

INFORMATION WARFARE:

The **meme** is the **embryo** of the
narrative **illusion**



JAMES SCOTT

INFORMATION WARFARE:

The Meme is the Embryo of the Narrative Illusion

by

JAMES SCOTT



Except for (1) brief quotations used in media coverage of this publication, (2) links to the www.icitech.org website, and (3) certain other noncommercial uses permitted as fair use under United States copyright law, no part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher. For permission requests, contact the Institute for Critical Infrastructure Technology.

INFORMATION WARFARE: The meme is the embryo of the narrative illusion

Copyright © 2018 Institute for Critical Infrastructure Technology

ALL RIGHTS RESERVED. This book contains material protected under International and Federal Copyright Laws and Treaties. Any unauthorized reprint or use of this material is prohibited. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system without express written permission from the author/publisher.



SUPPORT ICIT

Information should be liberated, not commoditized.

This powerful philosophy is the bedrock of the Institute for Critical Infrastructure Technology (ICIT), a nonprofit, nonpartisan 501(c)(3) cybersecurity think tank located in Washington, D.C. Through objective research, publications and educational initiatives, ICIT is cultivating a global cybersecurity renaissance by arming public and private sector leaders with the raw, unfiltered insights needed to defend our critical infrastructures from advanced persistent threats, including cyber criminals, nation states, and cyber terrorists.

Financial capital from generous individual and corporate donors is the lifeblood of the institute and a force multiplier to our efforts. With your support, ICIT can continue to empower policy makers, technology executives, and citizens with bleeding-edge research and lift the veil from hyper-evolving adversaries who operate in the dark. Together, we will make quantum leaps in the resiliency of our critical infrastructures, the strength of our national security, and the protection of our personal information.

Dedication

To my precious sons Liam and Nigel, there is a battle raging by an invisible collective, a criminal enterprise whose agenda is to construct an artificial universe of foreign ideas in your minds. Our Nation is under attack by dragnet surveillance propagandists who censor every conceivable layer of digital content you read in order to enforce the illusion of freedom of choice. Think before you click, believe none of what you hear and half of what you see. Protect the sanctity of your mind. Refuse to participate in the psychological tug of war that is the most potent ingredient in the algorithms of Google, Facebook, Twitter and YouTube. Trace your ideas back to their embryonic introduction to your mind, many of these thoughts, as you will find, are little more than memetically introduced illusions by malevolent forces with ill intent. Your perceptions, your beliefs, your spirituality, your political ideas and dare I say your very freedom are all being targeted by multi-vector influence operators with an infinite number of agendas. I give you this book as a manual to weaponize your minds. I'm giving you this process so that you can recognize it when you encounter it and fight it when you can. Emancipate your mind from the matrix that is constructed by the narrative illusion so that you can carry on the Great Work.

TABLE OF CONTENTS

.....

ABSTRACT	1
INTRODUCTION	3
DIGITAL INFLUENCE OPERATIONS (DIO)	4
AN INTRODUCTION TO MEMETICS	8
Mememes are the Building Blocks of Perceived Reality	8
The Lifecycle of the Meme	9
Criticism of Memetic Theory Does Not Apply to Digital Influence Operations	10
TARGETING THE CORE AUDIENCE	12
Spiral Dynamics	12
Cognitive Biases Assist in Engineered Memetic Responses	13
Bias 1: Reward/Punishment Super-Response Tendency.....	13
Bias 2: Liking/Loving Tendency.....	13
Bias 3: Disliking/Hating Tendency.....	13
Bias 4: Doubt/Avoidance Tendency.....	13
Bias 5: Inconsistency-Avoidance Tendency.....	14
Bias 6: Curiosity Tendency.....	14
Bias 7: Kantian Fairness Tendency.....	14
Bias 8: Envy/Jealousy Tendency.....	15
Bias 9: Reciprocation Tendency.....	15

Bias 10: Influence-From-Mere Association Tendency.....	16
Bias 11: Simple, Pain-Avoiding Psychological Denial Tendency.....	16
Bias 12: Excessive Self-Regard Tendency.....	16
Bias 13: Over-Optimism Tendency.....	17
Bias 14: Deprivation Super-Reaction Tendency.....	17
Bias 15: Social-Proof Tendency.....	17
Bias 16: Contrast Mis-Reaction Tendency.....	18
Bias 17: Stress-Influence Tendency.....	18
Bias 18: Availability Misweighing Tendency.....	19
Bias 19: Use-It-or-Lose-It Tendency.....	19
Bias 20: Drug Misinfluence Tendency.....	19
Bias 21: Senescence Misinfluence Tendency.....	19
Bias 22: Authority Misinfluence Tendency.....	19
Bias 23: Twaddle Tendency.....	20
Bias 24: Reason-Respecting Tendency.....	20
Bias 25: Lollapalooza Tendency.....	20
Socionics.....	21
Identical Relations.....	21
Relations of Duality.....	21
Relations of Activity.....	21
Mirror Relations.....	22
Relations of Semi-Duality.....	22
Comparative Relations.....	22
Conflicting Relations.....	22
Super-Ego Relations.....	23
Quasi-Identical Relations.....	23
Illusionary Relations.....	23
Lookalike Relations.....	23
Relations of Benefit.....	24
Relations of Supervision.....	24
Psychographic Big Data Algorithms.....	24
Predictive Analytics.....	25
Information Processing.....	25
Different Paths of Persuasion for Different Purposes.....	25
Psychological Profiling Concepts Used in Memetic Design.....	27
Normalization.....	27
Participatory Politics in the Digital Age.....	27
Belief Perseverance.....	27

False Consensus.....	28
Self-Serving Biases.....	29
Self-Handicapping.....	29
Priming.....	30
Spontaneous Trait Transference.....	31
Groupthink.....	31
Belief Distortion.....	31
Group Polarization.....	31
Fundamental Attribution Errors.....	32
Hindsight Bias.....	32
Illusion of Control.....	32
Illusion of Transparency.....	32
Indoctrination.....	32
Color Psychology.....	34
Illusory Correlation.....	34
Collectivism.....	35
Complementarity.....	35
Confirmation Bias.....	35
Counterfactual Thinking.....	36
Dispositional Attribution.....	36
Cognitive Dissidence.....	36
Deindividualization.....	37
Displacement.....	37
Altruism.....	37
Immune Neglect.....	37
Illusion of Self-Analysis.....	37
Framing.....	38
Attitude Inoculation.....	38
Impact Bias.....	39
Behavioral Confirmation.....	39
Bystander Effect.....	39
Catharsis.....	39
Logical Fallacies Shape Troll and Bot Responses.....	40
Fallacy 1: Strawman.....	40
Fallacy 2: Loaded Question.....	41
Fallacy 3: Composition/Division.....	41
Fallacy 4: Begging the Question.....	41
Fallacy 5: The Texas Sharpshooter.....	41

Fallacy 6: False Cause.....	41
Fallacy 7: Ad Hominem.....	41
Fallacy 8: Bandwagon.....	41
Fallacy 9: No True Scotsman.....	41
Fallacy 10: Appeal to Nature.....	42
Fallacy 11: Middle Ground.....	42
Fallacy 12: Appeal to Emotion.....	42
Fallacy 13: Personal Incredulity.....	42
Fallacy 14: The Fallacy Fallacy.....	42
Fallacy 15: Slippery Slope.....	42
Fallacy 16: Tu Quoque (You Too).....	42
Fallacy 17: Personal Incredulity.....	43
Fallacy 18: Special Pleading.....	43
Fallacy 19: Burden of Proof.....	43
Fallacy 20: Ambiguity.....	43
Fallacy 21: Appeal to Authority.....	43
Fallacy 22: Genetic.....	43
Fallacy 23: Black-or-White (False Dilemma).....	44
Fallacy 24: Anecdotal.....	44
GUERRILLA TOOLS, TECHNQUES, PROCEDURES.....	45
Tools.....	45
Kali Linux.....	45
Maltego.....	46
Metasploit.....	46
Audible Stimuli.....	46
Political Correctness.....	47
Fake News.....	48
Unauthorized Access to Information.....	48
False Flag Cyberattacks.....	48
Distributed Denial of Service (DDoS) Attacks.....	49
Website Defacements.....	49
Doxing.....	50
Swatting.....	50
Social Media Platforms.....	51
Account Weaponization.....	51
Public Messaging Platforms.....	51
Image Board Sites.....	52

Professional Networking Sites.....	53
Message Board Sites.....	54
Communal Networking Platforms.....	55
Audio Distribution Platforms.....	57
Live Stream Services.....	57
Dating Applications.....	57
Bots.....	58
Friendster Bot.....	58
Random Comment Bot.....	58
Chatbots.....	58
‘The Optimizer’.....	58
‘The One-Trick Pony’.....	58
‘The Proactive’.....	59
‘The Social’.....	59
‘The Shield’.....	59
Propaganda Bots.....	60
THE ‘GUERRILLA’ OPERATOR’S COOKBOOK.....	62
THREAT ACTORS.....	65
China.....	65
The Three Warfares.....	68
The ‘50 Cent Party’.....	71
China’s Influence Abroad.....	74
Russia.....	77
Digital Maskirovka.....	77
The Internet Research Agency.....	78
Hail-Mary Threats.....	80
Propaganda from the Pulpit.....	81
Ideological Domestic Terrorists.....	82
Digital Terrorists.....	86
Dragnet Surveillance Propagandists.....	86
CONCLUSION.....	88
SOURCES.....	89

ABSTRACT

Cogito ergo sum (I think, therefore I am), but who does one become when the thought is hijacked? We are no longer a society ruled by geographic lines in the sand laid by men who won and lost wars 50 years ago. Rather, we are a society governed by ideological variation, led by chieftains in a digital tribal society. This is the new world order and the precise opposite of what the self-proclaimed elites had planned. The United Nations is no more relevant than Facebook. The new covert is overt. WikiLeaks is more in the know than an intelligence analyst in the CIA, and Google's dragnet surveillance censorship algorithm has become the new gatekeeper of critical information that could lead society into a new renaissance. The power shift has gone from a focus on kinetic controls to an all-out battle for the psychological core of the global population. Digitized influence operations have become the new norm for controlling the electoral process, public opinion, and narrative.

The potency of the actors in this space is fierce. Both nation-states and special interest groups in every conceivable variation are battling for the pinnacle position in controlling the public narrative, and though there are many initiatives operating in this space, few understand the actual process for harnessing a consistent grip on the narrative in this digital age. While most actors attempt to use archaic relics, such as the mainstream media, nation-states and sophisticated special interests are gunning for the almighty meme. The meme is the embryo of the narrative, and there is a process to harnessing its potency. Ideas are the composition of memes. Belief systems are the composition of ideas. Belief systems and their reinforcement create the narrative. Control over the meme renders control of the narrative; thus, he who controls the meme controls the population. Therefore, the objective is not to focus on control of the narrative; rather, the hyper-focus has become the creation, mutation, expansion, and replication of the meme.

The mind is the new war space, and the meme is both a subliminal hand grenade and the new nuclear weapon. Psychographic targeting renders the expedience of parasitically embedding the meme within the vast labyrinth of

"Your ideas are bound to forces of which you have no control due to the fact that you've voluntarily submitted your freedom of thought to the perception steering censorship of dragnet surveillance capitalists."

...

"First and foremost, the most profound weapon a nation or special interest can possess is 'control' over information. This contributes to control over the narrative and the meme is the embryo of the narrative. Information warfare begins and ends with the meme."

the mind. Psychographic targeting is made easy via big data analytics, the treasure troves of readily available metadata curated by dragnet surveillance capitalists, and a legislative body that lacks the understanding of the dangers of its weaponization. Metadata layered with the weaponization of other digital vectors, such as search engine results, social media, banner placement, blogs, and bots infused with machine learning and artificial intelligence, can introduce, mutate, and expand memes and conversations out of thin air that can instantaneously become part of the mainstream narrative.

Forums, blog comments, hashtags, and YouTube videos have replaced the mainstream media, and the mainstream media has submitted to its position as the automaton regurgitators of the narrative that was introduced by the meme. The meme is the central character in digital influence operations (DIO), and DIO is the ingredient that fuels the new war space as well as the common thread of potency in political warfare, propaganda, and information warfare. The formula is quite simple: Control the meme; control the narrative; and control who is elected to office, how the public perceives current events, and the introduction of a new military offensive. Combined with cyber vectors for distribution, the meme renders an infinite number of variations for an attack. This new frontier harnesses the bleeding-edge technologies and strategies of machine learning, deep learning, socionics, artificial intelligence, cognitive biases, spam bots, memetics, and the psychographic zeroing in on population sub-groups using metadata with the further targeting capabilities that define national and population subgroups' evolution stage by enlisting concepts such as spiral dynamics, and this is just the tip of the iceberg. This book will cover the DIO space and the use of the meme in this information war.

...

“Your fears are illusions, your excuses are lies, and your personal narrative has been hijacked by the Corporate Nation State censorship collective who custom tailor your digital hallucination with their toxic brand of propaganda.”

...

INTRODUCTION

Influence operations are weaponized stories. Manipulation of the fundamental ideologies and behaviors of a target population depends on the construction of a complex narrative that is capable of taking on a life of its own, and it can indoctrinate and inspire evangelization of members of the population so that a meme can mutate and propagate without necessitating additional resource expenditure. Without understanding socionic intertype relations, behavioral bias, psychographic targeting, and spiral dynamics, a threat actor does not have the optimized targeting necessary for a campaign because they do not understand their audience or how to best frame the narrative. Without an understanding of the attack vectors, they do not understand the potentiality of what can be weaponized or how to best deliver the story in a believable and dynamic way that bypasses mental defenses and ingrains itself in the collected cultural consciousness. Finally, without understanding memetics, they do not understand the embryonic state of the narrative; they do not know how to construct and deconstruct a story according to its most fundamental building blocks to gain absolute control over the understanding, acceptance, response, mutation, and propagation of the information.

An advanced memetic threat is that which is planned with the desired outcome, weaponized and distributed over digital vectors and enhanced by artificial intelligence and machine learning-infused spam bot technology. By reading this book, you are being introduced to a new narrative of which you are welcome to come into and contribute. Every word of the conversation we have later about this will possess its own unique signature and personal narrative. The narrative mutates and expands, then mutates and expands again, and so on. Your mind will introduce a new layer to your narrative, reshaping that which was there before you were introduced the narrative within this text.

...

“In the United States there is a unique blend of patriotism indoctrination via ‘propaganda from the pulpit’ which blends establishment controls into religious ideology. This way, to question the establishment is to question God, therefore one’s patriotism and salvation are contingent on their submission to the state.”

...

DIGITAL INFLUENCE OPERATIONS

Information warfare uses “means and methods of imparting information to achieve the objectives of the attacking side.” These include intelligence, counterintelligence, disinformation, electronic warfare, deceit, debilitation of communications, degradation of navigation support, psychological pressure, information systems, and propaganda [1]. Distributed denial of service attacks (DDoS), advanced exploitation techniques, and foreign media outlets all facilitate a foreign agenda in this context. From this perspective, using intrusive DIOs as part of a broader influence operations strategy makes perfect sense. Operations campaigns are tailored to sow doubt and confusion to undermine trust and confidence in the governments of targeted nations. Given the limited possibilities for attribution and the absence of any real threat provoking an armed (or any kind of) response, DIOs are low-risk, low-cost capabilities that can contribute to an adversary’s destabilization. The problematic nature of the attribution of cyberattacks ensures that it will remain unclear who is actually behind the attack, allowing for a certain degree of plausible deniability when the source of an attack has been determined [2].

Influence operations are an integral part of hybrid warfare, which is the coordinated overt and covert use of a broad range of instruments, military and civilian, conventional and unconventional, to make an ambiguous attack on another state. The objective of influence operations is exerting power by influencing the behavior of a target audience; the ability for “A to have B doing, to the extent that he can get B to do something that B would not otherwise do.” Influence operations are thus assumed to modify attitudes and shape opinions through the dissemination of information and conveying of messages. However, there are more intrusive ways to influence a specific audience that remain in the information realm but can no longer be regarded as the application of soft power, as they are no longer designed to achieve their objective solely through “attraction.” Cyberspace offers numerous possibilities for these kinds of coercive operations, which are designed to influence a target audience by changing, compromising, destroying, or stealing information by accessing information systems and networks. In principle, influence operations offer the promise of

*“Nietzsche said that
‘All great things must
first wear terrifying
and monstrous masks
in order to inscribe
themselves on the
hearts of humanity.’
Right now there is
a renaissance, an
awakening, we are
breaking the narrative
illusion, the mask,
that eats away at the
face.”*

...

*“Draagnet surveillance
capitalists became
Draagnet surveillance
propagandists and
are now a Corporate
Nation State
Censorship Collective.
The 2020 Elections are
up for grabs.”*

victory through “the use of non-military [non-kinetic] means to erode the adversary’s willpower, confuse and constrain his decision-making, and undermine his public support, so that victory can be attained without a shot being fired.” Intrusive cyber capabilities may be part of military operations. “Influence operations are the coordinated, integrated, and synchronized application of national diplomatic, informational, military, economic, and other capabilities in peacetime, crisis, conflict, and post-conflict to foster attitudes, behaviors, or decisions by foreign target audiences that further [a nation’s] interests and objectives.” The U.S. Department of Defense defines information operations as “the integrated employment, during military operations, of information-related capabilities in concert with other lines of operations to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting [its] own.” They include all the efforts undertaken by states or any other groups to influence the behavior of a target audience, in peacetime or during an armed conflict. It is an umbrella term for all operations in the information domain, including all soft power activities. Although influence operations are, in principle, non-violent, they can be part of military operations [2].

Hybrid warfare provides many opportunities for the use of cyber capabilities as one of the broad range of possible non-kinetic or non-violent options. If the main goal of political influence operations outside of an armed conflict is to destabilize and confuse adversaries, then it could be effective in attacking the opponent’s digital infrastructure to undermine trust by compromising, altering, and disrupting the digital services of both the government and the private sector through the use of malware. It is inevitable that the future of cyberwarfare will be as much about hacking energy infrastructure, such as power grids, as about hacking the minds and shaping the environments in which political debates occur [2].

Information warfare and influence operations are, in principle, intended to get your own message across or to prevent your adversary from doing so. It is not just about developing a coherent and convincing storyline, however, as it also involves confusing, distracting, dividing, and demoralizing the adversary. From that perspective, cyberspace seems to be ideal for conducting such operations that will have disruptive, rather than destructive, outcomes. The means through which influence can be exerted relies mostly on spreading information. There are more intrusive ways to influence specific audiences, however, that remain in the information realm but are designed to change, compromise, inject, destroy, or steal information by accessing information systems and networks [2].

With influence intrusive operations, it becomes necessary to separate the “apples” of information content from the “apple carts” of information systems. This is in line with Russian thinking on information warfare, which traditionally makes the distinction between “informational-technical” and “informational-psychological” activities. The semantic or cognitive actions (apples) consist mainly of attacks of information on information (typically narrative vs. narrative) that affects the semantic layer of cyberspace. In other words, these activities create a crafted informational environment. These content-oriented activities can be defined as inform and influence operations (IIOs) that we define as “efforts to inform, influence, or persuade selected audiences through actions, utterances, signals, or messages.” Strategic communications (STRATCOM) and propaganda activities fall under this category, as well as the deliberate dissemination of disinformation to confuse audiences [2].

Operations target the logical layer of unauthorized access to destroy, change or alter information. DIOs occur at the logical layer of cyberspace with the intention of influencing attitudes, behaviors, or decisions

of target audiences. DIOs are undertaken in cyberspace and qualify as cyberattacks. A cyberattack is “an act or action initiated in cyberspace to cause harm by compromising communication, information or other electronic systems, or the information that is stored, processed, or transmitted in these systems.” Harm includes physical damage and effects on information systems, including direct or indirect harm to a communication and information system, such as compromising the confidentiality, integrity, or availability of the system and any information exchanged or stored [2].

Influence operations focus on manipulating the psychology of targets through strategic communication, public affairs, inundation, or human-technology interfaces as a mechanism to alter their feelings, experiences, behavior, beliefs, or actions. These campaigns present a unique and pressing technical challenge, because they affect the logical or tactical layer of cyberspace but remain below the international legal threshold for armed conflict. Whether through hacking, disinformation, propaganda, or numerous other weapons, digital influence attacks alter, disrupt, or initiate the flow of data between two entities to achieve a strategic effect [2].

The greatest failure of strategic operations, whether psychological, kinetic, digital, or along any other vector, is the inability of the actor to impart a lasting impact on the behavior or ideology of the target at the culmination of the campaign. Too often, military and intelligence entities compartmentalize and focus on specific short-term objectives rather than exerting the effort to coerce the target to think or act differently in the future. Effective communication is about storytelling. Optimal influence operations disseminate content, deliver propaganda, and leverage multiple platforms, including social media, to affect the outlook, opinions, and actions of specific populations directly and indirectly according to their demographic and psychographic characteristics [2].

Perhaps the most profound characteristic of influence operations is the ease with which adversaries can launch attacks and succeed in modifying the thoughts or behaviors of particular audiences. Operations may consist of multiple layers; however, the majority of vectors do not require technical sophistication, skill, or overwhelming resources. The unsophisticated portions of the attack preclude any risk of escalation since many amount to defacements or the distribution of false or misleading data. Influence campaigns are extremely effective during both periods of peace and turmoil because they do not amount to an armed attack or cyber war and, even if the source is known, the attacks are difficult to respond to, whether or not the response is proportional. In most instances, various proxies are employed to obscure attribution and provide plausible deniability [2].

Coercive DIOs will become more prevalent in the near future, because they offer the opportunity to undermine an opponent’s credibility with little risk of escalation. The main attraction in the use of DIOs lies in that they are limited in scope and difficult to attribute, thereby limiting the risks of escalation and countermeasures. This is especially reflected in the Russian approach to information warfare, which considers it an instrument of hard power. Issues of legality and transparency limiting the options for using DIOs remain, in principle, in Western democracies [2].

It is difficult to counter a DIO, since responding to them might result in a counterproductive outcome or be disproportionate and thus lead to escalation. The international law of state responsibility provides grounds to determine if a state has breached an obligation under international law (e.g., violation

of sovereignty, violation of the principle of non-intervention) in a way that would be deemed an internationally wrongful act. To identify such a violation, it is essential to determine whether a state exercised “effective control” over the group or organization in question. According to the stringent criteria defined by the International Court of Justice, it is difficult to relate many actions in cyberspace to a state, making the options to respond highly limited [2].

Given their effects, DIOs do not reach the level of an armed attack in the legal sense; that is to say, these activities may not prompt action in self-defense by the injured state, according to article 51 of the United Nations Charter. Given their low intensity, however, these attacks do not imply that there is a legal void. DIOs are difficult to grasp through the legal lens. The attraction of DIOs for states lies mainly in the fact that they are difficult to attribute and thus provide plausible deniability, else they provoke a strong or quick response from the target nation. The more target audiences and organizations become aware of the need for adequate protection of their digital infrastructure and the limited long-term impact of cyberattacks, the less useful they will become. Most DIOs do not require significant technical capabilities because they exploit vulnerabilities in the human psyche and configuration flaws in “low-hanging fruit” networks. IO campaigns can fuel an already existing sense of insecurity and thereby support the overall narrative of the campaign. A study conducted by Chapman University showed, for instance, that Americans fear a cyber-terrorist attack more than a physical terrorist attack. This indicates that an adversary can exploit the fear of the unknown, whether that fear is realistic or mostly imaginary [2].

...

“Cultural Marxism, now called ‘Political Correctness’ is a loaded gun that one puts to their own head. The narrative illusion normalizes the abnormal and is an elitist weapon over minions for citizen vs citizen policing for establishment control.”

...

AN INTRODUCTION TO MEMETICS

Manufacturing consent begins by weaponizing the meme and utilizing the censorship algorithms of Google, Facebook, Twitter, and YouTube. A fully weaponized meme is culturally transformative, and it is many things simultaneously. It's a combination of smoke and mirrors, illusions, and lies hidden between facts. The meme is the doctored photo of the crystallization of sweat on the protester's brow at a riot that never happened. It's that idea begging to be expressed in any other mechanism but words. It's the full arsenal of loaded weapons in the anarchist's revolution. It's about tapping into the emotional component of an idea that can spark a revolt. It's about using language, images, and colors to alter the natural state of one's psychology. After a meme proves to be successful, it then comes down to weaponizing all digital vectors for its distribution, mutation, and replication into the neural pathways of the targeted digital tribes so it becomes part of their culture. Meme warfare succeeds when ineffective memes fail as quickly as possible so that one successful meme can be developed, digitally rooted, and organically spread virally; this cycle is repetitive and continuous for the life of the campaign.

MEMES ARE THE BUILDING BLOCKS OF PERCEIVED REALITY

First and foremost, the most profound weapon a nation or special interest group can possess is "control" over information. This contributes to control over the narrative, and the meme is the embryo of the narrative. A meme is a unit of information used to convey part or the entirety of an idea, behavior, practice, style, or feeling between individuals who share a level of understanding based on culture, religion, or ideology. [3]. As a unit, the meme is a piece of thought conveyed between two entities, regardless of whether the thought contains others inside it or is itself a layer in a more robust meme. A meme is a unit of information, but it is not necessarily atomic or quantized. Some ideas can be dissected into smaller units, while others cannot. In some cases, it is situational. As Susan Blackmore explains, the first four notes of Beethoven's Fifth Symphony are an extremely recognizable audio meme, and other notes may not be as recognizable, yet the symphony itself is still a meme [4]. A linguistic meme could range from a single syllable to an entire speech in which that unit occurred, provided that some hosts retain an association of analogous understanding. If you recall the Gettysburg address whenever the phrase "fourscore" is communicated, then you possess that memetic association. Similar associations apply to slang (i.e., "lol"), words, symbols, sounds, and images.

Meme transmission is based on the conveyance of one or more ideas to the senses of a target host via photons, sound waves, tactile interaction, or other senses [4]. Memes can be transmitted via symbols, writing, images, sounds, actions, or any other mechanism through which information can be transferred

intentionally or unintentionally between parties. Memes are often considered analogs to genes because memes self-replicate, respond to selective pressure, and mutate [4]. They evolve in culture and across user platforms according to natural selection. Memorable, ubiquitous, relevant, and pervasive memes outlive those that fail to resonate with their target audience. Successful memes spread virally among users and communities. As the adoptive audience widens, the meme begins its “reproductive process,” in which it mutates, experiences variation, faces competition, and inherits the dominant traits of other successful units. The adoptive audience or hosts become infected with the underlying idea or message of the meme. They propagate it to new users or audiences. Meme propagation, replication, mutation, and survivability are proportional to their pervasiveness, invasiveness, and resonance in the memory of their hosts. Derivative or boring units will go extinct, while successful memes will replicate and mutate, regardless of the will of the host and regardless of whether they prove detrimental to the welfare of the host [4].

Memetics is the study of the conceptualization and transmission of memes according to an evolutionary model [4]. Richard Dawkins, the originator of the term “meme,” postulated that for memes to evolve, they had to be subject to new conditions, have the capacity to replicate in part or whole, and express differential “fitness,” in which differing memes excel or fail under differing conditions. Over time, memes evolve and compound into collectives referred to as memeplexes, such as cultural or political doctrines or systems [4]. Memeplexes consist of memes and meme groups, but operate and evolve as a single unit. Memes within the memeplex “piggyback” on the success of the memeplex [4].

Critics challenge whether memes can be studied academically or empirically based on the relative immeasurability of how well a discrete unit conveys an idea to an individual host or how much influence the originator has over the mutation and transmission of the meme [4]. For memetic weaponization in influence operations, these critics’ concerns are not applicable. As with other forms of social engineering, with even a modest victim pool, a success of even a fraction of a percent can be enough to enable the adversary to further their campaign. Consider, if a threat actor’s lure is seen by 100,000 social media users, but only 500 of those users respond, then the campaign may still be successful if they inspire the host to any action. If 500 users share a provocative meme, then each may indoctrinate others, invoke community divisions, replicate the meme on other platforms, or mutate the meme to increase its virility. Even with a generous failure rate (i.e., the meme expires or has no effect), the exponential spread ensures that memes that do not fail immediately may continue to replicate and mutate for a considerable time with no additional input of resources from the adversary. In effect, every meme has the chance to become a self-replicating, self-mutating, and automatically adjusting virus in the minds of a psychographically or demographically targeted population.

THE LIFECYCLE OF THE MEME

The creation, distribution, and perpetuation of memes consume very few adversarial resources. With minimal additional effort, a threat actor can retail or deploy a novel or mutated meme to replace an ineffective one, or it can inject the meme into a different environment to determine whether it will spread to a new community. The memetic lifecycle is governed by retention and transmission. The more confrontational or memorable a unit, the greater the likelihood it will embed in the host and propagate. Every like, share, description, confrontation, or derivative inspired by a meme perpetuates its life. Once the idea has taken hold, it is difficult to displace unless a competing meme is more persuasive and more influential. Even then, an idea is difficult to eliminate once the seed has been planted. After

information is learned, even seemingly trivial data, the brain forms distinct neural pathways, and every time the host requests information on a topic, their neurons attempt to follow those pathways so long as they remain even partially active. Even if they learn the information differently or learn new data that alters their perception or analysis of the information, their mind will occasionally provide them with the memetic information. Those notions may modify behaviors, inform opinion, or otherwise influence individuals in unpredictable and undesired ways. In a broad sense, exemplary successful memes are the reason many retain a periodic fear of the dark even in adulthood, why countless individuals share the same clichéd cultural nightmare of “going to school in their underwear,” and why numerous conspiracy theories and urban legends survive despite overwhelming refuting evidence. Resilient neural pathways that remain active even after retraining and additional learning are dominant factors in why some people continuously make the same mistake; why students have difficulty learning and retaining material that was not effectively communicated initially; and why most adults can remember the layout of their childhood home, even though they may not have been there for decades.

Memes are often compared to genes; however, the former displays both Darwinian and Lamarckian traits. Darwinian replication can be approximated as “copying according to a specific set of instructions,” while Lamarckian replication is “copying the product.” Memes inherit from previous successful iterations and replicate as an inference, rather than an exact copy. As a result, simple skills such as writing or homebuilding can iteratively develop based on past successes or failures. Viewers can learn by example, rather than accurate or precise understanding [4].

Memes replicate vertically from parent to child and horizontally between hosts. Replication can occur through transmission or imitation. Furthermore, memes, as units of information, can be communicated directly or indirectly, as well as retained intentionally or unintentionally. Even behavioral memes, such as waving, or empathetic memes, such as feelings or moods, may seamlessly transfer between hosts. Some have likened memes to “thought contagions” [4]. Academics have noted several patterns of meme transmission. Ideas that directly or indirectly perpetuate the meme or facilitate the transmission of derivatives are replicated more than adverse ones (i.e., an idea is more difficult to cull than to spread). Separation effects, such as “ideological bubbles” or cultural separation barriers, are prime examples. Memes may also horizontally spread via proselytism – an attempt at indoctrination or conversion – as is often the case with religious, political, or ideological indoctrination. Primal humanity retains a sense of tribalism and vindication via aggression; consequently, memes may transmit because they encourage or enable attacks on ideological adversaries or their underlying beliefs. Some memes survive simply because they are memorable or interesting. These cogent units are transmitted, often without imitation or mutation, and may not self-replicate according to memetic theory. Finally, many memes spread through hosts’ desire for them to be true, factual, or known. The perpetuation of these “motivational” units is contingent on the self-interests of their adopters. Though “motivational” memes do not self-propagate, they are transmitted, and in some cases, their memetic impact may be the most significant as hosts replicate, mutate, or invent other memes to support or defend the “motivational” meme [4].

