Words as Weapons: The 21st Century Information War

Margaret S. Marangione

"The Supreme Art of War is to subdue the enemy without fighting." Sun Tzu

"*If [the West] did not have press freedom, we would have to invent it for them.*" KGB General Ivan Agayants

"*Who are the bearers of truth? We are in an example of the post-enlightenment period where opinion and emotion is before logic and reason; I am worried for the whole world. I worry about truths future.*" General Michael Hayden Former Director, NSA

Abstract

Historians and scholars are already defining the twenty-first century as the century of post-truth and it is shaping up into an era where objective facts have lost merit and, instead, are replaced by appeals to personal beliefs and emotions. George Orwell forecasted this 72 years ago in his dystopian novel 1984. While propaganda has been utilized for centuries, cognitive hacking or the weaponization of information has subtle nuances that make it disturbingly different. Cognitive hacking includes the mass delivery of conspiracy theories and intentional lies with the desired effect that the receivers of the information take action, often through likes and shares on social media, sometimes with violence. Advances in computing and global hyper-connectivity through social media have empowered algorithms capable of profiling a user's preferences and placing the user in information silos ultimately changing the thinking of the individual it targets. Global powers including Russia and China have worked to hone their capabilities to exploit individual and group cognitive processes to achiever their desired ends. The psychological domain is in need of cognitive security.

Keywords: Information Warfare; Disinformation; Social Media; Fake News; Cognitive Bias

 doi: 10.18278/gsis.6.1.7

Palabras como armas: la guerra de la información del siglo XXI

Resumen

Los historiadores y académicos ya están definiendo el siglo XXI como el siglo de la posverdad y se perfila hacia una era en la que los hechos objetivos han perdido mérito y, en cambio, son reemplazados por apelaciones a creencias y emociones personales. George Orwell pronosticó esto hace 72 años en su novela distópica 1984. Si bien la propaganda se ha utilizado durante siglos, la piratería cognitiva o el uso de información como arma tiene matices sutiles que la hacen inquietantemente diferente. La piratería cognitiva incluye la entrega masiva de teorías de conspiración y mentiras intencionales con el efecto deseado de que los receptores de la información actúen, a menudo a través de me gusta y compartidos en las redes sociales, a veces con violencia. Los avances en la informática y la hiperconectividad global a través de las redes sociales han potenciado los algoritmos capaces de perfilar las preferencias de un usuario y colocar al usuario en silos de información, en última instancia, cambiando la forma de pensar de la persona a la que se dirige. Las potencias globales, incluidas Rusia y China, han trabajado para perfeccionar sus capacidades para explotar los procesos cognitivos individuales y grupales para lograr los fines deseados. El dominio psicológico necesita seguridad cognitiva.

Palabras clave: Guerra de información; Desinformación; Redes sociales; Noticias falsas; Sesgo cognitivo

信息武器：21世纪的信息战

摘要

历史学家和学者已将21世纪定义为后真相世纪，并且该世纪正形成一个时代，在这个时代里客观事实已失去价值，取而代之的是吸引个人信仰和情感的信息。72年前，作家George Orwell在其反乌托邦小说《一九八四》中便预测了这一现象。虽然几百年来政治宣传不断被使用，但认知侵入（cognitive hacking）或信息武器化的微妙差异使其有别于政治宣传，这是令人不安的。认知侵入包括大量涌入的阴谋论和编造的谎言，意图让信息接收者采取行动，通常是在社媒上点赞或分享，有时是实施暴力。计算技术的进步和通过社媒实

现的全球超-连通性（hyper-connectivity）让算法能够对用户的偏好加以定性，并将用户置入信息孤岛，最终改变用户的思维。包括俄罗斯和中国在内的世界强国已通过磨练各自的能力来充分利用个体和团体的认知过程，以期实现各自期望的目的。心理领域需要认知安全。

关键词：信息战，错误信息，社交媒体，假新闻，认知偏见

Overview

Historians and scholars are already defining the twenty-first century as the century of post-truth and it is shaping up into an era where objective facts have lost merit and, instead, are replaced by appeals to personal beliefs and emotions. George Orwell predicted this 72 years ago in his dystopian novel *1984*. He foretold the destruction of the foundations of democracy due to lies. His term for the outrageous flagellation of the truth was called *doublethink*. Doublethink is the more sinister twin of propaganda and while propaganda has been utilized for centuries, cognitive hacking or the weaponization of information has subtle nuances that make it disturbingly different. Cognitive hacking includes the mass delivery of conspiracy theories and intentional lies with the desired effect that the receivers of the information take action, often through likes and shares on social media, sometimes with violence. Algorithms can profile user preferences, and these preferences quickly put the social media user into information silos ultimately changing the thinking of the individual it targets.

What makes the current climate of fake news, misinformation or cognitive hacking so chilling and dangerous is that the weaponization of information magnifies the disconnect between reality, fact and falsehoods. Additionally, these falsehoods have the ability to undermine medical information, institutions, demoralize democracy and destabilize governments. The internet, social media, fringe commentators, state and non-state actors, and political leaders who further their own agendas, are the agent provocateurs. This is coupled with an increasing gap in critical thinking skills to decipher fact from fiction. Additionally, social media companies' aversion to mitigating their platforms, and policy and lawmakers' lack of definite action against these platforms has also contributed to the problem. These variables are all contributing to this twenty-first-century war.

Throughout the twentieth and early twenty-first century, there were old-fashioned stop gates, like editors, that provided some blockades for false, misleading, and violent information. As the internet and social media grew in reach and influence, Facebook and Twitter have been struggling to keep

pace with a mechanism that has outstripped their original ideas for social media platforms. It is no longer a stage to connect friends from high school, promote a business or let family know of milestones of children's achievements. It has become Victor Frankenstein's monster. Cybersecurity expert and journalist Patrick Tucker reports that these platforms, "have upped their efforts to stem the flow but remain overmatched by users' determination to spread it … half or more of the most shared posts on Facebook have been from high-follower sources and users with a record of posting false or misleading information. [This] presents Facebook with a growing dilemma" (Tucker, 2020). The sheer volume of information has stripped Facebook, Twitter, and all social media corporations' ability to keep pace, and it brings into question whether it is their responsibility to monitor the content.

The advertising algorithms embedded in social media utilize users' profiles and preferences for targeting with the stealth and accuracy of ICBM missiles, and it is not just rogue individuals that have entered this stage. Concerted efforts by state actors like China and Russia have resulted in the super-spreading of fabricated information. This new war is being waged by tech geeks, like Russia's Internet Research Agency, that can launch an organized tactical and strategic alternate reality campaign, and not by nuclear weapons, which are antiquated and expensive. Though China and Russia have different goals in the information wars, they still utilize and disseminate a dizzying amount of falsehoods that alter reality. According to Michael Morell, Former Deputy Director of the CIA, the Chinese are not interested in elections; they try to influence the public on policy issues towards China. Russia's goal is to influence American opinions, especially when it comes to presidential elections. He stated, "We did not have as much interference in Russia in 2021 as we did in 2016 because they did not have to work very hard. The divisiveness in America by 2020 was already very deep. It was a brush fire and they just added fuel by utilizing social media" (Morell, 2021).

As early as 2012, an organization called the Internet Research Agency (IRA), which is a troll farm in St. Petersburg, began functioning as a weapon of mass destruction (Weiner, 2020, 221). By 2014, the IRA had targeted the Pentagon and other U.S. government organizations, as well as the 2016 Presidential election. Russia turned freedom of press and information against Americans and flooded social media with false, misleading and weaponized claims to distort reality, which was documented in the 950-page report, *The U.S. Select Committee on Intelligence on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*.

Recently, The People's Republic of China (PRC) conducted an information warfare campaign against the United States in an attempt to protect its interests and limit its strategic losses caused by COVID-19. The PRC went to great lengths to misrepresent the severity of the virus and suppress information that

would have potentially helped the international community. Once it realized it could no longer suppress this emerging threat, it shifted its weaponized information campaign to projecting misinformation and blaming the U.S. for the virus's rapid spread (Easton, 2020).

