Digital Influence Warfare in the Age of Social Media

by James J.F. Forest (Praeger/ABC-CLIO, 2021)

APPENDIX A: Glossary of Terms

Draft, September 2020

accelerationism: a quasi-political theory arguing that amplifying the worst things about capitalism and disruptive technological changes will eventually make things so bad people will revolt; adherents are opposed to any restraints that social moderates, environmentalists, governments and others try to impose.[1]

Active Measures: a Russian strategic initiative involving the manipulative use of slogans, arguments, disinformation, and carefully selected true information in order to influence the attitudes and actions of foreign publics and governments.[2] Its strategic focus on defeating adversaries through the "force of politics rather than the politics of force" was adapted to the age of social media, and is frequently referenced in various investigations into Russia's digital influence operations against the U.S.[3]

Advanced Persistent Manipulators (APM): an actor or combination of actors perpetrating an extended, sophisticated, multi-platform, multimedia information attack on a specified target.[4]

affiliations: attributes of an individual Internet user that reveal specific relationships, such as educational institutions, political and social organizations, family members, friends, businesses, financial institutions, religion and much more. These data can then be used to craft messages that would be most likely to influence the individual.

affinity fraud: taking advantage of people's tendency to trust others with whom they share similarities, such as religion or ethnic identity, to gain their trust and then influencing them.[5]

agentic state: a shift in behavior and attitudes wherein individuals no longer view themselves as acting out of their own purpose, but instead come to see themselves as agents for executing the wishes of another person. When evoked by someone perceived as a legitimate and relevant authority, the agentic state can be a powerful facilitator for totalitarianism.[6]

algorithm: a fixed series of steps that a computer performs in order to solve a problem or complete a task.[7]

altered audios/photos/videos: a variant of fake audio and visual items, these are essentially authentic but with modifications that are meant to portray something different. Examples include a photo that has been enhanced to make someone look younger (or older), or an audio or video clip that has been edited or slightly slowed down to make it appear the speaker is slurring their words, possibly even inebriated. Sometimes the nuances of these alterations are more difficult to spot than an outright forgery.

ambit claim: extravagant initial demand made in expectation of an eventual counter-offer and compromise.[8]

amplifier accounts: social media accounts (typically automated bots) whose sole purpose is to boost the spread of content by automatically liking, sharing and reposting (or retweeting) the original message.

Anonymous: a loosely knit group of hacktivists that hack or break into computer systems, typically in support of social or political objectives.

anti-vaxxers: individuals who believe anti-science conspiracy theories about harm caused by vaccinations.

application program interface (API): a means by which data from one web tool, application or social media platform can be exchanged with or received by another.[9]

artificial intelligence (AI): computer programs that are 'trained' to solve problems that would normally be difficult for a computer to solve. These programs "learn" from data, continually adapting methods and responses in a way that will maximize accuracy.[10]

asymmetric warfare: digital influence warfare can be considered a type of asymmetric warfare, in which an adversary engages its target through alternate means rather than direct military confrontation. Other common examples include insurgency, terrorism, psychological operations, and cyberattacks.

astroturf: to create the image of public support or consensus where there is none.[11] Often, manufacturing a false sense of popularity or support involves creating buzz around a subject by posting what appear to be multiple spontaneous comments on social media, blogs, webpage comments sections, etc. The posts, while appearing random and uncoordinated, are in fact orchestrated for effect by the influencer, frequently using social media "bots" (*see below*).[12]

attention hacking: the strategic use of memes and amplifier accounts targeting journalists, bloggers, and others in order to spread messages on social media.[13]

attribution: the ability to determine the origins of an influence operation with a reasonably high level of confidence.

attribution theory: a theory that examines the ways in which people explain the causes of—and assign responsibility for—each other's behavior. As Taylor explains, this area of research has shown that "our tendency to attribute responsibility (in a case where no obvious reason for action is apparent) depends on the person and the action involved. Someone we like will be judged more responsible if the action is praiseworthy, and less responsible if the action deserves blame. For someone we don't like, the reverse is the case."[14]

automated "bots": computer-generated accounts on social media platforms that are programmed to do specific things autonomously and automatically.

automated retweet: a type of amplifier "bot" account unique to the social media platform Twitter, which is programmed to automatically re-post messages received from specific accounts.

auto-redirect URLs: a simple line of HTML code that automatically takes visitors at one website to another website at a different address.

bait and switch: tricking someone with an attractive offer that is then replaced with something else after they have shown some initial commitment *(see also: "foot-in-the-door").*

bandwagoning effect: a type of human behavior in which social proof and fear of missing out combine to attract individuals toward supporting an idea, political candidate, product, service, sports team, etc.

big-data analytics: a term often used to describe the ways in which massive amounts of data collected from a large population (e.g., social media profiles and daily activities) inform projections about their preferences and future behavior.

birther conspiracy: a false claim, consistently debunked, about former President Barak Obama's place of birth.

black hat search engine optimization: Aggressive and illicit strategies used to artificially increase a website's position within a search engine's results *(see also: "search engine optimization").*

blog: an online journal or informational website displaying information in reverse chronological order, with the latest posts appearing first, at the top. It is a platform often used by writers share to their views on topics of interest.[15]

bot: a fake social media account built with software or code designed to mimic human behavior online.[16] They are designed to generate posts and/or engage with content on a particular social media platform.[17]

botnet: a collection or network of bots that communicate across multiple devices to perform tasks.[18] They act in coordination and are typically operated by one person or group. Commercial botnets can include as many as tens thousands of bots.[19]

brainwashing: a term used (often incorrectly) to describe a kind of manipulation through which the victim becomes entirely committed to beliefs and behaviors that serve the manipulator's purpose.[20]

breadcrumming: a term that traditionally describes leaving a trail for others to find and follow, but in the context of digital influence warfare it refers to the act of slowly leading people deeper into a world of conspiracies and disinformation. The term is also used in reference to relationships in which one person provides just enough attention and care for another to keep that person believing the relationship could someday evolve into something deeper.

captology: the study of computers as persuasive technologies.[21]

chan (4chan, 7chan, 8chan, etc.): An imageboard website on which users upload and discuss visual images. It is divided into multiple channels, or boards, with particularly content and guidelines.[22] Wild, aggressive and often rude content can often be found here, which is attractive to a certain segment of Internet users.

cherry-picking: selecting only information and data that supports what you want to believe, and ignoring any contradicting information or data (even from the same source); very common behavior within influence silos.

chumming: Originally referring to the practice of luring animals (like sharks) with bait, the term

is now also used to describe a type of Internet advertising that involves "clickbait" (*see below*) to lure visitors to a website.

click fraud detection: technology and software used by businesses to monitor and prevent attempts by malicious actors to boost website advertising revenue through manual click fraud (performed by people with the intention of defrauding a business) or automated click fraud (done using specialized software, often called a click bot, designed to visit specific websites and click on ads).[23]

clickbait: digital media items (images, videos, headlines, etc.) designed to trigger an emotional response from a user that leads them to click on the item, because each person who does so generates revenue for the clickbait provider.[24] Often misleading or inaccurate, the provocative nature of the clickbait headline is typically more sensational than the content to which it directs the user.[25]

conditioning: in the context of influence warfare, developing a target's mental and emotional predisposition for (and responses to) a certain political view or platform

cognitive bias: a common human tendency to process information (and disinformation) in ways that conforms to previously held beliefs, values, frameworks, expectations, etc. One of the most common of these is confirmation bias (*see below*).

