake-websites-to-spread-propaganda-mandiant.

Kuznia, Rob, Scott Bronstein, Drew Griffin, and Curt Devine. 2020. “Weird Science: How a ‘Shoddy’ Bannon-Backed Paper on Coronavirus Origins Made Its Way to an Audience of Millions.” CNN. October 21, 2020. https://edition.cnn.com/2020/10/21/politics/coronavirus-lab-theory-yan-bannon-invs/index.html.

Mandiant. 2022. "HaiEnergy Information Operations Campaign | Inauthentic News." Google Cloud Blog. Google Cloud. August 4, 2022. https://cloud.google.com/blog/topics/threat-intelligence/pro-prc-information-operations-campaign-haienergy/.

Mandiant Threat Intelligence. 2022a. "Pro-PRC DRAGONBRIDGE Influence Campaign Targets Rare Earths Mining Companies in Attempt to Thwart Rivalry to PRC Market Dominance | Mandiant."

Google Cloud Blog. Google Cloud. June 28, 2022. https://cloud.google.com/blog/topics/threat-intelligence/dragonbridge-targets-rare-earths-mining-companies.
———. 2022b. "Service Not Allowed." Google.com. Google Cloud. July 26, 2022. https://cloud.google.com/blog/topics/threat-intelligence/prc-dragonbridge-influence-elections/.

Nie, Jing-Bao. 2020. "In the Shadow of Biological Warfare: Conspiracy Theories on the Origins of COVID-19 and Enhancing Global Governance of Biosafety as a Matter of Urgency." *Journal of Bioethical Inquiry* 17 (4). https://doi.org/10.1007/s11673-020-10025-8.

Nimmo, Ben, Camille François, Shawn Eib, and Léa Ronzaud. 2020. "Spamouflage Goes to America Pro-Chinese Inauthentic Network Debuts English-Language Videos." *Graphika*. Graphika. https://public-assets.graphika.com/reports/graphika_report_spamouflage_goes_to_america.pdf.

Paul, Ari. 2025. "Lab Leak: The Official Conspiracy Theory That Still Gets You Credit as a Free Thinker." FAIR. April 18, 2025. https://fair.org/home/lab-leak-the-official-conspiracy-theory-that-still-gets-you-credit-as-a-free-thinker/.

Serabian, Ryan, and Lee Foster. 2021. "Pro-PRC Influence Campaign Expands to Dozens of Social Media Platforms, Websites, and Forums in at Least Seven Languages, Attempted to Physically Mobilize Protesters in the U.S." Google.com. Google Cloud. September 7, 2021. https://cloud.google.com/blog/topics/threat-intelligence/pro-prc-influence-campaign-expands-dozens-social-media-platforms-websites-and-forums/.

Stubbs, Jack, Léa Ronzaud, Kyle Weiss, Avneesh Chandra, Rodrigo Ferreira, and Ira Hubert. 2021. "Likes for Lorestan Unravelling a Decade of Iran-Linked Information Operations Targeting Domestic Audiences and International Critics Executive Summary." *Graphika*. Graphika. https://public-assets.graphika.com/ reports/graphika_report_likes_for_lorestan.pdf.

Sweetman, Cassandra. 2020. "'Vote for Trump or Else': Oklahoma Student Describes 'Horrifying' Fake Proud Boys Email She Received." KSN-TV. October 22, 2020. https://www.ksn.com/news/vote-for-trump-or-else-oklahoma-student-describes-horrifying-fake-proud-boys-email-she-received/.

United States v. Seyed Mohammad Hosein Mousa Mazemi and Sajjad Kashian (US District Court Southern District of New York, November 18, 2021), https://www.justice.gov/d9/press-releases/attachments/2021/11/18/u.s._v._seyyed_mohammad_hosein_et_al_signed_indictment_redacted.pdf

Zeynep Tufekci. 2025. "Opinion | We Were Badly Misled about Covid." The New York Times, March 16, 2025. https://www.nytimes.com/2025/03/16/opinion/covid-pandemic-lab-leak.html.

The Richard S. Schultz '60 Symposium Fellowship was established in 2017 as an endowed fund in honor of "Dick" by his wife of fifty years, Myrna L. Schultz, their children, Marni and Alan, and his classmates and friends.

The fellowship enables Norwich undergraduates, from any academic discipline, the opportunity to pursue areas of inquiry and experiences that will promote and expand their understanding of the past and how it impacts the present and future. Through research, travel, and inquiry the Schultz Fellow and faculty advisor will offer perspectives for us to face the future with better understanding and confidence.

After a wide solicitation and competitive selection process, this annual fellowship is granted by the Norwich University Peace & War Center to an undergraduate student for a single project that may involve additional Norwich undergraduate students. The award includes a $3,500 grant.

NORWICH™
UNIVERSITY

Norwich.edu