Russia, China, and various non-state and rogue actors may have perfectly timed their delivery because, it has been argued, there has been a cognitive decline in critical thinking, which further exacerbates a vulnerable audience's susceptibility to information as a weapon. Researcher and professor Patricia Greenfield analyzed over 50 studies on learning and technology. Her findings indicate that, while visual intelligence has risen in the 21st century, it did not correlate to a rise in critical thinking and reading, which are intrinsically linked. IQs have also flattened (UCLA, 2009). This, coupled with the speed of information delivery, the inability of an information flooded audience to tell the difference between a conspiracy, hoax, manipulation or fact, has led to a society that has become increasingly defenseless to the new information war.

Strategies for combating the weaponization of information are crucial, and the approach will need to be aggressive and must be embedded with policies, laws, and tactical outcomes. While improving critical thinking is certainly a foundational proficiency, it is essential that social media platforms be held accountable for cognitive hacking, especially when these platforms are driving violence. Spokespersons in traditional and non-traditional media, as well as leaders who fail to refute lies and conspiracies, must also be held liable. In addition, consideration for a new intelligence arm of Cognitive Security may be needed, because the weaponization of information is not just an inconvenience—it is a deliberate attack designed to magnify divisive elements, fears, and prejudices in an effort to undermine and destabilize rational thought.

A Brief History of Disinformation

The recorded history of disinformation wars dates back to ancient Rome. As early as 32 B.C., Roman Emperor Octavian waged a propaganda campaign against Roman General Mark Antony that was designed to smear his reputation. This took the form of "short, sharp slogans written upon coins in the style of archaic Tweets." These slogans painted Antony as a womanizer and a drunk, implying he had become Cleopatra's puppet, having been corrupted by his affair with her (Posetti and Mathews, 2018). In 1493, the Gutenberg printing press, the Internet for the Feudal age, dramatically amplified the dissemination of disinformation, which included stories collected from seafarers seeing monsters in the deep ocean and the Catholic Church's deliberate use to spread pro-Crusade, pro-Church and anti-Islamic messages. Not surprisingly, the church felt the Gutenberg Press was a gift from God (Richelle, 2015). Unlike the critical thinking Dark Age occurring in twenty-first-century audiences, the invention of the Gutenberg Press

fostered and encouraged individuals to read and decipher information for themselves, which ultimately led to the Renaissance and the Enlightenment. Nonetheless, a watershed moment in fake news occurred in 1835 when *The New York Sun* published six articles about the discovery of life on the moon complete with illustrations of humanoid bat-creatures and bearded blue unicorns (see Figure 1). This moment of 19th-century fake news is eerily similar to much of the outlandish information contained in conspiracy theories today.

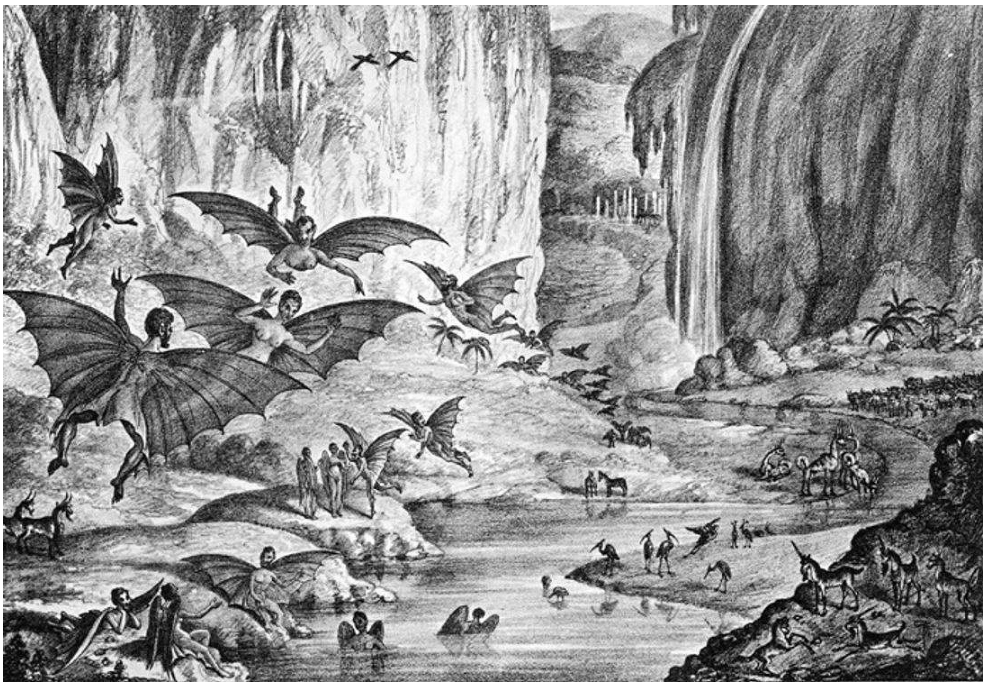

Figure 1: A lithograph that accompanied the *Sun* article.

There are many historic examples of disinformation. Some include, but are not limited, to the doctrine of Manifest Destiny, which led to the Mexican American War, propaganda espoused by the railroads that led to the settling of the West at the expense of the Native Americans, and the "yellow journalism" of the late 19th and early 20th century. Yet it was not until the early part of the twentieth century that modern propaganda and the Nazis ushered in contemporary information warfare. Joseph Goebbels established the Reich Ministry of Public Enlightenment and Propaganda in 1933 to spread Nazi messages of hatred by inciting violence against Jews and using all mediums, including theatre and the press. "Nazi propaganda was … essential to motivating those who implemented the mass murder of the European Jews and of other victims of the Nazi regime. It also served to secure the acquiescence of millions of others—as bystanders—to racially targeted persecution and mass murder" (Prosetti and Mathews, 2018). The Ministry's aim was to ensure

that the Nazi message was successfully communicated through art, music, film, literature, and newspapers similar to the Russian Internet Research Agency's targeting of populations via social media. Both are deliberate and meticulous campaigns and both strive to elicit information loyalty to a set of beliefs. Goebbels propaganda also sought to elicit political loyalty and nationalism and propaganda posters were an effective tool. (Figure 2)

Figure 2. Nazi anti-Semite propaganda poster.

The Nazis demonized and persecuted Jews so effectively that the atrocities of the concentration camps were committed with popular support and Holocaust denialism still continues in the 21st century.

During the same decade of Nazi propaganda, the War of the Worlds radio drama (1938) fooled its audience into believing that earth was being attacked, foreshadowing 21st-century conspiracy theories. "No one involved with War of the Worlds expected to deceive any listeners, because they all found the story too silly and improbable to ever be taken seriously" (Schwatrz, 2015). Yet it was taken seriously. Of the estimated two million people listening to Well's broadcast, one out of 12 thought a Martian invasion was happening in New Jersey (Memmott, 2015).

It was the Soviet Union, at the end of WWII, that began to perfect a propaganda technique that has revolutionized disinformation and was the forerunner of weaponized information. Two years after the surrender of Nazi Germany in 1947, the Soviets created the Committee of Information to run undercover operations to influence public opinion. This was followed by a specialized intelligence unit established in the 1950s to specifically disseminate disinformation. By the 1960s, disinformation measures were an active part of KGB Intelligence operations and the Cold War which resulted in more than 10,000 individual Soviet Bloc operations (Rid, 2017). By the 1970s, disinformation became a larger part of the Soviet strategy, and the unit was upgraded to a full service and was placed under the command of a KGB general (Deeks et al., 2017).

One of the most popular methods Russia used for disseminating disinformation was targeting legitimate news outlets. By anonymously sending forged documents, such as embassy communications or military memoranda, to credible publications, the Soviets attempted to create well-timed fake news stories that the public accepted as true. Once the stories caught on, they were reprinted extensively in Soviet-controlled papers in the hopes that the story would be picked up by more mainstream sources gaining credibility in the process (Deeks et al., 2017).

Russia: Not a One Trick Pony

Disinformation is an Anglicization of the Russian term "dezinformatsiya," which means the deliberate spread of inaccurate information. Traditionally, dezinformatsiya includes tactical information about an adversary coupled with dissemination of propaganda to gain an advantage (Rand, 2020). Furthermore, besides destabilization and informational gaslighting, weaponization of information is also economically more viable than martial military and, according to a Russian General, is conducted in a roughly 4:1 ratio of nonmilitary to military measures (Rand, 2020).