cognitive dissonance: a term from the study of psychology that refers to an internal tension that is created when we simultaneously believe two things that are in conflict with one another. When inconsistency between the two beliefs becomes apparent, the cognitive dissonance leads to stress and negative emotions that a person will naturally try to get rid of.[26]

confirmation bias: a common tendency for an individual to give more weight and credibility to information (or disinformation) that confirms one of their pre-existing beliefs.[27]

content farms: websites that mass-produce clickbait articles designed to generate traffic and ad revenue.[28]

compromise: in the context of digital influence warfare, the ability to violate the security of a computer and make it do something the attacker wants, like disclose sensitive information or be used as a bot or zombie (*see below*) in attacking others. The term also refers to forcing an individual to act in ways not in their best interests, but because they are threatened with extortion. Examples include threatening to release compromising information, like the Russian tactic of *kompromat* (*see below*) or "sextortion" (coercing someone to do something in order to prevent embarassing intimate photos from being posted online).

computational propaganda: a term used by the Oxford Internet Institute to describe "the use of automation, algorithms and big-data analytics to manipulate public life,"[29] and defined by Philip Howard as misleading news and information, algorithmically generated or distributed, that is served by social media firms to their users.[30]

conspiracy theories: fabricated "explanations" for events or situations that offer no solid evidence, only speculation, yet are believed by individuals for a variety of personal and idiosyncratic reasons.

conversion rate: when referring to the Internet and social media, this term describes the proportion of an audience that clicks on an advertisement and moves through to a deeper level of engagement.[31]

creeping normality: a corollary of the salami slice tactic (*see below*), the goal of the influencer is to make a significant change acceptable by making it happen very slowly, through small, often unnoticeable, increments of change. A popular example refers to boiling a frog—it would try to escape if you dropped it directly into the boiling water, but if you put the poor creature into room temperature water and then turn the stove on to heat up, the frog would not discover the danger until it is too late.

crowdsourcing: soliciting data and/or analysis related to a specific topic, idea or issue from a large population of public users, traditionally an online community, who have knowledge of that topic, idea, or issue.[32]

cyberattack: the process of finding and exploiting vulnerable devices and networks by entering them and copying, exporting or changing data within them.[33]

cyberbullying: a type of bullying that takes place using electronic devices and equipment such as cell phones, computers, and tablets as well as communication tools including social media sites, text messages, chat and websites.[34]

dark networks: covert or clandestine networks that purposefully try to conceal their existence, structure, members and activities (including those involving terrorist, criminal and insurgents) that try to remain hidden.[35]

data mining: the process of monitoring and examining large volumes of data by combining tools from statistics and artificial intelligence to recognize useful patterns.[36]

DDOS (Distributed Denial of Service): a type of coordinated cyber attack in which multiple computers simultaneously deliver requests for information to a targeted web server, with the intention of overwhelming the system and forcing it to freeze up or shut down.

debunk: proving with evidence that a claim or conspiracy theory is false.

deep fakes: fabricated media produced using artificial intelligence (*see above*). By synthesizing different elements of existing video or audio files, AI enables relatively easy methods for creating 'new' content, in which individuals appear to speak words and perform actions, which are not based on reality.[37]

deflection/redirection: common tactics used in arguments or debates to move the discussion in a different direction, like changing the subject and introducing a new topic for debate *(see "Whataboutism")*, questioning the motives of others, scapegoating, promoting stereotypes, and many others.

dehumanization: characterizing individuals as less than human, a dangerous form of "othering" that is often related to criminal and political violence.

dezinformatsia (also spelled dezinformatsiya): coordinated state efforts by Russia (and during the Cold War, by the Soviet Union) to disseminate false or misleading information to the media

in targeted countries or regions.[38]

digital influence mercenary: individuals whose main purpose for deceiving and provoking targets online is to generate profit. State governments may hire teams of mercenaries to carry out digital influence campaigns, but the individuals rarely believe in the political goals or objectives behind those campaigns (see Chapter 11).

digital influence warfare: combining the tools of digital influence and marketing with the psychology of influence and persuasion, technical tools of cyber attacks, and a political warfare strategy against one or more targets.

disinformation: the intentional dissemination of information that is wholly or partly false. It differs from "misinformation," which is initially provided without the direct intention to deceive.[39] Disinformation is often completely false, exaggerated, biased, or presented in manipulative and misleading ways (for example, through the manufactured illusion of popular support described in Chapter 3).

dog whistle: when referring to influence and persuasion, this term describes the use of coded or symbolic language that has a particular (often social or political) meaning for some people but not others.

door-in-the-face: a persuasion technique in which the influencer first makes a large request that the target is most likely to reject, and then makes a much smaller request which comparatively seems more reasonable. According to psychologists, the target is more likely to comply with the second request because of the principle of reciprocity—the target feels that the persuader is doing them a favor by making a much smaller request.[40] Essentially, a reverse approach to the "foot-in-the-door" technique (*see below*).

dopamine hit: when the chemical neurotransmitter dopamine is released in large amounts, it creates feelings of pleasure and reward, which motivates us to repeat the specific behavior that resulted in those feelings. The term is frequently used to describe a type of consistent social media use that feeds an individual's biases and ego.

DOS (Denial of Service): similar to DDOS, but usually involves just one computer flooding a server with information requests in order to overwhelm the system and force it to freeze up or shut down.

doxing (or doxxing): The act of publishing private or identifying information about an individual online, without his or her permission. This information can include full names, addresses, phone numbers, photos, and more.[41]

Dunning–Kruger Effect: A type of cognitive bias described in a popular 1999 research article by Cornell psychologists David Dunning and Justin Kruger, in which people tend to overestimate their abilities at certain tasks. They concluded that this inflated self-assessment occurs because their incompetence robs them of the cognitive ability to recognize their own incompetence.[42] When a social media user believes he or she is much more skilled at spotting fake news than they actually are, this type of cognitive bias makes them particularly vulnerable to digital influence efforts.

echo chamber: a form of digital influence silo, in which all the participants repeat, amplify and reinforce the same narrative and limited worldview, usually based on a limited number of information source, while differences of opinion or contradictory facts are actively excluded and denigrated. Social media platforms provide an unprecedented ability to surround ourselves with these kinds of echo chambers that confirm our biases and prejudices, and provide optimum opportunities for the spread of disinformation.

email phishing: *see "phishing" and "spear phishing".*

email spamming: sending repeated multiple junk email messages to one or more targets.

extremism: a set of beliefs encouraging an exclusive in-group identity and out-group "othering". According to J.M. Berger, "Extremism is distinguished from ordinary unpleasantness—blind hate and pedestrian racism—by its sweeping rationalization of why conflict exists and its insistence on the necessity of conflict … It is an assertion that an out-group must always be actively opposed because its fundamental identity is intrinsically harmful to the in-group."[43]

Facebook: the world's largest social media platform, with 2.7 billion users as of July 2020.[44]

fake news: fabricated information that mimics news media content.[45]

filter bubble: a type of digital influence silo that affects users like an echo chamber, but the key difference (according to Richard Fletcher) is that filter bubbles are formed by computer algorithms which the user has no real control over, while echo chambers can be opted into (or out of) by the user.[46]

flaming: posting insults, often laced with profanity or other offensive language on social networking sites.[47]

flat-earther: an individual who believes the earth is flat despite all available evidence disputing that belief.