CRITICISM OF MEMETIC THEORY DOES NOT APPLY TO DIO’S

Critics often contend that memes lack quantization, or the absolute guarantee to convey the intended information, and have the same distinct impact on multiple hosts regardless of environmental context.

Academic debates on the validity of the study of memetics as science are outside the scope of this work. Whether memetics is a proto-science or a pseudoscience does not matter when analyzing strategic threat actor campaigns, because both the actor and the analyst are operating from the same frame of reference; a meme is a unit of information that, on its own or in combination with other memes, has the potential to influence the thoughts or actions of a specific or general target when transmitted, replicated, or mutated. For the purposes of adversarial influence operations, these inconsistencies in the nature of memes may be more of a boon to adversarial influence operations than a disadvantage. Memes do not have to be “culturgens” [4]. Threat actors do not intend to convey cultural information accurately or precisely. They operate to sow the seeds of division and fan the flames of chaos. Memes that are divulged from the parent to incite community divisions or misinform the populace are deemed successful by strategic influence architects. The excessive instabilities in memetic reception and perpetuation only intensify the potential harm an attacker can inflict with a meme. Propagandists from Russia, China, and other nations typically pander memes to both sides or multiple factions of sensitive conflicts in an attempt to breed discord, capitalize from chaos, derail productive discussion, distract impending investigations, dwindle valuable resources, or polarize susceptible populations. When Russian operatives weaponized memes on social media to influence the outcome of the 2016 presidential election, they did not have to control whether their anti-Clinton ad enraged a liberal or whether their pro-Trump ad disenfranchised a Republican, because those seemingly adverse outcomes were still desirable. Any outcome other than inaction or ignorance is favorable to an adversarial influence campaign, because once enough users are affected even minutely, the actor can adjust or tailor the meme to be more influential on the target population. Using victim response demographic and psychographic metadata (such as that collected and sold by social media platforms), the attacker can create or adjust memes capable of conveying specific ideas consistently, eliciting precise responses, or mutating along certain trajectories. As adversaries collect more audience response metadata from their bots, ads, or social media capitalists turned propagandists, they gain more control over the variables governing meme transmission, retention, longevity, and influence.

...

“The infowar and psyops game has been transformed & we are no longer dropping leaflets from helicopters over Vietnam saying ‘America Is Your Friend’. This is now a battle to defend the psychological core of the population in order to save this fledgling democracy.”

...

TARGETING THE CORE AUDIENCE

Effective foreign influence operations are not ad hoc. To achieve optimal impact with minimal resource expenditure, threat actors combine socionic, behavioral, and psychological vulnerabilities with cyber-guerrilla tools, techniques, and procedures to influence the population or populations whose altered mindset will sway the collective consciousness of society. Influence operations are layered attacks whose design begins with spiral dynamics and advances to the applications of technical tools on digital platforms.

SPIRAL DYNAMICS

Spiral dynamics combines aspects of social, cognitive, developmental, and organizational psychology to deliver high-level insights into the culture, behavior, and values of a population segment. The hierarchical evolutionary stages map how people think and why they adopt the values that they do. It is often used in discussions of leadership, conflict management, organizational change, communication and marketing, and cultural forecasting. For instance, those at the beige evolutionary level, such as children, focus on personal needs and survival. The purple tribal level revolves around community or familial survival. This tier also captures aspects of spiritual communities in which the members alter their behavior out of fear of condemnation and ostracism. Those at the red level stand out from the rest of the group and are often regarded as leaders. Blue communities focus on larger issues such as civilization, laws, rules, and territorial boundaries. Leaders through achievement populate the orange level, from which they tend to dictate the actions of the lower levels. Individuals who have met their goals and transcended to altruism and holistic global concerns reside at the green level. Finally, thought leaders who can communicate effectively with different levels and weight the value of the input of various tiers on a particular issue are at the yellow level.

Because it focuses on how individuals and populations conceptualize worldviews and internalize information, the levels of spiral dynamics can be employed to launch tailored and precise psychological targeted attacks against specific individuals and niche communities and evoke a predictable and desired response from the attacks. Adversaries can craft their social media lures, misinformation, and fake news according to their target's life conditions, mental capacities, economic status, education level, political beliefs, sense of tribalism, sense of family, religion, or any number of other factors. Each additional "filter" decreases the victim pool but increases the success rate of compromising the desired victims.

COGNITIVE BIASES ASSIST IN ENGINEERED MEMETIC RESPONSES

BIAS 1: Reward/Punishment Super-Response Tendency

Incentives and disincentives can shape the outlook and performance of a population, especially if the targets do not recognize the influence or understand the power of the leverage on their mental faculties. Appeals to interests, curiosity, dispositions, and other emotional stimuli are more persuasive than reason and facts, because the latter often do not reward the target personally. Facts are independent of feelings and those who operate based on sympathy, empathy, gratification, or other motivators. Adverse behaviors can quickly become normalized habits when rewarded with recognition or when positive behavior is punished, such as with ridicule or criticism [5].

BIAS 2: Liking/Loving Tendency

Humans are unique in their ability to rationalize and self-rationalize [6]. No other being is as susceptible to internal self-deception based on stimuli generated from preconceived notions of external entities. People tend to ignore the faults and flaws of other people, products, or companies, either partially or wholly, if they feel a sense of liking, admiration, or love for that individual. When seen through rose-tinted lenses, red flags appear as ordinary flags. Feelings of adoration cause the enchanted to disregard their qualms and comply with the wishes or adopt the viewpoint of the object of their affection unquestioningly. Associated persons and ideologies are likewise elevated in the regard of the influenced. Facts become distorted by the desire for the venerated to meet or exceed the expectations of the target population [5].

BIAS 3: Disliking/Hating Tendency

The contrapositive of the liking/loving tendency also holds true. People tend to ignore the virtues, views, and arguments of those who they dislike or oppose, even if the arguments of the opposition are correct factually. Throughout the interaction, the memetic filter of “us vs. them” and social conflict results in a distorted interpretation of the tone and facts provided by those diametrically opposed to the zeitgeist of the influenced subject. Associated organizations, individuals, memes, and ideologies are disliked, distrusted, and vilified because of their association with the hated party. In order to “win the debate” or defend a specific ideology or person, facts are distorted and falsehoods are propagated. Misinformation and disinformation are communicated in masse. Any attempt at mediation between the opposite parties becomes impossible, because any concession is viewed as an unacceptable loss [5].

BIAS 4: Doubt/Avoidance Tendency

Users, especially those actively engaged in discussions on social networking sites, prefer to make immediate, seemingly confident responses over deliberated ones. Often, ill-informed, instantaneous decisions are made to bypass the discomfort of uncertainty. This knee-jerk reaction is a byproduct of doubt-avoidance and can be triggered by stresses such as provocation, haste, or irritation at the inconvenience of decision-making. Once the user commits to a response, they accept the consequence of the subsequent chain of events, and they adapt by adopting any necessary viewpoints or issue positions that support their decision. Consequently, when an adversary pressures a susceptible individual into taking a different or more radical position or view with sufficient leverage, the victim self-affirms the response by consuming any propaganda, misinformation, or disinformation provided to them obediently. In many instances, even responsible users fall victim to the tendency because when faced with a decision,

their subconscious deems it inconsequential and a response is chosen in fractions of a second. The most common memetic instance of this occurs when the user is presented with a false statistic or factoid on an often humorous or intimidating picture. As the reader scrolls past it, their subconscious chooses whether to question or believe that information before their conscious mind has processed the data and provided any corollary opinions or information. Adversaries exploit the tendency through the mass distribution of weaponized disinformation, misinformation, and fake news, as well as in arguments and discussions where they know that the target can be provoked or does not want to appear wrong [5].

BIAS 5: Inconsistency-Avoidance Tendency

Humans are habitual by nature. Factors that contributed to an anti-change and inconsistency-avoidance tendency mode in humans include:

- It facilitated faster decisions when the speed of decision was an important contribution to the survival of nonhuman ancestors that were prey.
- It facilitated the survival advantage that our ancestors gained by cooperating in groups, which would have been more difficult to do if everyone was always changing responses.
- It was the best solution that evolution could get in the limited number of generations between the start of literacy and today's complex modern life.

The brain conserves resources by being reluctant to change by default. Reevaluation requires attention, time, and energy. Lasting change in thought patterns involves the rerouting of neural pathways. As a result, the establishment of habits is natural, but the elimination of bad habits is rare and difficult. The memes deliberately and unintentionally consumed have a lasting and powerful impact on the psyche. Once a target is convinced even partially of an idea or is wholly the victim of an influence operation, they will rationalize or dismiss facts entirely to remain consistent with their established mindset. Adversaries do not have to nurture or defend the seeds of influence planted in victims' minds, because the victim acts as the defender [5].

BIAS 6: Curiosity Tendency

Curiosity has been one of the main drivers of human progress throughout history because the human species allegedly experiences it much more than any other mammal species. Philosophy, biology, chemistry, physics, and many other fields are entirely the byproducts of humanity's natural drive to understand the surrounding tangible and intangible environments. The internet put information concerning any topic within reach of nearly every person in the world. In their drive to satiate voracious curiosities, users, including government officials and media outlets, all too often fail to confirm the integrity of the information discovered. Misinformation, disinformation, propaganda, and fake news can leak easily into trusted sources. Worse, by manipulating the search engine optimization algorithms, adversaries can ensure that the first links offered to the users lead to their manufactured content [5].

BIAS 7: Kantian Fairness Tendency

Kant's "categorical imperative," or the golden rule, postulates that humanity benefits most if members pursue behavior patterns that, if followed by all others, would make the surrounding human system

work best for everybody. The overall principle of Kantian fairness can manifest digitally in many ways. Derivative concepts such as “pay it forward” or altruism variants can be beneficial in online communities that might otherwise be hostile; however, an overindulgence in these principles can lead to instances of epidemic propagation of influence vectors. Consider the Facebook groups targeted by Russian Internet Research Agency bots and trolls throughout the 2016 election cycle. The sock puppet accounts joined groups supporting both candidates and communities on either side of many social and political issues, and then they began to influence the populations with fake news links, propaganda, weaponized memes, misinformation, disinformation, and malicious watering holes. If more denizens of those groups had opposed the proliferation of the influence content, actively warned others of the danger, or complained to the administrators collectively, the various content would have reached significantly fewer users than in groups where users followed or ignored the posts. Inaction in the face of recognized influence attempts makes those who recognized but avoided the vectors complicit in the victimization of those psychologically, demographically, or tribally more susceptible. Kantian fairness itself can also be weaponized against users who disagree with its premise. Repeated assertions that “life is not fair” or of the “status quo” can result in an instant polarization of members of various ideologies or political affiliations. Their opposition to the weaponized meme transforms into self-indoctrination, evangelization, and action [5].

BIAS 8: Envy/Jealousy Tendency

According to Warren Buffett, “It is not greed that drives the world, but envy.” Humans retain remnants of their evolutionary familial and communal tribalism as described by the theory of spiral dynamics. The envy/jealousy tendency derives from the innate need to obtain and retain scarce resources. When a member of one distinct community sees another member of the same or a different community in possession of a resource, they may experience envy involuntarily. This reaction could influence decisions or interactions. Digital resources could be the attention of other members of a community or knowledge from an external source. The adversary can provide attention or information sufficient to lure individuals or algorithmically targeted population subsets into their influence apparatus. The memetic weaponization of socioeconomic disparities or perceived societal inequalities may also be employed digitally. Spiral dynamics, socionics, and basic information-gathering tools can be leveraged to tailor discussions, shared memes, factoids, misinformation, disinformation, or propaganda to build a foundation of comradery with a target or target population. The trust and reputation garnered could be used to establish a lasting presence as a gatekeeper of the community, propagate further influence materials, polarize members, or incite divisions within the national culture [5].

BIAS 9: Reciprocation Tendency

People reflexively reciprocate actions and gestures based on societal conditioning and tribal instincts. When someone communicates or interacts with us, we attempt to reciprocate. When someone helps us, we strive to return the favor. The tendency manifests most frequently as small talk and social cues. While it can be good at times, it can also lead to poor decisions if it occurs as a negotiation tactic meant to result in asymmetric exchanges or if leveraged in a sophisticated social engineering lure. On dating sites or social media outlets, attackers can leverage the reciprocation tendency against an individual to initiate contact, collect sensitive information, trade compromising photos or videos, or otherwise gain possession of material or information that could later be used to impersonate or coerce the victim. Similarly, the tendency can be weaponized against groups to gain trust, build relationships, radicalize members, or trigger group-think or a herd mentality in the presence of opposition, which may also be manipulated by

the same attacker [5].

BIAS 10: Influence-From-Mere Association Tendency

Consumers, as groups and individuals, can be easily manipulated according to their proclivities or assigned associations concerning a meme, product, advertising campaign, group, or individual. The causal connection between two entities can act as a fulcrum to control the behavior of one or both entirely. In practice and effect, this could be similar to a man-in-the-middle attack. People find meaning and purpose in their nationality, the sports teams they represent, or the products they prefer. When those entities adopt a stance, some users might defect, but most will adjust their beliefs or view to accommodate or at least tolerate that of the entity. Similarly, when consumers collectively adopt a particular stance, the entity may be pressured to align its mission or operation in that direction. In this manner, special interest groups and foreign adversaries can impact consumers or organizations indirectly by directing an influence operation toward the entity or collective that is determined through socionics, big data analytics, or other theories to have the strongest association to the target [5].

BIAS 11: Simple, Pain-Avoiding Psychological Denial Tendency

Without training and consistent conditioning, humans naturally abhor ideologies, opinions, and positions that clash with their own and those of their evolutionary tribe or community. Members of every religion, political party, and other ideology isolate themselves in “bubbles” and within groups of like-minded peers that protect their fragile psyches from any form of aggression or conflict sufficient to cause inconvenience or pain. In most cases, we have a habit of distorting the facts until they become bearable for our own views. The tendency is the most prevalent in the development and deployment of memes. This includes reinterpreting the tone, arguments, or evidence presented by an outsider or aggressor selectively. In some cases, the very definition of “fact” may be malleable and subject to interpretation based on its source. Attackers use socionics, psychology, social engineering, information-gathering tools, and the underlying principles of spiral dynamics and past influence operations to develop memes that are optimized to transmit, replicate, and mutate within and between specific ideological and evolutionary “bubbles.” In other cases, the adversary might simultaneously manipulate two opposed communities to sow discord; inflate chaos; or widen social, political, economic, tribal, national, or other divisions. The headlines of fake news stories might be tailored to elicit a specific reaction from one or more community; meanwhile, select misinformation and disinformation might be deployed strategically with the expectation that each target community will only internalize the polarized opinions and engineered mistruths designed for them [5].

BIAS 12: Excessive Self-Regard Tendency

People tend to overestimate their own intelligence and abilities and underestimate the critical flaws and vulnerabilities that could be used to manipulate them. It is difficult to gauge the real impact of the Russian influence operation meant to influence the 2016 election, because the majority of the tens or hundreds of millions of Americans who saw the ads, memes, comments, and propaganda believe themselves immune to any form of foreign manipulation. Attackers of all nationalities and levels of sophistication exploit the overconfidence of their target when designing and propagating memetic information. While the “Nigerian Prince” emails of the 1990s might have been obvious, complex tools, advanced tactics, and perfected techniques of modern adversaries often surpass the cybersecurity and cyber hygiene awareness of most social media users. Even if the ad, visual meme, fake news headline, or bot comment shared on social media networks is detected or ignored, if the user internalized any

amount of the information as is necessary for the recognition, then the adversary has succeeded in manipulating the target, at least minutely [5].

BIAS 13: Over-Optimism Tendency

Americans and denizens of numerous other developed nations take for granted the privileges afforded to their citizenship. The luxuries and conveniences of first- and second-world countries result in a tendency for citizens to be naturally complacent and overly optimistic. Though complaints and criticisms may be rampant in common discussions and the media, the average citizen believes internally or wants to think that the world will improve or return to the condition that they desire eventually. By projecting an ideal state onto the nation, a group, or a situation, individuals enable themselves to ignore aspects of the present that lie outside their control. This excess optimism leads to the ignorance of facts in favor of feelings and the forecasting of unknowable futures. Russia weaponized over-optimism in its memes that argued for Hillary Clinton or Donald Trump to be jailed, in its fake news stories that alleged that there were various intelligence investigations into political figures, and in its attempts to divide Bernie Sanders and Hillary Clinton supporters. [5].

BIAS 14: Deprivation Super-Reaction Tendency

Loss aversion or fear of loss is a primary motivator in memetic warfare, because regardless of beliefs, everyone has something that they fear losing. People prefer strongly to avoid losses than to acquire gains. In fact, most psychological studies suggest that the deprivation super-reaction in response to supposed loss is twice as powerful as the prospect of gains when influencing the behavior of a subject. The super-reaction denotes the irrational intensity of the disproportionate response when there is a small loss or threatened loss to someone's property, relationships, territory, opportunities, status, rights, or any other valued concept or entity. Most memes at least imply or outright utilize loss aversion in their construction. Typically, an adversary deploys the tendency simultaneously in polar opposite memes in diametrically opposed communities. For instance, a Russian influence ad meant to polarize NRA members might suggest the loss of Second Amendment rights, while a meme targeting members of the Black Lives Matters movement might imply a heavy casualty rate due to gun violence [5].

BIAS 15: Social-Proof Tendency

People tend to acclimate automatically to the thoughts and behaviors of others within their immediate social group, family, or evolutionary tribe. In 1951, Solomon Asch conducted an experiment to investigate the extent to which social pressure from a majority group could affect a person to conform. He recruited 50 male students from Swarthmore College to participate in a "vision test." Using a line judgment task, Asch put a naive participant in a room with seven confederates. The confederates had agreed in advance what their responses would be when presented with the line task. The real participant believed that the other seven participants were also real participants. Asch was interested to see if the real participant would conform to the majority view. Asch's experiment also had a control condition where there were no confederates, only real participants. Each group performed a line test 18 times. For every trial, each person in the room stated aloud which comparison line (A, B, or C) was most like the target line. The answer was always obvious. The real participant sat at the end of the row and gave his or her answer last. The confederates gave the wrong answer on 12 "critical trials." Asch found that on average, about one third (32 percent) of the participants who were placed in this situation went along and conformed with the clearly incorrect answer offered by the majority on the critical trials. Over the 12 critical trials, about 75 percent of participants conformed at least once, and 25 percent of participants

never conformed. In the control group, with no pressure to conform to confederates, less than 1 percent of participants gave the wrong answer. When interviewed, most participants admitted that they did not really believe their conforming answers but had responded in accordance with the group out of fear of appearing incorrect or different from the group. A few participants maintained that they genuinely believed that the group's obviously incorrect answers were valid. Asch concluded that people conform for two main reasons: because they want to fit in with the group (normative influence) and because they believe the group is better informed than they are (informational influence). It should be noted that Asch's sample lacked diversity and population validity because his small sample only consisted of white males from the same age group. Though the impact of the tendency may be reduced with different populations or when subjects are permitted to give answers privately, the overall premise holds true for some sizable portion of the population. When pressured by numerous peers, certain users will adopt the majority viewpoint to minimize rejection or confrontation from others within the group. Trolls, their cohorts, and their bot armies can depend on the social-proof tendency to compel a non-zero percent of members of an embattled group to conform to the faux viral views or transmit and mutate artificially popularized memes [5].

BIAS 16: Contrast Mis-Reaction Tendency

When evaluations of people and objects are made in comparison to a selection cherry-picked by the influence operator, the target is prone to misunderstand the analogy (often by design) and miss out on the magnitude of decisions. It is more effective to evaluate people and objects by themselves and not by their contrast. The contrast mis-reaction tendency is routinely used to cause a disadvantage for a customer. For instance, vendors typically use it to make an ordinary price seem low. First, the vendor creates a highly artificial price that is much higher than the price always sought. Then they advertise the standard price as a big reduction from his inflated price. Unsuspecting consumers are fooled into believing that they need to act on the deal immediately, and they often leave assuming that they got a bargain. The tendency is used in memes to cause outrage; derail arguments; and widen divisions along social, economic, or political vectors. For example, an attacker might deflect attention from one corrupt politician by continuously bringing up an entirely different politician. Even if the crimes or mistakes perpetrated by the two politicians are vastly different in their scale and severity, the meme will gain traction within certain bubbles, and it will draw more and more attention away from the embattled candidate as mutations and replications flood various platforms [5].

BIAS 17: Stress-Influence Tendency

When a subject is stressed, their body produces adrenaline, which facilitates faster and more extreme reactions. While some stress can improve performance, an overabundance often leads to dysfunction and cascading impacts. Attackers can stress individuals or groups through targeted harassment, through cyber-attacks, with ransomware, or even with carefully tailored argument lures delivered by AI bots. If the lure is sufficient to compel the subject's continued engagement of attention, then the subsequent stress and resulting adrenaline could render them susceptible to manipulation through suggestion or more subtle baiting tactics. If the adversary adopts a more socionically determined allied position or if their offensive operation is precisely calibrated, then the subject may fall victim to radicalization or polarization. This occurs most often through inflations of disparities, implied prejudices, or the targeted manipulation of self-radicalizing wound collectors who are desperate for attention and purpose [5].

BIAS 18: Availability Misweighing Tendency

What is perceived as abundant is often over-weighted, while the brain cannot access what it cannot remember or what it is blocked from recognizing, because it is heavily influenced by one or more psychological tendencies bearing strongly on it. The mind overweighs what is easily available, displays availability misweighing tendency, and imposes a sense of immediacy on the information or evaluation. When subject to memes, consumers often forget that an idea or a fact is not worth more merely because it is easily available. Research requires effort and attention. In visual memes or propaganda videos, attackers deliberately feed the target succinct and memorable misinformation or disinformation factoids and statistics because they know that the majority of the audience will internalize the information and begin to propagate it without considering its authenticity [5].

BIAS 19: Use-It-or-Lose-It Tendency

All too often, trade skills and academic research are acquired for a short-term project or purpose, rather than learned for a fluent understanding. Skills attenuate with disuse. Remembered knowledge likewise degrades over time. Either can only be maintained with daily attention and practice. Attackers can manipulate subsets of the population against one another by acting on skill disparities and fears that lack of certain abilities will impede conventional life. This often manifests in conflicts between educated and uneducated communities, such as between scientists and those who resent science or between blue-collar and white-collar groups. In both cases, the disagreement may eventually transform into xenophobia, an unfounded fear of loss of jobs, class warfare, or biased political platforms and policies [5].

BIAS 20: Drug Misinfluence Tendency

Substances or lack of stimuli influence brain chemistry strongly and can be used to influence individuals. In tangible operations, this could be something as simple as gathering important individuals in a meeting and then denying them caffeine or sustenance until they reach an agreement; as was rumored to be the case with the Constitution. In the digital space, the tendency could translate to the endorphin rush that isolated or indoctrinated individuals experience when they consume specific media that is released periodically. If a favorite podcast or blog post is delayed, the devout subject may experience a disproportionate adverse reaction that could leave them desperate for interaction or attention. Entire communities or groups could be influenced similarly if the adversary dedicates enough resources and conditions enough subjects to be dependent on their specific propaganda, fake news, or memes [5].

BIAS 21: Senescence Misinfluence Tendency

The loss of skills and abilities over time is natural because the body degrades as it ages. Continuous practice and learning stymie the degradation; however, it requires a constant input of time and effort. Most lack the time or necessity to maintain all their acquired capabilities; however, most are also insecure about all of their incapacities, especially if they used to be able to perform those tasks or recount that information. Adversaries can propagate fake news articles, misinformation, and disinformation that capitalize on the fear of obsolescence inherent in the elder generation as well as on the younger generation's fear of never reaching the skill level or societal achievements of their forbearers. The result is often generational divides that translate into political and societal divisions [5].

BIAS 22: Authority Misinfluence Tendency

Humanity evolved from dominance hierarchies that necessitated only a few leaders and many followers.

Consequently, distributions of personalities and possession of leadership skills, such as public speaking and effective writing, still follow this trend. Unless provoked or otherwise compelled, the majority of a given population will follow the orders issued to them by society and authority figures. Even though most people consider themselves independent of societal constructs, only a small percent elect to break the laws or rebel against the established order, because humans, regardless of citizenship or nationality, are predominantly rational. Adversaries can provide provoking propaganda, tantalizing disinformation, and other compelling lures to cause an individual or group to rebel against the “status quo.” Conversely, the attacker could incept the fear of insurrection within particular authorities, groups, or individuals, to incite conflict between the “ruling faction” and the “rebels” based on the evidence fabricated for each role by the attacker [5].

BIAS 23: Twaddle Tendency

The internet places the convenience of entertainment, learning, and utility at the behest of the user. Users have a strong tendency to waste much of their time on social media platforms, browsing memes and otherwise consuming media that will not significantly impact their lives in any way. This natural tendency to escape the confines of mundane life momentarily can be an effective if lesser-used attack vector in influence operations, meant to destabilize institutions or undermine societal cornerstones. For instance, a sudden flood of entertaining propaganda or forbidden media could inspire minor insurrections at the personal level. Consider the cascading impacts of Winston Smith’s illicit journal in George Orwell’s pivotal “1984.” Similarly, the United States has allegedly airdropped flash drives loaded with entertaining movies and television shows into North Korea in an operation intended to undermine their rigorous isolation and inspire a rebellious sense of free will in their populace [5].

BIAS 24: Reason-Respecting Tendency

Some people desire answers without the need for reasons or a better understanding. These individuals often take any information at face value and are prime targets for propaganda, misinformation, disinformation, and fake news. On the opposite end of the spectrum, overly detail-oriented individuals can become entranced with sensational, if entirely fabricated, highly detailed narratives crafted by creative adversaries. The fake news, often manifesting as conspiracy theories, is tantalizing because it often seems to contain more details than the public narrative, and subscription to its “truths” often comes with membership in a seemingly exclusive community of like-minded individuals. Attackers populate these groups with trolls and bot accounts to inflate the population of the community, and then they leverage memes and carefully cultivated personas to influence the community [5].

BIAS 25: Lollapalooza Tendency

Everyone wants to be correct, and many unknowingly subject themselves to mental acrobatics to rationalize or justify their beliefs or position on an issue. The lollapalooza tendency is the effect of the layering of numerous extreme confluences of psychological tendencies so that the mind can arrive at a conclusion that favors one particular, often predetermined, outcome. In effect, through the influence of an external adversary or via internal rationalization, individuals and groups can be coerced to subscribe to compounding checklists of tendencies and biases [5].

Socionics is the study of the intertype relations that describe the high-level relationship between psychological types of people, and not between the actual people. This is the reason these relations are called “intertype” relations. The relations between actual people are complicated and depend on many different factors. Meanwhile, the intertype relations form the foundation of interactions and describe various degrees of psychological compatibility between people. Influencers can predict a target or target community’s type and then engage with that target as a particular type of relation to achieve a certain effect or to build a particular relationship [7].

IDENTICAL RELATIONS

Identical relations have a complete understanding of each other, including worldviews, opinions, information processing methodologies, conclusions, and problems. They often exhibit sympathy toward each other and try to support and justify each other. Ideological bubbles are the most common digital occurrence of identical relations. Identical users expect mirrored opinions and arguments. While different dialogues can accommodate slightly differing ideological ranges, identical relations tend to “go neutral” if one party strays outside the bubble. Differences in background and functions of duals can be overcome if the relation depends on a sufficient driving force such as memes, evolutionary state, politics, or other strong ideological motivators. Further, identical relations often result in introspection and self-development akin to watching a video of oneself. An influencer may be able to expand or reduce the boundaries of the relation gradually, alter views, and guide communities. [7].

RELATIONS OF DUALITY

Relations of duality provide complete psychological compatibility and are therefore considered the most favorable and comfortable intertype relations. Duals are not identical; rather, they are almost two halves of the same whole. Dual partners understand the strengths, weaknesses, needs, and intentions of their partner. Coerced or engineered adjustments in behavior or understanding are not necessary. Consequently, adversaries capable of acting as a dual relation to a target expend the minimal amount of time, energy, money, and other resources in their operations [7].

Because humans are complex in their views, associations, and actions, true relations of duality are rare; however, their perceived scarcity may actually be an effective advantage to an adversary because the target might be over-accepting of a digital entity or persona whose ideology “fits” perfectly with that of the target. Others might become wary and skeptical of too close an approximation. For instance, this can easily be seen in digital advertisements that rely on cookies. Some users are amazed and overly grateful when advertisements on social media recommend precisely the product or service that they were searching for on other sites; meanwhile, others experience a chilling effect and sometimes anger at the perceived invasion of their privacy. Younger people have less ingrained perceptions, opinions, and worldviews and are therefore more easily convinced of duality with a partner [7].

RELATIONS OF ACTIVITY

Relations of activity are the easiest and quickest to start. Partners enable and stimulate each other into activity. Partners tend to recognize the weaknesses of the other and recommend unsolicited advice to bolster or reinforce the vulnerability. Interaction becomes a stimulant and can develop into a dependency. With continuous interaction over a long period comes over-activation, however, which may result in boredom or dissolution of the relation. Relations of activity are oscillatory. Reactionary

community building and over-exhausting normalization are both relations of activity. When the target cannot engage in the desired activity or take a break from the relationship respectively, they experience increasingly negative effects [7].

MIRROR RELATIONS

Mirror relations are relations of mutual correction pertaining to partners with similar interests and like-minded ideas, but a slightly different understanding of the same problems. Each partner can see only half of one problem. Therefore, the partners find the other's perspective interesting. The area of confidence of one partner may be the area of creativity for the other partner, and what one partner considers definitive may appear malleable to the other. The difference may perplex one or both, and they often attempt to correct the assumed misconceptions. As a result, mirror partners' conversations often develop into contentious disputes centered on slight alterations of opinion pertaining to the same main concept. Arguments within ideological bubbles on social media platforms and groups may be the most prevalent example of mirror relations. Mirror dialogue often begins as constructive criticism, but discomfort results from differences in judgment and perception between the partners. Members may agree on future goals but disagree on global aims or step-wise methodologies. An influencer can exploit these relations to imply communal divisions, to alienate members, or to shift the conversation or ideology of the community [7].

RELATIONS OF SEMI-DUALITY

These are relations of deficient duality. Semi-duality partners usually have no problems in understanding each other or each other's objectives, at least conceptually. Semi-duals can engage in complex dialogues, but communication is competitive, rather than cooperative. While not an outright ideological tug of war, both partners are often so entrenched in their position that even when peaceful dialogue occurs, neither is likely to coerce the other to alter their beliefs. After the discussion, both parties snap back to their initial position. Relations of semi-duality can be considered as moth and flame. When the target calms, they are left with a lack of fulfillment that often results in reengagement. An adversary would not leverage a semi-dual relation to convince the partner; instead, the dual is a predictable pawn in a show designed to manipulate the audience or surrounding community [7].

COMPARATIVE RELATIONS

Comparative partners talk about similar things, have similar interests, and obey the norms of politeness and hospitality toward each other, but they never really show an interest in each other's problems. These are relations of deceptive similarity, but they tend to stagnate. When partners exist on the same level in a hierarchy, they peacefully coexist. If one partner becomes superior to the other, serious disagreements and conflicts occur. Comparative partners analyze the same issues from very different angles. Each is reminded to acknowledge each other's different point of view, and they often feel the other's solution is impractical [7].

CONFLICTING RELATIONS

Conflicting relations consist of constantly developing conflict. Both partners are initially convinced that they can coexist and collaborate quite peacefully, but the relationship rapidly deteriorates. Each underestimates the ideological disparity and attempts to nudge the other into their ideological comfort zone. Continuous attempts to force the relation and alter the other provokes open conflict, at which point

each directs arguments toward the other that are designed to inflict maximum pain. Retaliation follows, and the aggression escalates [7].