Russia's early harbinger of this fake news storm occurred in the 1980s when the Soviet Union attempted to portray the AIDS epidemic as the work of the Pentagon in the Soviet publication *Literaturnaya Gazeta* in October 1985. The story claimed that scientists from the American Centers for Disease Control and the Army at Fort Detrick in Maryland had created HIV from two known viruses found in Africa and Latin America in an attempt to make a biological weapon (Disinformation, 2013). Over the next several years, Soviet media printed numerous stories reiterating and then embellishing their claims to include that U.S. military personnel were widely infected and vectors for the spread of HIV overseas (Geissler, 2013).

In the twenty-first century, Russia has utilized a concerted and calculated approach to information warfare that may be unprecedented in history.

The current technology, along with the ability to quantify an individual's social media likes and shares, has been effectively exploited as a new weapon system by fully manipulating the impact of the internet and social media's open access. For example, in October 2019, the Senate Intelligence Committee reported that Russia's Internet Research Agency (IRA) reached tens of millions of voters to include at least 126 million U.S. citizens via Facebook, 20 million on Instagram, and 1.4 million via Twitter (Issac, 2017). Coupled with the anonymity of the internet, this allowed Russia to set agendas and take advantage of societal vulnerabilities. While Russia is not the only player in the disinformation wars, Russia's hacks and leaks were well documented by the Senate Intelligence Committee in their report about Russian interference leading up to the 2016 U.S. election. According to Adam Chiara, Professor of Communications, he feels, "Vladimir Putin [and] the U.S.'s complacency and cultural divisions have led to [this] opportunity, one in which Russia took advantage of and struck the U.S. within its borders in a surprising manner" (Chiara, 2017).

Russia's unchecked influence in the 2016 election has reaped benefits to Russia far beyond the polls. Moscow has helped to turn American against American and chipped away at the foundations of democracy to the point that the American public and government officials can countenance unjustified accusations of fraud in the 2020 elections. These accusations of fraud and malicious intent in vote counting occurred despite a lack of evidence and Christopher Krebs, who led the 2020 federal government's election cybersecurity efforts, stating, "There is no evidence that any voting system deleted or lost votes, changed votes, or was in any way compromised" (Cybersecurity & Infrastructure Security Agency, 2020).

Putin learned the art of destabilization from the Stasi, East Germany's secret police. Russia built on Stasi tactics in creative targeting of online conversations and social media. As early as 2012, Putin dispatched the director of military intelligence to begin repurposing cyberweapons used in warzones for psychological operations use in American electioneering. (Bergman, 2017). Putin understands that truth and reality in the twenty-first century are malleable, and the Stasi method of *Zersetzung*, or decomposition, is ungluing the American psyche. Originally intended towards individuals, Stasi decomposition was designed to unhinge the spirit of an individual. In the words of a Stasi manual, the goal of decomposition was to, "[provoke] and [enforce] internal conflicts and contradictions within hostile-negative forces that fragment, paralyze, disorganize and isolate the opponent until the individual finds themselves in a Kafkaesque nightmare" (Tierney, 2020). A Stasi victim called the campaign an "assault on the human soul" (Tierney, 2020). Now, Russia is utilizing the Stasi playbook to weaken America's soul from the inside by identifying ethnic, racial and partisan discord and spreading dissonance about democracy, presidential elections and the election process, often through alt-right groups. Using a diverse toolbox of

propaganda and cyberattacks, Moscow employs hackers and trolls to propagate conspiracy theories and cultivate a skepticism of media, politicians, and government. A striking case in point was how the IRA targeted African Americans with dispatches about boycotting the 2016 election. These messages included, "Don't Vote For Hillary Clinton," and "Hillary Clinton Received $20,000 from the KKK" (Shane, 2018). Other messages drove home harsh and pointed pro-gun rights and anti-immigration messages that garnered American supporters with over a quarter of a million followers, 4.9 million shares, and 5.4 million likes. (Shane, 2018).

Project Lakhta was a Russian intelligence operation that as early as 2014, began spreading false and divisive messages on controversial topics like gun rights, immigration, the Confederate Flag, race relations and American politics and politicians. One employee of Project Lkhata utilized a bogus account to post, "Just a friendly reminder to get involved in the 2018 midterms. They hate you, they hate your morals. They hate your 1A and 2A rights. They hate the police. They hate the military and they hate your president [Trump]" (Tucker, 2020). The troll farms opened fake social media accounts that targeted both conservative and liberal social groups. This was done without any costly movement of troops or equipment and was often funded by Russian oligarchs with ties to the Kremlin. It is estimated that the IRA employs about 400 people with a budget of $400,000, with a typical employee working a 12-hour shift for approximately $700.00 a month. Employees are expected to post news articles 50 times a day and maintain six Facebook accounts with at least three posts a day. The goal is to win over 500 people a month (Waltzman, 2017).

China's Covid Campaign, Cyberattack, and Censorship

Most news sources were in agreement in reporting that conflicting information was coming out of China during the early stages of the COVID-19 infection. A Red Cross study of blood samples from China, taken from the fall of 2019, indicated that at least two percent of those samples had the COVID-19 antibodies in them, a date much earlier than when Beijing admits to discovering the disease (Weichart, 2020). By December 2019, China was aware of the human-to-human transmission of the virus, refused to share information with the WHO, and denied the virus's existence. Furthermore, doctors who initially raised alarm about the illness were arrested (Seaboyer, 2020). China also spread false narratives regarding the virus. According to Anthony Seaboyer, professor of Political Science at the Royal Military College of Canada, "Chinese agents have, for example, spread text messages and social media posts that falsely claimed the US president was locking down the country." This was in an effort to strike fear and sow seeds of chaos and unrest. The rumors became so widespread that the National Security Council had to issue an announcement stating they were fake.

Along with drastically under-representing the severity of the virus and using a tactic from Russia's playbook to sow discord, China has tried to censor any critical citizen commentary of the response to, and threat of, the virus. China banned online gaming and chatting with foreigners in an effort to reduce the spread of information on the virus (Seaboyer, 2020). *The Washington Times* journalist and author Brandon Weichart went further in accusations about China. He states, "Disparate reports came out this year [2020] suggesting that China's embattled regime, when faced with the prospect of being at the epicenter of a major epidemic, allowed for the disease to spread beyond their borders to even the global playing field. Beijing rightly understood that if they contained the disease too early, then the disease would only harm China, and give other countries, notably the United States, a significant advantage" (Weichart, 2020).

By early March 2020, China started spreading fake news about the virus's origins that were picked up at alarming speed by social media and conspiracy theorists. For example, China ironically began alleging the U.S. Army was responsible for the outbreak which was developed as a genetically engineered bioweapon, and that the virus was either intentionally or accidentally planted by U.S. military personnel in the city of Wuhan. To support this claim, an official of the Chinese Foreign Ministry tweeted support for an article that suggested the COVID-19 originated in the United States (Bajhema, 2020.) This was a similar tactic used during the 2002–2003 SARS epidemic when the *China Youth Daily* speculated that SARS was a genetic weapon developed by the National Institutes of Health in the United States.

A disinformation hacking tool, Hamilton 2.0, tracked this COVID disinformation campaign. Hamilton 2.0 is dedicated to tracing official accounts and media outlets linked to or funded by the Russian government, and it also examines account behaviors and trends among Chinese state-backed media by pursuing content that Chinese government officials share on Twitter, Facebook, YouTube, and on state news websites. According to CBS News reporter Olivia Gazis, "What was revealed was a marked evolution in the type of content Chinese accounts shared since the start of the COVID-19 outbreak. While early messaging focused on Beijing's efforts to stem the virus' spread, those messages grew more overtly hostile in February and March [2020], as cases proliferated outside of China. Some of those accounts shared conspiracy theories about the origins of the virus and attacked Western officials for criticizing China's role" (Gazis, 2020).

Sadly, China took an aggressive approach to one of the early heroes of COVID-19, Dr. Li Wenliang, who had warned about the new viral outbreak only to be threatened by the police and accused of peddling rumors. He died of COVID-19 and immediately China directed a disinformation campaign (See Figure 3).