FOMO (Fear of Missing Out): a type of anxiety generated by enviously feeling that others are experiencing better lives than you are.[48] It is often exacerbated by social media platforms, where users (afraid of missing something important or stimulating) repeatedly scroll through a constantly refreshing information feed. And similar to the discomfort of uncertainty, FOMO can be exploited by digital influencers.

foot-in-the-door: a persuasion technique in which the influencer first makes a small initial request, and when the target agrees, this creates the condition that they will more likely agree to a larger request made at some future point (in order to remain internally consistent with the earlier decision to comply).[49] Essentially, a reverse approach to the "door-in-the-face" technique (*see above*).

fragmentation: an influence strategy that involves instigating and amplifying disagreements among a society in order to divide its members into multiple opposing subgroups.

framing effect (or "framing bias"): the way in which people make decisions based on the way data or information is presented to them (e.g., with positive or negative connotations). An

example is found in Mark Twain's story of Tom Sawyer whitewashing the fence, in which he convinced his friends to pay him for the "privilege" of doing his work by framing the chore in positive terms.

gaslighting: a term derived from the 1938 play (and 1944 film) *Gas Light*, used to describe situations in which a person orchestrates deceptions and inaccurately narrates events to the extent that their victim stops trusting their own judgments and perceptions.[50] According to Robert Walker, "it is done slowly over time to keep the victims unaware of the process, to convince the targets that false information is factual, which then slowly erodes the targets' grip on reality and thus builds reliance on the purveyors of the false information."[51]

gatekeeper: in the context of influencing and the digital ecosystem, one who regulates the flow of information to or among his or her group.

Google bomb: an early type of "search engine optimization" strategy (now mostly prevented) in which a group of people would make as many links as possible to one website from various other websites in order to artificially increase the Google ranking of that website among the top search-engine results for a word or phrase.

group-think: a term used in social psychology to describe how individuals within a group decision-making situation typically seek consensus, leading many to set aside their own personal beliefs and embrace the majority opinion of the group.[52]

hacktivism: a type of cyberattack in which accounts or websites are violated in some way for social or political reasons rather than for profit. Examples range from website defacement to hijacked accounts.

Hamilton-68 Dashboard: an online monitoring and reporting system sponsored by the bipartisan group Alliance for Securing Democracy, which monitors the activity of Twitter accounts that are linked to Russian, Chinese, and Iranian government officials and state-funded media on Twitter, YouTube, state-sponsored news websites, and via official diplomatic statements at the United Nations.[53] The system has proved useful to researchers examining state-sponsored disinformation and other types of digital influence.

hashtag: a word or phrase preceded by a hash sign (#), used on social media websites and applications, especially Twitter, to identify messages on a specific topic.[54] Internet trolls often use multiple popular *hashtags* in their tweets in order to attract more visibility.

hashtag flooding: adding a hashtag to a flurry of messages, typically using thousands of automated bot accounts, in an effort to create the illusion of widespread support for (or against) an idea; often this tactic is used in attempts to manipulate the "what's trending" list on Twitter *(see also: "Twitter bomb")*.

hashtag hijacking: similar to hashtag flooding, this tactic involves adding a trending hashtag to information that disparages and contradicts the initial intent of the hashtag. An example involves white supremacists adding the #blacklivesmatter hashtag to overtly racist messages. The main purpose is to diminish the ability of a community to generate support for an idea

(see also: "Twitter bomb").

hijacked account: a type of cyberattack in which stolen login information is used to access someone else's account and send messages that are often meant to embarrass or discredit the account's true owner.

honeypot: a website designed to attract visitors but with the secret purpose of entrapment or tricking visitors into doing something that is not in their best interests, like revealing personal information.

identity masking: technical tools and methods used to protect the privacy of an individual's personal information while online.

implausible deniability: a term that refers to how some frauds and illicit campaigns are intentionally designed to be discovered, because this discovery then creates greater uncertainty about what people should or should not believe.

impressions: an online industry term for the total number of times an ad or post is displayed on users' screens.[55]

in-group: a term used in the field of social psychology to describe how a person's identity is often closely linked to others with shared interests and mutual affinity. According to J.M. Berger, efforts to promote greater cohesion among the in-group members can lead to increasingly hostile attitudes toward others (the "out-group").[56]

indoctrination: forcing a person to adopt a set of beliefs uncritically and unconditionally. As described in Chapter 8 of this book, in-group indoctrination is one of the common results of an echo chamber or influence silo.

influence bubble: a term loosely used interchangeably with echo chamber, influence silo, and filter bubble.

influence silo: a social construct in which individuals surround themselves with specific sources of information (including people) with whom they agree, while simultaneously blocking all sources of information with whom they disagree, or simply don't want hear or see. Social media platforms have provided an unprecedented ability to do this *(see also: "echo chamber" and "filter bubble")*.

influence warfare: a term originally referring to foreign state-based influence efforts of malicious intent, but in recent years has expanded to include the ways in which both states and violent non-state actors struggle against each other for influence and control over individuals' beliefs and behaviors *(see also: digital influence warfare)*.

information operations: initially a military term that referred to the strategic use of technological, operational, and psychological resources to disrupt the enemy's informational capacities and protect friendly forces, it is similar to the term "information warfare". Today, social networking services—most notably Facebook—have adopted this term when referring to unidentified actors' deliberate and systematic attempts to steer public opinion using inauthentic accounts and inaccurate information.[57]

information warfare: the offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy an adversary's knowledge, communications, and perceptive access and processes.[58]

infotainment: a term used to describe the melding together of information and entertainment provided on certain television channels, websites and other forms of media.

inoculation theory: a theory (from social psychology and communication studies) suggesting that psychological and emotional resistance to persuasive influence can be developed in a similar way as physical resistance to diseases—for example, by first exposing the target audience to weakened versions of whatever ideas you want the target audience to resist. A similar concept involves educating the target audience about the tactics and malicious intentions of those seeking to use disinformation to influence and deceive them.[59]

Instagram: one of the world's most popular social media platforms (owned by Facebook), through which users post, share and common on each other's photos and videos

intelligence-led social media defense: a term coined by Clint Watts, describing how governments and social media platforms can improve their ability to anticipate changes in adversary threat behavior and proactively disrupt those threats rather than reactively responding to them.[60]

intelligent agent: a computer program (and essential component of artificial intelligence) that can make decisions, complete tasks and perform services autonomously, including responding to changes in its operating environment or a prompt from a human user.[61]

Internet of things: networks of household devices with embedded power supplies, small sensors, and an address on the Internet. Most of these networked devices are everyday items that are sending and receiving data about their condition and our behavior (for example, a thermostat or an alarm system).[62]