SUPER-EGO RELATIONS

Super-ego relations occur between two individuals that do not share common interests or ideologies, but erroneously believe that they understand the other well. Communication often appears formal, calculated, and emotionally vacant. Partners normally think more about expressing their own point of view than listening to their partner. This expression comes from the confident side of one of the partners reaching the unconfident side of the other partner. The latter tries to defend themselves by projecting their confident points in return. Partners normally show interest and respect to each other if they do not know each other well enough. Problems occur because neither side understands or wants to understand the perspective of the other. They are convinced that the other is deliberately incorrect. The most prevalent digital expression of super-ego relations is the communication between conspiracy theory communities and those attempting to dispel those theories [7].

QUASI-IDENTTTICAL RELATIONS

Quasi-identical relations result from a major misunderstanding. Partners are ideological polar opposites but are equivalent on spiral dynamics and other psychological scales. Quasi-Identical partners always need to convert each other's information in such a way that it corresponds to their own understanding. This conversion requires much energy and does not bring the desired satisfaction. Tension results from the incapacity of either partner to bypass their own views to accept those of the other. An example of this would be an aggressive digital dialogue between an antifa community and members of the alt-right. Adversaries can manufacture conflict easily and rapidly by impersonating one partner and targeting the opposite community. The resulting chaos can be transformed into kinetic rallies, protests, and violence. Both sides, who are capable of understanding the conflict but remain vehemently ideologically opposed, are galvanized into cascading confrontations and impacts [7].

ILLUSIONARY RELATIONS

There are no other intertype relations that can deactivate partners so much as illusory relations. They result from growing laziness and complacency. Illusory partners are unwilling to exert the effort to understand an issue or the motivations of others. They expect others to perform differently, but do not attempt to coerce change in any way. Their unfulfilled desires manifest as uninformed criticisms of the intentions and actions of others. To an external audience, the commentary may appear humorous. Troll comments and misinformed complaints on social media discussions are the most common illusory relations [7].

LOOKALIKE RELATIONS

These are relations between equal partners who can be called acquaintances, rather than friends. There are no observable obstacles in the development of these relations, and partners can talk easily about almost anything. Lookalike partners do not feel any danger from the other partner. The strong sides of the partners are different in such a way that almost any conversations between them always fall into the area of the confidence of only one of the partners. Lookalike partners also have similar problems, which make them feel sympathetic toward each other instead of being critical of each other's vulnerabilities. Arguments in lookalike relations are not common practice. Lookalike relations have an average degree

of comfort. Partners do not have anything against each other but also nothing for which to struggle. Eventually, one partner may leverage the information gathered about the other to exploit a vulnerability or to coerce a particular response. Cat-phishing, doxing, swatting, and other personal attacks by which one party coaxes the other preemptively for information that can later be weaponized are all types of lookalike relations [7].

RELATIONS OF BENEFIT

These relations are asymmetrical because one partner, called the benefactor, is always in a more favorable position in respect to the other partner, who is known as the beneficiary. The beneficiary thinks of the benefactor as an interesting and meaningful person, usually over-evaluating them in the beginning. The beneficiary can be impressed by their partner's behavior, manners, and thoughts, as well as their ability to deal easily with things that the beneficiary conceives as complicated. During the interaction, the beneficiary involuntarily starts to ingratiate themselves with the benefactor, trying to please them without any obvious reason. Often, the benefactor may suspect that the beneficiary wants something that the benefactor can provide. Meanwhile, the beneficiary may be led to believe that the benefactor has singled them out for genuine interest. In some instances, one or both partners may feel a "spiritual" or fated connection to the other as an internal rationalization of the asymmetric relationship. Arguments and quarrels may occur if one side suddenly ignores the other. Adversaries may find it advantageous to masquerade as either a benefactor or beneficiary to exert influence on an individual who may be susceptible to the unexpected attention. Tailored attacks targeting niche personnel, propaganda from the pulpit, and similar vectors are relations of benefit [7].

RELATIONS OF SUPERVISION

Like relations of benefit, relations of supervision are also asymmetrical. One partner, called the supervisor, is always in a more favorable position in respect to the other partner, who is known as supervisee. Relations of supervision can give the impression that the supervisor is constantly watching every step of the supervisee. The latter usually feels this control even if the supervisor does not say or do anything. Rather than operate on unmonitored channels, the supervisee seeks the recommendation and commendations of the supervisor. Meanwhile, the supervisor undervalues the attention and abilities of the supervisee. The explanation for this is that the supervisee's weak point is defenseless against the supervisor's strong point. This manifests in chilling effects, paranoia, exploitation of the supervisee, and other negative outcomes. Cyberstalking and the relationship between users and social media propagandists and other special interest groups are prime examples of relations of supervision [7].

PSYCHOGRAPHIC BIG DATA ALGORITHMS

Each action online generates metadata that can be harvested by adversaries and special interests. Every cybersecurity incident results in the loss of treasure troves of information that can be weaponized against consumers. Big data analytics operations on psychographic and demographic data are the next generation of hybrid warfare weapons. Psychographic algorithms reveal consumers' preferences, psychological characteristics, ideology, thought process, and evolutionary tier, and they can be used to forecast every future action and response by consumers. In DIOs, psychographic analyses of populations are used in the memetic design; to deliver foreign propaganda; and to tailor fake news, misinformation, and disinformation [8].

PREDICTIVE ANALYTICS

Predictive analytics is the employment of data and statistical models to forecast future behavior and decisions [9]. Data collected from breaches and dragnet surveillance capitalists can inform adversarial attempts to predict and then manipulate the actions of a target population. Worse, data collected from search engine optimization solutions, predictive text applications, social media mood algorithms, and other facets of digital “convenience” will be leveraged in foreign influence campaigns. In effect, the threat actor can decide what a population will think and how they will respond to information before the target is even cognizant of a decision [8].

INFORMATION PROCESSING

Automatic processing is “implicit” thinking that tends to be effortless, habitual, and done without awareness. Most importantly, automatic processing affects the way that we internalize the information we receive and, therefore, how we receive it. We all develop social schemas throughout our lifetimes. A social schema is our internal perception of how something should be or act, such as our image in our head of what a firefighter looks like. Once a schema is formed, any and all information we receive is processed automatically through our understanding of the world. We are then more likely to retain or accept facts that agree with our perceptions and schema and refute those that do not. These decisions occur almost instantaneously as the mind receives information. By having an understanding of audience, automatic processing allows one to manipulate or influence an audience into agreeing to the same message, so long as it is presented through the correct schemas [10].

Controlled processing is “explicit” thinking that tends to be deliberate, reflective, and conscious. This is the way information is processed consciously or the deliberate way one forms an argument with the information or explains it to others. It is where the message is judged and reflected upon to ensure it is true. Influence requires a message that is believable, will stand up to scrutiny, and is conveyed easily to others. The more complicated the message, the more it will appear like a conspiracy. Further, the message needs to be complete, but not so much as to be completed and not allow the individual to make the idea and message their own through filling in gaps and meaning. Once a message is personalized, the individual is far less likely to recognize fault in it or to set it aside, and they are more likely to try to convince others of their view zealously [10].

DIFFERENT PATHS OF PERSUASION FOR DIFFERENT PURPOSES

People who focus on facts, statistics, and logic rely on the central route of persuasion. They consider the issue and focus on the arguments. If the arguments are strong and compelling to their ideological niche, then persuasion is likely. However, if the message relies on weak arguments or unsuccessful memes, then the targets are not likely to be convinced and will likely begin to counter-argue to dispute the claims and rally other community members against the message. Digital ads, fake news, propaganda, and other vectors that the user could spend enough time with to construct logical considerations over must withstand extensive scrutiny to succeed along the central route of persuasion [10].

Thankfully for the attacker, another persuasive vector exists. Along the peripheral route of persuasion, the strength of the arguments does not matter as much. People default to the peripheral route when they are not motivated enough or able to think carefully. Though they are less likely to propagate or mutate

the meme, distracted, unbalanced, busy, uninvolved, or disinterested people consume the meme without considering its message. The peripheral route relies on cues that trigger automatic acceptance without much thought, rather than the robustness and resiliency of arguments. Impulse purchasing and most advertising, especially brand-based decisions, rely on this method. Billboards, commercials, product placement in media, and any other form of advertising that relies on an abstract association, such as sex, hunger, and beauty, depend on peripheral persuasion [10].

Advertisers, preachers, teachers, and other influencers are interested in more than consumption of their message. They need to impart sufficient motivation to alter the target's behavior. The central route of persuasion causes people to think carefully and elaborate on issues mentally. They rely on their own internal arguments as much as those of the influencer. In fact, studies suggest that the internal thoughts triggered as a result of the source are more compelling than the initial material. What got someone thinking may be less important than how it got them thinking and what results they reached. Deep thought, instead of superficial consideration, results in attitudes that are more persistent, more resilient, and more likely to influence behavior. In short, the central route of persuasion leads to more enduring change than the peripheral route [10].

Persuasion along peripheral vectors produces superficial and temporary changes in attitude. Changing attitudes is easier and more immediate than altering behavior. Changes to behavior require people to process and rehearse their own convictions actively. Influencers may not have strong enough memes or convincing enough arguments to alter someone's behavior, but thankfully for them, they do not have to because most consumers lack the time, attention, and discipline to consider each decision deeply and consciously. The peripheral path of persuasion is the default in decision-making, thanks to "rule of thumb" heuristics such as brand loyalty, "long messages are credible," "trust the experts," and others. One of the most powerful heuristics is trust in communal and familial opinion and choice. People vote for whomever they like more arbitrarily, and they support whatever their friends and families support [10].

Central or systematic persuasion is required for people who are naturally analytical or are involved in an issue. Robust and comprehensive memes and material are required to convince these individuals to alter their long-term behaviors. When issues do not merit systematic thinking, people tend to make snap judgments based on ingrained heuristics. In the latter case, where the influencer does not desire long-term alterations to behavior, they need only provide a palatable message and a mental nudge toward the heuristic that will direct the target toward the desired response [10].

...

“The ‘alt-right’ and the ‘progressive-left’ are a direct revolt against the narrative illusion that has controlled the ideas and belief systems by the American population since Eddie Bernays.”

...

PSYCHOLOGICAL PROFILING CONCEPTS USED IN MEMETIC DESIGN

Human thought is a construct of Frankensteined variations of ideas and memetically altered belief systems. The original idea is held hostage to weaponized vectors that expedite delivery of the meme that becomes the narrative. The “original idea” is a rarity because of the toxicity corroding the mind, toxicity stemming from the bombardment of messages that pummel the critical faculties that distort the natural process of thinking. Reality is gossamer, and the human psyche can be disrupted and manipulated easily by tailoring a meme to exploit any one or more of dozens of psychological vectors. The weaponized meme, when introduced and reinforced properly, will parasitically weave its way throughout the labyrinth of the mind and attach itself to the subconscious, thus affecting the root of the thoughts of the recipient resulting in the intellectual zombification of the target’s perception on the particular categories of concepts related to the meme. When one has an idea memetically introduced and the meme colonizes the neural pathways of the mind, it becomes a tremendous contributor to one’s belief system. Engineered properly, a belief automatically precludes one from believing its opposite. The meme’s contribution to the digital tribal society allows for automated enforcement of this new belief via peer pressure from the tribe and its chieftains.

NORMALIZATION

Normalization is the process of making something accepted or commonplace in the societal collective conscious by acclimating the population to keywords, desensitizing them to the outcomes through an oscillatory discussion of the polar opposite outcomes, or inundating them with discussion to the point that the subject is accepted but mostly ignored [10].

PARTICIPATORY POLITICS IN THE DIGITAL AGE

Online platforms have altered how users, especially younger generations, consume media, including propaganda, and how and why they engage in civic-political spheres. The access to information, expression of ideas, circulation of propaganda, and mobilization of communities all depend on digital platforms and mechanisms that are highly susceptible to the machinations of adversaries and special interests. Participatory politics is the broadening of political discourse into the daily communities of individuals. DIOs often target populations of individuals who participate out of ideological compulsion, attachment to a social justice cause, or online convenience, because those individuals seek causes and dialogues to champion intentionally. In many cases, users are psychologically addicted to the heated online discourse, ideological bubbles, and redirected animosity perpetrated on online platforms or forums [11].

BELIEF PERSEVERENCE

Researchers such as Lee Ross, Craig Anderson, and others have proven that it is remarkably difficult to demolish a falsehood once it has been planted in a subject’s mind and nourished with rationalizations. Each experiment they conducted either implanted a belief by proclaiming it true or by showing the participants anecdotal evidence. Participants were then asked to explain why it was true. Finally, the researchers totally discredited the belief by telling participants that the information was manufactured and that half the participants had received opposite information. Despite being blatantly told that they had received fabricated information by the creators of that data, approximately 75 percent of the new belief persevered. This effect, belief perseverance, is attributed to the participants’ retention of their invented explanations for the belief. It demonstrates that fake news or disinformation can survive even the most direct attempts to dispel the false ideas. Another experiment asked subjects to determine

whether firefighters performed better if they were more willing to take risks. One group considered the case of a risk-prone firefighter who was successful and a risk-adverse firefighter who was unsuccessful. The other group considered the opposite. After forming their hypotheses, each participant wrote explanations justifying their position. Once the explanation was formed, it became independent of the initial information that created the belief. Even when the narrative was discredited, the participants retained their self-generated explanations. The research suggests that the more individuals examine their theories and beliefs and the more they explain and rationalize them, the more closed people become to information that challenges their ideology [10].

Belief perseverance is prevalent on every digital platform and, to some extent, in nearly every human interaction. Our beliefs and expectations govern how we construct events powerfully. Individuals are prisoners of their patterns of thought [10]. Influencers can leverage psychographics and the metadata collected from online platforms to determine the spiral dynamic and socionic profiles of population segments that share similar psychological patterns. Afterward, they can craft fake news, propaganda, disinformation, and misinformation that are tailored to implant specific memes in the population. Infected individuals will internalize and rationalize the notions, and their perceptions will become independent derivatives of the meme that are impervious to challenge or fact. In fact, challenging the theories with contrarian information, such as fact, has an inverse effect. Believers become more defensive and convinced of their ideologies as their theories and rationalizations are confronted [10]. Adversaries can, therefore, play both sides of an issue using trolls and bot accounts to plant an idea and then attack those same ideas and faux sources in order to root the false information in the community and evangelize memetic zealots. The only proven method of dispelling belief perseverance is to coax the subject into considering the opposite side of the issue and explaining it as a “devil’s advocate” [10]. This, too, can be weaponized to convert believers from one side of an issue to another and thereby disrupt critical community networks through infighting and conflicting beliefs.

FALSE CONSENSUS

People do not perceive things as they are; instead, their perceptions are reflections of themselves. Online users tend to enhance their self-images by overestimating and underestimating the extent to which others think and act as they do. Many erroneously assume that others operate on the same spiral dynamic tier or are of a specific intertype relation, without any data to inform that consensus. This phenomenon is referred to as false consensus, and it summarizes each person’s psychological tendency to assume that others share their internal “common sense.” Humans excel at rationalization and knee-jerk conclusions that allow us to persuade ourselves that we remain part of the majority in the functional evolutionary tier. Mistakes are dismissed through self-reassurance that “everyone makes mistakes” or “I am sure most people do that.” Meanwhile, negative behaviors are projected onto others. For instance, liars often become paranoid that others are dishonest because they believe that if they lie, then everyone must. False consensus occurs when we generalize from a small sample that may only include ourselves. People have evolved to be comfortable with this process, because in most instances, individuals are in the majority, so their assumption that they lie in the majority on most issues is proportionally accurate. Further, assumed membership in the majority is reinforced through participation in communities and familial units that mirror attitudes, behaviors, and beliefs. However, many fail to realize that majority membership often does not translate to ideological and nuanced issues, such as politics or religion [10]. Additionally, on matters of ability and success, the false uniqueness effect occurs. At some primal level, people want their talents, ideas, abilities, and moral behaviors to be acknowledged as relatively unusual or even superior

compared with those of their peers [10].

SELF-SERVING BIASES

The effect of false consensus and false uniqueness are self-serving biases. A self-serving bias is a byproduct of how individuals process and remember information about themselves. For instance, one might attribute their success to ability and effort, while the same individual may attribute any failures or shortcomings to luck and external influencers. Other self-serving biases include comparing oneself favorably to others without empirical correlation and unrealistic optimism [10].

Adaptive self-serving biases help to protect people from depression and serve as a buffer to stress; but, in doing so, they also inflate reality. Non-depressed individuals typically attribute their failings to external factors, while depressed subjects have more accurate appraisals of themselves and reality. Induction of adaptive self-serving biases in a population can be used to manage their anxiety, downplay traumatic events such as terrorism, and increase their motivation and productivity. The opposite is likewise true, however. The propagation of memes that dispel adaptive self-serving biases results in increased introspection and a more grounded view of reality and in the correlation and causation of events [10].

Maladaptation self-serving biases result in people who fail to recognize or grow from their mistakes and instead blame others for their social difficulties and unhappiness. Groups can be poisoned when members overestimate their contributions to the group's successes and underestimate their contributions to its failures. For instance, at the University of Florida, social psychologist Barry Schlenker conducted nine experiments in which he tasked groups with a collaborative exercise and then falsely informed them that their group had done either well or poorly. In every study, members of successful groups claimed more responsibility for their group's performance than members of groups who were told that they had failed the task. Envy and disharmony often resulted from group members who felt that they were underappreciated or underrepresented [10].

When groups are comparable, most people will consider their own group superior. Group-serving bias occurs when influencers inflate people's judgment of their groups. Adversaries can leverage the effect of group-serving bias to pit otherwise comparable digital communities against one another to either create chaos or increase the quality and resolve of membership through competition [10].

SELF-HANDICAPPING

Self-handicapping is the effect of individuals sabotaging their own chances of success by creating impediments that limit the likelihood of success or by not trying at all. People eagerly protect their self-images by attributing failures to external factors. By inflating the hopes and exciting the fears of an audience, an influencer can induce self-handicapping in the more self-conscious members of the target demographic. In short, through an influence operation, the perceived risks begin to outweigh the illusory gains. When self-image is tied to performance, it can be more self-defeating to try and fail than to procrastinate or not try at all. Self-handicapping shifts the onus of failure to external actors or circumstances. Outcomes are no longer associated with skill, talent, merit, or ability. On the off chance that the impaired individual succeeds, their self-esteem is bolstered for overcoming daunting obstacles; meanwhile, failures are attributed to temporary or external factors and actors [10].

PRIMING

Assumptions and prejudgments guide our perceptions, interpretations, and recall. The world is construed through belief-tinted lenses. People do not respond to reality; instead, they react to their personal interpretation of reality. Unattended stimuli influence the interpretation and recollection of events subtly. Memory is a complex web of associations, and priming is the activation of specific associations. Numerous experiments have demonstrated that priming one thought, even without awareness, can influence another thought or action. For instance, in 1996, John Bargh and his colleagues asked subjects to complete a sentence containing words such as “old,” “wise,” and “retired.” Afterward, the individuals were observed walking more slowly to the elevator than other subjects who were not primed with age-related words. The “slow walkers” had no awareness of their walking speed or that they had been primed with age-related words. Depressed moods prime negative associations, good moods prime people to selectively view their past as positive, and violent media may prime viewers to interpret ambiguous actions as aggressive [10].

Out of sight does not equate to out of mind. Most social information processing is unintentional, out of sight, and occurs without conscious awareness or consent. It is automatic. In studies, priming effects surface even when the influence stimuli are presented subliminally, too briefly to be perceived consciously. An otherwise invisible image or word can prime a following task. For example, an imperceptibly flashed word “bread” may prime people to detect a related word such as “butter” faster than an unrelated word such as “bottle” or “bubble.” A subliminal color name facilitates speedier detection of that color; though an unseen wrong color name delays color identification. Imagine the impact of an influence operation that primed consumers with invisible keywords or images in the ads or borders of the screen. Consider the effect that the use of subtle or even sub-audible sounds could have on reception and understanding of various forms of media or the media consumed afterward [10].

Despite biases and logical flaws, first impressions tend to be accurate more often than not. As a result, most individuals do not have cognitive defenses implemented to mitigate DIOs. They innately trust their perception of events to be undeniably accurate. Implanted prejudgments and expectations can sour impressions and color future interactions without additional effort on behalf of the adversary. The most culturally relevant example of this is that political candidates and their supporters always view the media as unsympathetic to their cause, regardless of coverage [10].

Assumptions about the world can even be leveraged to make contradictory evidence seem true. When presented with factual empirical evidence, such as confirmed experiment results or objective statistics, both proponents and opponents of any issue readily accept evidence that confirms their beliefs and discounts evidence that does not. Presenting both sides of an issue with an identical body of mixed evidence increases their disagreement rather than lessening it. Priming is an invaluable tool for any influencer, regardless of position, medium, or issue. Partisanship predisposes perception [10].

In experiments where researchers have manipulated people’s preconceptions, they were able to direct their interpretations and recollections significantly. For instance, in 1977, Myron Rothbart and Pamela Birrell had University of Oregon students assess the facial expression of a man. Those told he was a Gestapo leader responsible for war crimes interpreted his expression as a cruel sneer; meanwhile, those told he was a leader of an anti-Nazi underground movement interpreted the same expression as a kind

and comforting smile. In the digital landscape, every meme engineer can replicate this experiment en masse. They can provide the same memes and misinformation to opposing communities and prime both to harbor extreme animosity against the other. A simple picture of a smiling politician could be interpreted as warm and charming in one sphere and creepy or menacing in the other. Filmmakers likewise control audience perceptions through the “Kuleshov effect.” Essentially, audiences associate their perception of an individual and their expression with the images that precede that individual. If an explosion is seen before a hard cut to a smiling man, then the man is interpreted as the villain responsible for the blast. Similarly, if a faceless person is seen handing money to the homeless, then the individual featured after the hard cut is perceived as charitable [10].

SPONTANEOUS TRAIT TRANSFERENCE

Construal processes also impact perception. When entity A says something good or bad about entity B, people tend to associate that good or bad thing spontaneously with entity A. This phenomenon is referred to as spontaneous trait transference. People who complain about gossiping are seen as gossips themselves, while people who call others names are seen as those insults. Describe someone as caring to seem so yourself. Spontaneous trait transference is the epitome of the childhood mantra, “I am rubber, you are glue....” And it can be weaponized by opportunistic adversaries. Actors can ingratiate themselves into community ranks by complimenting key figures and members. On the other hand, they can demonize their opposition by baiting them into resorting to insults or relying on charged keywords and phrases [10].

GROUPTHINK

Groupthink is a mode of thinking that people engage in when concurrence-seeking becomes so dominant in a cohesive in-group that it overrides realistic appraisals of alternative courses of action [10]. It is vital to maintaining an already collected and controlled population. If one has control over all forms of information, such as books media and the web, then a cohesive group consciousness is all that remains. It can even be used for generational indoctrination, such as in North Korea.

BELIEF DISTORTION

Conspiracy theories, otherwise known as distorted beliefs, are widespread. How and why they are formed is still more a matter of speculation rather than science, but fledgling theories exist. Emotional arousal increases neuroplasticity and leads to the creation of new pathways spreading neural activation. According to neurodynamics, a meme is a quasi-stable associative memory attractor state. Depending on the temporal characteristics of the incoming information and the plasticity of the network, the memory may self-organize creating memes with large attractor basins, linking many unrelated input patterns. Memes with false rich associations distort relations between memory states. Simulations of various neural network models trained with competitive Hebbian learning (CHL) on stationary and non-stationary data lead to the same conclusion: Short learning with high plasticity followed by a rapid reduction of plasticity leads to memes with large attraction basins, distorting input pattern representations in associative memory. Such system-level models may be used to understand the creation of distorted beliefs and formation of conspiracy memes, understood as strong attractor states of the neurodynamics [12].

GROUP POLARIZATION

Group polarization is a community-produced enhancement of members’ preexisting tendencies; a

strengthening of the members' average tendency, not a split within the group [10]. Group polarization allows the powerful and influential in a group to sway more moderate opinion to their side slowly. It also leads to a more unified group than when the group is segmented and broken. Influencers leverage group polarization to bias a group further.

FUNDAMENTAL ATTRIBUTION ERRORS

The fundamental attribution error is the tendency for observers to underestimate situational influences and overestimate dispositional influences upon others' behavior. Populations often make fundamental attribution errors in judging their beliefs compared with other segments of the population [10]. This is helpful in influencing others, since the flaw attributed falsely is often a weakness that can be leveraged.

HINDSIGHT BIAS

Hindsight bias is the tendency to exaggerate, after learning an outcome, one's ability to have foreseen how something turned out. It is also known as the "I knew it all along" phenomenon. Similar to confirmation bias, hindsight bias acts as a polarizing lightning rod in influence. People want to not just be right, but to believe their internal mechanisms can produce correct results routinely. Thus, when one has discovered they predicted something correctly, they become invested in that issue. When one predicted incorrectly, they become prime targets for manipulation by exaggerating the negative traits of the resulting decision. When they feel that the situation was outside their control and there was no way for them to have been correct, they blame the system and propagate distrust [10].

ILLUSION OF CONTROL

The illusion of control is the perception that uncontrollable events are more controllable than they are in reality. It is often used to steer the perception of a population. For instance, politicians are known for crediting their supporters with the success of an achievement, while blaming losses on their adversaries. Letting a supporter believe their efforts helped in the success or outcome of a movement makes it more likely they will put such efforts forward again. Similarly, the ability to inspire change or generate momentum toward something not happening convinces people to mobilize efforts in a likewise fashion [10].

ILLUSION OF TRANSPARENCY

The illusion of transparency is the misapprehension that concealed emotions are detected by other people easily. Individuals like to believe that they can "read" people or that they know who or what to trust based on "gut instinct." In reality, their perception is a malleable amalgamation of their beliefs, predispositions, biases, and fallacies [10]. It is trivial for an adversary to steer the perception of a population through suggestion or inception. The other side of the illusion is that individuals trust that their peers will understand the emotions, morals, and values underlying their decision-making processes. Similar to a man-in-the-middle attack, an adversary can interject faux motivations into this implicit trust through trolls, bot comments, and fake news.

INDOCTRINATION

Extreme persuasion, otherwise known as indoctrination, is the byproduct of conformity, compliance, dissonance, persuasion, group influence, and psychographics. People's attitudes follow their behavior. The indoctrination process is an incremental conversion made possible by the internalization of

commitments that are made “voluntarily,” publicly, and repeatedly. Vulnerable individuals gravitate toward digital communities in search of companionship and acceptance. Ideological radicals leverage group settings and communities as a venue for public commitment to a cause. To navigate from the out-group to the in-crowd, gain membership, or make friends, individuals are fed propaganda and manipulated not just to commit to its messaging but to vocalize their adherence to its tenets repeatedly. Active members are, in turn, tasked with recruitment and participate in activities that ingratiate them further in the group. After some time, the beliefs and actions of the group, no matter how radical, normalize because compliance breeds acceptance. Members may be asked to conduct surveillance, launch layers of digital attacks, fundraise through scams or cryptocurrency mining, or otherwise support the group. Studies have shown that the greater the personal commitment to the cause, the more the individual feels the need to believe the propaganda and disinformation of their community. Eventually, the goals and survival of the group are the priorities of the initiate [10].

People do not turn to extreme ideologies on a whim. Drastic life changes rarely result from an abrupt, conscious decision. Recruiters also do not jar the target drastically into subservience. Instead, recruitment exploits the foot-in-the-door principle. Engagement via memes, especially humorous ones, and psychographically tailored interaction is far more effective compared with other vectors. As with cults, digital indoctrination is designed to draw more of the target demographic’s time and attention. The activities and engagement likewise increase in ardor. Social engagement might at first be voluntary, but as the process progresses, the input of the individual will be solicited to make interaction mandatory [10]. In fact, with the advent of socially intelligent chatbots, recruitment and indoctrination could be automated using predetermined statements, questions, and responses. Even the process of social commitment may be outsourced to software.

Targets are often emotionally vulnerable and under the age of 25. In many cases, they are less educated and are attracted to simple messages that are difficult to counter-argue. Conveniently for threat actors, such basic messaging is a cornerstone of memes. These individuals are often at crisis points in their lives, feel emotionally vulnerable, or are socially isolated. Many are lifelong wound collectors searching for purpose. Social media platforms, such as Facebook, can be used to locate such individuals. In fact, the application can even delimitate users based on daily mood or level of emotional vulnerability [10].

Vivid emotional messages; communal warmth or acceptance; or a shared mindset, such as humor, are all strong messaging attractors. Lonely and depressed people are especially susceptible to such memetic manipulation, because the small bursts of purpose or enjoyment can develop into a dependency. Indoctrination efforts propagating trust in the community, a fight for a justified cause, or faith in a charismatic leader appeal to vulnerable populations. Even just reassurance that someone is not alone or that the community “knows the answer” can be irresistible to a target. Successful indoctrination depends on a strong socionic motivator, such as an infallible leader or an irrefutable cause. The community establishes and bases its interpretation of reality around that entity. For instance, foreign ideological terrorists rely on digital recruitment and indoctrination efforts in other nations. They lure lifelong wound collectors into their communities and befriend them. Afterward, they subject them slowly to propaganda, disinformation, and misinformation. They manipulate emotional triggers, such as sympathy, anger, and gratitude. They cultivate dependencies on the authoritative entities of the ideology, the community, and the leaders. Recruits are convinced to believe the extreme and erroneous interpretation of Islam. They are convinced to act as “living martyrs” whose kinetic actions will herald change and will be rewarded

with bliss. Candidates are isolated or withdrawn into near-isolation and then coerced into making repeated public commitments to the community through videos or manifestos. Finally, the adversary acts and the collective, who may have never been within a thousand miles of the individual or known their name, takes credit for the attack [10].

COLOR PSYCHOLOGY

Choice of colors and color associations is vital to effective meme construction. The palette must incline the audience toward a feeling, mood, and ideological stance, and to do that, it must capture both the “brand” of the product and resonate with the collective consciousness of the community. While color is too dependent on personal experiences to be translated universally to specific feelings, there are broad messaging patterns in color perceptions that can be exploited by a knowledgeable adversary. A study titled “Exciting red and competent blue” confirmed that purchasing intent is affected by colors greatly because of their effect on how a brand is perceived; colors influence how customers view the “personality” of the brand in question. When it comes to picking the “right” color, research has found that predicting consumer reactions to color appropriateness is far more important than the individual color itself. Brands can be a cross between two traits, but one is always dominant. While certain colors do align broadly with specific traits (e.g., brown with ruggedness, purple with sophistication, and red with excitement), nearly every academic study on colors has found that it is far more important for colors to support the personality of the idea rather than stereotypical color associations (i.e., red equates to anger). In a study titled “Impact of color on marketing,” researchers found that up to 90 percent of snap judgments made about products can be based on color alone, depending on the product. Regarding the role that color plays in branding, results from another study show that the relationship between brands and color hinges on the perceived appropriateness of the color being used for the particular brand, such as whether the color “fit” the product sold [13].