CHINESE MEDIA DIRECTIVES

TO CHINESE NEWS WEBSITES AND SOCIAL MEDIA PLATFORMS:

关于武汉市中心医院李文亮医生去世一事，各网站、新媒体要严格规范稿源，严禁使用自媒体稿件擅自报道，不得弹窗PUSH，不评论、不炒作。互动环节稳妥控制热度，不设话题，逐步撤出热搜，严管有害信息。

"… do not use push notifications, do not post commentary, do not stir up speculation. Safely control the fervor in online discussions, do not create hashtags, gradually remove from trending topics, strictly control harmful information."

TO LOCAL PROPAGANDA WORKERS:

各区、县（市）网信办：根据2月7日省网信办视频例会精神，现就近期工作提示如下：一、准确把握网上舆情严峻复杂的形势日前，李文亮医生去世已迅速成为网络热点。我们要清醒认识到此事所引发的蝴蝶效应、破窗效应、雪球效应，对我们的网上舆论管控工作提出了前所未有的挑战。各地网信部门要高度关注网上舆情，对于严重损害党和政府公信力、矛头直指政治体制的，要坚决管控；在其他事情上对于宣泄性的要引导，注意方式方法。

"We must recognize with clear mind the butterfly effect, broken windows effect and snowball effect triggered by this event, and the unprecedented challenge that it has posed to our online opinion management and control work. All Cyberspace Administration bureaus must pay heightened attention to online opinion, and resolutely control anything that seriously damages party and government credibility and attacks the political system …"

XIAOSHAN DISTRICT, FEB. 12

加强网军统一指挥，组织全区网评员实时待命，及时开展舆论引导。强化网络正能量推送及疫情防控科普工作，组织区级媒体、网评员撰写、转发正能量推文400余则，开展防疫科普宣传100余次，三是加强舆论引导，凝聚网络共识。加强网军统一指挥，组织全区网评员实时待命，及时开展舆论引导。强化网络正能量推送及疫情防控科普工作，组织区级媒体、网评员撰写、转发正能量推文400余则，开展防疫科普宣传100余次，发动网评员跟评、引导4万余人次，有效消除市民恐慌心理，提振防控信心，为打赢疫情防控阻击战营造良好的舆论氛围。

"Mobilized online commenters to comment and guide more than 40,000 times, effectively eliminating city residents' panic, boosting confidence in prevention and control efforts, and creating a good atmosphere of public opinion for winning the battle against the epidemic."

TONGLU COUNTY, FEB. 13

通过重点加强对论坛、微博、微信、移动新闻客户端等网上互动区域的实时监测，确保及时发现、研判、处置重要舆情及各类谣言等有害信息。此外，积极发挥全县网评员和属地瞭望哨信息员作用，重点加强对朋友圈、微信群等封闭、半封闭网络平台的信息监测，为打击网络谣言和正面宣传引导搜集基础素材。针对网上发现的谣言信息，加强与涉事区域和涉事单位的沟通，并会同公安机关严厉打击。截止2月13日，我县共发布辟谣信息15条，转载辟谣信息62条，由公安机关落地查人16人，教育告诫14人，行政拘留2人，传谣造谣当事人自行删除不实信息20余条，组织网评员转发辟谣信息6000余条，及时解疑释惑，回应网民关切。

"As of Feb. 13, our county published 15 rumor-debunking posts, reposted 62 rumor-debunking posts, 16 people were investigated by public security organs, 14 people were educated and admonished, two people were put in administrative detention …"

FUYANG DISTRICT, EARLY FEBRUARY

及时处置防疫工作中涉确诊数量、夸大疫情影响、人员感染隔离等谣言信息。防疫期间，与公安网警共同依法落地查处28人次，官方平台发布和转载辟谣信息56条。避免不实信息蔓延造成公众恐慌，消解防疫工作成效。联动网军、自媒体、舆情监测服务公司力量，捕捉敏感线索，确保舆情发现早。发动全区1500余名网军力量，及时上报微信群等半封闭圈子舆情信息。发挥区自媒体联盟作用，借助其爆料通道收集一手线索。与中青舆情监测服务公司保持密切联系，加大软件巡查频次，精准设置关键字，提升灵敏度。

"Mobilized the force of more than 1,500 cyber-soldiers across the district to promptly report information about public opinion in WeChat groups and other semiprivate chat circles."

Figure 3. False information distributed via China's information channels. C/o *NY Times*.

"China has a politically weaponized system of censorship; it is refined, organized, coordinated and supported by the state's resources," said Xiao Qiang, a research scientist at the School of Information at the University of California, Berkeley, and the founder of *China Digital Times*. "It's not just for deleting something. They also have a powerful apparatus to construct a narrative and aim it at any target with huge scale." Like Russia's troll armies, it has been estimated that hundreds of thousands of people in China work to post comments and share content that reinforces state ideology. Many of them are low-level employees at government departments and party organizations. Universities have recruited students and teachers for the task. Local governments have also held training sessions for them (Zong, 2020).

There has also been evidence that coronavirus-related information is being used to disguise malware-laced messages and apps. According to a team at Check Point, a cybersecurity firm, they exposed a Chinese APT. Check Point stated that the Chinese APT had "weaponized documents to deliver previously unknown malware. This was a targeted cyber-attack by a Chinese APT group on a public sector entity of Mongolia [that] leveraged the coronavirus pandemic." The APT sent two documents in the form of press briefings about COVID-19 that masqueraded as the Mongolian Ministry of Foreign Affairs and contained a remote access malware (Doffman, 2021).

The Information Highway: Algorithms and Avatars

Russia and China have not acted in a void. They are utilizing a black hole of social media that is a breeding ground of fake news and conspiracy theories where everyone is an author. While this has certainly democratized data, it has also resulted in the dynamic that for every fact, there is a counter fact, or alternative fact, that often has no basis in reality. Fighting this digital disinformation is difficult, and social media companies have been slow to respond. As Facebook founder Mark Zuckerberg has stated, he does not want to be "the arbiter of truth" (Levy, 2020). Unfortunately for users, social media companies make money from users' activity and utilize mathematical equations to identify patterns in behaviors quantified by clicks, shares, comments, replies and video views. These algorithms predict what content to show and to whom (Jones, 2020). Only recently, after January 6, 2021, did Facebook respond to pressure, and has convened an internal Supreme Court to rule on Facebook postings and content.

Ironically, in 2004, Google was celebrated when it launched Gmail with its ability to read users' email and then filter information to a user based on preferences. Data mining practices continued to get more sophisticated throughout the twenty-first century in manipulating what a social media user sees through "nudging." Digital nudging is an approach based on insights from behavioral economics that applies

user interface design elements to affect the choices of users in digital environments, which ultimately puts them in a marketing and information silo. These continuously updated and pervasive algorithmically driven systems provide users with highly personalized environments by providing a narrow range of choices, based on a user's preferences, thereby artificially engineering a very narrow view. According to Professor Karen Yeung, this personalized propaganda can gradually shift moral norms and priorities (Ignatou, 2019).

Facebook was questioned about this in 2018 when Mark Zuckerberg went to Capitol Hill to explain to members of Congress how the detailed personal information of up to 87 million Facebook users ended up in the hands of a voter-profiling company called Cambridge Analytica (Kang, 2018). As early as 2014, *The New York Times* reported that contractors and employees of Cambridge Analytica sold psychological profiles of American voters to political campaigns by acquiring the private Facebook data of tens of millions of users—the largest known leak in Facebook history. According to former Cambridge employees, associates and documents, the breach allowed the company to exploit the private social media activity of a huge swath of the American electorate (Confessore, 2018).

Christopher Wylie, who helped found Cambridge Analytica and worked there until late 2014, said of its leaders, "Rules don't matter for them. For them, this is a war, and it's all fair…" (Rosenberg, 2018). Wylie, an eventual whistleblower, was the mastermind in the plan to harvest the Facebook profiles and to use private and personal information to create sophisticated psychological and political profiles. The goal was to then target these users with political ads designed to work on their particular psychological makeup. "We 'broke' Facebook," Wylie says. "I *made* Steve Bannon's psychological warfare tool" (Cadwaladar, 2018).