Internet Meme: *see "meme".*

Internet Research Agency (IRA): an infamous Russian troll farm (*see below*) originally based in St. Petersburg, from which many efforts were launched to influence U.S. social media users during the 2016 presidential election.

kompromat (a.k.a *compromat*): a Russian influence warfare tactic involving the theft of secret, compromising information about the target, and using it to coerce the target to do something (*see also: "compromise"*).

legend: a fabricated biographical background, supported by a stream of photos, comments, and online activity, that makes a fake social media account appear to represent a real person.[63]

liar's dividend: the concept that the mere existence of fake information and lies gives more credibility to a person when denying their lies. Essentially, this means that publicly revealing materials (like videos, audios or documents) as fake or manipulated can backfire, because it means the public will have more problems determining what is or is not fake. Essentially, as

Joan Solsman explains, "deepfakes make it easier for candidates caught on tape to convince voters of their innocence—even if they're guilty—because people have learned they can't believe their eyes anymore."[64]

LinkedIn: a social media platform used more for professional networking than for sharing photos, videos and personal opinions.

low-ball: a persuasion tactic in which the target is provided only partial (or false) information, like a lower price than they might expect for a product, and then suddenly other information is introduced, like a higher price to cover essentials services or components for that product. Somewhat similar to the "foot-in-the-door" tactic, the goal of the influencer is to create the conditions that will lead the target to comply with increasingly costly requests (in order to remain internally consistent with the earlier decision to comply).

malinformation: a term used to describe genuine information that is shared to cause harm to the target of an influence effort. This includes private or revealing information that is spread to harm a person or reputation *(see also "doxing")*.[65]

malware: malicious software or code that is programmed to infiltrate a computer system in order to carry out a variety of tasks, like steal confidential information, spy on the computer user, disrupt or damage the operating system, or even take over the system and convert it into a "zombie" (*see below*). E-mail phishing (*see above*) often involves the use of a "trojan horse" containing a virus which begins attacking the computer when activated.[66]

manufactured amplification: a term used to describe how the reach or spread of information is boosted through artificial means, including by human and automated manipulation of search engine results and trending lists, generating fake votes and signatures in online polls and petitions, and by promoting certain links or hashtags on social media. As mentioned in Chapter 11, digital influence mercenaries provide this type of service to their clients.[67]

meme: a term introduced by Richard Dawkins in his 1976 book *The Selfish Gene*, referring to small cultural units of transmission, analogous to genes, which are spread from person to person by copying or imitation. At any given moment, many memes are competing for attention, but only memes suited to their sociocultural environment spread successfully, while others become extinct. As Limor Shifman explains, online memes are a group of digital content units sharing common characteristics of content, form, and/or stance; created with awareness of each other; and circulated, imitated and/or transformed via the Internet by many users. They are multiparticipant creative expressions through which cultural and political identities are communicated and negotiated.[68]

microtargeting: the process of preparing and delivering customized digital messages to voters or consumers. According to Philip Howard, contemporary microtargeting involves preparing and delivering a message that is customized for particular individuals using their data, social ties, cognitive biases, and big data records, often in ways that are unsupervised, untraceable, and unaccountable and unknown to the individuals.[69]

misinformation: The unintentional spread of information that is wholly or partly false. It differs from "disinformation," (*see above*) which is intentional. Misinformation has also been described as "contested information that reflects political disagreement and deviation from expert consensus, scientific knowledge, or lived experience."[70]

narrowcasting: as opposed to broadcasting to mass audiences, narrowcasting involves providing information to a carefully selected or segmented audience, often defined by specific attributes of the audience members (e.g. demographics, locality, education level, political preferences, purchasing habits, etc.).

Occam's Razor: a principle of analysis commonly phrased as "simpler explanations are more likely to be correct," essentially meaning (in the words of J.M. Berger) that theories should stipulate only as much as is necessary to explain an observation about the world.[71]

othering: the act of blaming an out-group for all the problems faced by an in-group, encouraging an us-vs-them mentality that fuels hostility and sometimes violence.

out-group: all people outside a particular in-group (*see above*), who are typically seen as inferior compared to the revered in-group members because of key differences like race, gender, religion, nationality, sexual orientation, and other attributes.

Overton Window: A concept developed by Joseph Overton during the 1990s to describe the range of ideas and policies that are viewed as acceptable by a target audience at any given moment.[72]

phishing: using fraudulent email or text messages, often with embedded hyperlinks, intended to trick the recipient into doing something that proves harmful, like clicking on a link and revealing sensitive data and information (like passwords, usernames and credit card numbers), or downloading some sort of malware onto their system *(see also: "spear phishing" and "Trojan Horse").*[73]

Pizzagate: an infamous (and repeatedly debunked) conspiracy theory that went viral during the 2016 U.S. presidential election, claiming that Hilary Clinton and other Democrats were involved in a child sex ring headquartered at a pizza parlor in Washington, D.C.

platform manipulation: a term used by Twitter to describe the act of using a social media platform "in a manner intended to amplify or suppress information or engage in behavior that manipulates or disrupts people's experience."[74]

podcast: a recording (often in MP3 format) of one or more speakers talking about a topic of interest to the listener.

political warfare: using political, informational, military, economic, financial and other measures to influence, coerce or undermine a country's government.[75]

post: information added to a Facebook, Instagram, Twitter or other social media platform account by the owner of that account; also used a verb (e.g., she wanted "to post" something

online).

postmodernism: beliefs associated with a movement in art, architecture, music, literature and other avenues that discount the idea of objective truth and a politically neutral frame of evaluation.[76]

post-truth: a term, sometimes associated with postmodernism, describing how objective facts are less influential in shaping public opinion than appeals to emotion and personal belief.[77] According to McIntyre, post-truth puts forth a "contention that feelings are more accurate than facts, for the purpose of the political subordination of reality."[78]

projection: a term from the field of psychology describing attempts to displace responsibility of one's negative behavior and traits by attributing them to someone else.

propaganda: true or false information spread to persuade an audience, but often has a political connotation and is often connected to information produced by governments.[79]

provocation: an act meant to generate some kind of emotional response from the target.

psychological operations: a term generally used in military strategies to describe efforts to influence the emotions and behaviors of target audiences (e.g., military, government and civilian).

push polling: an insidious form of negative campaigning that plants disinformation and doubt with citizens under the pretense of running an opinion poll.[80] An example would be a "birther conspiracy" group asking a survey participant a question like "assuming President Obama was not born in the U.S., where do you think he was born?"

QAnon: an extreme far-right conspiracy theory claiming that Donald Trump is fighting against a powerful "deep state" secret network of government, business and media figures led by Satan-worshipping Democratic pedophiles.[81]

"Question More": the slogan of Russian media outlet RT, used primarily as a cover to spread a variety of unfounded accusations, conspiracies and disinformation.

radicalization: A process of adopting increasingly extreme and radical views about specific political, religious, social or other topics. Terrorism and other forms of political violence are often the result of radicalization.[82]

rationalization trap: a term from the field of psychology describing how a person's efforts to reduce cognitive dissonance (*see above*) may lead them to defensively justify a variety of bad, unintelligent and potentially immoral decisions (see Chapter 7). In some cases, the person will find increasingly bizarre ways to rationalize their behavior, decision, or previously held belief even in the face of overwhelming evidence that they are wrong.

reactance: a term from the field of psychology that describes, in the words of Kathleen Taylor, "a negative emotional state trigger by a perceived threat to personal freedom which can motivate extremely vigorous defensive action."[83] Provoking this emotional state is one of the primary objectives of digital influence mercenaries when targeting individuals within a

digital influence silo.[84]

red pill (or "redpilled"): a reference to the popular sci-fi movies series *The Matrix*, in which reality is only revealed to those who take the risks to uncover it, while everyone else is duped into believing in an illusion.