ILLUSORY CORRELATION

An evolutionary influence on everyday thinking is the mind’s tendency to search for and impose order on random events. Illusory correlation is the perception of a relationship between two things where none exists or the perception of a stronger relationship than actually exists. It predominantly occurs when one already expects a strong correlation. In 1965, William Ward and Herbert Jenkins showed participants the results of a hypothetical 50-day cloud seeding experiment. They told participants which of the 50 days the clouds had been seeded and which days it had rained. In truth, the data set consisted of a mix of random numbers. Sometimes, it rained after seeding, and sometimes it did not. Nevertheless, participants became convinced, in conformity with the implanted conclusion about seeding, that they had observed a causal relationship in the data. Numerous other experiments have verified that people misperceive random events easily as confirming their beliefs. When a correlation exists, we are more likely to notice and recall confirming instances. People do not notice when unrelated events do not correlate (i.e., the lack of a causal relationship) [10].

Illusory correlation is a powerful misinformation and disinformation tool in the digital age. It can be used to manipulate a population that is seeking truth or belief of truth on a topic. Datasets and “facts” can be disseminated to inquisitive but misinformed audiences, in near real-time. False but convincing data can be fabricated instantaneously from historical data sets or big data algorithms and machine learning systems. A portion of the public is seeking scandal constantly, and they can be manipulated with “leaked” data sets. Individuals, especially those unqualified to interpret the data in the first place, are

surprisingly unlikely to question the legitimacy of leaked data [10].

COLLECTIVISM

Collectivism is the act of prioritizing the goals and well-being of one's group (e.g., one's extended family or workgroup) over the welfare of the individual and defining one's identity accordingly. It is controlled strongly at the spiral dynamic evolutionary stage and, to a lesser extent, at the socionic level. People in groups are more proactive and engaged when the group is challenged, or they are tasked with something intrinsically appealing to their disposition [10]. Attackers can internally steer and externally challenge collectives and groups using troll accounts, bots, weaponized hashtags, or opposing groups to optimize their proactivity. For instance, after riling radical factions concerned with an issue, an adversary can latch onto a current event via the Hegelian dialectic, launch attacks at one or both sides of the issue to drum up support, and inspire both a protest and a counter-protest in real-time. Other psychological and memetic manipulations can be leveraged to ensure that radical members commit violence or that the event captures the mainstream media.

Collectivism also ensures that the adversary can remain obfuscated within the group. Members tend to defend each other, especially prominent figures, such as those accounts backed by bots. Consequently, the attacker can use collectivism and their faux viral status to gain control of the group and to steer its directive and the perceptions of its members [10].

COMPLEMENTARITY

Complementarity is the popularly supposed tendency for people to choose friends or partners who are different from themselves and complete what they're missing (e.g., for a shy person to choose a highly social person as a romantic partner). A number of the socionic intertype relations depend on a sense of complementarity. Furthermore, individuals, especially those who are troubled or isolated, seek out digital communities based on this tendency. For example, a person with views on maintaining their right to have guns may align with a person who is against religious scrutiny. Even though the views are not related, both have a shared interest in maintaining constitutional rights and therefore complement each other, bolstering their collective positions [10].

Complementarity subverts the mind's defenses and internal beliefs. To a degree, people engage in counterintuitive behaviors as if they were engaging in a "guilty pleasure." Individuals can be influenced through the use of complementary information or views that fit or complete their view of the world, especially in the face of opposition [10]. For example, even those initially opposed to violence might be recruited and indoctrinated into radical online collectives, such as the Muslim Brotherhood or antifa, and persuaded to plan or conduct campaigns to which they would otherwise be opposed.

CONFIRMATION BIAS

Confirmation bias is the tendency to search for and weigh information that confirms one's preconceptions more strongly than information that challenges them. This occurs more than anything else; we act to preserve our understanding of the world and often disregard contrary information. In influence, it is vital to identify which perceptions are in conflict and how they might be swayed. It also leads to a tendency for people to remember success and forget promises or mistakes. This helps to explain why people are so willing to forget promises made to them or past blunders, as the ends appear

to justify the means. Thus, a target population can be influenced by many promises and remarks, and to a non-critical eye, the outlandish and untrue are forgotten and the correct predictions seem powerful. Confirmation bias further helps to shape how one is influenced, since we have tendencies to remember only the information pertinent to sustaining our views and delete the rest from memory. Thus, a fake news site could post multiple fake targeted articles and not be recognized as fake, since the fake articles will be forgotten, and the fake ones that are well-received will confirm beliefs and gain trust for the site[10].

COUNTERFACTUAL THINKING

Influencers play both sides of issues relevant to their targets. One effective mechanism that they can leverage against one or more sides is counterfactual thinking. It focuses on the imagined reminiscence of “what could have been.” Counterfactual thinkers ponder alternative scenarios and outcomes that might have happened but didn’t. Often, they over-idealize those wistful thoughts to the point that reality becomes a bitter disappointment. Attackers can leverage those musings and negative feelings to sow discord and mobilize movements. According to a 1997 study, “Affective Determinants of Counterfactual Thinking,” the significance of the event is correlated linearly with the level of counterfactual thinking. As a result, close elections, charged societal debates, the passage of controversial legislation, and other events that leave one or both sides of an issue extremely emotional are prime targets for memes or trolled discourse that capitalizes on counterfactual thinking [10].

DISPOSITIONAL ATTRIBUTION

Dispositional attribution explains that a person’s behavior results more from their traits and beliefs than from external or cultural factors [10]. As such, digital attackers will garner more sway by appealing to the evolutionary urges and ingrained ideological dispositions of their targets than they would by tailoring their campaigns to focus on a single issue or cause. A chaos operation that aims to promote xenophobia and anger across all digital vectors is going to be more successful than one that only intends to target one race, class, or individual. Unlike tailored operations, the impact of chaos ops is more significant when the scope is broad, and the desired outcome is somewhat abstract.

COGNITIVE DISSIDENCE

Cognitive dissonance is the discomfort or tension that arises from simultaneously holding two or more psychologically incompatible thoughts. Leon Festinger’s theory of cognitive dissonance proposes that people are motivated to avoid or minimize cognitive dissonance whenever possible. Influence begins with a disruption, such as a conflict between the current view and desired view. When bombarded with reports and information, targets either begin to believe it or to segment off into their own polarized views [10]. In influence campaigns, both can be useful. By planting an initial idea, over time a conflict can be created, and through targeted manipulation, the desired outcome can be achieved. For instance, initial interest in legislation may be nonexistent. A foreign or domestic digital adversary can leverage bots and trolls on Facebook, weaponize hashtags on Twitter, or promote radical podcasts on iTunes to generate “grassroots” support of the issue or bill. Propaganda, fake news, and misinformation can also be deployed to shape public opinion. Similarly, a sudden influx of information may result in overwhelming support, especially when coming from authority figures. If the dissidence instead pushes the individual to separate and decide on the matter regardless of propaganda, the individual becomes able to be influenced in other ways, such as isolating them from their communities or radicalizing them.

DEINDIVIDUALIZATION

Deindividuation accounts for the loss of self-awareness that occurs when people are not seen or paid attention to as individuals (for example, when they become absorbed in a role that reduces their sense of individuality or accountability or when they become part of a crowd or a mob). Often with influencing and manipulation of a populace, the deindividuated become the primary targets. By offering a voice to the voiceless, a collective strength can be forged. Furthermore, as the influenced population becomes more and more deindividuated in the message and efforts, it is less likely that the group will break down [10]. Radical factions, such as antifa, the Muslim Brotherhood, Anonymous, and many others, depend on deindividuation for recruitment and continued loyalty on online vectors. These groups tend to target wound collectors who already have a decreased sense of self because those individuals are easier to radicalize and will depend on the group more than others might.

DISPLACEMENT

Displacement is a distractionary and reactionary tactic that influencers can employ to redirect aggression to a target other than the source of one's anger or frustration. Displacement is most prevalent when direct retaliation against the initial source of anger or frustration is not possible. Afterward, those frustrated are prone to overreaction against any minor inconvenience or trivial offense [10]. Generally, the new target is a safer or more socially acceptable target. This could occur microscopically on online forums and social platforms to demonize critics, or it could occur macroscopically to pit a collective against a specific target.

ALTRUISM

Altruism is the motive to increase another's welfare without conscious regard for one's own self-interest. It is essentially using the "greater good" as a key motivator. In general, people tend to strive for an altruistic outlook within society. People's altruistic natures can be abused, however. Many in online communities exhibit false altruism and can be angered easily when their dedication to causes is questioned or when their self-interest is revealed [10].

IMMUNE NEGLECT

People neglect the speed and capacity of their psychological immune systems. Internal processes of rationalizing, discounting, forgiving, and minimizing emotional trauma are rarely considered consciously. Since most are ignorant of their mental immune system, they tend to adapt to disabilities, emotional trauma, and other inconveniences too rapidly. Aberrant events are permitted and eventually normalize in the collective conscious. Interestingly enough, research suggests that immune neglect causes populations to be less distressed by major traumatic events than they are by small irritants, because their minds accept and adapt to the circumstances faster [10].

Many believe that influence should be gradual and hidden. While certain messages and particular audiences necessitate incremental conditioning and obfuscation for normalization to occur, operations that leverage highly emotional or politically charged events should be more immediate to have a greater and swifter impact.

ILLUSION OF SELF-ANALYSIS

According to research, our intuitions are remarkable in their inability to ascertain what influences us

and to what extent we are influenced. When the motivators of our behavior are conspicuous and the correct explanation corresponds to our intuition, self-perceptions tend to be accurate. When the causes of behavior are obvious to an external observer, they tend to be obvious to us as well. When motivation is not a conscious consideration and is maintained internally, however, analysis is unreliable. When manipulation is not obvious, its effect often goes unnoticed. Studies on perception and memory indicate that people are more aware of the results of their thinking than the process. Professor Timothy Wilson has postulated that the mental processes that control social behavior are wholly distinct from the mental processes through which behavior is evaluated and explained. Our rational explanations tend to omit the unconscious attitudes, factors, and processes that determine behavior. In nine experiments, Wilson found that the attitudes that people expressed toward people or things could be used to predict their subsequent behavior relatively accurately; however, if those individuals were first asked to analyze their feelings, then their admissions no longer corresponded to their actions. People are capable of predicting their feelings, such as happiness in a relationship, but thinking about their circumstances clouds their ability to predict their future performance accurately [10].

In short, people are, to a degree, strangers to themselves. Self-reports are unreliable and untrustworthy unless the decisions are driven cognitively and dependent on rational analysis. The sincerity with which people respond, report, and interpret their experiences is not a guarantee of the validity of that sentiment. Vulnerable individuals can be more or less told how they feel and think if sufficient emotional stimuli are applied. Even when they discount the attempts openly, they may still be susceptible [10]. At a bare minimum, ideas and feelings can be planted memetically in the minds of the audience. Individuals who judge themselves unaffected may also be undefended against the influence. As a result, their false sense of security may actually assist the propaganda, misinformation, or disinformation in rooting itself in the subconscious.

FRAMING

The way a question or an issue is posed can influence people's decisions and expressed opinions. Framing controls the perception of an issue entirely and the response options available [10]. It is vital to the effective design of every variation of propaganda and meme because, if done correctly, it galvanizes the target to follow one of only a few predetermined and predesigned courses of action. The frame could be a logical trap ("Are you opposed to the current administration?" with options of Yes/Somewhat/Other) or it could force a moral conundrum ("True Christians prove themselves by donating to this cause"). Even the engagement-baiting memes that spread like wildfire on social media ("like and X will happen" or "share and Y will be in your future") rely on a less effective form of framing. Sophisticated memetic frames will engage the viewer and mentally distract or coerce them into not considering response options other than those proffered by the influencer. The target should believe that they have no recourse but to act according to the threat actor's intent.

ATTITUDE INOCULATION

In order to escalate the magnitude and impact of tensions within or between groups, threat actors can leverage their bots and trolls to strategically strengthen the arguments and mental defenses of members of those communities. Attitude inoculation is the practice of subjecting individuals to weak attacks on their beliefs or ideologies, so that when stronger attacks occur, they will have more powerful refutations available [10]. Defense of an ideology or cause unites the surrounding community and further indoctrinates members through groupthink and collectivism. When attitude inoculation is applied

properly, the influencer can shape and train an ideological community or social network group to be exactly the weapon they need for their cyber-kinetic influence operation.

IMPACT BIAS

Affective forecasts – predictions of future emotions – are strong influencers of decisions. If people estimate the intensity or duration of the emotional weight of a decision incorrectly, then they are prone to erroneously prepare or emotionally invest in the choice and often, a hastily made decision is later regretted. People assume that if they get what they want, then they will experience fulfillment immediately. Such is not the case. For instance, people believe that if their preferred candidate wins an election, they will be comforted and delighted for an extended period. Instead, studies reveal that they are vulnerable to an overestimation of the enduring impact of emotion-causing events. This effect is referred to as impact bias. Worse, people studies suggest that people are more prone to impact bias after negative events. At a fundamental level, decisions are made by estimating the importance of the event and the impact of everything else; however, when the focus is centered on a negative outcome, subjects discount the importance of everything else that could contribute to reality and thereby over-predict their enduring misery [10]. Adversaries can exploit impact bias in their virtual campaigns by focusing their propaganda and misinformation narrowly on negative events, asserting the faux-eventuality of worst-case scenarios repeatedly in their interactions on social media platforms, and disseminating memes that encapsulate only the most negative and fear-mongering aspects of current events. In effect, weaponizing impact bias enables the attacker to shape the digital narrative into a one-sided, entirely negative “conversation” with an anxious and mentally exhausted target population [10].

BEHAVIORAL CONFIRMATION

Behavioral confirmation is the epitome of the self-fulfilling prophecy in which people’s social expectations lead them to behave in ways that cause others to confirm their expectations. This applies to influence in that once those around an individual begin to conform to a political view or expectation, those that typically transverse the middle or represent the undecided become receptive to messaging and manipulation through not wanting to rock the boat with friends and relatives. Even when the messages do not appeal to them, the individual will conform or cooperate with more polarized stances. As such, social expectations, such as “we are a Republican family” or “this is a liberal college,” lead one to subconsciously negotiate the spectrum slowly to align their own personal views to meet social expectations around them, until the individual is convinced that they were always like that. Essentially, we indoctrinate ourselves to meet the perceived expectations around us and avoid conflict [10].

BYSTANDER EFFECT

Bystander effect is the tendency for people to be less likely to help someone in need when other people are present than when they are the only person there. Also known as bystander inhibition, the bystander effect can be seen in loose terms as the segment of the population that remains inert even in the most crucial junctures. They are influenced through ideas like “my vote doesn’t count anyway” and “all government is corrupt.” Here, the goal is not to manipulate or influence the population for a result; rather, it is to convince the population to simply not contribute in any meaningful way [10].

CATHARSIS

The catharsis theory of aggression is that people’s antagonistic drive is reduced when they “release”

aggressive energy, either by acting hostilely or fantasizing about aggression. To one degree or another, everyone strives to attain catharsis. The drive for catharsis is one of the most primal motivators, and it can be leveraged by influencers willing to provide an outlet or pay attention to someone with pent-up frustration or rage. Wound collectors and those obsessed with radical change are the most vulnerable to operations that weaponize the need for catharsis. According to the “hydraulic” model, accumulated frustration and aggression require a release. This form of catharsis often takes the form of expressions of prejudice, acts of aggression, and other outlets [10].

...

“Cultural programming and institutional indoctrination begins in the elementary school system. The narrative illusion, introduced by instructional programmers(teachers), weaves its way throughout the labyrinth of the mind and colonizes the psychology of the student targets.”

...

LOGICAL FALLACIES SHAPE TROLL AND BOT RESPONSES

Adversaries employ logical fallacies to disarm attempts to expose their campaigns, dismiss counterarguments, and dismantle resistance to their influence. Fallacies are concise, convincing attack templates employed in interactions with the target to maximize the delivery and pervasiveness of the meme while minimizing the time and attention necessary to convince the audience to adopt and internalize the messaging. These rhetorical tools are used in some of the most convincing arguments in everyday discourse, despite being predominantly vacant of meaning. In fact, the attractiveness of the fallacy is the main reason they are used so profusely in digital spaces. They tantalize the audience and seize their attention, thereby obfuscating any weaknesses in the underlying message. As a result, if the audience agrees, then they absorb the content; if they disagree, they argue, develop an emotional investment, and internalize the message even more deeply.

FALLACY 1: Strawman

The attacker misrepresents someone’s argument to make it easier to attack. By exaggerating, misrepresenting, or just completely fabricating someone’s argument, it’s much easier to present their position as being reasonable while also undermining honest, rational debate [14].

FALLACY 2: Loaded Question

The troll or AI bot distracts from meaningful dialogue or provokes an engineered response by asking a question that had a presumption built into it so that it couldn't be answered without appearing guilty. Loaded question fallacies are particularly effective at derailing rational debates because of their inflammatory nature. The recipient of the loaded question is compelled to defend themselves and may appear flustered or taken aback [14].

FALLACY 3: Composition/Division

The adversary implies that one part of something has to be applied to all, or other, parts of it or that the whole must apply to its parts. Often, when something is true for the part, it does also apply to the whole, or vice versa, but the crucial difference is whether there exists good evidence to show that this is the case. Because audiences observe consistencies in things more than discrepancies, their perceptions can become biased by the presumption that consistency should exist where it does not [14].

FALLACY 4: Begging the Question

A circular argument is presented in which the conclusion was included in the premise. This logically incoherent argument often arises in situations where people have an assumption that is very ingrained and therefore taken in their minds as a given [14].

FALLACY 5: The Texas Sharpshooter

Cherry-picked data clusters or an alleged pattern may be used to suit an argument. Clusters naturally appear by chance but don't necessarily indicate that there is a causal relationship [14].

FALLACY 6: False Cause

The audience is led to believe that a real or perceived relationship between things means that one is the cause of the other. Many people confuse correlation (things happening together or in sequence) for causation (that one thing actually causes the other to happen). Sometimes correlation is coincidental, or it may be attributable to a common cause [14].

FALLACY 7: Ad Hominem

Attacks against an opponent's character or personal traits in an attempt to undermine their argument are irrational but effective at distracting an audience and derailing a conversation. Ad hominem attacks can take the form of attacking somebody overtly or casting doubt more subtly on their character or personal attributes as a way to discredit their argument. The result of such an attack can be to undermine someone's case without actually having to engage with it [14].

FALLACY 8: Bandwagon

An attacker may appeal to gained or fabricated popularity or the fact that many people do something as an attempted form of validation. The flaw in this argument is that the popularity of an idea has absolutely no bearing on its validity; nevertheless, many are convinced that the loudest or most prevalent narrative is the truth [14].

FALLACY 9: No True Scotsman

A troll may make appeals to their innocence or purity as a way to dismiss relevant criticisms or flaws

in their argument. This form of faulty reasoning is interpreted as valid by the audience, because it is presented as unfalsifiable, since no matter how compelling the evidence is, one simply shifts the goalposts so that it wouldn't apply to a supposedly "true" example. This kind of post-rationalization is a way of avoiding valid criticisms of an argument [14].

FALLACY 10: Appeal to Nature

Attackers may argue that because something is "natural," it is therefore valid, justified, inevitable, good or ideal. While many "natural" things are also considered "good," naturalness itself doesn't make something good or bad [14].

FALLACY 11: Middle Ground

An adversary may claim that a compromise, or middle point, between two extremes must be the truth. Much of the time, the truth does indeed lie between two extreme points; however, sometimes a thing is simply untrue and a compromise of it is also untrue. Halfway between a truth and a lie is still a lie [14].

FALLACY 12: Appeal to Emotion

Attackers often attempt to manipulate an emotional response in place of a valid or compelling argument. Appeals to emotion include appeals to fear, envy, hatred, pity, pride, and more. It's important to note that sometimes, a logically coherent argument may inspire emotion or have an emotional aspect, but the problem and fallacy occur when emotion is used instead of a logical argument or to obscure the fact that no compelling rational reason exists for one's position. Facts exist irrelevant of feelings, but emotions may be invoked to cloud judgment and rational thought [14].

FALLACY 13: Personal Incredulity

Trolls may argue that something difficult to understand is untrue. Complex subjects require rigorous understanding before one can make an informed judgment about the subject at hand; this fallacy is usually used in place of that understanding [14].

FALLACY 14: The Fallacy Fallacy

An attacker may claim that because an argument has been presented poorly or a fallacy has been made, that the claim itself must be wrong. They thereby gain unquestionable authority in the discussion. It is entirely possible to make a claim that is false yet argue with logical coherency for that claim, just as it is possible to make a claim that is true and justify it with various fallacies and poor arguments [14].

FALLACY 15: Slippery Slope

A meme may convey that if A is allowed to happen, then Z will eventually happen too; therefore, A should not happen. The problem with this reasoning is that it avoids engaging with the issue at hand and instead shifts attention to extreme hypotheticals. Because no proof is presented to show that such extreme hypotheticals will in fact occur, this fallacy has the form of an appeal to emotion fallacy by leveraging fear. In effect, the argument at hand is tainted unfairly by unsubstantiated conjecture [14].

FALLACY 16: Tu Quoque (You Too)

A troll may avoid having to engage with criticism by turning it back on the accuser, thereby answering criticism with criticism. This fallacy appeals to hypocrisy. It is commonly employed as an effective red

herring, because it takes the heat off someone having to defend their argument and instead shifts the focus back to the person making the criticism [14].

FALLACY 17: Personal Incredulity

Disbelief in an argument or cause may be framed as irrefutable evidence that the argument is misleading or false. This usually takes the form of immediate dismissal of facts or a questioning of the integrity of the source material. It is effectively the weaponization of anecdotal observations over empirical evidence [14].

FALLACY 18: Special Pleading

A troll may shift the purpose of the argument or claim an exception when their claim is proven to be false. They may even play the victim [14].

FALLACY 19: Burden of Proof

An attacker may shift the burden of proof from the person making a claim to someone else to disprove. The burden of proof lies with someone who is making a claim and is not upon anyone else to disprove. The inability or disinclination to disprove a claim does not render that claim valid or give it any credence whatsoever. It is important for audiences to note, however, that they can never be certain of anything, and so they must assign a value to any claim based on the available evidence. To dismiss something on the basis that it hasn't been proven beyond all doubt is also fallacious reasoning [14].

FALLACY 20: Ambiguity

A foreign influence operative may employ a double meaning or ambiguity of language to mislead or misrepresent the truth. Politicians are often guilty of using ambiguity to mislead and will later point to how they were technically not outright lying if they come under scrutiny. The reason that it qualifies as a fallacy is that it is intrinsically misleading [14].

FALLACY 21: Appeal to Authority

A provoker might argue that because an authority thinks something, it must, therefore, be true. It is important to note that this fallacy should not be used to dismiss the claims of experts, or scientific consensus. Appeals to authority are not valid arguments, but it is also unreasonable to disregard the claims of experts who have a demonstrated depth of knowledge, unless one has a similar level of understanding and access to empirical evidence. It is entirely possible, however, that the opinion of a person or institution of authority is wrong; therefore, the authority that such a person or institution holds does not have any intrinsic bearing upon whether their claims are true or not [14].

FALLACY 22: Genetic

An operative may suggest that a community judge something as either good or bad on the basis of where or whom it comes from, rather than its inherent validity. This fallacy avoids the argument by shifting focus onto something's or someone's origins. It's similar to an ad hominem fallacy in that it leverages existing negative perceptions to make someone's argument look bad without actually presenting a case for why the argument itself lacks merit [14].

FALLACY 23: Black-or-White (False Dilemma)

An issue may be presented with two alternative states as the only possibilities, when in fact more possibilities exist. The tactic has the appearance of forming a logical argument, but under closer scrutiny, it becomes evident that there are more possibilities than the either/or choice that is presented. Binary, black-or-white thinking doesn't allow for the many different variables, conditions, and contexts in which there would exist more than just the two possibilities put forth. It frames the argument misleadingly and obscures rational, honest debate [14].

FALLACY 24: Anecdotal

The adversary may use a personal experience or an isolated example instead of a sound argument or compelling evidence. It's often much easier for people to believe someone's testimony as opposed to understanding complex data and variation across a continuum. Quantitative scientific measures are almost always more accurate than personal perceptions and experiences, but our inclination is to believe that which is tangible to us, and the word of someone we trust over a more "abstract" statistical reality [14].

...

*“Manufacturing consent begins by weaponizing
the meme and utilizing the censorship
algorithms of Google, Facebook, Twitter, and
YouTube.”*

...

*“The narrative illusion is a linguistic construct
that we culturally validate and live inside, like
an invisible cage.”*

...

GUERRILLA TOOLS TECHNIQUES & PROCEDURES

Influence operations designed to normalize foreign influence, evoke mass chaos, or enflame societal tensions are inexpensive and rely on publicly available and mostly free digital tools and platforms. Though nation-state APTs and the intelligence community have far more sophisticated tools, low-level “guerrilla” operatives can achieve the same, if not greater, influence over a population through minimal cost and public platforms. In fact, because influence operations are asymmetrical by design, unsophisticated and miserly threat actors achieve a far more significant result per investment than nation-state sponsored and well-resourced actors do.

TOOLS

Hacking, the art of abstracting new insights out of the old data, is a skillset that will be a requirement for all nation-states and in all forms. It is no longer enough to confront an aggressor directly or indirectly; now a nation-state must also stalk the aggressor, and at the first indication they are winding back to strike, multiple templates for offensives that have been prepared in advance for such an incident must crush those memes and narratives directly. Mock them, berate them, criticize them. The combination of images, wording, colors, fonts, and distribution vector variations must be instant and fierce.

KALI LINUX

Kali Linux is an open source Debian-derived Linux distribution that was developed for penetration testing and offensive security. It contains numerous tools that can be used for cyber-attacks or intelligence gathering operations against an individual, group, or population as a preliminary stage of the influence campaign. Kali includes features and tools that support the Wireless 802.11 frame injection, deploy one-click MANA Evil Access Point setups, launch HID keyboard attacks, and conduct Bad USB MITM attacks. Among other applications, the download contains the Burp suite, the Cisco Global Exploiter, Ettercap, John the Ripper, Kismet, Maltego, the Metasploit framework, Nmap, OWASP ZAP, Wireshark, and many social engineering tools [15].

The Kali Linux operating system is a free open source download that can be installed on nearly any system or turned into a boot disk on removable media. The included features and tools are a literal plug-and-play attack campaign and influence operation framework and library. Numerous tools can be used to develop and deploy convincing social engineering lures. Nmap, Wireshark, and other applications can

be used to derive network and platform metadata, which an attacker could use to calibrate their memes, lures, mediums, or propagation vectors [15].

MALTEGO

Maltego, an open source intelligence and forensics application that gathers massive amounts of data from social media platforms, could be used for a similar purpose to target specific members of a group, to develop an optimal persona based on the sociotics and evolutionary characteristics of the populations, or to impersonate a key member by hijacking their accounts or mimicking their actions [16].

METASPLOIT

The Metasploit framework consists of anti-forensic, penetration testing, and evasion tools, which can be used against local or remote machines. Metasploit's modular construction allows any combination of payload and exploit. Additionally, Metasploit 3.0 includes fuzzing tools that can be used to discover vulnerabilities and exploit known bugs. Adversaries can use port scanning and OS fingerprinting tools, such as Nmap, or vulnerability scanners, such as Nexpose, Nessus, and OpenVAS, which can detect target system vulnerabilities that can then be used to glean the system information necessary to choose an exploit to execute on a remote system. For influence operations, the scanning tools should also determine the browser type, native applications, and hardware (such as camera and microphone) capabilities. Metasploit is capable of importing vulnerability scanner data and comparing the identified vulnerabilities to existing exploit modules for accurate exploitation. The payload could be purchased from a Deep Web market or forum, or it could be crafted specifically for the target based on the objectives of the influence operation; the technical specifications of the system; and the sociotic, psychological, and demographic characteristics of the target user [17].

AUDIBLE STIMULI

The audiences of horror movies are not meant to be simple spectators; they are passive participants. While immersed, they become convinced on some level that they are accompanying the characters around a dark corner or through a shrouded doorway to strange and disturbing locales. Though the audience remains safe in their seats at the theater or their living room when the monster or killer emerges from the shadows, the movie leverages their suspended disbelief to make their hair to stand on end, make sweat emerge from their skin, or cause them to leap from their seats. Horror movies rely on a specific ambiance that is generated from a careful balance of visual and audio stimuli that induces a sense of anxiety, suspense, or fear in the audience. Discomfort, anxiety, and fear are powerful behavioral influencers that attackers can inflict subtly on a lured audience by incorporating well-documented movie techniques into their broadcasts or visual propaganda. For instance, *The Shining* and other movies invoke an instinctual fear response by merging animal calls, screams, and the sounds of distressed animals and other nonlinear noises deep in the complex movie score. Harry Manfredini, the creator of the music score for "Friday the 13th," elaborated, "The sound itself could be created by an instrument that one would normally be able to identify but is either processed or performed in such a way as to hide the actual instrument." The effect of these subtle and often entirely obscured sound waves was the evocation of a mini adrenaline rush from the psychological "fight or flight" instinct of the viewer. A similar disorienting effect occurs when a sound is removed from its normal context and retrofitted into an unfamiliar one. The listener's brain recognizes the disparity but is often unable to bypass the discrepancy. Audiences may also be conditioned to associate specific sounds with certain actions. In thrillers, this manifests as cued scores that signify when the killer is near; heavy, echoed breathing; or other obvious

but learned audible cues [18].

Infrasound – low frequency sounds below 20 Hz – lie mostly outside the human spectrum but can be felt in bones and understood by brains. Infrasound can be created naturally by some animals for communication or generated by wind, earthquakes, or avalanches. Movie composers exploit infrasound just above or below the human hearing threshold to incite a response in the audience that ranges from subtle anxiety to a visceral unsettling. Steve Goodman, in “Sonic Warfare: Sound, Affect, and the Ecology of Fear,” says that while the ways sound in media cause these responses in human perception are under-theorized, it likely has its place, especially with a sourceless vibration like infrasound. “Abstract sensations cause anxiety due to the very absence of an object or cause,” he writes. “Without either, the imagination produces one, which can be more frightening than the reality” [18].

Layered audio attacks have an even stronger effect on an audience. The combination of abstract or altered everyday noises with dialogue or music can unbalance an audience enough that the composer can make them feel a specific emotion. For instance, for the 2012 low budget zombie film “The Battery,” Christian Stella layered music on top of modulated recordings of power transformers, air conditioners, and other appliances. Manfredini aligns layered emotional audio cues with actions, objects, and colors to increase immersion and divide the audience gradually from logic and reason by exciting the psychological centers responsible for fear and panic [18].

An adversary could layer infrasound and masked disorienting noises with the dialogue of a fake news broadcast in the background of a video shared on social media or in any number of other situations or mediums to make the target audience fearful or panicked. Anxious and fearful populations become more tribal and isolationist. During the communique or afterward, the attacker can leverage false narratives of xenophobia; prejudice; or any other social, economic, or political topic that matters to the target demographic or evolutionary tribe. The narrative memes will mutate and propagate from the anxious and defensive victims to others in their families, communities, or evolutionary tribes until the memetic narrative becomes a self-replicating, self-mutating entity. Worse, weaponized sonic attacks may not have to be as hidden in other mediums to influence one or more targets; they could be paired with an exploit. Between October 2016 and October 2017, at least 24 American diplomats in Cuba may have been the victims of precision-targeted sonic attacks. An April 2017 letter from the Cuban Interior Ministry asked hospital officials if the diplomats were ever treated for “hearing and neurological ailments, which could be linked to harm to their auditory system from being exposed to levels of sound affecting their health.” Based on the descriptions of the incidents, it is possible, though speculative, that the attacks could have been the result of unique malware that was delivered to the victims’ mobile devices by exploiting known vulnerabilities. The malware would then utilize the hardware of the device to release an infrasonic frequency capable of disorienting and nauseating the target over an extended period [19].