The New York Times reported that Cambridge's British affiliate, the SCL Group, were in contact with executives from Lukoil, a Kremlin-linked oil giant. Lukoil was interested in the ways data was used to target American voters (Confeseroe, 2018). Wylie supported this claim. The work, he said, would be, "shared with the CEO of the business," a former Soviet oil minister and associate of Putin. "It didn't make any sense to me," says Wylie. "I didn't understand either the email or the pitch presentation we did. Why would a Russian oil company want to target information on American voters?" (Cadwaladar, 2018). Mueller's investigation traces the first stages of the Russian operation to disrupt the 2016 US election back to 2014. Coincidently, that is the same year that Cambridge Analytica presented the Russian oil company with an outline of its datasets, capabilities and methodology (Cadwaldar, 2018).

Facebook's algorithms are sophisticated when it comes to data mining the preferences of its users. According to Peter Eckersley, Chief Computer Scientist at a digital rights nonprofit, "Facebook can learn almost anything

about you by using artificial intelligence to analyze your behavior. That knowledge turns out to be perfect both for advertising and propaganda. If Facebook is being singled out for such practices, it is because it is a market leader and its stockpiling of personal data is at the core of its $40.6 billion annual business" (Rosenberg, 2018). Jonathan Albright, Director of the Digital Forensics Initiative at Columbia University's Tow Center for Digital Journalism, has mapped out how social networks, including Facebook and YouTube, acted as amplification services for websites that would otherwise receive little attention online (Lapowsky, 2018). Facebook uses a number of software tools to do this tracking. When internet users venture to other sites, Facebook can still monitor what they are doing with software like its ubiquitous "Like" and "Share" buttons, and something called Facebook Pixel, an invisible code that's dropped onto the other websites that allows that site and Facebook to track users' activity (Singer, 2018).

This monitoring has occurred as Facebook has grown to be one of the largest sources of news. The Pew Research Center reports that 43% of Americans get their news from Facebook, and each year that percentage increases (Gramlich, 2019). This is, at a minimum, a two-fold problem. First, information feeds provide users a very narrow world-view based on their preferences. The second issue is the sharing and retweeting of false information. A team of researchers at Princeton University tracked the internet use of over 3,000 Americans in the lead-up to the 2016 presidential election. They found Facebook to be the referrer site for untrustworthy news sources over 15% of the time. By contrast, Facebook referred users to authoritative news sites only 6% of the time as seen in Figure 4 (Travis, 2020).

Because of the increasing backlash that social media organizations have been facing for their role in the spread of disinformation and alternate truths, Facebook has made attempts to outwit the buzz feeds. An early effort was the revamp of its News Feed algorithm to prioritize content shared by friends and family over posts from publisher pages. As Facebook noted, "Most of the news stories people see in News Feed are from sources they or their friends follow, and that won't change" (Hutchinson, 2020). News Feed distribution comes down to what individuals share, so Facebook can't intervene and make people share the original report. "When multiple stories are shared by publishers and are available in a person's News Feed, we will boost the more original one which will help it get distribution" (Hutchinson, 2020). Because it is based on what an individual user or group shares, there still is not control of content and at least one study of the platform since that make-over suggests that the change actually rewards engagement, outrage, and division.

Another early effort by Facebook has been to label content and monitor toxic groups on their site. This is similar to the way Twitter finally started labeling some disputed posts from highly influential users such as political

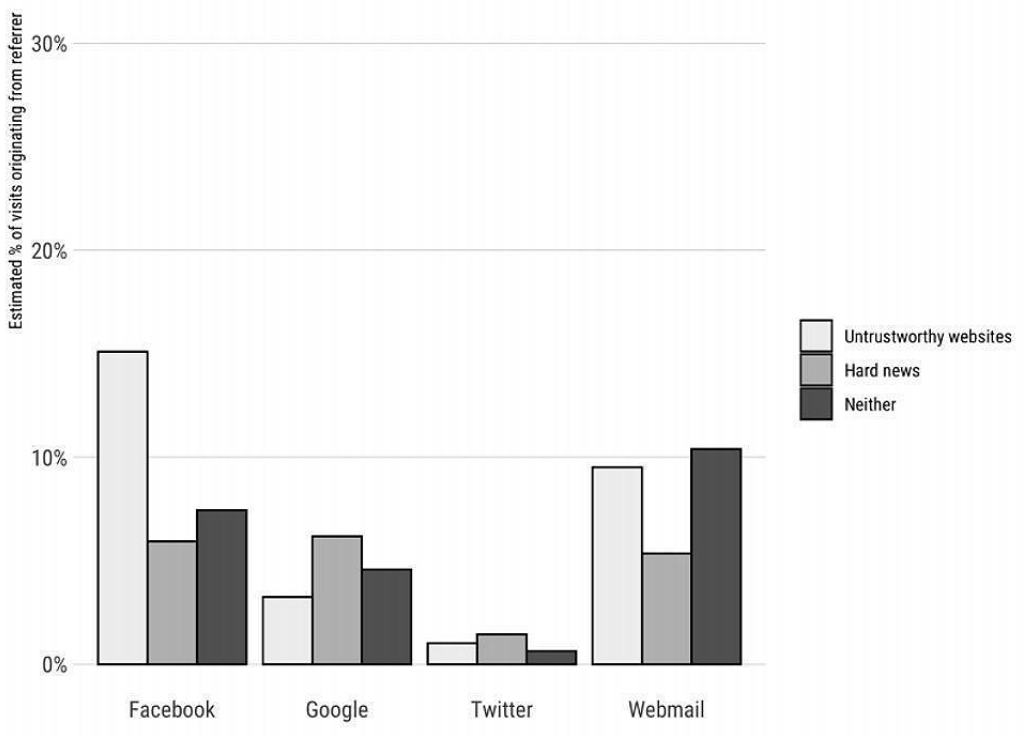

Figure 4. (Copyright Pew Research Center).

leaders. In early 2020, Twitter started to include labels of coronavirus misinformation, misleading tweets about elections and civic processes, and labeling information that is fabricated or manipulated media (Reuters, 2020). Facebook's Monica Bickert stated, "If there's content that is delegitimizing the [2020] election process, for instance, an inaccurate claim that mail-in voting is not secure, we would put a label on there" (Tucker, 2020). As of January 8, 2021, they are also banning users whose tweets incite violence (Twitter, 2021). On January 6, 2021, Facebook also took similar measures. Facebook Vice President Nick Clegg stated, "Every day, Facebook makes decisions about whether content is harmful, and these decisions are made according to Community Standards we have developed over many years. It would be better if these decisions were made according to frameworks agreed by democratically accountable lawmakers. But in the absence of such laws, there are decisions that we cannot duck" (Lyons, 2021).

In the months leading up to the 2020 election, the warning of Russian interference and domestic terrorism was discussed by FBI Director Christopher Wray at a meeting of the House Homeland Security Committee. He cautioned, "We certainly have seen very active—very active —efforts by the Russians to influence our election in 2020" Mr. Wray said, specifically "to both sow divisiveness and discord, and I think the intelligence community has assessed this publicly, to primarily …

denigrate … what the Russians see as a kind of an anti-Russian establishment," (Kanno, 2020). According to Max Bergman, Senior Fellow of U.S./Russia Policy and former State Department senior adviser to the assistant secretary of state for political-military affairs, he feels the connection to Russian interference and alt-right groups is glaring. He states, "A number of academic experts in social media analysis have documented the role of Russian trolls, bots, … in Russia's growing links to the alt-right. Russia's messaging and posturing has also demonstrated an intimacy with alt-right content, as shown by Russia's tweeting of a racist meme used by white supremacists. These links are not surprising given Russia's well-documented backing of far-right political parties and extremist groups" (Bergman, 2017).

Bergman mentions this was also true for the 2016 election. One report found that a popular pro-Trump, anti-Clinton Facebook group called Secure Borders, which at the time of the 2016 election boosted 140,000 subscribers, was actually a Russian troll factory. Alarmingly, one of the posts at the height of the election campaign reached 4 million Facebook users and was liked more than 300,000 times and shared more than 80,000 times and published as many as 50 million posts a month with anti-Clinton posts getting the most attention (Bergman, 2017).