Reddit: a content aggregation site that consists of user-generated news links. These links are voted up-or-down by the community members, tagged as "redditors." It also contains a wide variety subreddits, discussion and file/image sharing boards dedicated to various topics.[85]

RT (formerly Russia Today): a media outlet funded by the Russian government that disguises disinformation and falsehoods beneath a veneer of ordinary news broadcasts.

retweet: the act of re-posting someone else's message on Twitter so your own followers will see the original message and (presumably) your endorsement of it.

sabotage: similar to subversion, the ability to disrupt the effectiveness of a digital influence effort through a unique level of access to its origins or mechanisms of distribution.

salami tactics (a.k.a. salami-slice strategy): a way of engineering a type of creeping normality (*see above*) that is also similar to gaslighting, in which the objective is to slowly break down the target's established reality and eventually replace it with a different view of reality.

Search Engine Optimization (SEO): making modifications to a website in order to improve its performance in search engine results.[86]

selective exposure: similar to "cherry-picking" (*see above*), selecting only information and data that supports what you want to believe, and ignoring any contradicting information or data (even from the same source). A very common behavior within influence silos, the term describes (as Philip Howard explains) how we manifest our preference for news and information that fits an ideology that we subscribe to, is consistent with things we already know, or helps us avoid the work of rethinking our assumptions.[87]

smokescreen: an influence strategy involving the manufacturing and dissemination of distractions in order to confuse the target and keep them from focusing on the true (often malicious) intentions of the influencer.

SnapChat: a personal messaging platform used for chatting and sharing photos; the unique feature that led to its popularity is that the photos and videos shared will disappear after they have been viewed by the recipient.

sniffing: a term used in network security (and hacking) that describes the process of monitoring and capturing packets of information passing through a particular network connection.

social capital manipulation: in the context of persuasion, this term describes an effort to leverage the shared norms, values and trust within an influence silo as a means to connect a target's sense of identity with objectives pursued by the influencer.

social influence: a term that describes how an individual's behavior can be shaped in accordance with the expectations of others whom they value (particularly within an influence silo). Related terms include peer pressure, conformity, social proof and socialization.

social media: online services which encourage their users to digitize and publicly share previously private personal information. Related technologies like email, electronic mailing lists and instant messaging simply do not encourage users quite so much to make our own personal details public.[88]

social media kill chain: a phrase coined by Clint Watts that describes a multi-stage process to identify and disrupt the efforts of advanced persistent manipulators (*see above*).[89]

social network analysis: a set of tools used to map patterns of behaviors and relationships among networks of individuals who are connected in some way. These tools are often used to study terrorists, insurgents, criminals and other clandestine networks, and can be useful for identifying who directs (or influences) the actions of others in a network, revealing operational or inspirational leaders and followers.

social proof: a term coined by psychologist Robert Cialdini that is used to describe how the views and behavior of those around us influence our own views and behavior. Typically, social proof leads people to copy the actions of others because they believe those actions will be positively rewarded within their social context.[90]

social structure: the enduring patterns of behavior and relationships within social systems (e.g. roles) or the social institutions and norms that have become embedded in social systems in such a way that they shape behavior.[91]

sock puppet: a social media account that uses a false identity designed specifically to deceive others, particularly for the purposes of infiltrating an online community and then manipulating it from the inside.[92] Sock puppets are often used on social platforms to inflate another account's follower numbers and to spread or amplify false information to a mass audience,[93] or make controversial or offensive comments while taking sides on a particular issue. Sock puppets have also been known to post commentary on content that they might have produced themselves under a different identity.[94]

Sovereign Citizens: a movement of anti-government extremists who believe that even though they physically reside within the United States, they are separate or "sovereign" and therefore do not have to answer to any government authority, including courts, taxing entities, motor vehicle departments of law enforcement.[95]

spear-phishing: a type of phishing or spoofing attack in which the perpetrator is disguised as someone known and trusted by the specific target, and who tricks that target into clicking on a link embedded within an email, text message or instant message. Unlike basic phishing messages—which are frequently send to a broad number of recipients—spear phishing is highly individualized, usually drawing on information gained beforehand about the target.

spamming: a term originally associated with e-mail—where an unsolicited message is sent to lots of recipients for the purpose of commercial advertising, phishing (*see above*), or just to harass them—it now also describes new forms such as posting unrelated comments to blog posts, disseminating unwanted content (like hate speech, profanity and porn) on a social networking site, posting fake reviews on product websites, and much more.

spoofing: pretending to be something else in an attempt to gain the target's confidence (using e-mails, text messages, websites, et al.), in order to gain access to their computer system and then steal data, spread malware, or conduct other kinds of malicious activity.

stop-and-think: a strategy, recommended by psychologist Kathleen Taylor, for how we can resist influence attempts by pausing, thinking critically and skeptically when we analyze the message, and checking the logic of its arguments, its use of emotive language, or the accuracy of its factual statements. The strategy also involves questioning the authority and motive of the message's source.[96]

Stormfront: the most prominent website/discussion forum promoting white supremacy and other right-wing extremist ideologies.

subtweeting: sometimes referred to as insulting someone via stealth or talking about someone behind their back, this generally refers to posting something on Twitter that is about and/or subliminally directed at someone, but without using the symbol @ before their name (which would notify them of the post), or without mentioning them by name at all.

swarming/swarmcast: a term used by Ali Fisher to describe the ways in which terrorist networks (like the Islamic State) disseminate content online through an interconnected network that is constantly reconfiguring, akin to the way a swarm of bees or flock of birds constantly reorganizes in flight.[97]

Telegram: an online message app with encryption, through which users can share photos, videos, documents and more.

TikTok: a popular video and social media platform, based in China but with hundreds of millions of users worldwide.

Tinder: one of the most popular dating apps, on which an increasing number of fake accounts are used to influence users by exploiting their desires to be liked.

totalism: the tendency to think in black and white and to dislike and denigrate those who prefer shades of gray. While extreme totalist thinking is a characteristic vice of totalitarian regimes, it would be hard to find a human being who has not succumbed at some time to the lure of prejudice and thinking in stereotypes. Highly totalist thinkers extol values such as simplicity, purity, loyalty and authority over more liberal ideas like freedom and diversity.[98]

Trojan Horse: in the context of cyber security, this term refers to a kind of code or software (malware) that is often disguised to appear legitimate. Once the user has activated the malware, the hacker can gain access to their system and perpetrate a variety of attacks.

troll: in relation to digital influence warfare, this term refers to a person or persons who post inflammatory and often false social media content or remarks in order to provoke a desired reaction, engage in harassment, or generate negative discourse. This is frequently done as a response to someone else's content that the troll disagrees with. Trolls often conceal their real identity or post anonymously and thus assume little risk for making inflammatory remarks compared to making them openly or in person.[99]

troll farm: a group of individuals engaging in trolling or bot-like promotion of narratives in a

coordinated fashion.[100]

trolling: the act of deliberately posting offensive or inflammatory content to an online community with the intent of provoking readers or disrupting conversation.[101] Trolling is often motivated by a political conviction or simply for the "thrill" of provoking a response from the target.