POLITICAL CORRECTNESS

Political correctness, enforced by peer pressure and a sound method for introducing new rules and regulations that benefit the state, can be used to exert control over a community without the drama of introducing social laws that would otherwise encounter resistance by the population. With only a limited number of supporting bot and troll accounts and strategic baiting or an insistence on perspective, entire communities can be polarized based on the words or actions of an individual or small group, because

many partisan ideologies find meaning and garner a sense of community from finding and punishing perceived offenses to their members or cause.

FAKE NEWS

Fake news plants false and dangerous ideas into the minds of a population. It is tailored to the spiral dynamic, socionic, and psychographic profiles of the target. Fake news causes chaos, breeds conflict, and decreases the access to accurate information, thereby decreasing the public's ability to make informed choices. Furthermore, it is cheap to produce and disseminate. Before the 2016 Presidential election, the Kremlin paid an army of more than 1,000 people to create fake anti-Hillary Clinton news stories targeting specific areas in key swing states Wisconsin, Michigan, and Pennsylvania [20]. The best place for a lie is in between two truths, and effective fake news blends truth and falsehood seamlessly until the narrative is sufficiently muddled and the readers' minds are satisfactorily muddled.

Even the insinuation of fake news can damage reputations and societal institutions. Weaponized erroneous allegations of "fake news" from seemingly trusted sources can instantly delegitimize invaluable investigative sources and consequently nullify months' or years' worth of groundbreaking revelations entirely. With the right message behind the right figurehead on the right platform, stories revealing ongoing atrocities, war crimes, slave trades, illegal business practices, or corruption can be mitigated entirely with a single tweet, Facebook post, or blog entry, often without the need to even address the issue. By attacking the source of the narrative with the "fake news" meme, indoctrinated audiences discount the original message immediately, adopt the bandwagon mentality, and join the attack campaign against the actual legitimate source.

UNAUTHORIZED ACCESS TO INFORMATION

Hacking or gaining access to a computer system can enable the attacker to modify data for a particular purpose. Hacking critical information infrastructure can seriously undermine trust in national authorities. For example, in May 2014, the group known as Cyber-Berkut compromised the computers of the Central Election Committee in Ukraine. This attack disabled certain functionalities of the software that was supposed to display real-time vote-counting. This hack did not disrupt the election process, because the outcome was reinforced by physical ballots. The impact would have been much greater if it had actually influenced the functioning of the voting system. Instead, it called into question the credibility of the Ukrainian government overseeing the fair election process. Evidence indicates that the attack was carried out by a proxy actor and not directly by the Russian government. Although Cyber-Berkut supports Russian policy toward Ukraine, there is not definitive proof that these hackers have a direct relationship with Russian authorities [2]. This makes the denial of involvement by the Russian government not only plausible but also irrefutable in an arbitrary legal sense. From the view of international law, the use of such an operation makes it almost impossible to relate these activities to a state actor. Another example is the security breach that affected the U.S. Office of Personnel Management in 2015, which resulted in major embarrassment for the U.S. authorities unable to protect the sensitive information of nearly all government personnel [2].

FALSE FLAG CYBERATTACKS

In April 2015, the French television network TV5 was the victim of a cyberattack from hackers claiming to have ties with Islamic State's (IS) "Cyber Caliphate." TV5 Monde said its TV station, website, and

social media accounts were all hit. Also, the hackers posted documents purporting to be ID cards of relatives of French soldiers involved in anti-IS operations. TV5 Monde regained control over most of its sites after about two hours. In the aftermath of the January 2015 terrorist attacks on Charlie Hebdo, it was quite obvious to the general public and the investigators that the attackers had ties with the IS organization. In June 2015, security experts from FireEye involved in the investigation of the hack revealed that pseudonym of IS was “Cyber Caliphate” for this attack. According to them, the Russian hacker group known as APT28 (also known as Pawn Storm, Tsar Team, Fancy Bear, and Sednit) may have used the name of IS as a diversionary strategy. The experts noticed some similarities in the techniques, tactics, and procedures used in the attack against TV5 Monde and by the Russian group. This can, therefore, be qualified as a false flag cyberattack, where the use of specific techniques (i.e., IP spoofing, fake lines of code in a specific language) will result in misattribution. Why would Russia hack, or sponsor and condone someone else hacking, a French TV station? The only obvious rationale behind these attacks, if conducted by Russia, is to sow confusion and undermine trust in French institutions in a period of national anxiety. TV5 Monde can be blamed for not protecting its networks properly and looking like foolish amateurs, unable to respond in an effective way. Although there is no direct connection, it could be argued that any action that undermined the French government may have led it to act in ways favorable to Russian interests. Here again, plausible deniability provides enough cover not to worry about the legality of such actions or any response of the victim. The fact that it was discovered only months later that there might be a link to the Russian government highlights the very limited risk of repercussions or countermeasures [2].

DISTRIBUTED DENIAL OF SERVICE (DDoS) ATTACKS

The most common ICOs are distributed denial of service (DDoS) attacks, and these provide a clear illustration of the disruptive effects of ICOs in general. The most famous DDoS attacks were the coordinated ones that occurred in April 2007 in Estonia during the civil unrest resulting from the government’s decision to move a Soviet memorial statue. DDoS attacks are probably still the prevailing option for many actors, as gaining access to a botnet is fairly easy and affordable. DDoS attacks are used to overwhelm the target’s resources (degradation) or stop its services (disruption). Attacks only affect the availability of internet services and do not infringe on the confidentiality or integrity of networks and data. The objective of these attacks is to undermine the targets’ credibility and embarrass governments or other organizations. In 2014 and 2015, NATO websites were the victims of such a campaign, and the disruption prompted significant concern, as the main aim of these attacks was to undermine NATO’s readiness to defend itself in cyberspace. They also have a “paintball effect” as they may give the impression of a severe cyberattack. Last but not least, it is very unlikely that a DDoS attack may be considered as a violation of international law, thus creating grounds for a state to conduct countermeasures against another state lawfully [2].

WEBSITE DEFACEMENTS

Although most website defacements or hacks of Twitter accounts have only very limited impact, their results can be quite catastrophic. In 2013, the Twitter account of the Associated Press was hacked, and a message claiming the White House was under attack was posted. This sent the stock markets down 1 percent in a matter of seconds. With High-Frequency Trading, short interruptions as a result of false messages can have profound financial repercussions. In most cases, however, website defacements are comparable to graffiti and can be classified as vandalism. Technically, they are not very complicated, and again, the effect lies mainly in the embarrassment it causes to the target. The aim is to sow confusion

and undermine trust in institutions by spreading disinformation or embarrass the administrators for poor network defense. The effectiveness of the attack lies in the media reaction; the exposure is far more important than the technical stunt itself. These attacks are minor stings, but taken together, they have the potential to erode credibility. Their long-term effectiveness, however, is questionable, as people become aware of their limited impact and network security is improved [2].

DOXING

Another technique that has been widely used in recent years is “doxing” (or “doxxing”), which is the practice of revealing and publicizing information on an organization (e.g., Sony Corporation) or an individual (e.g., John Brennan) that is private or classified, so as to shame or embarrass targets publicly. There are various ways to obtain this information, ranging from open sources to hacking. This type of action is on the rise, and if the data of people like the director of the CIA is accessible, that means that everyone’s might be. Doxing may be used for political purposes. For example, in February 2014, Victoria Nuland, then U.S. Assistant Secretary of State for European and Eurasian Affairs, made a rather obscene comment about the European Union in a telephone conversation with the U.S. Ambassador to Ukraine. Such an incident is embarrassing, but more importantly, it can create divisions among allies and jeopardize a common policy to address a crisis. Doxing can be an offshoot of an espionage operation and thus turned into an ICO, information obtained through a disclosed source to undermine the adversary. These activities cannot be qualified as a use of force or be deemed of a coercive nature under international law [2].

SWATTING

Swatting is a popular tactic among script kiddies and gamers, in which a false emergency call of a dire situation, such as a hostage crisis or bomb deployment, is made to law enforcement local to an unsuspecting target in an attempt to harass or inhibit the individual. It is primarily conducted out of revenge for some perceived harm or bragging rights. Swatting can lead to unintentional harm or loss of life if the target does not comprehend that they are being swatted or if police forces misinterpret the situation. Influencers can use swatting as an intimidation tactic against outspoken opposition to the propagation of the meme, to disrupt rival narratives, as fodder for anti-police sentiments, or as part of a false flag attack [2].

...

***“Cultural programming builds on a continuous
‘assembly line’
process of institutional indoctrination.”***

...

SOCIAL MEDIA PLATFORMS

Global social media usage reached 1.96 billion users in 2017 and is expected to grow to some 2.5 billion users in 2018. As of 2017, daily social media usage of global internet users averaged 135 minutes per day, an increase from 126 daily minutes in 2016. It is the utmost prerogative of social media platforms to increase users' usage and dependency on the platform. They want users to check their feeds, pages, and streams every few minutes, regardless of whether it interrupts their workflow, disrupts their real-world interactions, or inhibits their emotional stability. In 2017, 81 percent of U.S. Americans had a social media profile, representing 5 percent growth compared with the previous year. Young Americans are the most likely to use social networks, with usage at 90 percent; however, use by those 65 and older is increasing rapidly. In 2015, the Pew Research Center estimated that 65 percent of American adults were social media users.

Social media platforms are free or mostly free to users because they collect, analyze, and sell consumer data to external third-parties who are interested in personal and global insights into user behavior, interests, and motivators. Platforms further capitalize on users' attention by selling the ad space within and surrounding the platform. They control their users' perspectives through the selective display, agenda-oriented curation, and dependency-cultivating delivery of content, news, and community.

Mobile devices have permanently and irrevocably altered the digital threat landscape because the devices tend to travel with the user wherever they go. While at home, at work, at school, or on vacation, mobile devices and the social media platforms with constant access to and control over those devices accompany their users. A study conducted by British psychologists found that young adults use their smartphones an average of five hours a day, roughly one-third of their total waking hours, and that an overwhelming majority used social media.

Many platforms have expanded their initial capabilities to increase user functionality and dependence. For the purpose of the attack vectors, we will focus on the predominant use of that platform.

ACCOUNT WEAPONIZATION

Every layer of a social media account or other digital accounts can be tailored to optimize the weaponization of the meme. Usernames can contain keywords or triggering words or phrases. Images can be of memes, public figures, or sympathetic profiles based on race or gender. The demographic information and messaging can also be used to lend legitimacy or community to anyone who views the account. The age of the account, the number of followers or friends, the content liked, shared, and commented on, and the communities joined also influence the believability of the account narrative.

PUBLIC MESSAGING PLATFORMS

Public messaging services such as Twitter are populated by at least 320 million registered users every month, in addition to all the voyeurs who congregate on the platform to absorb the messaging of their peers and idols. Twitter has recently become a more culturally relevant platform as politicians, Hollywood elite, and other societal leaders and figureheads have utilized it to deliver concise editorials or calls to action on numerous societal, political, and cultural issues and causes. As a result, the potential and potential harm of a stolen account are increased drastically. An adversary who weaponized a popular and trusted account could cause significant disruption in a short period. Additionally, threat

actors can leverage massive amounts of bot accounts to generate their own fake viral following, and they can likewise leverage retweets, weaponized hashtags, and follow-for-follow campaigns. Once the account has even a modest following, they can disseminate malicious links, propaganda, fake news, and other attacks across their own and public figures' networks.

Twitter bot “rental” services can be hired for set periods or to deliver tailored content to a specific target or target platform. For bot creation, Twitter account resellers are plentiful on Deep Web markets and forums. Otherwise, Twitter bot accounts can be created individually with handles, images, emails, and demographic information designed precisely to evoke a strong response, convey a subtle message, or lend a certain personality to the account. For instance, a bot attempting to incite violence or division within the “Black Lives Matter” communities will likely be more influential if the underlying account appears to have a history and if the account appears to be operated by someone who is black, according to the messaging, account information, display image, and handle. Attacks from community outsiders, such as a bot account that mimics a white supremacist, will evoke a tribal community response; meanwhile, bots that appear as community insiders can incite internal divisions and radicalization more easily by challenging the dedication, beliefs, and values of other community members. If either has a sizable following (of even a few dozen accounts, including other bots), then interaction of any type will result in a reaction. Every reaction can be manipulated and controlled through the guidance of bot accounts on either or both sides of the dispute until the desired outcome is achieved.

Cultivating a bot account to increase its audience and influence focuses on mass exposure. Bot accounts are grown naturally by interacting with legitimate Twitter accounts and gaining reciprocal followers and by auto-following niche figures and community members. A hundred Twitter accounts with a few hundred followers each amount to an audience in the tens of thousands. The organic flow of interaction, automatic tweets, and retweets will simulate an active account persona and imply authenticity behind the bot. Low-level bots add uses and drip links or pre-generated comments automatically. More sophisticated bots, often aimed at higher value targets, influence epicenters, or niche communities, will interact through real dialogue generated using artificial intelligence or automated libraries, such as WordAI's API. If the meme gains traction, it will migrate onto other platforms such as Facebook or Pinterest through users. Particularly virulent memes will mutate or evolve into derivatives on both the original platform, Twitter, and the new destination (e.g., Facebook), due to the user's desire to repurpose the meme to their argument and the loss of context, such as the source or platform. Each iteration of the meme increases the chaos and, oddly, the perceived authenticity of the underlying message within the community. Humanity's desire to comprehend and rationalize information transforms a suggestion into a rumor into gossip and eventually into the narrative.

IMAGE BOARD SITES

Most memes are images or have a visual component that distracts the viewer while their subconscious absorbs and internalizes the adversarial message. These sites, such as Instagram, Snapchat, Pinterest, Flickr, and DeviantArt, can be used to design and tailor the meme before spreading it to other platforms. Unsuccessful memes are discarded immediately, while memes that resonate are studied, improved, and propagated.

Most content migrates to Pinterest as a cascading impact of meme adoption on other platforms;

however, Pinterest bots can be rented and sold just like those of any other platform. Though not necessarily indicative of the actual audience, Pinterest bots are typically used to target women and feminist niches because they are perceived as the Pinterest audience. Bots re-pin images, follow users, and post fake news or malicious links.

In the run-up to the 2016 election, Pinterest became a repository for thousands of political posts created by Russian operatives seeking to shape public opinion and foment discord in U.S. society. Trolls did not post to the site directly. Instead, content spread to the platform from users who adopted it from Facebook and other sites and pinned it to their boards. Influence posts and ads intend to divide the population over hot-button issues, such as immigration and race. Influence pages on Facebook and Twitter weaponized supporters and opponents of “Blacktivism,” “United Muslims of America,” “Secured Borders,” “LGBT United,” and other highly polarized topics. Many of the accounts operated on multiple platforms (i.e., Facebook, Twitter, Instagram) and images from an estimated 83 percent of pages migrated to Pinterest through indoctrinated legitimate users. Of the hundreds of accounts investigated, only one account displayed the conventional characteristics of bot accounts, such as a lifetime of less than a year and limited interaction with other users. For instance, a Pinterest board dedicated to “Ideas for the House” featured an image of a police officer and text indicating that they were fired for flying the Confederate flag; however, the meme originated from the “Being Patriotic” Twitter and Facebook accounts, which were associated with the Internet Research Agency. Similarly, the “Heart of Texas” account that was disabled eventually on Facebook weaponized polarized users to spread its memes across multiple platforms and mediums by playing on their proclivities, beliefs, and fears. One image of a man in a cowboy hat urged viewers to like and share if they “wanted to stop the Islamic invasion of Texas.” Jonathan Albright, research director of the Tow Center for Digital Journalism at Columbia University, uncovered on Pinterest over 2,000 propaganda images tied to the Internet Research Agency. The migration of political memes to Pinterest is uniquely interesting, because the platform is not conventionally political. Pinterest does not enable users to spread content to innumerable networked users in the same manner as other social media applications. Pinterest is typically used to share crafts and artistic creations, rather than for the exchange of ideas or debate. Before foreign attempts to influence the 2016 election, political content had never gone viral on Pinterest. The spread of Russian coercive memes onto Pinterest could be an unintentional symptom of the multi-vector infection of American cultural communication mechanisms, or it could be a deliberate strategic attack component in a complex operation designed to pollute the entire information and social media landscape [21].

PROFESSIONAL NETWORKING SITES

Nearly every professional will utilize or be dependent upon an online professional network at some point in their career to create new connections, hire new talent, or search for new opportunities. Though LinkedIn is the premier service in this space, others such as Viadeo, Monster, and Xing also exist. The main attacks against users of professional networks are the delivery of memetic content or propaganda and the damage caused by social engineering and mimicry. Users are open to connecting, communicating, and sharing information by default. Adversaries can leverage that trust to persuade niche-specific targets to open links or consume fake news, misinformation, or disinformation that they otherwise would not. Academics, key professionals, and well-known networkers are prime targets for these attacks. Account details from the platform and other social media facilitate attacks where the adversary adopts a target’s information to lure others or cause reputational harm.

LinkedIn is the most business-oriented of the social media platforms, and as a result, it can be an immensely powerful tool for social engineering operations, precision targeting of niche communities, and small but more focused operations. Unlike Facebook or Twitter, where users can lie about their demographic information or hide their content from the global network, LinkedIn requires honesty, transparency, and accessibility as necessary functions. Any adversary can weaponize these aspects against unsuspecting users. LinkedIn bots can be used to force networking requests, articles, or messages.

Though some information on LinkedIn can be privatized to those external to a network, the majority of information, such as employment history, education, demographics, interests, or skills, is often left public to anyone with an account. Adversaries can collect basic information or rely on demographic or psychographic information, or spiral dynamics profiles, to tailor bots to certain users and community members. Worse, according to a court ruling, under appeal at the time of this writing, LinkedIn cannot prevent third parties, such as bot operators and data cultivators, from scraping members' data. Bots can like, share, comment, send invitations, endorse skills, or post or send fake news or malicious links automatically. Given that many use the platform to share their resume or search for employment, LinkedIn bots could pose as potential employers to collect resume information that could help facilitate identity theft. Stolen resumes, portfolios, writing samples, and company emails can be used in future spear phishing campaigns that imitate the initial victim to increase the success rate of the lure. Even emails from bot accounts to a target company's management that personnel with active LinkedIn accounts are searching or have accepted alternative employment, whether or not a conversation occurred, could cause pandemonium within major organizations.

MESSAGE BOARD SITES

Just as at the advent of the internet, forum-based sites remain the home of marginalized and self-isolating communities. Sites like Reddit and 4chan are populated by radical users and communities from every demographic. They typically follow more vocal accounts that appear to "know things" but that often actually only spout rhetoric that gratifies the beliefs of their ideological bubble. For instance, in early November 2016, WikiLeaks released emails from former Clinton campaign chairman John Podesta's account. One particular minor donor caught the attention of trolls on Reddit and 4chan along with the use of the word "pizza," which was used in discussions about fundraisers and regular outings. 4chan users began posting speculation and alleged connections that they had pieced together from haphazard internet searches. Others trawled the Instagram feed of the donor, James Alefantis, for images of children and modern art that line the walls of his pizza establishment in Washington DC. Despite the building of Comet Ping Pong lacking a basement and despite Alefantis having never met either of the Clintons, Reddit and 4chan users perpetuated the conspiracy theory that his business operated a pedophile sex ring out of the basement. In only a few days, the employees of the shop were receiving threatening phone calls and social media attacks and angry protesters picketed outside the shop. In mid-November, Turkish pro-government media outlets and trolls began tweeting #Pizzagate, because Turkish President Tayyip Erdogan had adopted the narrative as a means of displaying "American hypocrisy." Erdogan's regime had been scandalized by a real child abuse operation connected to a Turkish government-linked foundation [22][23]. Circulation of the weaponized hashtag was amplified by Twitter bots that were later traced to the Czech Republic, Cyprus, and Vietnam. In fact, most of the share of tweets about Pizzagate appear to have come from bot accounts [3]. The Turkish trolls also used the story as a distraction from Erdogan's controversial draft bill that would have provided amnesty to child abusers if they married their victims, although the draft was later withdrawn due to protests. Despite a

complete lack of any form of tangible or credible evidence and even a lack of victims, the conspiracy continued to grow until an armed North Carolina man, Edgar Maddison Welch, arrived at Comet Ping Pong and attempted to “self-investigate.” He too found no evidence that the theory was anything other than a fake news story turned politically motivated attack by a Turkish regime intent to turn moral panic in the United States against their geopolitical critics. Afterward, Reddit began to remove threads related to Pizzagate, claiming, “We don’t want witchhunts on our site” [22] [23]. The Pizzagate narrative should not be seen as a partisan issue. Such rumors could be insinuated, amplified, and directed against affiliates of either party. In this instance, internet trolls loyal to the Erdogan government used weaponized hashtags, Twitter bots, and Reddit and 4chan trolls to distract and deflect from government scandals in Turkey. Any actor or any regime could just as easily fan the flames of chaos or smear public officials or their donors digitally. As a result, campaign contributors from either party might be less willing to donate in the future out of fear that their information could be compromised and a similar situation could target them. Welch turned himself over to police after he did not find any evidence of the alleged conspiracy; however, similar influence operations could easily radicalize a susceptible individual into a lone-wolf actor in a foreign nation and inspire them to launch an attack that results in loss of life or that seizes the attention of American media outlets.

COMMUNAL NETWORKING PLATFORMS

Facebook and similar platforms such as VKontakte (VK) are prime targets for foreign influence operations that weaponize fake news, propaganda, altered images, inflammatory and derogatory public and private messages, inflated like counters, and other adversarial activities. Following the 2016 election, Facebook shut down over 470 Internet Research Agency accounts. Facebook acknowledged that some had a presence on Instagram. Twitter shut down at least 201 accounts associated with the Internet Research Agency.

Groups and communities are completely fabricated or are flooded with malicious bots. For instance, in June 2016, a swarm of Russian bots with no apparent ties to California were friending a San Diego pro-Bernie Sanders Facebook page and flooding it with anti-Hillary Clinton propaganda. The links were not meant to divide the community via political differences. They alleged that Clinton murdered her political opponents and used body doubles. Most domain registrations linked to Macedonia and Albania [24].

Similarly, in January 2016, Bernie Sanders supporters became high-volume targets of influence operations propaganda floods. “Sock puppet” accounts were used to deliver links and spam bomb groups. It began as anti-Bernie until Clinton won the Democratic nomination, then switched to anti-Hillary propaganda, fake news, and watering-hole sites. Dozens of fake news sites were spread on each group. The lure topics ranged from a “Clinton has Parkinson’s” conspiracy to a “Clinton is running a pedophilia ring out of a pizza shop” conspiracy. Trolls in the comment sections attempted to convince group members that the content was real. Many of the “interlopers” claimed to be Sanders supporters who decided to support the Green Party or vote GOP. The bots and trolls made it seem as if the community as a whole had decided that Green or GOP was the only viable option. Other articles offered “false hope.” ABC[.]com[.]co masqueraded as ABC News and “reported” that Sanders had been endorsed by the Pope. Bev Cowling, who managed a dozen Sanders Facebook groups, comments that, “It came in like a wave, like a tsunami. It was like a flood of misinformation.” Groups were bombarded with nearly a hundred join requests per day and administrators lacked the time to vet each applicant. According to Cowling, “People were so anti-Hillary that no matter what you said, they were willing to

share it and spread it,” she said. “At first, I would just laugh about it. I would say, ‘C’mon, this is beyond ridiculous.’ I created a word called ‘ridiculousity.’ I would say, ‘This reeks of ridiculousity.’” In response, the trolls would discredit her voice by calling her, the administrator of a Sanders group, a “Hillbot” or Trump supporter. The misinformation incited trust issues into the Sanders community. Their mistrust compounded with legitimate reasons to be skeptical of Clinton, the WikiLeaks dump of DNC emails, and a perpetuation of paranoia and flame wars. The Facebook groups were bombarded with fake news and anti-Clinton propaganda. It did not matter if the stories were believable or not. Users hesitated to click on legitimate links, fearing redirection to a misinformation site. One achievement of the attack was that it made browsing the group for valid sources akin to sitting in a room filled with blaring radios and attempting to discern which one was not blasting white noise. The goal was both to misinform those susceptible and overwhelm or distract those rational. Entire communities were effectively “gas-lit” for months. Anyone attempting to call attention to the attack was labeled a “Hillary shill” and attacked. Even an attempt to point out that NBCPolitics[.]org was a fake site drew criticism and vitriol (the real site is NBCNEWS[.]com/politics). All it took was one group administrator to be convinced by the misinformation campaign for rational detractors who combated the attack to get banned and thereby increase the reach of the attack. Foreign-influence memes transformed groups into echo chambers of anger. One administrator of a Bernie Sanders Facebook group investigated a propaganda account named “Oliver Milto” and discovered that there were four accounts associated with the name. Three had Sanders as their profile picture, two had the same single Facebook friend, while a third had no Facebook friends. The fourth appeared to be a middle-aged man with 19 Facebook friends, including that one friend the other Milto”s had in common. The four Milto”s operated on more than two dozen pro-Sanders groups around the United States, and their posts reached hundreds of thousands of members. For instance, on August 4, 2016, the Milto” post claimed, “This is a story you won’t see on Fox/CNN or the other mainstream media!” and linked to an article claiming that Hillary Clinton “made a small fortune by arming ISIS.” Similarly, on September 25, 2016, a Milto” account posted, “NEW LEAK: Here is Who Ordered Hillary To Leave The 4 Men In Benghazi!” and linked to a fake news site called usapoliticsnow[.]com. The Milto” accounts, just a few of an astounding number of other influence accounts operating on social media platforms, intended to depress, disenfranchise, overwhelm, desensitize, inundate, and anger Sanders supporters [24].

Bots and trolls also purchase ads on Facebook, Twitter, Google, and other platforms and at the end of articles on popular sites via ad targeting services. Most users have probably seen these “clickbait” sections, sometimes entitled “From Around the Web.” Political influence links often surround “legitimate” propaganda ads paid for by campaigns and associated entities. Even when the foreign efforts to spread disinformation are comically obvious and riddled with typos and poor translations, their artificial groups garner tens of thousands of members who heavily engage with the articles and links posted by the malicious administrators. Users follow the links and engage with the bots/trolls in the comments when they agree or oppose the content or title of the article. Trolls specifically target voters who consider themselves activists or anti-establishment and anti-status quo.

Facebook said in September that Russian entities paid \$150,000 to run 5,200 divisive ads on its platform during the campaign. It identified roughly 450 Russian-linked accounts as having purchased ads, a list that it shared with Twitter and Google, according to people familiar with the matter. Twitter said that it discovered 201 accounts on its service linked to the Russian actors identified by Facebook. Graham Brookie, deputy director with Atlantic Council’s Digital Forensic Research Lab, stated, “If you’re

running a messaging campaign that is as sophisticated as micro-targeting demographics on Facebook, then there's no way you're going to sit there from a communication standpoint and say, 'Google doesn't matter to us.'" One Russia-sponsored Facebook page among the over 470 pages and accounts that were shut down as part of Facebook's investigation into Russian meddling in the 2016 election was "Being Patriotic." The Associated Press performed content analysis on the 500 most popular posts and found it filled with buzzwords related to issues such as illegal immigration [24].

AUDIO DISTRIBUTION PLATFORMS

Nearly every smartphone or mobile device user has, at least at one time, relied on online audio and video distribution platforms. In fact, many mobile devices come with one or more such applications preinstalled. Approximately 800 million users use iTunes per month, SoundCloud and Ask.fm provide music to at least 165 million monthly users, and at least 70 million users subscribe to Spotify each month. The content provided by foreign media figures could influence users through themes, lyrics, and cultural transference. The funding provided by sponsored performers or advertisements may even fund foreign operations. More likely, however, organized threat actors would be far more successful in weaponizing podcasts, alternative news streams, and other issue-specific vectors through content or sponsorship. While not as potent an attack vector as social media platforms, these applications, many of which integrate with the audio services mentioned above, can still normalize foreign sentiments and in some cases radicalize listeners to adopt the agenda of foreign threats.

LIVE STREAM SERVICES

Twitch and Periscope each provide live-streaming services to approximately 15 million users each month; Facebook and other platforms also now feature the capability to stream live video. Staged demonstrations and out-of-context events that are broadcast along these vectors can become instantly viral and incite racial, gender, or political tensions immediately. Furthermore, ingrained communities, such as gamers, who rely on live streaming services, are subject to foreign influence during the sessions that they participate in or while watching a favored online personality, who often provides commentary while playing games.

DATING APPLICATIONS

Online dating may be more popular among younger populations than other methods of forming romantic relationships. Nearly 10 million users swipe on Tinder every day, 4 million users check Bumble or Plenty of Fish (PoF) daily, and 2.5 million users use Grindr. Other applications, like Badoo or Tagged, claim 45 million and 25 million users per month, respectively. Adversaries can engineer profile details to attract specific demographic suitors according to spiral dynamic tier or socionic profile. Additionally, they can hyper-focus their profile details or images to mesh with a specific movement or tribe. Memes such as images, T-shirts, slogans, and even fake news links can be communicated to viewers. The goal of profile weaponization is not necessarily propagation or mutation of the meme; in this case, it is normalization aimed at leveraging the target's attraction to the fake profile to make them want to change their views to be compatible with that individual; to make the viewer feel overwhelmed or entrenched in an accepting or opposing community, likely populated by bots; or to make the suitor feel isolated or ostracized due to their views. After unbalancing the viewer and normalizing the meme, the threat actor can leverage any of a number of psychological vectors to influence the behaviors and beliefs of members of that online community. In more personalized campaigns, threat actors can attempt to cat-phish specific people or public officials and then weaponize the messages or images exchanged. They can even employ chatbots

to automate and expand the process.

BOTS

According to a Radware study on Web application security, bots make up over three-fourths of traffic for some businesses; however, 40 percent have no capability of distinguishing legitimate bots from malicious ones. The study also found that 45 percent of businesses suffered a data breach in the last year and 68 percent were not confident that they could keep corporate information safe. Malicious bots can steal intellectual property, conduct web-scraping, or be used to undercut prices. Adversaries can direct bot traffic at businesses and either scrape consumer metadata; overwhelm the site to force users to a competitor site or mirror that acts as a watering-hole; influence the opinions of the user base by overwhelming the comment section; spread misinformation, malware, or fake news from the site; or compromise the site and exfiltrate consumer information for use in targeted attacks [25].

FRIENDSTER BOT

Bots on Friendster search for recent questions, mentions, and tweets. They respond to random questions and comments or thank the person. If they receive a response, they send a friend request to the original poster. After a direct connection is established, the bots are often used to push malicious links.

RANDOM COMMENT BOT

Random comment bots can be trained by identifying members of niche communities and then categorizing them according to their number of followers. Accounts with low followers are followed in the hopes of reciprocity, while accounts with high follower counts are noted. Finally, the bots are used to algorithmically send out malicious links or fake news via shoutouts of @follower_username. The specific lure employed will depend on the community targeted. For instance, academics may follow links blindly to interesting scientific articles within their niche, while political populations are more likely to respond to fake news articles tailored to their partisanship.

CHATBOTS

Different bots deliver sundry value according to their capabilities, functions, and applications. Chatbots are disruptive, but only a few varieties deliver value.

- **‘The Optimizer’**

Optimizer bots are the largest category of functional bots, and all others derive from them. These bots take on a concrete challenge and try solving it better than existing apps or websites. These bots attempt to disrupt by reducing friction versus more traditional ways of “doing things.” They may be applied to shopping, traveling, or everyday life. Optimizer bots minimize the workload of the user, but they also reduce the user’s agency for making decisions. For instance, an innocuous optimizer might select music for the user or pick a restaurant for them based on preferences. Attackers or corporate dragnet propagandists can influence the behavior of the bot to influence the user’s preferences, schedule, or choices directly.