The dilemma for all social media companies is they have their finger in the hole of the bursting dyke. Alex Stamos, Director of the Stanford Internet Observatory Policy Center, defined part of the problem this way. "You have a relatively small number of people with very large followings who have the ability to go and find a narrative somewhere, pick it out of obscurity … one tweet, one photo, one video, and then to harden it into these [false] narratives … that will be the absolute biggest challenge for the platforms going forward. It's relatively easy for social-media platforms to program their newsfeed algorithms to filter out, say, Russian trolls. But, when you talk about people that have millions of folks who have decided that they're going to make the affirmative step of following this person's account, they're going to religiously reload their YouTube page for the newest video. They're going to watch their Facebook Lives. How do you handle those people is a humongous problem" (Tucker, 2020).

Because of the sheer scale in monitoring the information highway, the competing priorities of private profit vs public good, with private profit tied to users' preferences and psychology, perhaps the real defense in fighting digital disinformation should happen in the brain of the social media users. Cybersecurity and internet researcher Richard Fomo stated the best protection of cognitive hacking is the users themselves. "But that defense fails if people don't have critical thinking skills, or worse, don't use them to think critically about what they are seeing and examining claims of fact before accepting them as true" (Fomo, 2020).

Cognitive Biases, Conspiracy Theories and De-evolution of Critical Thinking Skills

A disturbing trend of the information age is the idea that while everyone is allowed their own personal and often emotional opinion, somehow they also feel they are entitled to their own facts as well. This can be a slippery slope because currently, opinion is being masqueraded as fact. Once upon a time, there were logical thinkers who vetted ideas and theories, and these speculations were driven by evidence and science before being promoted as truth. In Jonathan Rauch's essay, "The Constitution of Knowledge," he considers how every society has an epistemic regime, an arena of ideas where what is knowledge is validated by logic. In democratic societies, this often includes clergy members, teachers, journalists, researchers, scientists, etc. and while there is plenty of room for counterarguments, there is an agreed-upon shared system of rules for weighing evidence, building knowledge and awareness of logical fallacies. According to Rauch, this system operates like a funnel. It allows a wide volume of ideas to pour in but only a narrow group of ideas survives collective scrutiny. "We let alt-truth talk," Rauch said, "but we don't let it write textbooks, receive tenure, bypass peer review, set the research agenda, dominate the front pages, give expert testimony or dictate the flow of public dollars" (Rauch, 2018). In the information age, we are in an epistemic assault. "These are truly uncharted waters for the country," wrote former NSA Director Michael Hayden. "We have, in the past, argued over the values to be applied to objective reality, or occasionally over what constituted objective reality, but never the existence or relevance of objective reality itself" (Rauch, 2018).

When 2 + 2 equals 5, authority and power cannot be challenged, and humans might find themselves in a post-societal nightmare. Many argue that this is the forerunner to the decline of democracy. Facts are a democratizing tool in and of themselves as they are evidence that everyone can agree on, share and relate to. If all information is true then people will no longer be able to speak truth to power and all becomes spectacle. How to train brains in the fight against fake news is daunting. Many feel that social media and the internet have increased individuals' vulnerability to cognitive hacking, and this information environment has also been the catalyst in declining skills in critical thinking.

Not surprisingly, 75 percent of employers claim the students they hire after 12, 16 or more years of formal education lack the ability to think critically and solve problems (Haber, 2020). The reality for most of these Gen Z workers has been digital media, online transparency and the internet (the iPhone was launched in 2007, Facebook was founded in 2004), which encourages the skimming and scanning of info bites. *The Wall Street Journal* analyzed results from the College Learning Assessment Plus, a critical-thinking test given annually to freshmen and seniors from 200

U.S. colleges. The test tasks students to use data, articles, blog posts and emails to answer questions and demonstrate skills that are important "not only for success in high school and college [but also] for success in the workplace and other aspects of life outside the classroom." The *Journal* found that at about half of schools, large groups of seniors scored at basic or below-basic levels. They can generally read documents and communicate to readers but can't make a cohesive argument or interpret evidence (Belkin, 2017).

Professor Perry Neel, with over 30 years of college teaching, also attributes the lack of intellectual efficacy to a solipsist attitude.

> "Often, a student feels that the only concerns he/she has are their own concerns. The result of this is a lack of curiosity about others and the world. The most telling example of this has occurred several times in my Applied Ethics Class. Part of the course involves the selection of news articles that present examples of ethical issues in society. I have had students incapable of reading news sources to find ethical issues. The excuse offered is 'I don't like reading about other people's problems.' Or, 'It makes me feel bad to know about all the trouble in world.' I would describe these students' reaction as an intellectual paralysis. In fact, the result has been that these students dropped the class rather than challenging their ideas. A big part of this change I attribute to technology. Whereas, the promise of the worldwide web was access to an almost unlimited amount of information, it has instead helped create these self-contained bubbles for individuals or particular groups. Rather than curiosity about what they don't know, too many students only use technology to suit their own personal needs and desires. I think one of the most important critical thinking skills is self-criticism. When technology conforms to the individual's whims, there is little in the way of self-criticism." (Neel 2020).

A study at California State University in Los Angeles echoed Neel's observations. Thirty-five percent of seniors had below-basic critical thinking skills and 29 percent had basic skills. At the University of Kentucky, six percent of seniors were below-basic, and 14 percent were basic, according to the *Journal*'s statistics (Belkin, 2017). A Stanford University study tested over 7,800 students in a study of reasoning concluding a "… stunning and dismaying consistency of critical thinking skills. Overall, young people's ability to reason about information can be summed up in one word: bleak. Students were unable to tell real news from lies" (Levittan, 2017).

Critical thinking requires the ability to address counterarguments, interrogate, examine, and follow logical structured thinking, and necessitates some degree of innate skepticism. This

is difficult if all the messages an individual is receiving is supporting their worldview, which then becomes an echo chamber. Also, without self-criticism and the ability to distinguish logical fallacies, an individual is isolated and polarized into their own alternate reality. University of Virginia Professor Donald Leech, who is co-author of the book *COVID-19 Conspiracy Theories*, states, "You have people who are literally in different reality bubbles … you pick what fits your beliefs best" (Leech, 2020). Then individuals can isolate themselves into their own reality, which is supported by the algorithms fed to them via social media. Author Timothy Snyder feels these alternative reality bubbles are a slippery slope for humanity and civic engagement. He states, "It is our ability to discern facts that makes you an individual and our collective trust in common knowledge that makes us a society. The individual who investigates is also a citizen who builds. The leader who dislikes investigators is a potential tyrant" (Snyder, 2017: 3).

Thomas Jefferson, in his Bill for the More General Diffusion of Knowledge, wrote, "the most effectual means of preventing [tyranny] would be, to illuminate, as far as practicable, the minds of the people at large, and more especially to give them knowledge of those facts." Yet egocentric thinking, groupthink, drone mentality, biased experiences, arrogance, and intolerance are the foundation of many Facebook groups and Twitter Feeds. Objectivity rests on intellectual humility, knowledge of our extensive ignorance and the need to consider competing sources of information. This lack of suspicion is also driving the belief in conspiracy theories.

A conspiracy theory (CT) is diametrically opposed to critical thinking and individuals who believe in conspiracy theories will believe it regardless of the amount of disconfirming evidence. So, without any evidence, what makes a conspiracy believable? Two primary things: a motive that hooks people, and a claim of abuse of power. What matters less than any evidence is the image a conspiracy theorist can put in someone's mind that there is an engaging motive for an illuminati or special organization whose only goal is to manipulate the public. The demand for evidence of a cabal can be easily dismissed that the people in power would never let evidence reach the public. It's a circular logic based in fallacy, but airtight if one accepts every claim as truth.