Tweet: a message posted to the Twitter social media platform. A user can indicate that they like the message, and can share it with others ("retweet") with or without additional commentary.

Twitter bomb: similar to hashtag hijacking or flooding, the term describes an incident in which attackers post a flood of tweets with the same hashtags and other similar content from multiple accounts, often with meaningless, satirical or provocative messages intended to confuse and derail a discussion started by someone else.

Tumblr: a social networking and microblogging platform on which users follow each other and upload short posts (typically including images), many of which can be defined as memes.[102]

uncertainty-identity theory: from the field of psychology, this theory explains how an individual will adopt a group identity in order to diminish the discomfort and anxiety produced by uncertainty. This in turn influences the behavior of that individual, particularly regarding members of an in-group or out-group, and can lead to extremism and violence.[103]

viral: in the context of digital influence efforts, this term describes a diffusion process in which a certain message (catchphrase, video, image, etc.) spreads repeatedly from one person to another via digital and social media platforms, eventually reaching a broad audience. When something has been shared and viewed by many thousands (or millions) of users, it is often considered to have "gone viral".[104]

virus: when used in terms of network security, this term describes a type of computer program or software created by a hacker that once activated will replicate itself by modifying other computer programs and inserting its own code, leading the computer to then do things that benefit the hacker.

VKontakte: also called VK, this Russian social media platform is very similar to Facebook, and has several hundred million users.

watermark (digital): this term refers to a data pattern embedded into a digital file that—while not easily detected by a casual Internet user—can identify a piece of content's origin or authenticity. While digital watermarks are often inserted to deter the illegal distribution of commercial content and intellectual property, they can also be used to track nefarious content.[105]

weaponized narrative: a term used by some researchers to describe "an attack that seeks to undermine an opponent's civilization, identity, and will. By generating confusion,

complexity, and political and social schisms, it confounds response on the part of the defender. A fast-moving information deluge is an ideal environment for this kind of adversarial attack. A firehose of narrative attacks gives the targeted populace little time to process and evaluate. It is cognitively disorienting and confusing—especially if the opponents barely realize what's occurring. Opportunities abound for emotional manipulation undermining the opponent's will to resist."[106]

website defacement: a conventional type of cyber attack in which the hacker(s) modify the content displayed on a website, usually replacing it with provocative, derogatory or misleading photos and messages.

WeChat: A Chinese multi-purpose messaging, social media and mobile payment app for smartphones, with over a billion users.

Whataboutism: a verbal or rhetorical tactic (used often by Russian propagandists since the 1970s) in which one person tries to discredit another person's statement by accusing them of hypocrisy or other (often unrelated) offenses. The tactic is frequently used to deflect attention from one's own lack of evidence or credibility *(see also: "deflection/redirection").*

What'sApp: a messaging app for computers and phones that lets users text, chat, and share media, including voice messages and video, with individuals or groups.

zombie: a computer that has been compromised by a hacker who is using it remotely to conduct any number of clandestine (and often illegal) actions online, typically without the computer's owner knowing anything about it (though they may notice the computer is running much more slowly than it used to).[107]

Note to Readers: An online version of this glossary of terms, posted to the website http://www.DIWbook.com, will be periodically updated with additional terms and new information. Please feel free to suggest updates via e-mail, at jjforest@gmail.com.

Notes and Sources of Definitions

[1] Robin Mackay and Armen Avanessian (eds.) *#Accelerate: The Accelerationist Reader* (Cambridge, MA: MIT Press, 2014). See also: Steven Shaviro, *No Speed Limit: Three Essays on Acceleration.* University of Minnesota Press, 2015. Online at: https://doi.org/10.5749/9781452958552; and "What is Accelerationism?" *New Statesman* (August 5, 2016). https://www.newstatesman.com/politics/uk/2016/08/what-accelerationism

[2] U.S. Information Agency (June 1992) Soviet Active Measures in the "Post-Cold War" Era 1988-1991. U.S. House of Representatives Committee on Appropriations. Online at: http://intellit.muskingum.edu/russia_folder/pcw_era/exec_sum.htm

[3] For example, see Clint Watts, "Disinformation: A Primer in Russian Active Measures and Influence Campaigns," U.S. Senate Select Committee on Intelligence hearing on Russian Intelligence Activities (March 17, 2017). Online at: https://www.intelligence.senate.gov/sites/default/files/documents/os-cwatts-033017.pdf; and Clint Watts, "Russia's Active Measures Architecture: Task and Purpose," Alliance for Security Democracy (May 22, 2018). Online at: https://securingdemocracy.gmfus.org/russias-active-measures-architecture-task-and-purpose/

[4] Clint Watts, "Advanced Persistent Manipulators, Part One: The Threat to the Social Media Industry," Alliance for Securing Democracy (February 12, 2019). Online at: https://securingdemocracy.gmfus.org/advanced-persistent-manipulators-part-one-the-threat-to-the-social-media-industry/

[5] Michael Erbschloe, *Social Media Warfare: Equal Weapons for All* (Boca Raton, FL: CRC Press, 2017), p. 279

[6] Stanley Milgram, *Obedience to Authority* (London: Pinter and Martin, 1974); described in Kathleen Taylor, *Branwashing: The Science of Thought Control* (London: Oxford University Press, 2004), p. 112-114.

[7] Claire Wardle, "Information Disorder: The Essential Glossary." Shorenstein Center, Harvard University (July 2018). Online at: https://medium.com/1st-draft/information-disorder-part-1-the-essential-glossary-19953c544fe3 (Also, see Chapter 3 of this book).

[8] https://www.definitions.net/definition/ambit+claim

[9] Ibid.

[10] Ibid.

[11] Philip N. Howard, *Lie Machines: How to Save Democracy from Troll Armies, Deceitful Robots, Junk News Operations and Political Operatives* (New Haven, CT: Yale University Press, 2020), p. 171

[12] Robert Walker, "Combating Weapons of Influence on Social Media," (Final Thesis) Naval Postgraduate School (June, 2019). Online at: https://www.chds.us/ed/items/20165

[13] Alice Marwick and Rebecca Lewis, Media Manipulation and Disinformation Online, Data & Society (May, 2017), p. 1. Online at: https://datasociety.net/output/media-manipulation-and-disinfo-online/

[14] Kathleen Taylor, *Brainwashing: The Science of Though Control* (London: Oxford University Press, 2004), p. 295 (citing Fincham and Hewstone, "Attribution Theory and Research: From basic to applied," in *Introduction to Social Psychology,* edited by M. Hewstone and W. Stroebe, 3rd Edition (Oxford: Blackwell) pp. 197-238.