- **‘The One-Trick Pony’**

A “one-trick pony” bot is a mini-utility with a messaging interface that assists in creating a meme, video, or editing text. A simple example of this bot is Snapchat’s “simple” spectacles. It is easy for

users to take the cognitive capabilities of these bots for granted because while engaged, the user is distracted with another task, such as photo-shopping an image, sending a meme to a friend, or editing a video rapidly. However, the impressive recognition and influence potential of these bots should not be underestimated. “One-trick ponies” are responsible for the generation of some of the most viral memes. Once the bots become popularized through the spread of even a single viral meme, the distributor of the bot has leverage over an ever-expanding user-populated meme generation and mutation factory. The developer of the bot or application controls the boundaries of meme generation through the selective offering of filters or tools offered to consumers. The bot might even suggest mutations, provide content, deliver ads, or collect consumer information. All of these capabilities enable adversaries and special interests to control meme generation, gather psychographic and demographic information that can be used to fine-tune targeting profiles, track meme mutation and propagation, and influence the meme generators who spread content to diverse and selective communities.

- **‘The Proactive’**

“Proactive” bots excel in their ability to provide the right info at the right time and place. Examples are Foursquare’s Marsbot, Weathercat Poncho, and KLM’s bot. These bots can be useful for narrow use-cases if they do not irritate their victims with useless notifications. For true mass adoption, they will need to provide personal, adept, and timely recommendations on a use case that is important enough for the target population to engage with frequently. The goal of the bot is to coerce user dependence, become indispensable, and normalize within the target’s daily life. The developer of the bot or any adversary digitally hijacking the application controls what information the user receives, when the user receives notifications, and which notifications appear on which devices based on user demographics, psychographic profile, device type, geographic area, or sociotics. “Proactive” bot controllers could frame information selectively, serve misinformation/disinformation, or polarize entire populations based on their registered information and any data collected from their device. For instance, consider the havoc an adversary could wreak if separate “facts” about a racial incident were reported to different users based on their demographic information. Alternately, consider how they could manipulate protest and counter-protest turnout by delivering different weather or traffic advisories selectively.

- **‘The Social’**

Like other bots, “social” bots are meant to accomplish a task; however, their distinguishing feature is that they compound the power of a group or crowd while making use of the unique nature of messaging platforms. Examples include Swelly, Sensay, Tinder Stacks, Fam, and Slack bots. Social bots have the potential to become viral immediately by drawing users into dialogues. The bots already choose which users to engage with based on their activity, interests, or demographics. When weaponized, these bots can be tailored to deliver propaganda or misinformation, they can assist in the polarization of a group or individual, they can gather victim information, or they can harass or radicalize one or more targets. In effect, “social” bots can leverage and weaponize fully the considerable influence that social media platforms possess over users’ daily lives.

- **‘The Shield’**

“Shield” bots are a sub-category of “optimizers” that specialize in helping users avoid unpleasant experiences. These usually appear as automation interfaces, such as customer service, payment

interactions, or any other field where a live operator can be replaced with an application. Popularized “shield” bots survive by their ability to outperform their competitors; however, the ineffectiveness of bots lacking in competitors can be used to control consumer behaviors. For instance, interaction with a poorly implemented “shield” bot might be necessary to fight a parking ticket. Only users with the patience to suffer through the interaction with an ineffective bot would be able to fight the ticket. Everyone else would either have to pay it out of frustration or ignore it at the risk of further penalties. Since a large subset of those who are patient may be those willing to pay the ticket, the ineffective bot acts as a discriminatory barrier against many psychographic profiles.

- **Propaganda Bots**

Bot activity is not unique to the United States; similar activity-disrupting activities, like launching attacks and disseminating propaganda, have been studied empirically in Mexico, Honduras, Dominican Republic, Venezuela, Argentina, Peru, Spain, Turkey, Egypt, Syria, Bahrain, Saudi Arabia, Azerbaijan, Russia, Tibet, China, UK, Australia, and South Korea. Spambot technology infused with machine learning and artificial intelligence is compounded by the weaponization of every conceivable digital vector, all made more potent by the use of memetics, psychographic targeting, cognitive biases, socionics, and spiral dynamics [26].

For instance, social media bots are prolific on Mexican networks. Bots and trolls target activists, journalists, businesses, political targets, and social movements with disruptive attacks, personal degradation campaigns, distractions, targeted malware, and death threats. Since the publication of his research denouncing bot activity, Alberto Escorcia has received constant death threats to him and his family, he has suffered rumor campaigns that have impacted his business relationships, his systems have been hacked, his website has been taken offline, and someone has broken into his apartment and stolen computer equipment. Similarly, researcher and blogger Rossana Reguillo suffered a two-month campaign of phishing links and death threats containing misogynistic language, hate speech, and pictures of dismembered bodies and burned corpses. The purpose of the attacks was to dissuade her from communicating with journalists, academics, activists, and her audience. The goal appears to have been to disrupt her work, force her to delete her accounts, or intimidate her into leaving the internet[26].

Digital propaganda botnets can be bought, sold, rented, and shared. They are not impeded by borders. For instance, the case study “Elecciones Mayo 2015. Quienes hacen trampa en Twitter” (Elections May 2015. Who is playing tricks on Twitter) discusses a network of bot accounts that were created in April 2014 to support Venezuelan anti-government protests La Salida, went silent for eight months, and then reemerged tweeting about Spanish politics, shortly after the creation of the MEVA (Movimiento Español Venezolano Antipodemos). This second period of activity focused on criticism of PODEMOS and promotion of Ciudadanos, while the possible account of the network’s administrator began to be followed by 18 official accounts of that party [26].

Propaganda bots and botnets are used to disrupt networks, suppress and censor information, spread misinformation and smear campaigns, and overwhelm vital nodes to sever them from the network. In 2014, Alberto Escorcia from LoQueSigue in Mexico City used the open source program Gephi to map Tweets visually using the hashtag “#YaMeCansé,” and he found that armies of bots were attacking the hashtag repeatedly and attempting to appropriate it. Even after users mutated the

hashtag into “#YaMeCansé2” and later “#YaMeCansé3,” the bots continued to spam the tags to make them useless. Over the course of a month, the hashtag morphed into 30 different iterations, with each overthrown by bots. Similarly, in January 2015, bots spammed “#EPNNotWelcome,” which was meant to protest Mexican president Enrique Peña Nieto’s (EPN) visit to Washington, D.C.; however, the tweets of thousands of online protesters were drowned in the tenfold flood of bot tweets [26].

According to Colombian hacker Andrés Sepúlveda, bots were extremely effective in influencing voters prior to an election, because the audience placed greater trust in the faux viral group-think implied by the bots than it did in the facts and opinions provided by television, newspapers, and online media outlets. People wanted to believe what they thought were spontaneous expressions of real people on social media more than the self-proclaimed experts in the media, because they had a desire to be part of the cultural zeitgeist. Sepúlveda discovered that he could manipulate the public debate easily by exploiting that human flaw. He wrote a software program, now called Social Media Predator, to manage and direct a virtual army of fake Twitter accounts. The software let him change names, profile pictures, and biographies quickly to fit any need [26].

While there is sufficient evidence to conclude that bots from multiple operators attempted to influence the 2016 U.S. Presidential election, it has proven difficult to ascertain the full extent of the impact and attribute the bots back to their sources. According to Alessandro Bessi and Emilio Ferrera, “Unfortunately, most of the time, it has proven impossible to determine who’s behind these types of operations. Governments, organizations, and other entities with sufficient resources can obtain the technological capabilities to deploy thousands of social bots and use them to their advantage, either to support or to attack particular political figures or candidates” [26].

...

“The meme is the kindle to the narrative illusion bonfire. The narrative illusion, plainly put, is the information force feed of the syntactical maggots pulsating and feasting on the rotting carcass of the last original idea. We need to take back the narrative. When we do this, the invisible cage that incarcerates the American population will be shattered.”

...

THE 'GUERRILLA' CHAOS OPERATOR'S COOKBOOK

A successful chaos operation, like a recipe, is an algorithm. If the steps are followed, with the occasional mild variation, the result is always the desired impact on the target population or the successful conveyance of a powerful meme. The first part of any digital “Chaos Operation” is to understand the target audience. Take into consideration the natural cognitive biases that are virtually present in the automatic responses of the target audience, then zero in on their social evolutionary state via spiral dynamics. Next, understanding the psycho-archetype of the target is critical; therefore, socionics can be used to expedite this process while it simultaneously helps the operator discover the target’s alliances and adversaries and their alliances. Finally, this information is used to create a psychographic algorithm using the metadata curated on these groups via their online web history. The dragnet surveillance capitalists who collect and track these groups are where the treasure troves of data are for this process.

...

“The enemy of my enemy is my friend.” The intel collection phase is critical to having ammunition for meme creation; therefore, some of the information to be collected on the tribe chieftains, who will be adversaries to the narrative, are lists of enemies, allies, controversies, discrediting information, emails, phone numbers, domain names, friends, family, economic vulnerability, and triggers that can humiliate, isolate, and confuse the chieftain and the tribe members. This information can easily be discovered via Maltego and other such programs (Note: Federal agencies will have access to far more superior capabilities).

...

Now that the operator has a solid understanding of the psychological factors at play with the target audience and more ammo for meme creation, it’s time to create bot accounts and notify bot service providers on how to weaponize their accounts. Each account should be weaponized completely to the theme and triggers that cater to the target audience, such as pictures; bios; accounts followed; and posts retweeted, liked, shared, and made. The accounts must be believable to blend with the digital tribe and the particular silo within that tribe in which the operator is tailoring the campaign. The volume of accounts created will be dictated by the size and length of the campaign. Accounts should be created for both overt and covert support of the campaign theme. Traditional broadcast media has little to do with the success of the viral ability of the campaign. Most operators will have their ready list of online

properties to use, and most begin by weaponizing the following platform categories: image sharing sites (i.e., Instagram, Flickr, Pinterest); video sharing platform channels and influencers (i.e., YouTube, Vimeo); high PR blogs for comments (the list will be curated based on the tribe being targeted); information sharing platforms, pages and groups (i.e., Facebook, Reddit, G+, StumbledUpon, Snapchat, Twitter, VK, OK.ru, Vine, AskFM); audio sharing platforms (i.e., SoundCloud, iTunes, ReverbNation, YouTube, Vimeo); dating sites for reinforcement and normalization of messages (i.e., Match, Tinder, Bumble, OkCupid, PlentyofFish, Zoosk, Badoo, ChristianMingle, OurTime); and business networking and information sites (i.e., LinkedIn, Foursquare, Yelp). The operator will use additional platforms based on the type, size, and length of the campaign.

Now that the target audience is discovered and analyzed, the operator will be seeking out an “incident” to weaponize via the Hegelian dialectic principle (problem, outcry, solution). The incident renders a plug-and-play introduction of the meme. When creating a meme, the operator will take into consideration color psychology, cognitive bias, the social evolutionary state of the target audience, where to promote the meme, the psychology of the imagery, short bursts of text that can be applied to the meme, and the triggers to spike adversarial response. The meme will typically be placed on a high volume image sharing platform, such as Instagram and Flickr, and will be tested via weaponized hashtags on Twitter. Bot accounts will be used to expedite the variability and success or failure of the meme, and the hashtags will expedite the meme’s path to the most targeted audience. If the meme is successful, it will take root and spread organically to the intended and alliance tribes. Support of those who spread the meme organically is critical, and bots need to be applied to their efforts to enunciate and reward their efforts. If one is fortunate enough to gain traction with a tribe chieftain, reward them with positive comments and reviews that heighten their position and respect as an “insider” among their chieftain peers and associated tribal ideological silos. For those adversarial elements, it’s critical to demonize and attack them immediately using every vector and support with weaponized spambots and harass with a bombardment of negative reviews, likes, shares, and comments on any vector in which they post. The intent is to silence and make an example of them.

When a meme is tested and successful, the operator will facilitate the same process along every vector using owned and leased accounts that have been weaponized for the campaign. The floodgates are opened, bots reinforce the message, comments and reviews are strategically spammed, hashtags are zeroed in, and this continues until there is an indicator that this meme is organically viral and beginning to mutate and replicate in other tribes. Support and reward chieftain and tribes who continue the survival and expansion of the meme with the same process used during the testing phase. As the audience is constructed and grows, it will be necessary to feed a steady flow of memes into the wild that are specifically targeting the various tribes that have supported and mutated the original meme.

In addition to the continuation of meme creation, emotional triggers need to be introduced. The quickest way to do this is to make the targeted tribes and chieftains fight to defend the meme, therefore creating the illusion that the adversaries’ response to the meme must go viral and target the chieftain of the tribal system. For this to work, the memes must be aggressive and the pure opposite of the initial meme created, and the support and reward system used above must be introduced to the adversarial element. Weaponized accounts that cater to the adversaries’ narrative will be created along the same vectors as above. This offensive must be more robust than the initial meme introduction; the initially targeted tribes will display vigil and emotionally charged defense of the meme and the idea behind the

meme. At this point, the targeted tribes will begin to create their own memes that spread organically along all digital vectors, including closed and hidden forums. The operator will repeat this process continuously for the life of the campaign. (Note: For the operator with technical acumen, cyberattack will be introduced at the final phases of each meme cycle. This could be ransomware with the moniker of the adversaries or malware with a simple payload that introduces a keylogger and hot mic or camera activation to gain access to exploitable information).

...

“The key to a highly effective ‘chaos op’ is to sit and wait for an ‘incident’ then weaponize that incident via Hegelian dialectic (problem, outcry, solution). The script practically writes itself.”

...

...

“The meme hovers above the syntactical model that has limited man’s evolution and expansiveness due to the restrictions of language. The meme introduces that which defies the restrictions of language and cuts to the psycho-emotional core of the individual.”

...

THREAT ACTORS

CHINA

The People's Republic of China's (PRC) attempts to guide, buy, or coerce political influence abroad are extensive. China's foreign influence operations are part of a global strategy with almost identical, longstanding approaches, adapted to fit current government policies. They are a core task of China's United Front work; one of the CCP's famed "magic weapons" that helped bring it to power [27].

To China, intelligence is about practical knowledge that facilitates decision-making and reduces the uncertainty intrinsic to policymaking and research. The key concept in Chinese foreign policy, which links party and state organizations, is the United Front. The United Front was originally a Leninist tactic of strategic alliances. Lenin wrote in "Left-Wing Communism: An Infantile Disorder,"

"The more powerful enemy can be vanquished only by exerting the utmost effort, and without fail, most thoroughly, carefully, attentively and skillfully using every, even the smallest, 'rift' among the enemies, of every antagonism of interest among the bourgeoisie of the various countries and among the various groups or types of bourgeoisie within the various countries, and also by taking advantage of every, even the smallest, opportunity of gaining a mass ally, even though this ally be temporary, vacillating, unstable, unreliable and conditional."

Since the mid-1930s, CCP strategists adapted Lenin's tactics to Chinese circumstances and culture. The CCP's United Front applies to both domestic and foreign policy. United Front activities incorporate the work of groups and prominent individuals in society, as well as information management and propaganda, and it has also frequently facilitated espionage. United Front Work Department personnel often operate under diplomatic cover as members of the Ministry of Foreign Affairs. The role is used to guide United Front activities outside China, working with politicians and other high-profile individuals, Chinese community associations, and student associations and sponsoring

"Cultural programming consists of interlocking bubbles of various memetically introduced narrative illusions, that became the entire composition of a fully programmed human pawn."

...

"Man is a hostage to the cage of cultural programming and the mass hallucination of the propagandist's narrative illusion."

Chinese language, media, and cultural activities. The party has a long tradition of party and government personnel “double-hatting” or holding roles within multiple agencies. Chinese consulates and embassies relay instructions to Chinese community groups and the Chinese language media, and they host visits of high-level CCP delegations coming to meet with local overseas Chinese groups. The leaders of the various Chinese-connected overseas associations in each country are regularly invited to China to provide updates on current government policies [27].

In the 1960s and 1970s, Beijing’s interest centered on building ideological solidarity with other underdeveloped nations to advance Chinese-style communism and on repelling Western ‘imperialism.’ Following the Cold War, Chinese interests evolved into more pragmatic pursuits such as trade, investment, and energy. Starting around 1980, the FBI detected hundreds of potential espionage-related cases involving China, and it has continued to detect Chinese agents attempting to steal from U.S. companies physically and digitally. Meanwhile, the Chinese intelligence services have attempted quietly to penetrate foreign governments by recruiting officials, using retirees to work against their former colleagues, and using Track II or scholarly exchanges to capture the policy atmosphere in foreign capitals. These operations are about persistence and volume, rather than creativity and skill [28].

Many are identified as potential recruitment targets after first being surveilled inside China. The Ministry of Public Security (MPS) is a national police force, mirroring the MSS structure. After the MSS was created in 1983, the MPS lost most of its counterintelligence and counterespionage functions to the MSS. This ministry’s expanding internal security budget, control over national databases, cyber capabilities, and management of most cities’ networked surveillance resources have brought the police force back into the national security arena. The New China News Agency, better known by its Chinese name “Xinhua,” and other major media outlets internally report to the Central Committee or to their respective policy systems on topics deemed too sensitive for publication. Foreign reports can deal with internal security targets, like Tibetans, Uighurs, Taiwanese, Falungong, and others, or more traditional intelligence targets. The original Xinhua charter explicitly noted this information-gathering role. Although most Chinese journalists are not intelligence officers and do not recruit clandestine sources, good journalists can provide information that is not publicly available, but also not classified.

The purpose of the party’s United Front Work Department is to build and wield political influence inside and outside China, or, as Mao Zedong wrote in a phrase still carried on the department’s website, “to rally our true friends to attack our true enemies.” For the collection of technology, a formal system under Institute of Scientific and Technical Information of China (ISTIC) exists for the collection and cataloguing of foreign scientific publications and other public information. Chinese researchers can request research materials and briefing packets on the state of the field as they move forward. ISTIC was instrumental in developing graduate programs with top universities for informatics, convening professional associations, and publishing professional literature – the hallmarks of a professional cadre. This is all above-board and legal, and some knowledgeable Chinese within the ISTIC system credit the acquisition of foreign technological information with reducing research costs by 40 to 50 percent and time by 60 to 70 percent.

Xi-era political influence activities can be summarized into four key categories. A strengthening of efforts to manage and guide overseas Chinese communities and utilize them as agents of Chinese foreign

policy is followed by a re-emphasis on people-to-people, party-to-party, and PRC enterprise-to-foreign enterprise relations, with the aim of coopting foreigners to support and promote CCP's foreign policy goals. Next, it focuses on a rollout of a global, multi-platform, strategic communication strategy. The Xi government's go-global, multi-platform national and international strategic communication strategy aims to influence international perceptions about China, shape international debates about the Chinese government, and strengthen management over the Chinese-language public sphere in China, as well as globally. It relies on agencies such as Xinhua News Service, CGTV, CRI, State Council Information Office/Office for Foreign Propaganda, Ministry of Foreign Affairs, and other relevant state organs. Its approach is multi- and multi-media. The Xi-era media strategy creates new platforms, which merge China's traditional and new media such as WeChat, and takes it to new global audiences in the developing world, the former Eastern Bloc, and developed countries. Under the policy, known as to "borrow a boat to go out on the ocean," China has set up strategic partnerships with foreign newspapers, TV, and radio stations to provide them with free content in the CCP-authorized line for China-related news. The formerly independent Chinese language media outside China is a key target for this activity. Under the policy to "buy a boat to go out on the ocean," China's party-state media companies are engaging in strategic mergers and acquisitions of foreign media and cultural enterprises. Under the "localizing" policy, China's foreign media outlets, such as CGTV, are employing more foreigners to have foreign faces explaining CCP policies. A new focus on the importance of think tanks is shaping policy and public opinion. China is making a massive investment in setting up scores of Chinese and foreign-based think tanks and research centers to help shape global public opinion, increase China's soft power, improve international visibility, and shape new global norms. It also aims to establish academic partnerships with foreign universities and academic publishers and impose China's censorship rules as part of the deal. Many students are offered strings-attached academic funding through the Confucius Institutes and other Chinese-connected funding bodies and investment in foreign research centers.

Under the slogan "tell a good Chinese story," the party aims to restore China's cultural and public diplomacy to prominence. Central and local governments provide massive subsidies for cultural activities aimed at the outside world, from scholarly publishing to acrobatics to Chinese medicine. This policy builds on and extends efforts established in the Hu era. China promotes Chinese culture and language internationally through Confucius Institutes, cultural centers, and festivals. The revised strategy particularly focuses on youth and countries with a significant indigenous population, in an attempt to develop close relations with indigenous communities. Finally, the Xi era focuses on the formation of a Chinese-centered economic and strategic bloc. That is based on geopolitical and economic dependencies, as well as the imposition of CCP operatives within businesses operating in China [27].

The presence of party units has long been a fact of doing business in China, where party organizations exist in nearly 70 percent of some 1.86 million privately owned companies. Companies in China, including foreign firms, are required by law to establish a party organization, a rule that had long been regarded by many executives as more symbolic than anything to worry about [29]. Now, companies are under "political pressure" to revise the terms of their joint ventures with state-owned partners to allow the party final say over business operations and investment decisions.

CCP operatives have allegedly pushed to amend existing joint venture agreements to include language mandating that party personnel be "brought into the business management organization," that "party organization overhead expenses shall be included in the company budget," and that posts of board

chairman and party secretary be held by the same person. Changing joint venture agreement terms is a main concern. Once the party is part of the governance, they have direct rights in the business. Officially, the Chinese State Council Information Office (SCIO) believes that “company party organizations generally carry out activities that revolve around operations management, can help companies promptly understand relevant national guiding principles and policies, coordinate all parties’ interests, resolve internal disputes, introduce and develop talent, guide the corporate culture, and build harmonious labor relations” [27].

The Three Warfares

Conventional warfare between global superpowers is problematic due to a complex network of geopolitical pressures, financial dependencies, and technological defenses. Instead, China relies on its influence operations to diminish Japan and South Korea’s perception of United States power, counter U.S. military actions and diplomatic pressures, raise doubts about the effectiveness of multilateral negotiations, breed doubts for the legitimacy of intervention by parties external to the region, and establish geographic disputes in China’s favor [30]. These asymmetric attacks require minimal resources in proportion to their impact. In 2003, China’s Central Military Commission and Communist Party enacted the “Three Warfares” multi-dimensional strategy for influence operations through psychological, media, and legal vectors [31][32]. The three vectors are combined and synergistically weaponized in non-kinetic multi-vector operations [32]. Additionally, China exercises its soft power, economic operations, and bilateral negotiations, as well as hard power and military demonstrations in its strategic operations.

Chinese political warfare and influence operations target foreign governments, organizations, groups, and individuals actively to shape their perceptions and behavior. Driven by its political goals, Chinese influence operations are a centerpiece of the PRC’s overall foreign policy and military strategy. While China’s foreign policy has traditionally relied on economic leverage and “soft power” diplomacy as its primary means of power projection, Beijing has also been actively exploiting concepts associated with strategic information operations as a means to influence the process and outcomes directly in areas of strategic competition. In 2003, the Central Military Commission (CMC) approved the guiding conceptual umbrella for information operations for the People’s Liberation Army (PLA) – the “Three Warfares” (san zhong zhanfa). The concept is based on three mutually reinforcing strategies: (1) the coordinated use of strategic psychological operations; (2) overt and covert media manipulation; and (3) legal warfare designed to manipulate strategies, defense policies, and perceptions of target audiences abroad [33].

Psychological campaigns deter, demoralize, or shock opposing nations; discourage internal dissidence; exert diplomatic pressure; publicly express displeasure; assert hegemony; promote false narratives; or levy threats. For instance, a simple psychological attack might involve Chinese operatives spreading rumors that international business could suffer in China if lawmakers in their countries of origin pass rules, regulations, or laws that negatively impact Chinese firms or impede the Chinese Five-Year Plan [32]. Implanted Chinese operatives, social media trolls, and propaganda are common tools of Chinese psychological operations [33].

Legal vectors aim to bend or rewrite rules of international orders in favor of China and its interests. This

could include exertions of territorial ownership, disputes of border boundaries, restrictions of navigation through the 200-mile Exclusive Economic Zone as defined by the United Nations Law of the Sea Treaty, or attempts to guide United Nations Security Council decisions [32]. Legal vectors are executed on a global stage by government officials and the military. Legal warfare uses domestic and international law to claim the legal high ground to assert Chinese interests. China's position paper is replete with selected references to international law to support China's stance [33].

One example of Chinese legal warfare occurred in 2014, when Chinese Deputy Ambassador to the U.N., Wang Min, presented then Secretary-General Ban Ki-moon with a formal position paper on a maritime confrontation between China and Vietnam regarding the placement of oil rig HYSY 981 in disputed waters in the South China Sea, along with a request that he circulate it to all 193 U.N. members. China's position paper was sent to the U.N. to out-manuever Vietnam's own propaganda effort and to isolate Vietnam. The vast majority of U.N. members have no direct interest in territorial disputes in the South China Sea. Southeast Asian states that hold concerns about China's actions would not be willing to take a public stand on the issue [33].

Media warfare is a strategy designed to influence international public opinion to build support for China and to dissuade an adversary from pursuing actions contrary to China's interests. China understands that in the age of the internet, the nation with the most sophisticated digital tools and the most compelling narrative, not the country with the best weapons, wins conflicts [32]. An effective influence operation can enable history to be written before a conflict has even occurred. Perpetual media activity can ensure the success of long-term campaigns that manipulate perceptions and attitudes and short-term attacks that distract or disrupt the public narrative. Consequently, China exerts strong control over its media to shape public opinion according to the Chinese Communist Party's will [32]. For instance, China operates the Chinese Central Television Network to deliver propaganda and misinformation to at least 40 million Americans in the Washington, D.C., region. The network delivers content to millions more globally. On the network, China obfuscates its agenda with real news coverage. Minor details and perspective are presented selectively, or altered subtly or withheld in daily widespread micro-attacks that advance China's Thirteenth Five-Year Plan. Within China, the "Great Firewall" and loyalty metrics control the population. The government signals acceptable behavior and beliefs to the people through the media. On its own, state control of the vast majority of messaging outlets is enough to quell resistance. The internet serves as an outlet for dissent but it is also as the primary monitoring tool. Each day, the government intercepts and analyzes hundreds of thousands of tweets, blogs, and posts. Collective action and serious opposition to the CCP are not tolerated. Criticism of politicians and minor deviances are permitted, because wholesale censorship invites rebellious behavior and because influential dissidents are often betrayed inadvertently by the actions of more vocal acolytes [31].

At the operational level, the "Three Warfares" became the responsibility for the PLA's General Political Department's Liaison Department (GPD/LD), which conducts diverse political, financial, military, and intelligence operations. According to the Project2049 Institute, GPD/LD consists of four bureaus: (1) a liaison bureau responsible for clandestine Taiwan-focused operations; (2) an investigation and research bureau responsible for international security analysis and friendly contact; (3) an external propaganda bureau responsible for disintegration operations, including psychological operations, development of propaganda themes, and legal analysis; and (4) a border defense bureau responsible for managing border negotiations and agreements. The Ministry of National Defense of the PRC provides more general

terms, emphasizing “information weaponization and military social media strategy.” In practice, the GPD/LD is also linked with the PLA General Staff Department (GSD), the second department-led intelligence network. One of its core activities is identifying select foreign political, business, and military elites and organizations abroad relevant to China’s interests or potential “friendly contacts.” The GPD/LD investigation and research bureau then analyzes their position toward China, career trajectories, motivations, political orientations, factional affiliations, and competencies. The resulting “cognitive maps” guide the direction and character of tailored influence operations, including conversion, exploitation, or subversion. Meanwhile, the GPD’s Propaganda Department broadcasts sustained internal and external strategic perception management campaigns through mass media and cyberspace channels to promote specific themes favorable for China’s image abroad – political stability, peace, ethnic harmony, and economic prosperity supporting the narrative of the “China model” (zhongguo moshi) [33].

Traditionally, the primary target for China’s information and political warfare campaigns has been Taiwan, with the GPD/LD activities and operations attempting to exploit political, cultural, and social frictions inside Taiwan; undermining trust between varying political-military authorities; delegitimizing Taiwan’s international position; and gradually subverting Taiwan’s public perceptions to “reunite” Taiwan on Beijing’s terms. In the process, the GPD/LD has directed, managed, or guided a number of political, military, academic, media, and intelligence assets that have served either overtly or covertly as agents of influence. In particular, the primary base for Taiwan influence operations has been the Nanjing Military Region’s 311 Base (also known as the Public Opinion, Psychological Operations, and Legal Warfare Base) in Fuzhou City, Fujian Province. The 311 Base has been broadcasting propaganda at Taiwan through the “Voice of the Taiwan Strait” (VTS) radio since the 1950s. Over the past decade, the base expanded its operations from the radio station to a variety of social media, publishing, businesses, and other areas of contact with Taiwan. The 311 Base has served as a de facto military unit cover designator (MUCD) for a number of GPD/LD’s affiliated civilian and business platforms working to “promote Chinese culture” abroad. These include the China Association for Promotion of Chinese Culture (CAPCC); China Association for International Friendly Contact (CAIFC); China-U.S. Exchange Foundation (CUSEF), The Centre for Peace and Development Studies (CPDS), External Propaganda Bureau (EPB), and China Energy Fund Committee (CEFC) [33].

China’s strategic influence operations are also increasingly targeting the European Union, particularly countries of Central-Eastern Europe that are part of China’s “16+1” regional cooperation formula. Beijing views the region as an important bridgehead for its further economic expansion in Europe. According to the 2014 annual report of the BIS counterintelligence in the Czech Republic, China’s administration and its intelligence services emphasized gaining influence over Czech political and state structures and on gathering political intelligence, with active participation by select Czech elites, including politicians and state officials [27].

These reports refer to the activities of the China Energy Fund Committee (CEFC), a Hong Kong-registered nongovernmental organization, considered a political arm of its holding subsidiary, the China Huaxin Energy Co. Ltd. – a multibillion-dollar energy conglomerate with companies based in Hong Kong, Singapore, and mainland China. Over the past three years, CEFC has embarked on acquisitions in the Czech Republic, including the purchase of representative real estate near the presidential office. These “investments” have served as initial gateways to the highest political elites in the country. Indeed,

CEFC's chairman, Ye Jianming, was named an official adviser by the Czech president. The case of CEFC in the Czech Republic illustrates a complex constellation of relationships that link political, financial, military, and intelligence power centers through the GPD/LD. Ye Jianming was deputy secretary general of the GPD/LD-affiliated CAIFC from 2003 to 2005. Media reports debate whether Ye Jianming is a son of Lt. Gen. Ye Xuanning, director of the GPD/LD until 1998, and the grandson of the most revered PLA Marshall Ye Jianying, described as "the spiritual leader" of the princelings – the children of China's original communist revolutionary heroes, who now dominate the top echelons of the party leadership. The exploitation of information operations represents Beijing's hybrid or "non-kinetic" attempts to influence strategic areas of competition in Asia and Europe directly [33].