There are fundamental reasons why conspiracies are so attractive to some people. First, it offers conspiracy believers a clear villain. Ironically, by believing that the forces that govern the world are far beyond their own control, they then gain a sense of control for themselves in believing a conspiracy theory. "It becomes a tool of comfort, and a knowledge that the world is not orchestrated by confused, unconnected, chaotic processes, but instead by people (or lizards, aliens, illuminati, etc.) who are powerful and connected" (Dawson, 2020). Over a fifth of Americans still believe the conspiracy theory that climate change is a hoax, while over a tenth insist that the moon landing was faked,

including so-called "Flat Earthers" who deny that the Earth is a sphere (Statista, 2019). Many of these conspiracy beliefs are generally harmless. However, the ability to spread ideas through the internet without fact-checking can result in crises. QAnon, COVID, and the 2020 election results are startling examples.

The QAnon conspiracy theory has been linked to several violent acts since 2018, with QAnon supporters arrested for threatening politicians, breaking into the residence of the Canadian prime minister, an armed standoff near the Hoover Dam, a kidnapping plot and two kidnappings, and at least one murder (See Figure 5). Qanon adherents believe that Donald Trump is trying to save the world from a cabal of satanic pedophiles. The conspiracy theory's narrative includes centuries-old anti-Semitic tropes, like the belief that a league of elites is harvesting blood from abused children, and it names specific people, including Democratic politicians and Hollywood celebrities, as participants in a global plot (Beckett, 2020).

The Pew Research Center examined the belief that COVID-19 was planned and correlated that belief to a user's reliance on social media for information (see Figure 6). A majority of U.S. adults (71%) say they have heard at least "a little" about the conspiracy theory that the COVID-19 outbreak was intentionally planned by powerful people, including 19% who say they have heard "a lot" about this theory. Those who frequently turn to social media for news about the outbreak are especially likely to be aware of the theory. 30% of individuals who often get COVID-19 news from social media say they have heard "a lot" about the theory that the outbreak was intentionally planned, compared with half as many (15%) among those who turn to social media for COVID-19 news less often. Americans' assessments of the truth of this theory also differ substantially based on the sources of information they turn to most for news about the pandemic (Mitchell et al., 2020).

Americans who have heard of the claim that powerful people planned the pandemic, a majority of those who mainly rely on tweets from political leaders for COVID-19 news (56%), say the conspiracy theory is probably or definitely true. That outpaces those who rely most on local news outlets (42% who have heard of the theory think it is likely true), state and local officials (32%), public health organizations (25%), and national news outlets (22%). Those who rely mainly on national news outlets and are aware of the theory are most likely to say the theory is probably or definitely *not* true (68%) (Mitchell et. al., 2020) (See Figure 6).

The COVID 19 conspiracy theory rejection of science, that it was planned and hatched in a lab, that it is a political tool of manipulation, that it is a purposeful bioweapon, etc. eerily resembles how fourteenth-century people reacted to the bubonic plague. According to David Leech, "In medieval times people turned to religion for answers as to why the plague was killing so many. As fear and superstition took hold, so did the need to blame something or

QANON: A TIMELINE OF VIOLENCE LINKED TO THE CONSPIRACY THEORY

15 JUNE 2018	An Arizona resident blocks a bridge near the Hoover Dam with an armored vehicle. He later pleads guilty to a terrorism charge.
19 DECEMBER 2018	A California man is arrested after being found with what appeared to be bomb-making materials in his car, in an alleged plot to blow up a satanic display in the capitol in Springfield, Illinois.
13 MARCH 2019	In Staten Island, a 24-year-old man allegedly murders a leader in the Gambino crime family.
25 SEPTEMBER 2019	A QAnon supporter allegedly smashes up the Chapel of the Holy Hill in Sedona, Arizona, while shouting about the Catholic church supporting human trafficking.
30 DECEMBER 2019	Montana police arrest a QAnon supporter from Colorado in connection with an alleged kidnapping scheme.
26 MARCH 2020	A Kentucky mother is charged with kidnapping twin daughters.
2 APRIL 2020	A man is charged with intentionally derailing a freight train near the navy hospital ship Mercy in Los Angeles.
30 APRIL 2020	A woman is arrested after driving to New York and allegedly making threatening statements against Joe Biden and Hillary Clinton.
11 JUNE 2020	A Boston man leads police on a 20-mile car chase while livestreaming himself talking about QAnon.
3 JULY 2020	Corey Hurren, a reservist in the Canadian Rangers, allegedly rams a truck through the gates of the prime minister's residence in Ottawa.
12 AUGUST 2020	A Texas woman is arrested after allegedly chasing and crashing into a car, then telling police she thought she was chasing a pedophile.
1 OCTOBER 2020	Utah woman arrested in Oregon for allegedly kidnapping her young son.
6 JANUARY 2021	The QAnon conspiracy theory and significant misinformation fueled the insurrection at the Capitol.

Figure 5. Violence and QAnon Conspiracy theories.

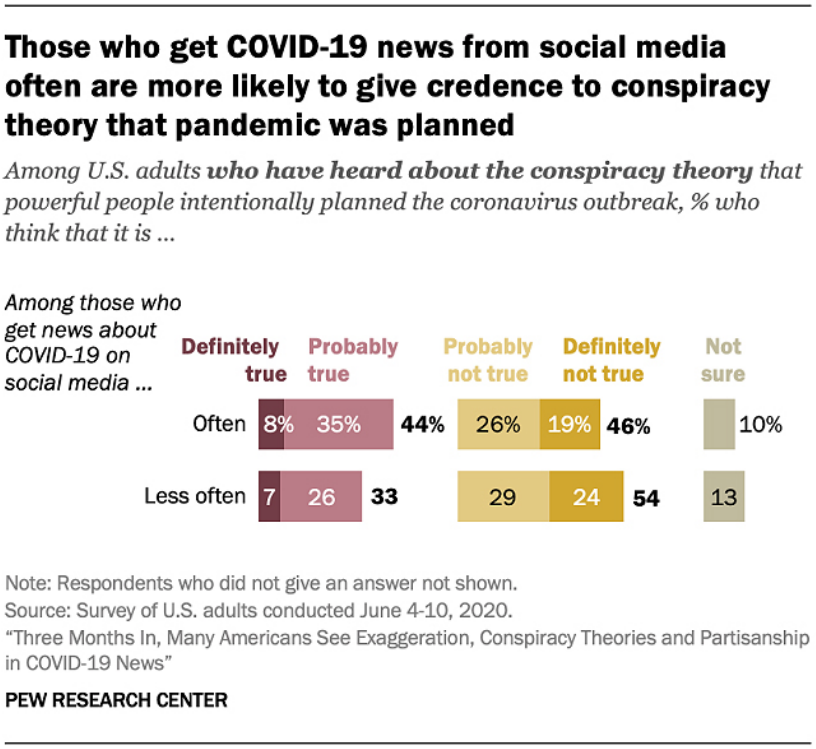

Figure 6.

someone. That fed into existing prejudices about the Jews and Muslims … six hundred years later, we've accumulated a lot more knowledge but we're clearly not smarter. We've just got more science to ignore" (Still, 2020).

Who is Prone and Why: Seizing, Freezing, and Cognitive Closure

Belief in conspiracy theories appears to be driven by motives that can be characterized as epistemic (understanding one's environment), existential (being safe and in control of one's environment), and social (maintaining a positive image of the self and the social group). Along with the dopamine hits everyone gets from *likes* on social media, it turns out it is not completely random who will and will not believe in a conspiracy theory. Yet while our predilection to social media magnetism might be a tragic flaw in the human genome, psychological profiles of individuals who believe in one or more conspiracy theories have some significant trends. It is easy to demonize and stereotype conspiracy believers into the comedic "tin foil hat" depiction often mocked in media, but many are people who simply fall victim to misinformation. Unlike ordinary lies and propaganda, which try to make you believe *something*, disinformation tries to make you disbelieve *everything*. It scatters so much bad information, and casts so many aspersions on so many sources of information, that people throw up their hands and say, "They're

all a pack of liars." As Steve Bannon, former Trump aide and former leader of *Breitbart News*, succinctly put it in an interview with *Bloomberg*, "[T]he way to deal with [the media] is to flood the zone with shit" (Rauch, 2020).

One of the most fascinating things about those who believe in a conspiracy is their likelihood to believe another. As Psychology Professor Viren Swami puts it, "the best predictor of belief in a conspiracy theory is belief in other conspiracy theories" (Koerth-Baker, 2013). This is likely because conspiracies tend to have crossover in themes (and occasionally even details), which almost always contains a lack of control on the part of the believer directed to a shadowy organization far larger and more powerful than themselves.