[15] https://firstsiteguide.com/what-is-blog/

[16] Claire Wardle, "Information Disorder: The Essential Glossary."

[17] Ibid.

[18] Philip N. Howard, *Lie Machines,* p. 172 –

[19] Claire Wardle, "Information Disorder: The Essential Glossary."

[20] For a detailed analysis, see: Kathleen Taylor, *Brainwashing: The Science of Thought Control* (London: Oxford University Press, 2004)

[21] Stanford Persuasive Technology Lab, at: https://captology.stanford.edu/

[22] Limor Shifman, *Memes in Digital Culture.* (Cambridge, MA: MIT Press, 2014), p. 178

[23] Boris Mustapic, "5 Ways to Detect Click Fraud," Cheq (April 20, 2020). Online at: https://www.cheq.ai/click-fraud; and Nishant Kadian, "Click Fraud Prevention," FaaS (June 7, 2019). Online at: https://mfaas.com/resources/click-fraud-prevention/

[24] Yochai Benkler, et al. *Network Propaganda* (London: Oxford University Press, p. 9

[25] Robert Walker, "Combating Weapons of Influence on Social Media."

[26] Kathleen Taylor, *Branwashing*, p. 173

[27] Lee McIntyre, *Post-Truth.* (Cambridge, MA: MIT Press, 2018), p. 173

[28] Renee Diresta, et al. *Telling China's Story: The Chinese Communist Party's Campaign to Shape Global Narratives.* Stanford Internet Observatory and Hoover Institution, Stanford University (July 20, 2020), p. 13. Online at: https://cyber.fsi.stanford.edu/io/news/new-whitepaper-telling-chinas-story

[29] Philip N. Howard and Samuel Woolley, "Political Communication, Computational Propaganda, and Autonomous Agents." *International Journal of Communication* 10 (2016), p. 20; Samantha Bradshaw and Philip N. Howard, *Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation.* Computational Propaganda Research Project, Oxford Internet Institute (2018), p. 4.

[30] Philip N. Howard, *Lie Machines,* p. 172

[31] Ibid., p. 172

[32] Michael Erbschloe, *Social Media Warfare: Equal Weapons for All* (Boca Raton, FL: CRC Press, 2017), p. 282

[33] Philip N. Howard, *Lie Machines,* p. 172

[34] Michael Erbschloe, *Social Media Warfare*, p. 282

[35] Sean F. Everton, *Disrupting Dark Networks* (Cambridge University Press, 2012), p. 397

[36] Claire Wardle, "Information Disorder: The Essential Glossary."

[37] Ibid.

[38] Caroline Jack (2017) "Lexicon of Lies: Terms for Problematic Information," *Data & Society,* https://datasociety.net/pubs/oh/DataAndSociety_LexiconofLies.pdf, p 9.

[39] J.-B. Jeangène Vilmer, A. Escorcia, M. Guillaume, J. Herrera, "Information Manipulation: A Challenge for Our Democracies," report by the Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces (Paris, August 2018), p. 20.

[40] Robert G. Cialdini, et al. "Reciprocal Concessions Procedure for Inducing Compliance: The door-in-the-face technique. *Journal of Personality and Social Psychology*, 31(2) (1975), p. 206.

[41] Claire Wardle, "Information Disorder: The Essential Glossary."

[42] David Dunning and Justin Kruger, "Unskilled and Unaware of it: How difficulties in recognizing one's own incompetence lead to inflated self-assessments." *Journal of Personality and Social Psychology* 77(6) (1999), p. 1121-34. DOI:10.1037/0022-3514.77.6.1121

[43] J.M. Berger, *Extremism* (MIT Press, 2018) p. 75-76.

[44] "Facebook Reports Second Quarter 2020 Results." Facebook (Press Release (July 30, 2020). Online at: https://investor.fb.com/investor-news/default.aspx

[45] Greg Sargent, *An Uncivil War* (New York: Harper Collins, 2018), p. 125.

[46] Richard Fletcher, "The Truth Behind Filter Bubbles: Bursting Some Myths," Reuters Institute, University of Oxford (January 22, 2020). Online at: https://reutersinstitute.politics.ox.ac.uk/risj-review/truth-behind-filter-bubbles-bursting-some-myths.

[47] "Flaming" *TechTerms*. Online at: https://techterms.com/definition/flaming

[48] Elizabeth Scott, "How to Deal with FOMO in Your Life," *Very Well Mind* (February 19, 2020). Online at: https://www.verywellmind.com/how-to-cope-with-fomo-4174664

[49] Neil Patel, "Foot-in-the-Door Technique," *Forbes* (October 13, 2014). Online at: https://www.forbes.com/sites/neilpatel/2014/10/13/foot-in-the-door-technique-how-to-get-people-to-take-seamlessly-take-action/#7095dbc67d9e

[50] Caroline Jack (2017) "Lexicon of Lies," p. 9; citing Gibson, C. (2017, January 27). "What we talk about when we talk about Donald Trump and 'gaslighting.'" *The Washington Post*. https://www.washingtonpost.com/lifestyle/style/what-we-talk-about-when-we-talk-about-donald-trump-and-gaslighting/2017/01/27/b02e6de4-e330-11e6-ba11-63c4b4fb5a63_story.html; and Calef, V., and Weinshel, E. M. (1981). "Some Clinical Consequences of Introjection: Gaslighting." *The Psychoanalytic Quarterly* 50, 44-66.

[51] Robert Walker, "Combating Strategic Weapons of Influence on Social Media."

[52] "Groupthink" definition, *Psychology Today.* Online at: https://www.psychologytoday.com/us/basics/groupthink

[53] "Hamilton-68 Dashboard," Alliance for Securing Democracy at the German Marshall Fund of the United States. Online at: https://securingdemocracy.gmfus.org/hamilton-dashboard/

[54] *Oxford English Dictionary,* 2020

[55] Philip N. Howard, *Lie Machines,* p. 173

[56] J.M. Berger, *Extremism*, p. 60-64.