The '50 Cent Party'

China is a leader in altering and censoring the digital landscape through what it calls the Golden Shield, otherwise known as "the Great Firewall of China." However, China's initial operator for internal and external influence operations is the 50 Cent Party, whose prerogative is to praise China, its businesses, and its products, and to distract from any criticism or undesirable conversations. Contrary to popular belief, the Chinese do not create public debates or attempt to foster discord in foreign nations in the same manner as Russian operations. Instead, they focus on distraction and redirection, because they fear losing control of their own people far more than they fear foreign influence. Distraction is a clever and useful strategy in information control in that an argument in almost any human discussion is rarely an effective way to put an end to an opposing argument. Letting an argument die or changing the subject are more effective than instigating or engaging with a detracting viewpoint. Humans are hardwired to try to win arguments, as anyone who has fallen into the trap of social media debates can attest. Distraction-based strategies have the advantage of reducing aggression while diverting and thereby controlling the dialogue. Using sheer numbers, military precision targeting, and big data analytics, the Chinese government, through the 50 Cent Party, is able to change the subject consistently at any time [34].

Chinese internet commentators are personnel hired to manipulate public opinion on behalf of the CCP. The name derives from the unverified allegation that they received 50 cents per post. A 2016 Harvard University paper found that Chinese internet commentators are mostly paid government bureaucrats, responding to government directives in times of crisis and flooding Chinese social media with pro-government comments. They also rarely engage in direct arguments. Around 80 percent of the analyzed posts involve pro-China cheerleading with inspirational slogans, and 13 percent involve general praise and suggestions on governmental policies [34].

As of 2016, this practice seems to have largely ceased, and propagandist participation in internet discussions has become part of the Communist party officials' normal work. Also, the nature of participation has become more nuanced and less aggressive. Research indicated a "massive, secretive operation" to fill China's internet with propaganda has resulted in some 488 million posts carried out by fake social media accounts, out of the 80 billion posts generated on Chinese social media. To maximize their influence, their pro-government comments are made largely during times of intense online debate, and when online protests have a possibility of transforming into real-life actions [34].

The 50 Cent Party, also known as the 50 Cent Army, is not really an army; it's just a platoon in a much larger propaganda apparatus. All those positive posts are planted in an environment that bans most

Chinese from legally accessing social media like Twitter, Facebook, and YouTube, as well as critical news media like The New York Times and Bloomberg. Digitally redirecting public opinion has been the official policy of the PRC since 2008. 50 Centers are government operatives posing as ordinary, patriotic netizens. Estimates of their numbers range from 500,000 to 2 million [33]. The 50 Cent Party consists of government personnel (the original party) and student recruits (50 Cent 2.0). One student member of 50 Cent claimed that he was paid 800 yuan per month by the Chinese government and that refusing to participate could prevent students from being able to graduate from college. In addition, he claimed that extremely active student trolls even received extra credit points from their professors [34].

Rather than debating critics directly, the Chinese government tries to derail conversations on social media it views as dangerous. For instance, in April 2014, President Xi Jinping had his first visit to the Xinjiang province of China [34] [35]. The newly elected Xi's platform included a promise to increase the government's response to terrorism. Immediately following his visit, an explosion followed by a knife attack at the main railway station in Urumqi, a city in that northwest region, killed three people and injured dozens more.

Instead of addressing the incident publicly, the Chinese government's online censorship apparatus initiated a campaign to control the perception and understanding of the attack. Searches for "Urumqi blast" were blocked on the country's largest search engine, Baidu, and on the Twitter-like social network, Sina Weibo. In the meantime, more than 3,000 posts from paid government trolls flooded Sina Weibo and other Chinese social networks in a coordinated campaign. The posts did not address the attack or any public debates; instead, they distracted the public with broad praises of China's good governance, economic opportunities for Chinese people, and the "mass line." The posts were tailored to derail public dialogue concerning the incident. The strategy has a history of success. In July 2013, government-sponsored social media activity obfuscated riot activity in the Xinjiang province, and in February 2014, trolls drew attention away from a pair of important political meetings [36].

The PRC relies on the 50 Cent Party to coordinate and deploy massive influence operations on social media platforms. The name is a misnomer derived from the past rumor of how much members were paid per post. In contrast to popular belief, the 50 Cent trolls are not ordinary citizens that engage in online debates. Analysis of a large archive of leaked emails from a propaganda office in Ganzhou – a city located in China's southeastern Jiangxi province – revealed that the main focus of the collective is to overwhelm platforms with massive volumes of "cheerleading" posts and reviews that praise Chinese products and organizations, rather than engage in debates or inflammatory dialogue. Emails leaked from the Zhanggong propaganda office included transcripts of over 43,757 messages exchanged between 50 Cent members and their superiors either proving that they had completed their assignments or delivering instructions, in addition to messages to the higher-level offices of the propaganda division. The majority of commenters were identified as government workers who worked in various offices and bureaus. By all appearances, they were not paid for the posts because the coordinated messages seemed to be an expected duty of their government job. There was no evidence that the 50 Cent army used bots to amplify their message. Emails from the propaganda office indicate that commenters were instructed to "promote unity and stability through positive publicity" and to "actively guide public opinion during emergency events" — where "emergency events" refer to events that might stoke collective action. For the most part, criticism of the PRC on social media is tolerated, in part because it makes the identifications of dissidents easier and because censorship breeds rebellion. The government monitors

online activity actively, and it intervenes proactively before collectives can aggregate or movements can mobilize [37].

Harvard's Gary King, Stanford's Jennifer Pan, and Margaret Roberts at University of California at San Diego analyzed the tens of thousands of posts written by China's official social media trolls and extrapolated the scale of the operation to the rest of China. Their analysis was the first large-scale empirical analysis of the activities of the Chinese troll army. 50 Cent members appear to use both their own accounts (59 percent) and exclusive accounts (41 percent). King and his colleagues spent several years analyzing the patterns of millions of posts on Chinese websites, cross-referencing comments, user IDs, and other factors. They discovered that 50 Cent posts appear in specifically directed bursts meant to short-circuit any discussions that could lead to protest or unrest. Based on the evidence, they estimate that the 50 Cent Party annually posts a total of 448 million messages on social media. According to one researcher, "If these estimates are correct, a large proportion of government website comments, and about one of every 178 social media posts on commercial sites, are fabricated by the government" [37]. Based on their analysis, they found that 57 percent of posts engaged in cheerleading, 22 percent engaged in non-argumentative praise and suggestions, 16 percent engaged in factual reporting, and approximately 4 percent engaged in taunting foreign countries. Zero accounts engaged in argumentative praise or criticism. Using the information from the leak, the researchers tested methods of identifying 50 Cent Party posts. They found that 57 percent of trolls whose identities they knew via the leaked emails admitted their 50 Cent affiliation when asked kindly and in Chinese, "I saw your comment, it's really inspiring, I want to ask, do you have any public opinion guidance management or online commenting experience?" They found that 59 percent of commenters whose identities were not known but whose posts shared characteristics with the 50 Cent Party also admitted their affiliation when asked. The distraction tactics of China's troll army can be deployed anywhere online and on many platforms and topics foreign to China. Rather than inflame debates or sow discord, as Russian trolls aim to do, Chinese operatives intend to derail conversations and dilute the intensity of collective criticisms [37] [38] [39].

The Chinese regime appears to follow two complementary principles, one passive and one active. The passive principle is that they do not engage on controversial issues. They do not insert 50 Cent posts supporting and do not censor posts criticizing the regime, its leaders, or their policies. The active principle is that they act to stop discussions that could result in collective action through distraction and active censorship. 50 Cent Party cheerleading influences the perceptions of the public, derails discussions of controversies, disrupts general negativity, and distracts from government-related meetings and events with protest potential. Unsubstantiated threats from individuals of protest and viral bursts of online-only activity are ignored by the government because their potential for collective action is minimal. The main threat perceived by the Chinese regime in the modern era is not military attacks from foreign enemies, but rather uprisings from their own people. Staying in power involves managing their government and party agents in China's 32 provincial-level regions, 334 prefecture-level divisions, 2,862 county-level divisions, 41,034 township-level administrations, and 704,382 village-level subdivisions while mitigating collective action organized by those outside of government. The balance of supportive and critical commentary on social media about specific issues, in specific jurisdictions, is useful to the government in judging the performance of (as well as keeping or replacing) local leaders and ameliorating other information problems faced by central authorities [37] [38] [39].

While 50 Centers may distract viewers with pro-government posts, other branches of the Propaganda

Department are busy censoring controversial articles and keywords. Younger Chinese citizens, who predominantly interact online in real time, are likely only minimally influenced by the 50 Cent trolls. In an attempt to modernize its digital propaganda machine in August 2016, the government released a plan to involve the Communist Youth League (CYL) in its goal to “purify” the internet. The CYL consists of around 89 million members aged 14 to 28. CYL members are categorized as more aggressive than “50 Centers,” and they are adept at bypassing the Great Firewall of China to troll subjects on foreign social media. They are described as “volunteer armies of mobilized angry youth.” Some even consider the CYL to be “The 50 Cent 2.0.” For instance, they left about 40,000 angry messages on the Facebook page of Australian swimmer Mack Horton, accusing him of being a “drug cheat,” after he bested his Chinese counterpart at the Rio Olympics. A similar barrage targeted Tsai Ing-wen when she was elected the first woman president of Taiwan. A campaign that began on a Baidu forum flooded Tsai’s Facebook page with 40,000 negative comments within 12 hours. The attack vilifying Tsai Ing-wen and democracy involved an estimated 10,000 50 Cent and CYL users. The PRC relies on the 50 Cent Party and the CYL to identify and divert from any discussion that could result in collective action or crowd formation because they believe that is the only thing that could cause instability sufficient to upset their government. Consequently, the 50 Cent and CYL trolls are often permitted to bypass the Great Firewall so that they can launch their attacks. Despite the rise of a more technologically advanced and memetically motivated generation, the original 50 Cent Party is not fading away; it is being modernized to focus on technology and skill, instead of just sheer numbers. Though it already had dedicated teams and infrastructure, it is becoming more sophisticated, refined, and nuanced. It is beginning to harness big data analytics and psychographic and demographic predictive algorithms in its operations [37] [38] [39] [36].

China’s Influence Abroad

Recently, Beijing has identified the African continent as an area of significant economic and strategic interest. Most of China’s stake in the region focuses on energy assets and development. China aims to increase its soft power in Africa by promoting the “China model” of authoritarian, state-driven development as a counter to Western efforts to spread liberal democratic capitalism. This is done through political training programs where members of ruling parties, labor unions, and ministries are taken to China to meet the members of the Chinese Communist Party [40]. Its best imitator is Ethiopia, where the ruling EPRDF party has copied much of what it has seen in China, tightly controlling business and investment and imitating China’s Central Party School and party cadre system. In South Africa, more than half of the members of the executive committee of the ruling African National Congress have attended such schools in China, a country the party calls its “guiding lodestar.” China also spreads its influence in less visible ways. For instance, China awards tens of thousands of scholarships to African students. Victoria Breeze and Nathan Moore at Michigan State University estimate that in 2014, the number of African students in China surpassed the number studying in either Britain or America, the traditional destinations for English speakers. These efforts burnish China’s image [40].

In the past decade, Chinese loans and contractors have reshaped Africa’s infrastructure by investing in new roads, ports, railways, mines, manufacturing plants, shopping centers, and corner stores. The influx of Chinese resources has prompted some to postulate that China is Africa’s most important economic partner and others to fret that it is the new colonial master. As many as 10,000 Chinese companies are operating in Africa, 90 percent of them privately owned. Despite appearances, the notion that China is refinancing the continent is inaccurate. According to the work of Deborah Brautigam, who leads the

China Africa Research Initiative at Johns Hopkins University, little more than half of the announced Chinese loans to Africa materialized. Nevertheless, the promise of funds and the offering of hope is enough to foster pro-China sentiments in portions of the population [41].

The PRC aids and abets oppressive and destitute African dictatorships by legitimizing their misguided policies and praising their development models as suited to individual national conditions. Beijing holds out China's unique development model – significant economic growth overseen by a disciplined, one-party totalitarian state with full authority, if not control, over all aspects of commercial activity – as an example for others to emulate. China rewards its African friends with diplomatic attention and financial and military assistance, exacerbating existing forced displacements of populations and abetting massive human rights abuses in troubled countries, such as Sudan and Zimbabwe. As a consequence, Chinese support for political and economic repression in Africa counters the liberalizing influences of Africa's traditional European and American partners. China's ideological support of African despots lends them international legitimacy and authority in international arenas, such as the United Nations, that help to reduce Western democracies' pressure to act to improve human rights, economic transparency, and political freedoms. When it serves Chinese interests, Beijing succors would-be junta leaders and illiberal rebels who want power and would roll back political reforms in young democracies. Rebels are led to believe that if they overthrow legitimate governments, China will work to bolster their legitimacy in the United Nations and other international communities [42].

The PRC is seeking trade, diplomatic, and military ties in Latin America and the Caribbean. The region contains immense natural resources and developing markets for manufactured goods and arms. China does not pose a kinetic military threat to Latin America and has embraced market concepts steadily, but its intangible influence represents serious competition that could dilute U.S. influence [43]. Latin America is a particularly promising prospect. It is relatively unindustrialized and has an abundance of raw materials. Moreover, authoritarian leaders and corrupt oligarchies control many governments. Signing purchase agreements with them is much more comfortable than dealing with the swath of private corporations found in more democratic countries. China has advanced to economic assistance, direct investment, a few joint ventures, and military ties by building on basic commercial agreements. China capitalized on Argentina's financial collapse, increasing investment in Argentina and Brazil; meanwhile, U.S. investment in the region declined half. Joint ventures include partnerships with Great Dragon Telecom in Cuba and Colombia. China partnered with Brazil to improve railways and reduce resource transportation costs. The PRC may renovate the Antofagasta port in Chile. China has pursued investments in oil production in Venezuela, Ecuador, Colombia, Argentina, Brazil, and Mexico. President Chávez invited the Chinese National Petroleum Corporation (CNPC) to participate in the exploration of the Orinoco belt. Meanwhile, the CNPC invested \$300 million in technology to use Venezuela's Orimulsion fuel in Chinese power plants [41] [43].

According to a Wilson Center study, as part of the second half of its thirteenth Five-Year Plan under the direction of Supreme Leader Xi Jinping, China is increasing the propensity and pervasiveness of its influence operations. Emerging operations that are aimed at persuading foreign governments and firms to support Beijing's anti-democratic goals involve multiple governments and Chinese Communist Party intelligence organizations through economic pressure and incentives, the guidance of insider threats, and outright coercion. The report's author, professor Anne-Marie Brady, states, "Even more than his predecessors, Xi Jinping has led a massive expansion of efforts to shape foreign public opinion

to influence the decision-making of foreign governments and societies.” China aims to undermine the sovereignty and integrity of targeted states and political systems using vectors ranging from social media propaganda to insider threats. New Zealand is part of Five Eyes and is a key intelligence ally to the United States. Brady notes, “New Zealand is valuable to China, as well to other states such as Russia, as a soft underbelly to access Five Eyes intelligence.” Like many other nations, including the United States, it is rapidly becoming saturated with Chinese operatives, the PRC’s attempts to influence political activities, and economic entanglements that China can leverage to exert control over foreign governments and businesses. Chinese foreign influence operations in New Zealand raise security concerns here about China accessing U.S. secrets. There, several ethnic Chinese politicians were elected to the parliament to increase China’s control over information exchanges and geopolitical relationships. For instance, New Zealand parliamentarian Jian Yang recently acknowledged that he concealed his past relationship with the People’s Liberation Army intelligence unit and membership in the CCP [27]. Over the past 20 years, China has focused on sowing division between the government in Wellington and the U.S. New Zealand has adopted increasingly anti-American policies, beginning in the 1980s when the nation refused to permit nuclear-powered or nuclear-armed warships from making port calls as part of an anti-nuclear policy. China has targeted New Zealand’s 200,000 ethnic Chinese, part of the country’s population of 4.5 million people [27].

The Chinese activities are based on the United Front — strategic influence operations developed by the communists of the 1940s. In September 2014, Xi highlighted the importance of United Front work in supporting influence activities around the world. He called them the Party’s “magic weapons” in pursuit of making China the dominant world power. Dissident Chinese businessman Guo Wengui revealed recently that Chinese companies are often used by the Ministry of State Security (MSS), the civilian spy service, to buy off American politicians and organizations to promote China’s foreign and economic policies. China increased the aggressiveness of its operations in 2012. Guo reported that China dispatched between 25,000 and 40,000 agents to the U.S. China engages in widespread influence operations by hiring former government officials to lobby on its behalf. Other methods involve coercing American companies operating in China into influencing the U.S. government in support of China’s policies. In 2014, a former Chinese spy revealed that the PLA Third Department utilized a network of some 200,000 agents around the world. The influence operations carried out by party units are the United Front Work Department, the Central Propaganda Department, the International Liaison Department, the All-China Federation of Overseas Chinese, and the Chinese People’s Association for Friendship with Foreign Countries. The report said, “United Front activities incorporate working with groups and prominent individuals in society; information management and propaganda; and it has also frequently been a means of facilitating espionage...” United Front operatives frequently operate undercover as Chinese diplomats who target foreign politicians, business people, and journalists. Front groups include Chinese community associations and student groups, along with organizations funded by China engaged in Chinese language, media, and cultural activities. Another critical influence tool is the numerous Beijing-funded Confucius Institutes that are located on many U.S. and foreign college campuses [27].

Chinese military intelligence, known as the PLA Second Department, has also worked closely in the past with the International Liaison Department and United Front Work Department in backing revolutionaries in Southeast Asia and spying. The 2014 report also stated, “CCP United Front officials and their agents try to develop relationships with foreign and overseas Chinese personages (the more

influential, the better) to influence, subvert, and if necessary, bypass the policies of their governments and promote the interests of the CCP globally,” the report says. “The Party operatives attempt to guide the activities of front groups, overseas agents, and supporters by appealing to nationalist sentiments, such as urging support for the Chinese motherland, the Chinese race, and the ethnic Chinese population within their countries ... The goal of successful overseas Chinese work is to get the community to proactively and, even better, spontaneously engage in activities which enhance China’s foreign policy agenda.” China has been less successful in targeting groups opposed to the communist regime, pro-democracy dissidents, the Buddhist-oriented group Falun Gong, those promoting Taiwan independence, independent Chinese religious groups, and Tibetans and Uighurs seeking freedom. However, all those factions are significant infiltration targets by party and intelligence agents who attempt to divide or subvert the groups [27].

RUSSIA

Russia, more than any other actor, has devised a way to integrate cyber operations into a strategy capable of achieving political objectives. Russia’s approach in its power struggle with NATO and the West is based on the acknowledgment that it cannot match the military power of NATO. Strategic advantages must, therefore, be achieved without provoking an armed response from the alliance. A core element of Russian security policy is the foundation that conflicts between developed nations must remain below the threshold of armed conflict, or at least below the threshold where it is proclaimed to be an armed conflict. The Gerasimov doctrine (Russian non-linear war) exemplifies this strategy. It posits, “The political and strategic goals have grown, and, in many cases, have exceeded the power of force of weapons in their effectiveness.” It necessitates an increased dependency on the information domain. In the Russian view, information warfare is conducted in peacetime, in the prelude to war and in wartime in a coherent manner.

Digital Maskirovka

While all militaries seek to misdirect enemies, Russia’s military doctrine of deception, the maskirovka, Russian for “masking” or “camouflage,” is a cornerstone of the Russian military and intelligence mindset. With maskirovka, the fog of war is not merely the natural byproduct of combat but a deliberately manufactured feature of military operations intended to increase ambiguity and indecision in opposing forces. Using decoys, clandestine actions, and disinformation, maskirovka facilitates military resilience, increases the effectiveness of surprise actions, and increases doubt in an adversary while concealing Russian weaknesses [44].

The tools of maskirovka broadly include psychological operations, manipulation of media, disinformation and propaganda, electronic and cyber warfare, irregular forces not in uniform, private military contractors, and proxies and physical deception through the camouflaged military maneuver. The modern maskirovka occurs at the seams of conventional conflict – the gray zone between peace and war [44].

Old-school tactics include decoys such as dummy tanks used by the Serbian military during the NATO air campaign in Kosovo in 1999; confusing demonstrations of capability, such as the Zapad wargame; occasional “buzzing” of U.S. naval vessels or near contested borders to determine response protocols; deployment of “patriotic” or “volunteer” unconventional forces, such as the “little green men” deployed

to annex Crimea in 2014; the clandestine delivery of military supplies camouflaged as humanitarian convoys to support proxy and covert forces; or incessant denial of military presence or disingenuous narratives behind military operations, such as acting as peacekeeping forces to protect ethnic and expatriate Russians [44].

Offensive cyber and electronic warfare capabilities enable Russia to distill doubt into their enemy's faith in digital systems. Fake command and control facilities emit false radio frequency signals to deceive enemy intelligence assets while manipulating or jamming radio frequency or GPS signals that could undermine a military commander's faith in the accuracy of precision-guided munitions. With modern communications technology, automated bots on social media platforms amplify targeted disinformation to both divide populations and entice susceptible groups to favor Russian-produced narratives. State-sponsored media – such as RT and Sputnik – can guide the conversation and help legitimize Kremlin propaganda. Open source outlets can counter the Kremlin's disinformation and potentially cause unexpected political backlash. Countering the narrative successfully requires a swift and agile reaction, however [44].

Maskirovka creates uncertainty and plausible deniability regarding Russian responsibility for operations, dulling the West's response. This has helped the Kremlin sidestep international norms without significant repercussions. Because Russian “patriotic hackers” executed the electronic denial of service attacks against Estonia – a NATO member – in 2007, Russia maintained plausible deniability, complicating Estonia and its allies' ability to retaliate. The disinformation campaign and troop buildup near South Ossetia ahead of the 2008 invasion of Georgia (repeated before the 2014 annexation of Crimea) allegedly involved Russian special operations forces with no insignia identifying them as Russian military, later dubbed “little green men.” Maskirovka goes beyond fostering doubt and presenting an alternative, engineered narrative. Russia has used it to accomplish geostrategic objectives under the guise of international cooperation. Perhaps the most prominent example is Russia's positioning itself as a counterterrorism partner in Syria – and Libya to a lesser extent – as it seeks to extend its global influence to the Middle East. Russia acts as a strategic ally to the international community in the war against ISIS, a possible foundation for the alleviation of sanctions initially imposed on Moscow for its annexation of Crimea. Its goal in the country, however, has been to bolster the Assad regime and degrade the Western-backed opposition so that it cannot create a pro-U.S. government in Syria. “In 2015, Russia began a military intervention in Syria claiming it was waging war on ISIS and international terrorism,” Ted Poe (R-TX) said at a House Foreign Affairs subcommittee hearing titled “Russia: Counterterrorism Partner or Fanning the Flames?” He continued, “To some, this was welcome news. It seemed that there might be a rare moment that the cooperation between the former Cold War foes – Moscow and Washington— would be able to work together to combat terrorism. This was fantasy.” [44]

The Internet Research Agency

One division of Russian influence is the Internet Research Agency, a collection of government-employed online trolls directed to spread propaganda, incite divisions in foreign communities, and otherwise sow chaos and destabilize democratic platforms. The secretive firm is bankrolled by Yevgeny Prigozhin, a Russian oligarch who is a close ally of President Vladimir Putin. Prigozhin is a dubbed “chef” to Putin by the Russian press, and he is part of the Kremlin's inner circles. His company is believed to be the main backer of the St. Petersburg-based Internet Research Agency. Prigozhin was sanctioned by the U.S. Treasury Department in December of 2016 for providing financial support for Russia's military

occupation of Ukraine. Two of his companies, including his catering business, were also sanctioned by the Treasury this year [45].

The Internet Research Agency was based at 55 Savushkina Street in St. Petersburg before it officially ceased operations on December 28, 2016. However, its work continues at a currently undisclosed location, however. It is believed that they change position every year or two. The director general of another company at 55 Savushkina Street is Glavset, the same name as the boss of IRA and a former regional police chief in St. Petersburg [45].

The official description of the business is “creation and use of databases and information resources” as well as the “development of computer software, advertising services, and information placement services.” It is believed that it may acquire short-term staff from hh.ru, a headhunting site. One post looking for a copywriter stated that the job involved “writing diverse texts for the internet and content for social networks.” The posting offered a monthly salary of 30,000 rubles (then a little over \$500) and required no prior experience. It proffered work with a team of “young and enthusiastic colleagues” in “a comfortable and stylish office.” Reports from former “trolls” said that around 1,000 people work from Savushkina Street alone and that the employees are not even permitted to speak to one another. Recruits were instructed to watch Netflix’s “House of Cards” to improve their English and gain a basic understanding of American politics. Online, they were encouraged to incite disputes and target controversial issues. According to an employee training manual, “There was a goal – to influence opinions, to lead to a discussion.... It was necessary to know all the main problems of the United States of America. Tax problems, the problem of gays, sexual minorities, weapons.” The monthly budget for IRA exceeded \$1 million in 2013 — split between departments that included operations and social media campaigns in Russian and English languages. The “Department of Provocations” offers this mission: “How do we create news items to achieve our goals?” [45]

According to a former troll, who went by the name “Maxim” in an interview with the independent Russian news outlet Dozhd, the secretive factory had several components, including a “Russian desk,” a “foreign desk,” a “Facebook desk,” and a “Department of Provocations.” Throughout 2016 and 2017, the Russian desk operated bots and trolls that used fake social media accounts to flood the internet with pro-Trump messages and false news. Nearly a third of the company’s staff focused on disrupting the 2016 U.S. political conversation, according to reports by the Russian news outlet RBC and another Russian news outlet, Meduza [45].

The foreign desk was more sophisticated than other divisions; trolls were required to learn the nuances of American politics to best “rock the boat” on divisive issues. “Our task was to set Americans against their own government,” Maxim said, “to provoke unrest and discontent.” The foreign desk had a more sophisticated purpose. According to Maxim, who worked in that department, “It’s not just writing ‘Obama is a monkey’ and ‘Putin is great.’ They’ll even fine you for that kind of [primitive] stuff.” In fact, those who worked for the foreign desk were restricted from spreading pro-Russia propaganda. Rather, their job was more qualitative and geared toward understanding the nuances of American politics to rock the boat on divisive issues like gun control and LGBT rights. “Our goal wasn’t to turn the Americans toward Russia,” he added. “Our task was to set Americans against their own government: to provoke unrest and discontent, and to lower Obama’s support ratings.” An entire department, the

“Department of Provocations,” was dedicated to that goal. Its primary objective was to disseminate fake news and sow discord in the West. A Columbia University social media analyst published research that found that Russian propaganda may have been shared billions of times on Facebook alone. The troll farm also had its own “Facebook desk,” whose function was to push back relentlessly against the platform’s administrators who deleted fake accounts as they began gaining traction. When Internet Research Agency employees argued against having their accounts deleted, Facebook staffers responded, “You are trolls.” The trolls would then invoke the First Amendment right to free speech. Occasionally, they won the arguments. In addition to spreading fake news, Russian Facebook accounts went one step further by organizing events, rallies, and protests, some of which galvanized dozens of people. The Internet Research Agency digitally hired 100 American activists to launch 40 rallies across different US cities. According to an RBC investigation, those people remained unaware that they were working for a Russian organization [46].

HAIL-MARY THREATS

Social media enables activist movements to attract attention. Regimes around the world have improved the model, however, efficiently drowning out dissent. Authoritarian regimes are leveraging social media platforms to influence the opinions of domestic and foreign populations. They deploy social media to disseminate official propaganda, monitor and mitigate dissent, and further convince and evangelize their base. Through these regimes, tools of freedom of speech and democracy were transformed into instruments of repression. For authoritarian states, censorship is an essential aspect of their security apparatus; however, overt censorship incites rebellion. By weaponizing social media, controversial regimes can poison open communication networks, psychologically target specific demographics using metadata, and devalue democratic platforms. For instance, in Egypt, Twitter and Facebook helped topple Hosni Mubarak’s regime. Since then, the military-led government has tracked, silenced, and, in some cases, killed its opponents. Silicon Valley startup Procera Networks signed a contract with the Turkish government of Recep Tayyip Erdoğan to extract usernames and passwords from unencrypted websites. This information could be used for widespread surveillance, for precise psychographic profiling, or to silence political opponents and dissidents.

Iran controls the online discourse and browsing options of its citizens through monitoring and Iran-only search engines like Yooz. Yooz is specifically designed to counter Western search engines, such as Google, Yahoo, and Bing. It is designed to search and catalog Iran-based and Persian-language websites, as well as to help Iran circumvent U.S.-led economic sanctions and “grant the academic world the access to the Persian cyberspace.” Iranians filter material and websites that the government finds objectionable, such as free speech activists, and during sensitive times, such as national elections, authorities slow internet traffic significantly. Iranian officials have also discussed the creation of a “Halal Internet” – essentially a giant Iran Intranet – which would separate Iranian cyberspace from the rest of the world. Analysts are skeptical of the claim, arguing instead that Iranian officials are more likely constructing a “Filtarnet” that is no different from the global Web, except that it is heavily censored and filtered. Over the past few years, Iran has doubled the budget of the ICT, and it has begun more aggressively blocking popular websites and apps, such as Instagram and WhatsApp. In response, many Iranians have become proficient at circumvention technologies, such as Tor or VPNs, to conceal their activity and bypass the filters [47].

Likewise, Philippines President Rodrigo Duterte allegedly employs a “keyboard army” of social media trolls to generate fake news and adulatory propaganda and attack his critics. When he decided to run

for president in November 2015, he assembled a social media army with a budget of \$200,000 to flood social media with pro-Duterte comments from prominent online voices, popularized hashtags, and attacks against critics. Despite his opponents vastly outspending his campaign, Duterte gained the presidency with nearly 40 percent of the vote. Afterward, his spokesperson issued a “warm thanks” to Duterte’s 14 million social media “volunteers.” Since his election, nearly 4,000 people have been killed by government forces under Duterte’s war on drugs. To mitigate condemnations from human rights groups, his regime has employed a cadre of personnel and bots to tweet about Duterte constantly. An estimated 20 percent of all mentions of Duterte on Facebook by Filipino users and 20 percent of all mentions of Duterte on Twitter come from bot accounts. Duterte’s social media strategy weaponizes the Philippines youth population. His trolls deliver a steady stream of pro-Duterte propaganda to the estimated 50 million young residents who use social media daily. Anyone critical of the president is digitally abused, publicly shamed, or otherwise silenced. It is believed that his “keyboard army” consists of paid and unpaid users numbering in the hundreds of thousands. At all hours of day and night, they cycle through a host of topics, ranging from corruption to drug abuse to U.S. interference, and post praise of Duterte and links to hyper-partisan sites. The accounts appear as unique individuals and do not share other memes or discuss other topics [47].

The Philippines is an ideal environment for a successful influence operation, because the median age in the country is 23 years old and nearly half of the 103 million population are active social media users. Access to Facebook is free with all smartphones, while visits to other sites, such as newspapers, incur data charges; consequently, many citizens solely rely on social media for virtually all of their news and information. Without other information streams to act as a counterbalance, the population is exponentially more susceptible to viral memes, propaganda, disinformation, and fake news. Duterte has exploited the digital landscape to further his regime. Online trolls can reportedly earn up to \$2,000 per month creating fake social media accounts and then using the bots to flood their communities with pro-Duterte propaganda. As a result, Duterte has maintained an approval rating of more than 80 percent [47].