[57] Caroline Jack (2017) "Lexicon of Lies," p. 6, citing Boyd, C. D. (2007). "Army IO is PSYOP: Influencing more with less." *Military Review* 87(3), 67-75.
[58] Peter W. Singer, "Winning the War of Words" Information Warfare in Afghanistan," Brookings Institution (October 23, 2001). Online at: https://www.brookings.edu/research/winning-the-war-of-words-information-warfare-in-afghanistan/
[59] Josh Compton, et al. "Persuading Others to Avoid Persuasion: Inoculation Theory and Resistant Health Attitudes." *Frontiers in Psychology* vol. 7, no. 122 (February 9, 2016). doi:10.3389/fpsyg.2016.00122. See also, Kurt Braddock, *Weaponized Words* (Cambridge University Press, 2020), particularly Chapter 4: "Vaccinating against the enemy: Attitudinal inoculation, radicalization, and counter-radicalization."
[60] Clint Watts, "Advanced Persistent Manipulators, Part Two: Intelligence-led Social Media Defense," Alliance for Securing Democracy (April 24, 2019). Online at: https://securingdemocracy.gmfus.org/advanced-persistent-manipulators-part-two-intelligence-led-social-media-defense/
[61] Michael Wooldridge "Intelligent Agents: The Key Concepts." In: Mařík V., Štěpánková O., Krautwurmová H., Luck M. (eds) *Multi-Agent Systems and Applications II. ACAI 2001. Lecture Notes in Computer Science,* vol 2322 (2002). Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-45982-0_1
[62] Philip N. Howard, *Lie Machines,* p. 173
[63] Ibid.
[64] Joan E. Solsman, "Deepfakes' Threat to 2020 US Election Isn't What You'd Think," *CNET* (May 5, 2020). Online at: https://www.cnet.com/features/deepfakes-threat-to-the-2020-us-election-isnt-what-youd-think/
[65] Claire Wardle, "Information Disorder: The Essential Glossary."
[66] Cindy Takara, "The different types of malware (trojan, zombie, bots, spyware), Medium (June 25, 2018). Online at: https://medium.com/@cyntakara/the-different-types-of-malware-trojan-zombie-bots-spyware-44ab5adaae71
[67] Claire Wardle, "Information Disorder: The Essential Glossary"; Claire Wardle and Husseign Derakshan, *Information Disorder: Toward an interdisciplinary framework for research and policy making,* Council of Europe (September 27, 2017). Online at: https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c; and Lion Gu, Vladimir Kropotov, and Fyodor Yarochkin, "The Fake News Machine: How Propagandists Abuse the Internet and Manipulate the Public" Oxford University, TrendsLab Research Paper (2017). Online at: https://documents.trendmicro.com/assets/white_papers/wp-fake-news-machine-howpropagandists-abuse-the-internet.pdf
[68] Limor Shifman, *Memes in Digital Culture,* p. 177 (paraphrased)
[69] Philip N. Howard, *Lie Machines*, p. 173-174
[70] Ibid., p. 174
[71] J.M. Berger, *Extremism* (MIT Press, 2018), p. 84; citing Pedro Domingos, "The Role of Occam's Razor in Knowledge Discovery," *Data Mining and Knowledge Discovery* 3, No. 4 (1999), p. 409-425.
[72] "The Overton Window." Mackinac Center. Online at: https://www.mackinac.org/OvertonWindow (See Chapter 5)
[73] Cindy Takara, "The different types of malware (trojan, zombie, bots, spyware), Medium (June 25, 2018). Online at: https://medium.com/@cyntakara/the-different-types-of-malware-trojan-zombie-bots-spyware-44ab5adaae71
[74] Twitter, "Platform Manipulation and Spam Policy" (September 2019). Online at: https://help.twitter.com/en/rules-and-policies/platform-manipulation
[75] "Modern Political Warfare," International Institute for Strategic Studies (December 5, 2018). Online at: https://www.iiss.org/events/2018/12/modern-political-warfare
[76] Lee McIntyre, *Post-Truth,* p. 174.
[77] Oxford Dictionary, 2016
[78] Lee McIntyre *Post-Truth,* p. 173.
[79] Claire Wardle, "Information Disorder: The Essential Glossary"; citing Caroline Jack (2017) "Lexicon of Lies: Terms for Problematic Information," *Data & Society,* https://datasociety.net/pubs/oh/DataAndSociety_LexiconofLies.pdf
[80] Philip N. Howard, *Lie Machines,* p. 174
[81] "Facebook removes QAnon conspiracy group with 200,000 members," *BBC* (August 7, 2020). Online at: https://www.bbc.com/news/technology-53692545
[82] For a detailed discussion of radicalization, see J.M. Berger, *Extremism* (MIT Press, 2018).

[83] Kathleen Taylor, *Brainwashing*, p. 462
[84] According to Kathleen Taylor, once reactance is triggered, a target is primed for opposition and much harder to control. The influencer may therefore attempt to make the victims feel that they are in charge, for example by explicitly requesting their consent, adding phrase like "it's your decision", "you choose" and "it's up to you." In the modern era, think of presidential candidate Trump's fear mongering followed by the appeal, "will you join me in making America great again"? For more on this, see: Kathleen Taylor, *Brainwashing*, p. 319.
[85] Limor Shifman, *Memes in Digital Culture*, p. 178
[86] Search Engine Optimization (SEO) Starter Guide," Google. Online at: https://support.google.com/webmasters/answer/7451184?hl=en
[87] Philip N. Howard, *Lie Machines,* p. 174
[88] Ciarán Mc Mahon, *Psychology of Social Media* (London: Routledge, 2019), p. 5. A list of major social media platforms can be found online at: https://en.wikipedia.org/wiki/List_of_social_networking_websites
[89] Clint Watts, "Advanced Persistent Manipulators, Part Three: Social Media Kill Chain," Alliance for Security Democracy (July 22, 2019). Online at: https://securingdemocracy.gmfus.org/advanced-persistent-manipulators-part-three-social-media-kill-chain/
[90] Robert B. Cialdini, *Influence: The Psychology of Persuasion* (New York: Harper, 1984), p. 114-166.
[91] Sean F. Everton, *Disrupting Dark Networks* (Cambridge University Press, 2012), p. 402
[92] Peter Pomerantsev, *This is Not Propaganda* (New York: Public Affairs, 2018), p. 54.
[93] Claire Wardle, "Information Disorder: The Essential Glossary."
[94] Robert Walker, "Combating Weapons of Influence on Social Media."
[95] Michael Erbschloe, *Social Media Warfare: Equal Weapons for All* (Boca Raton, FL: CRC Press, 2017), p. 286; and J.M Berger, *Without Prejudice: What Sovereign Citizens Believe,* GW Program on Extremism (June 2016). Online at: https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/Occasional%20Paper_Berger.pdf
[96] Kathleen Taylor, *Brainwashing,* p. 376
[97] Ali Fisher, "Swarmcast: How Jihadist Networks Maintain a Persistent Online Presence," *Perspectives on Terrorism,* vol. 9, no. 3 (June, 2015), p. 3-20.
[98] Kathleen Taylor, *Brainwashing*, p. 462
[99] Robert Walker, "Combating Weapons of Influence on Social Media"; also, see Philip N. Howard, *Lie Machines,* p. 174.
[100] Claire Wardle, "Information Disorder: The Essential Glossary."
[101] Ibid.
[102] Limor Shifman, *Memes in Digital Culture,* p. 178
[103] Michael A. Hogg, "Self-Uncertainty, Social Identity and the Solace of Extremism" in Michael Hogg and Danielle Blaylock (eds.) *Extremism and the Psychology of Uncertainty* (Malden, MA: Wiley, 2012), p. 19-30; and J.M. Berger, *Extremism,* p. 136-183.
[104] Limor Shifman, *Memes in Digital Culture,* p. 177
[105] Robert Walker, "Combating Weapons of Influence on Social Media."
[106] Threatcasting, "What is Weaponized Narrative?" (Arizona State University: Weaponized Narrative Initiative, 2019), p. 16. Online at: https://weaponizednarrative.asu.edu/.
[107] Cindy Takara, "The different types of malware (trojan, zombie, bots, spyware), *Medium* (June 25, 2018). Online at: https://medium.com/@cyntakara/the-different-types-of-malware-trojan-zombie-bots-spyware-44ab5adaae71