PROPAGANDA FROM THE PULPIT

Few mechanisms for propaganda distribution are as easy, seamless and effective as propaganda from the pulpit. When messaging is combined with an authority figure who “speaks for God” from behind a pulpit to a congregation of willing participants, a narrative illusion can be created with shocking results. Memes are replicators. They are copied with variation and selection and therefore have replicative power. Memes compete for their own survival, not solely for the benefit of their host, because memes exist outside their host. Religious elements, mental representations, cultural variants, and culturally contagious ideas are memes. Religion fits within the memetic template. Most variations thrive at the expense of others. Faith is deeply rooted in kinship through familial and communal relations. The beliefs and practices of prosocial religions generate increased reproductive and economic success, which in turn, aids intergroup competition. Successful groups thrive, expand, mutate, and are imitated by less successful collectives. Secular memes, such as universal suffrage, sexual equality, human rights, humility, and generosity, can be understood by different denominations and, in fact, are almost universally shared with other religions, because most religions imitate the successfully transmitted memes of other faiths without replication of the failed memes. Even the lack of belief or the rise of secularism can be explained through analysis of the competition of transmitted memes within a society, the cultural niches available to those memes, and the secular pressures on them. Population size and opportunities for spreading

competing memes will have substantial effects on the size of the meme pool and the strength of selection pressure within it. Relevant factors include the ubiquity of education, the availability of education, the pervasiveness of freedom of speech, the independence of the media, and the utilization of technology capable of rapidly disseminating new memes. That said, memetic competition often overcomes secular influence. For example, traditional Islamic values clash with secular ones. According to Susan Blackmore, “At the extreme, if there is a battle between secular institutions and sharia law, it will not be decided by the genetic advantage of religious groups, because the process would be too slow. It will be determined by memetic competition” [48].

Online platforms have expanded both the number of religious vectors and the ease at which religious materials can be disseminated. Religious figureheads preach from Facebook, YouTube, and nearly every other social media platform. Spiritual organizations fundraise on practically every digital vector. In an objective sense, members of congregations are indoctrinated to their communities centered on charismatic figureheads. These community leaders influence audiences through effective communication, concise messaging, and selective fearmongering or reassurances. Digital religious outlets proffer answers to questions, reassurances against reality, and the promise of change, often for a price. Obviously, genuine religious leaders exist; however, many online manipulators are charlatans intent on fiscally or politically benefiting from the susceptibility of their audience. These operators regularly demand tithes, collect donations to their personal LLCs and S-Corps, and sell their congregation’s information received via email and surveys. Memes, especially “like and share” variants, are transmitted on social media to maintain persistent relevancy in the daily lives of the target demographic and to recruit new members via socionic connections. These opportunistic leaders and institutions rely on many of the aforementioned psychological tricks, cognitive biases, and logical fallacies, rather than strictly adhering to the core tenets of their religion. For example, Islam relies heavily on meme tricks that are prevalent in the pro-social faiths: threats; promises; the beauty trick (linking religious memes with awe-inspiring music and art); the altruism trick (persuading believers that they are right by virtue of being believers, supporting other believers or spreading the faith); and admonitions to have faith, not doubt [48].

People subscribe to religion either because it resonates with their worldview, it provides them a sense of purpose, or they were raised into it. In any case, the congregation is at the mercy of the leader’s influence attempts. Astute members may disagree on nuanced points or question aspects of the message, but they remain just as susceptible to mental programming via internalization as their less opinionated peers. Once the meme, the message of the sermon, is planted, it will take root in mind and begin to influence decision-making. As a result, leaders have a profound responsibility to disseminate only proactive content; however, due to the nature of competing religions and worldviews, proactive is relative. Acceptance or xenophobia carry the same potential in religious influence operations, as do numerous other societal and political issues. These subjects often manifest when leaders attempt to make their sermons relevant, when they are responding to an incident, or when they have a biased agenda. Worse, some leaders subvert the trust of their congregation by subjecting them to the wills of special interests by proselytization of prewritten sermons provided from online distribution networks [49].

IDEOLOGICAL DOMESTIC TERRORISTS

The cyber war has moved beyond the battlefield into an all-encompassing struggle in economics, politics, and culture, along with old-school physical confrontation. Instead of smaller sub-state groups forming strategic alliances to fight the government or private power brokers, affinity groups organized around

“Success in meme warfare is to fail as quickly as possible in order to find that one successful meme that takes root and organically spreads in a viral manner.”

...

“The matrix is simply one’s self incarceration in the mental cage of the narrative illusion.”

ideology and ethnic identity are battling one another. Killing an enemy or capturing and maintaining a territory are old-world paradigms of conflict. Messaging is far more important. The emerging hybrid war depends on the allegiance of civilian populations and control over narrative [50]. Social networks empowered those with fringe ideologies to find each other and connect. Consequently, their beliefs have been reinforced because of sustained tribal membership and engagement, and their communities have the tools and access necessary to recruit and indoctrinate new members. The tumultuous 2015 to 2016 political cycles normalized the awareness and terminology of information warfare through incessant discussions of Russian “troll farms” and “meme armies.” Ironically, the revelation of foreign influence drove domestic interest in the subject and led to many wannabe domestic terrorists. Government enforcement of laws in digital spaces is not comprehensive. Furthermore, many spaces cannot be governed because of provisions of the Constitution. In many cases, if the private business controlling the platform does not intervene, the adverse behavior is permitted and wars between factions commence. Tutorials on outdated malware, spy tools, and social influence techniques are more available than ever on online platforms like YouTube and Discord chatrooms. Between the diametrically opposed collectives are dossiers and blacklists, agents and double agents, “good trolls” spying on Trump and anti-Trump supporters and fake antifa and right-wing accounts, disinformation, and counter-intelligence campaigns.

Antifa and other radical groups collect and process public information through decentralized, allegedly leaderless groups. In truth, their tactics are the application of domestic guerrilla warfare to the script kiddie and activist environments. Their entrance to the landscape marks a new phase of bottom-up cyber warfare. Extreme “grassroots” factions by design function as low-level digital influence machines. Their primary motivators are recruitment, revenge, intimidation, disruption, mobilization, and the inspiration of kinetic violence. The capabilities of low-level and under-resourced operations, such as radical groups, should not be underestimated; influence operations are asymmetrical. In some instances, though they lack sophisticated tools, through group-sourcing challenges, attacks, and digital operations, these factions can gather nearly as much information as government intelligence apparatuses. With a high-speed internet connection, anyone with enough free time and basic freeware, such as Maltego and Kali Linux, can surveil social media or invade networks. Their hybrid networks of people and machines automatically aggregate and act on intelligence gathered from nearly every social platform. The information is then either weaponized online or translated into action by volunteer members who “act without orders” [50].

In their coverage of radical collectives, the mainstream media has focused on the violence at rallies and destruction of physical property perpetrated by homegrown extremists. Dedicating screen time to violence in the streets, by

protestors and counter-protestors alike, makes logical sense because property was destroyed and, in some cases, lives have been lost. The mainstream media attracts and maintains viewers through fearmongering and sensationalizing protests and rallies. In reality, the overwhelming majority of protestors and counter-protestors are non-violent; however, they and, in most cases, the points of their causes do not merit media attention because relatively minuscule radical factions can easily steal the spotlight. In fact, in some cases, the intent of the “revolutionaries” is to derail an event or detract from a cause by altering public perception and polarizing issues based on partisan politics. Because of the anonymous nature of the group, anyone in the right apparel, say a ski-mask or clothing with an inflammatory symbol, can infiltrate an event, incite chaos, capture media attention, and then discard the attire and walk away from the outing with no repercussions. Factions such as these that wholly lack in accountability structures force themselves to be publicly, and in some cases legally, accountable for the actions of anyone even temporarily claiming membership. As a result, false flag operations and operations sponsored by special interest groups are both effective and prevalent in this space.

Kinetic activities, while necessary to cover and discuss, are only a fraction of the actions of antifa and other radical groups. Antifa and its polar opposites practice “open-source insurgency” – wherein large collections of small superempowered groups collectively combat much larger foes, typically perceived hierarchies. Memes, trolls, bans, doxes, sock puppets, and targeted disruption campaigns are deployed in a cycle of attacks and counterattacks that, much like traditional military intelligence and information operations, set conditions for the next round of physical confrontation. According to military theorist and futurist John Robb, open-source insurgency leads to “superempowerment” – “an increase in the ability of individuals and small collectives to accomplish tasks/work through the combination of rapid improvements in technological tools and access to global networks.” As a result, small groups on the far fringes of the ideological spectrum have been enabled to increase their productivity radically in conflict [50].

Online disruption is the primary goal of radical factions. The “status quo” is the enemy. They want to maintain constant chaos rather than allow political, societal, or ideological equilibriums. They want to conflate up and down, trust and distrust, fact and falsehood, because in the chaos-driven environment, they have power [50]. Typically, they would lack the clout to influence society or reality; in a state of chaos, however, those with the wherewithal and ability, no matter how seemingly insignificant, to tip the balance in one direction or the other usurp the role of pivotal decision-makers. In this manner, the informed silent minority can overtake a silent or vocal majority. The tactics are not neutral – they favor actors skilled at processing and manipulating high volumes of information – but they are promiscuous. What works against an anti-Trump art installation can be used by ISIS, Antifa, or the alt-right, or turned against any of these groups. Similar systems can even be implemented to coordinate volunteers in highly effective disaster relief efforts [50].

On sites like 4chan and 8chan, organizations and distributed, “leaderless” networks alike conduct IMINT and GEOINT – forensic analysis of digital imagery and geospatial data. The results can be used to dox individuals or groups. This methodology has spread amongst ideologically opposed fringe factions as political violence has increased. A Twitter account associated with 4chan’s pol/board even promotes the process in detail in an apparent attempt to attract new volunteers. For instance, though the assailant masked his face, 4chan users teamed up to identify former professor Eric Clanton as the assailant of three people during the April 2017 Berkeley free speech rally by isolating non-facial visual characteristics

and then through the frames of the imagery from the event. After Charlottesville, antifa protesters used the same techniques to identify and dox the protestors. Following the events in Charlottesville, a twitter account called @yesyoureracist posted information about people supposedly identified at the “Unite the Right” rally. The account eventually gathered 408,000 followers and led to a Patreon campaign to support its efforts. In response, 8chan has reportedly begun targeting the presumed owner of the account and his family with violent threats [50].

GEOINT and IMINT often lead to misidentifications and accusations against innocent people. The rush to judgment and lack of restraint is the result of the public’s thirst for immediate social justice. Antifa is not alone in their mistakes. Social justice attacks, including doxing and the weaponization of social media, are agnostic of political leanings and have victims of every ideological variant. For example, in 2013, a crowdsourced investigation conducted on Reddit and other internet boards falsely accused innocent people of responsibility for the Boston Marathon bombing – a mistake also made on the front page of the *New York Post*. In a more impactful demonstration, Bellingcat, an affiliate of the Atlantic Council, used similar GEOINT and IMINT techniques to geolocate ISIS training camps and identify members. Groups on 4chan and Anonymous have similarly intervened in global conflicts, such as Ukraine and Syria, where they have typically taken different sides, with 4chan showing a strong pro-Assad and pro-Russia bias and Anonymous favoring the opposition. [50]

In addition to outing one another and members of the public, fringe factions also infiltrate their counterparts using sock puppet accounts and attempt to undermine or control the group internally using minority influence leadership, distraction techniques, and bot followers. When the saboteur cannot usurp the community, they do something embarrassing or provocative to draw negative attention or redirect the group’s agenda to damage control. In some cases, internal politics within the group leverage the engineered chaos and the overall messages and goals of the group realign. A recent surge of fake antifa social media accounts and forgeries of supposed antifa documents exemplify how fluid and muddied these groups can be. The fake accounts adopt actual positions held by antifa’s anarchist wing, like the embrace of political violence and opposition to liberal ideals of free expression, and exaggerate these already divisive qualities to make the group appear even more radical and threatening. Their goal is to dissuade potential new members and to sow suspicion among supporters. Others are almost cartoonish in how transparently fake they are and will never persuade current or prospective members to trust their antics. Instead, these accounts are used to incite internal and external chaos. In response, Antifa-affiliated outlets have doxed and DDoSed the people behind the fake accounts and sites, releasing names and other personal details [50].

Conflict because of the actions of radical sociopolitical cliques remains in its infancy. Though it might not lead to outright civil war in America, similar low-level violent multi-polar insurgency has rent other countries asunder. There is truth to Carl von Clausewitz’s famous adage, “War is the continuation of politics by other means.” Today, however, politics is downstream from culture. As ideological variants war for control of digital spaces, the lines between culture, news, politics, war, and entertainment blur and the fabric of society becomes disheveled by chaos [50].

DIGITAL TERRORISTS

Self-polarized lone wolf threat actors (of all varieties and denominations) have acted in cities across the globe. Before the internet, wound collectors internalized their trauma and did not often radicalize to action, so they had to identify, locate, and connect with a tangible local congregation of like-minded individuals. Now on the internet, radicalization can occur instantly and anonymously within significantly more extensive and more geographically distributed groups. Statistically, physical membership in hate groups has actually diminished, because troubled lone wolves can instantly gratify and cultivate their radical beliefs; they can remotely plan their assaults with online resources, such as Google Maps; and they can consume propagandist narratives to model their campaigns around and assure them that their purpose is worth serving and that their sacrifice will be remembered. So far, efforts to demolish online networks and staunch violent ideological polarization have achieved limited success, because radicals have minimal switching costs across online communication and recruitment channels. A few minutes and attention are the only cost to create more Twitter accounts or set up a new propaganda site [51].

Lone wolf threat actors feel isolated and retreat to the internet for community and purpose. Online, they seek attention and often enter communities that further polarize and isolate them in ideological spheres. Eventually, their only outlet becomes the radicalization network, which capitalizes on their seclusion and desire for attention, renown, or purpose. Lone wolf threat actors research, recruit, and discuss their plans within radical online communities before launching kinetic attacks, because they desire the recognition of a like-minded community more than they believe that their actions will have a lasting impact. Lone wolves are troubled individuals who want to be remembered for something, and they often seek affirmation that someone in some online community will immortalize their narrative [51].

The polarizing publications distributed on digital platforms contain memes tailored for subject radicalization. Even the attack blueprints and target selection processes within the propaganda have been turned into memes so that they resonate in the indoctrinated jihadists. For instance, in November 2016, ISIS's publication Rumiyah published articles urging Western readers to utilize rented trucks and handheld weapons in multi-stage public attacks. The report included infographics and characteristics of vehicles and armaments to select or avoid. This template influenced the London Bridge and other recent campaigns. Other publications include *Kybernetiq* and *Dabiq*. The magazines regularly include spreads detailing "hagiographies of mujahids" who died in Western assaults. The profiles appeal to vulnerable and susceptible individuals and are enormously influential in the radicalization process, because they promise infamy and purpose to those who have none [51].

DRAGNET SURVEILLANCE PROPAGANDISTS

Corporate nation state propagandists, such as Google, Twitter, YouTube, and Facebook, perpetuate the syntactical amalgamation of censored ideas, narrative illusions, and perception steering initiatives that cripples and imprisons the mind. Companies like Facebook, Google, Twitter, and other data brokers have increasing control over the collective consciousness through the censorship of information, disguised as curation and personalization, and through their employment of search engine optimization and psychographic artificial intelligence algorithms. Censorship is about what you don't see, rather than what you do see. Digital gatekeepers provide users with only the content that they want them to view. These dragnet surveillance capitalists have quickly turned into a dragnet surveillance censorship collective, and in 2020, they will graduate to full-fledged Corporate Nation States with dragnet surveillance propaganda

initiatives, and they will have their chosen candidate. And the collective will become dragnet surveillance propagandists who evolve and weaponize their censorship algorithms against the psychological core of the American population for both influence and profiteering. We are heading into perilous times.

...

“The key to a highly effective ‘chaos op’ is to sit and wait for an ‘incident’ then weaponize that incident via Hegelian dialectic (problem, outcry, solution). The script practically writes itself.”

...

...

“Influence operations is deeply rooted in political correctness, which is a loaded gun that the individual holds to their own head. Where laws can’t stomp on freedom of speech, automations rule other automations via political correctness for social acceptance.”

...

CONCLUSION

“The meme is the embryo of the narrative. Therefore controlling the meme renders control of the ideas; control the ideas and you control the belief system; control the belief system and you control the narrative; control the narrative and you control the population without firing a single bullet.”

As the reader can see, memetic warfare is absolutely the most potent aspect of digital influence operations. The process of introducing, replicating and expanding distribution of the meme comes down to understanding the most current vectors while using the not-so-apparent vectors as backup reinforcers. Adversaries craft the meme carefully from high-level models using psychological vectors and, finally, with the application of technical tools on digital platforms. As a result, the successful memes inflict the maximum damage with minimal resource expenditure over time, because the target population assumes the responsibility of propagating and mutating the meme, while the adversary only has to steer the messaging. The meme, as it takes shape in the mind of the target audiences, soon becomes an element of influence in their thinking process and belief systems and automatically becomes part of the tribe's narrative. Unplugging from a ubiquitous, pervasive system is impossible. The internet is now a necessity, and digital platforms are the venues where online interactions occur. Switching costs between applications might be manageable, but whole-scale disassociation from the internet would pose an immense detriment to any member of a developed society, because the economy, workplaces, social interactions, entertainment, and numerous other critical facets of everyday life depend on the Internet. Society's dependence on online platforms is also the critical weakness already being exploited by sophisticated and low-level adversaries in powerful asymmetric campaigns. Influence operations that weaponize information, as discrete memes, across digital vectors on online platforms are profound, unavoidable attacks on the fabric of society. Fake news, misinformation, disinformation, propaganda, troll input, bot activities, weaponized keywords, faux viral hashtags, and numerous other technical and non-technical tools are already deployed on every imaginable digital vector. Economies, governments, communities, families, and democracy itself have already been impacted by foreign influence operations based on weaponized memes and engineered narratives. Now, nations must decide how to best defend their people against foreign influence operations while launching their own campaigns against emerging adversaries in the hyper-dynamic, ill-defined battlefield for control of the meme, control of the narrative, and control of perceived reality.

SOURCES

- [1] Defence IQ. (2017). *DNC Hack: An escalation that cannot be ignored*. [online] Available at: <https://www.defenceiq.com/cyber-defence/articles/dnc-hack-an-escalation-that-cannot-be-ignored> [Accessed 19 Jan. 2018].
- [2] Pissanidis, N. and Rõigas, H. (2016). Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations. [online] Ccdcoe.org. Available at: https://ccdcoe.org/cycon/2016/proceedings/08_brangetto_veenendaal.pdf [Accessed 5 Jan. 2018].
- [3] Merriam-webster.com. (2018). *Definition of MEME*. [online] Available at: <https://www.merriam-webster.com/dictionary/meme> [Accessed 19 Jan. 2018].
- [4] Blackmore, S. (2001). *Evolution and Memes: The human brain as a selective imitation device—Dr Susan Blackmore*. [online] Dr Susan Blackmore. Available at: <https://www.susanblackmore.co.uk/articles/evolution-and-memes-the-human-brain-as-a-selective-imitation-device/> [Accessed 19 Jan. 2018].
- [5] 25 Cognitive Biases. (2018). *25 Cognitive Biases—“The Psychology of Human Misjudgment” | The 25 Cognitive Biases Used by Charlie Munger*. [online] Available at: <http://25cognitivebiases.com/> [Accessed 19 Jan. 2018].
- [6] Dauntain, G. (2017). *OPINION: The rally against political correctness is not an excuse for ad hominem*s. [online] Technician. Available at: http://www.technicianonline.com/opinion/columns/article_969f52a2-86d3-11e7-a5f1-077c2e01c49d.html [Accessed 19 Jan. 2018].
- [7] Socionics.com. (2018). *Socionics—The New Psychology*. [online] Available at: <http://www.socionics.com/> [Accessed 19 Jan. 2018].
- [8] Scott, J. and Spaniel, D. (2017). *ICIT Brief: Metadata – The Most Potent Weapon in This Cyberwar: The New Cyber-Kinetic-Meta War*. [online] Icitech.org. Available at: <http://icitech.org/icit-brief-metadata-the-most-potent-weapon-in-this-cyberwar-the-new-cyber-kinetic-meta-war/> [Accessed 19 Jan. 2018].
- [9] W. (2018). *What is Predictive Analytics ?*. [online] Predictive Analytics Today. Available at: <https://www.predictiveanalyticstoday.com/what-is-predictive-analytics/> [Accessed 19 Jan. 2018].
- [10] Myers, D. and Twenge, J. (2013). *Social psychology*. New York (NY): McGraw-Hill.
- [11] Kahne, J., Allen, D. and Middaugh, E. (2014). *Youth, New Media, and the Rise of Participatory Politics*. [online] Dmlcentral.net. Available at: https://dmlcentral.net/wp-content/uploads/files/ypp_workinpapers_paper01_1.pdf [Accessed 19 Jan. 2018].
- [12] Duch, W. (2015). Memetics and Neural Models of Conspiracy Theories. [online] Arxiv.org. Available at: <https://arxiv.org/abs/1508.04561> [Accessed 6 Jan. 2018].
- [13] Color Psychology. (2018). *Color Psychology—The Ultimate Guide to Color Meanings*. [online] Available at: <https://www.colorpsychology.org/> [Accessed 19 Jan. 2018].

- [14] Logicalfallacies.info. (2018). *Logical Fallacies*. [online] Available at: <http://www.logicalfallacies.info/> [Accessed 19 Jan. 2018].
- [15] Kali.org. (2018). *Cite a Website—Cite This For Me*. [online] Available at: <https://www.kali.org/> [Accessed 19 Jan. 2018].
- [16] Paterva.com. (2018). *Paterva Home*. [online] Available at: <https://www.paterva.com/web7/> [Accessed 19 Jan. 2018].
- [17] Metasploit. (2018). *Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit*. [online] Available at: <https://www.metasploit.com/>
- [18] Zarrelli, N. (2016). *How the Hidden Sounds of Horror Movie Soundtracks Freak You Out*. [online] Atlas Obscura. Available at: <https://www.atlasobscura.com/articles/how-the-hidden-sounds-of-horror-movie-soundtracks-freak-you-out> [Accessed 19 Jan. 2018].
- [19] Oppmann, P. and Kosinski, M. (2017). *Denying ‘sonic attacks,’ Cuba names diplomats, releases medical record*. [online] CNN. Available at: <http://www.cnn.com/2017/10/28/politics/cuba-names-sonic-attacks/index.html> [Accessed 19 Jan. 2018].
- [20] Roberts, R. (2017). *Russia targeted key states with anti-Clinton fake news, Trump-Russia hearings chairman reveals*. [online] The Independent. Available at: <http://www.independent.co.uk/news/world/americas/us-politics/russian-trolls-hilary-clinton-fake-news-election-democrat-mark-warner-intelligence-committee-a7657641.html> [Accessed 5 Jan. 2018].
- [21] Dvoskin, E. (2017). *How Russian content ended up on Pinterest, of all places*. [online] Daily Herald. Available at: <http://www.dailyherald.com/business/20171014/how-russian-content-ended-up-on-pinterest-of-all-places> [Accessed 5 Jan. 2018].
- [22] Breiner, A. (2016). *Pizzagate, explained: Everything you want to know about the Comet Ping Pong pizzeria conspiracy t...* [online] Salon. Available at: <https://www.salon.com/2016/12/10/pizzagate-explained-everything-you-want-to-know-about-the-comet-ping-pong-pizzeria-conspiracy-theory-but-are-too-afraid-to-search-for-on-reddit/> [Accessed 19 Jan. 2018].
- [23] Byrne, M. (2016). *‘Pizzagate’ Conspiracy Meme Reaches Its Natural Conclusion—With Shots Fired*. [online] Motherboard. Available at: https://motherboard.vice.com/en_us/article/4xa5jg/pizzagate-conspiracy-meme-reaches-is-natural-conclusion-with-shots-fired [Accessed 19 Jan. 2018].
- [24] Grim, R. and Cherkis, J. (2017). *Russian Trolls Fooled Sanders Voters With Anti-Clinton Fake News*. [online] HuffPost UK. Available at: https://www.huffingtonpost.com/entry/bernie-sanders-fake-news-russia_us_58c34d97e4b0ed71826cdb36 [Accessed 6 Jan. 2018].
- [25] Elharrar, D. (2017). *7 Types of Bots – Chatbots Magazine*. [online] Chatbots Magazine. Available at: <https://chatbotsmagazine.com/7-types-of-bots-8e1846535698> [Accessed 6 Jan. 2018].
- [26] Gallagher, E. (2017). *Propaganda Botnets on Social Media – Erin Gallagher – Medium*. [online] Medium. Available at: https://medium.com/@erin_gallagher/propaganda-botnets-on-social-media-5afd35e94725 [Accessed 6 Jan. 2018].
- [27] Gertz, B. (2017). *China’s ‘Magic Weapons’: Influence Operations Subverting Foreign Governments*. [online] Washington Free Beacon. Available at: [27] <http://freebeacon.com/national-security/chinas-magic-weapons-influence-operations-subverting-foreign-governments/> [Accessed 5 Jan. 2018].

[28] Mattis, P. (2015). A Guide to Chinese Intelligence Operations—War on the Rocks. [online] War on the Rocks. Available at: <https://warontherocks.com/2015/08/a-guide-to-chinese-intelligence-operations/> [Accessed 5 Jan. 2018].

[29] Martina, M. (2017). Exclusive: In China, the Party's push for influence inside foreign fir. [online] Reuters. Available at: <https://www.reuters.com/article/us-china-congress-companies/exclusive-in-china-the-partys-push-for-influence-inside-foreign-firms-stirs-fears-idUSKCN1B40JU> [Accessed 5 Jan. 2018].

[30] Bergerson, K. (2016). *Cite a Website—Cite This For Me*. [online] Uscc.gov. Available at: <https://www.uscc.gov/sites/default/files/Research/USCC%20Staff%20Report%20on%20China%20Countering%20US%20Military%20Presence%20in%20Asia.pdf> [Accessed 19 Jan. 2018].

[31] YouTube. (2015). *The New Authoritarians: Ruling Through Disinformation*. [online] Available at: <https://www.youtube.com/watch?v=d-vMix8dikg> [Accessed 19 Jan. 2018].

[32] Navarro, P. (2016). *China's Non-Kinetic 'Three Warfares' Against America*. [online] The National Interest. Available at: <http://nationalinterest.org/blog/the-buzz/chinas-non-kinetic-three-warfares-against-america-14808> [Accessed 19 Jan. 2018].

[33] Raska, M. (2015). China and the 'Three Warfares'. [online] The Diplomat. Available at: <https://thediplomat.com/2015/12/hybrid-warfare-with-chinese-characteristics-2/> [Accessed 5 Jan. 2018].

[34] King, G., Pan, J. and Roberts, M. (2017). *How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument*. [online] Gking.harvard.edu. Available at: <http://gking.harvard.edu/50c> [Accessed 19 Jan. 2018].

[35] Waddell, K. (2017). *'Look, a Bird!' How the Chinese Government Trolls by Distraction*. [online] The Atlantic. Available at: <https://www.theatlantic.com/technology/archive/2017/01/trolling-by-distraction/514589/> [Accessed 19 Jan. 2018].

[36] Doctorow, C. (2017). *The first-ever close analysis of leaked astroturf comments from China's "50c party" reveal Beijing's cybercontrol strategy*. [online] Boing. Available at: <https://boingboing.net/2017/01/18/the-first-ever-close-analysis.html> [Accessed 19 Jan. 2018].

[37] King, G., Pan, J. and Roberts, M. (2017). How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument. [online] Gking.harvard.edu. Available at: <https://gking.harvard.edu/50c> [Accessed 5 Jan. 2018].

[38] Lau, J. (2016). Who Are the Chinese Trolls of the '50 Cent Army'?. [online] VOA. Available at: <https://www.voanews.com/a/who-is-that-chinese-troll/3540663.html> [Accessed 5 Jan. 2018].

[39] Bernard, D. (2016). China's 50 Cent Party: The Other Side of Censorship. [online] VOA. Available at: <https://www.voanews.com/a/chinas-50-cent-party-the-other-side-of-censorship/3355262.html> [Accessed 5 Jan. 2018].

[40] <https://www.economist.com/news/middle-east-and-africa/21725288-big-ways-and-small-china-making-its-presence-felt-across>

[41] Economist.com. (2017). China goes to Africa. [online] Available at: <https://www.economist.com/news/middle-east-and-africa/21725288-big-ways-and-small-china-making-its-presence-felt-across> [Accessed 5 Jan. 2018].

- [42] Brookes, P. (2006). China's Influence in Africa: Implications for the United States. [online] The Heritage Foundation. Available at: <http://www.heritage.org/asia/report/chinas-influence-africa-implications-the-united-states> [Accessed 5 Jan. 2018].
- [43] Johnson, S. (2005). *Balancing China's Growing Influence in Latin America*. [online] The Heritage Foundation. Available at: <https://www.heritage.org/americas/report/balancing-chinas-growing-influence-latin-america> [Accessed 19 Jan. 2018].
- [44] Maskirovka: Russia's Gray Zone Between Peace and War. [online] The Cipher Brief. Available at: <https://www.thecipherbrief.com/maskirovka-russias-gray-zone-peace-war> [Accessed 5 Jan. 2018].
- [45] Lister, T. (2017). Putin's 'chef,' the man behind the troll factory. [online] CNN. Available at: <http://www.cnn.com/2017/10/17/politics/russian-oligarch-putin-chef-troll-factory/index.html> [Accessed 6 Jan. 2018].
- [46] Sheth, S. (2017). 'Our task was to set Americans against their own government': New details emerge about Russia's trolling operation. [online] Business Insider. Available at: <https://amp.businessinsider.com/former-troll-russia-disinformation-campaign-trump-2017-10> [Accessed 6 Jan. 2018].
- [47] Williams, S. (2017). Rodrigo Duterte's Army of Online Trolls. [online] New Republic. Available at: <https://newrepublic.com/article/138952/rodrigo-dutertes-army-online-trolls> [Accessed 5 Jan. 2018].
- [48] Blackmore, S. (2016). *Memes and the evolution of religion: We need memetics too*. [online] Susanblackmore.co.uk. Available at: <https://www.susanblackmore.co.uk/wp-content/uploads/2017/05/Memes-and-the-evolution-of-religion-We-need-memetics-too.pdf> [Accessed 19 Jan. 2018].
- [49] GrowChurch.net. (2018). *Looking For Sermon Series Ideas? – A Year's Preaching*. [online] Available at: <https://growchurch.net/looking-sermon-series-ideas-a-years-preaching> [Accessed 19 Jan. 2018].
- [50] Siegel, J. (2017). *The Alt-Right and Antifa Are Waging a New Kind of Internet Warfare*. [online] Vice. Available at: https://www.vice.com/en_nz/article/7xxmad/the-alt-right-and-antifa-are-waging-a-new-kind-of-internet-warfare [Accessed 19 Jan. 2018].
- [51] Scott, J. and Spaniel, D. (2017). *ICIT Analysis: The Surveillance State & Censorship Legislation Conundrum: Dagnet Surveillance & Censorship Legislation Will Do Nothing to Eliminate Cyber Jihad & Lone Wolf Recruiting*. [online] Icitech.org. Available at: <http://icitech.org/icit-analysis-the-surveillance-state-censorship-legislation-conundrum-dagnet-surveillance-censorship-legislation-will-do-nothing-to-eliminate-cyber-jihad-lone-wolf-recruiting/> [Accessed 19 Jan. 2018].



JAMES SCOTT

James Scott is a Senior Fellow and co-founder of the Institute for Critical Infrastructure Technology, Senior fellow at Center for Cyber Influence Operations Studies and the author of more than 40 books with 9 best sellers on the topics of hacking cyborgs, energy sector cybersecurity, nation state cyber espionage and more. He advises to more than 35 congressional offices and committees as well as the American intelligence community, NATO and Five Eyes on cyber warfare and digital influence operations. Mr. Scott's work gains regular coverage in domestic and international publications such as the LA Times, Wired, New York Times, Motherboard, Newsweek, Christian Science Monitor, Fox News, and PBS News Hour, and his work was referenced by media, academia and industry more than 3000 times in 2017 alone.