Professor Joseph Hart interviewed 1,200 Americans to understand the correlation of partisan leanings, personality traits and demographics in understanding conspiracy theories. His research suggests that people with certain personality traits and cognitive styles are more likely to believe in conspiracy theories (*Science Daily*, 2018). "These people tend to be more suspicious, untrusting, eccentric, needing to feel special, with a tendency to regard the world as an inherently dangerous place. [Additionally], they are also more likely to detect meaningful patterns where they might not exist. People who are reluctant to believe in conspiracy theories tend to have the opposite qualities," (*Science Daily*, 2018). This is because belief in conspiracy theories also has much to do with the ways in which individuals interpret and accept the legitimacy of evidence. For instance, psychological heuristics, such as the quick linking of a major event with a major cause, may account for the attribution of conspiracy theories to explain major public events. Once conspiracy beliefs become established, confirmation biases prevent consideration of disconfirming evidence. Information that confirms an individual's existing beliefs will tend to be unquestioned and accepted whereas disconfirming evidence will often be blatantly rejected.

Also driving the psychological tendencies towards noncompeting information is a need for cognitive closure, which drives an individual to grasp onto views that support their need for order and structure; many people have discomfort with ambiguity. A quick solution provides cognitive closure, referred to as seizing. Once an individual has cognitive closure, they want to maintain it, which is referred to as freezing (Leman, 2013). Cognitive dissonance, personality tendencies and psychological heuristics coupled with the possible decline of critical thinking skills mean there is a portion of the public that is unable or unwilling to tap into the higher end of Bloom's Digital Taxonomy and higher-order thinking skills (HOTS) as illustrated in Figure 7. For social media users, a quick like, share or three-sentence reply falls somewhere on step 1 or 2 of the pyramid. (See Appendix 1 for a deconstruction of a recent conspiracy theory and social media post).

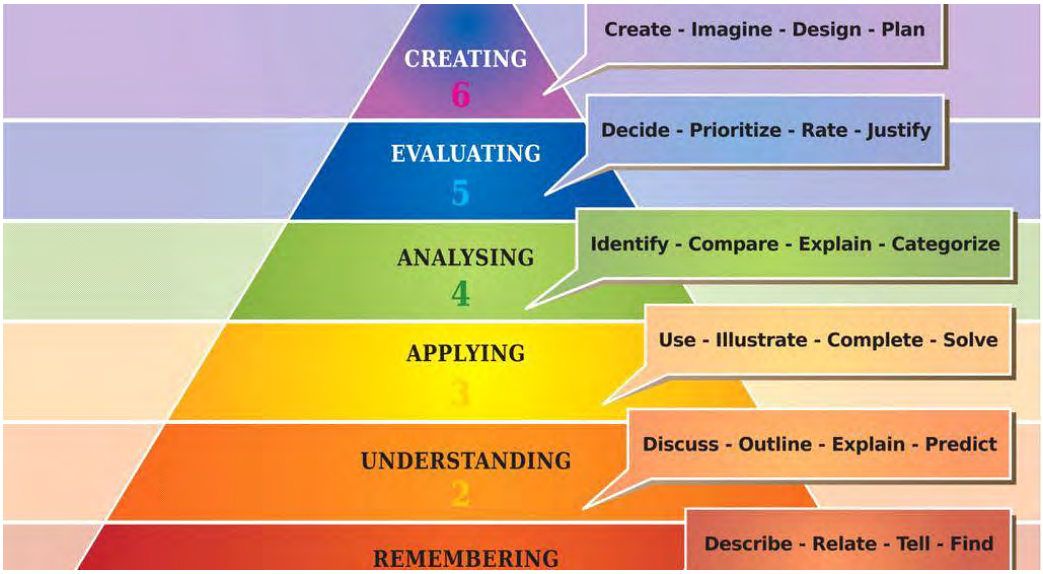

Figure 7. (thinkingmaps.com)

Behavioral conditioning, psychological tendencies plus neurological rewards increases the vulnerability of individuals to cognitive hacking. Social media is habit-forming and addictive. Research has found that social media *likes* are akin to social rewards. Providing and receiving *likes* to people's posts activates regions of the brain that release dopamine. This positive feedback has been found to mimic the same qualities as the positive feeling a person has when they donate to charities. This feedback loop of likes and sharing instills reinforcement learning and encourages a person to seek that outcome again. Although not as intense as a hit of cocaine, positive social stimuli result in a release of dopamine, reinforcing whatever behavior preceded it. Cognitive neuroscientists have shown that rewarding social stimuli—laughing faces, positive recognition by our peers, messages from loved ones—activate the same dopamine reward pathways (Haynes, 2018). This dopamine influx is addicting regardless of the driver.

Researchers from the University of Michigan by Kent Berridge and Terry Robertson developed the "Incentive Sensitization Theory of Addiction"' theory that has been applied to social media. Rewards are both "liked" and "wanted," and this process creates a dopamine loop, which creates addiction and cravings in the social media users. "When you bring up the feed on one of your favorite apps the dopamine loop has become engaged," said Dr. Susan Weinschenk. "With every photo you scroll through, headline you read, or link you go to you are feeding the loop which just makes you want more." Many social media platforms are taking advantage of research in neuroscience to increase social media use and encourage people to return, using some of the same principles casinos use to entice repeat gamblers (McKorkindale, 2019).

State and non-state actors have taken advantage of these psychological, behavioral and neurological paradigms and have an operational strategy for targeting social media users as outlined by Rand Waltzamn of Rand Corporation (see Figure 8). In the world of social media, it is easy to distort reality and exploit a user's neurological, intellectual, and psychological vulnerability to weaponization of information. Individuals are poor judges of true versus false information online, information overload leads people to take shortcuts in determining the trustworthiness of messages, and familiar themes or messages can be appealing even if they are false.

Figure 8.

The Way Forward: Cognitive Security (COGSEC)

Currently, most of the capability associated with Information Operations mission lies within DoD. P.L. 115-232 Sec 1284 tasked the State Department's Global Engagement Center (GEC) to "direct, lead, synchronize, integrate, and coordinate efforts of the Federal Government to recognize, understand, expose, and counter foreign state and foreign non-state propaganda and disinformation efforts." DHS also has a Countering Foreign Influence Task Force. Documents to support these missions include: The CRS Defense Primer-Information Operations as updated on 12/15/2020 Defense Primer; Information Operations (fas.org); 2018 Joint Concept for Operating in the Information Environment joint_concepts_jcoie.pdf (jcs.mil); P.L. 115-232 Sec 1284 PUBL232.PS (congress.gov) P.L. 116-92 Sec 1631. Yet these manuals have not caused policymakers to enact laws or legislation. They are simply awareness and advising tools. Craig Terberg, *Washington Post* Technology writer, feels we have not had meaningful or any legislation to support the misinformation war (Davies, 2021).

COGSEC may need to be a new frontier in intelligence to protect peo-

ple from online exploitation, cognitive hacking and weaponized information. This is different from cybersecurity, which is the protection of internet-connected systems such as hardware, software and data to defend against unauthorized access. Cognitive Security protects people from their own thinking. In the arena of all information all the time by all individuals, COGSEC is essential. Admittedly, it is a problematic issue in a democratic society with freedom of speech, yet there can be a differentiation between voicing an opinion and weaponizing information. For example, people are not allowed to yell "FIRE" in a crowded movie theater.

Also, this is not one entity's job. There needs to be a consortium of actors involved in a coordinated effort for countering weaponized information. As early as 2017, Rand Waltzamn of Rand Corporation testified before the Cybersecurity Committee on Armed Services promoting the necessity of COGSEC. He stated in his testimony that it will take all players like researchers, governments, social platforms and private actors to "be engaged in a continual arms race to influence and protect from influence large groups of users online" (Walltzman, 2017). According to Ronald Joy, Deputy Program Manager of Intelligence Programs with 22 years of intelligence, security and operational planning, he feels, "Our adversaries understand that unlike conventional 'military' operations, the weaponization of information in the public sphere currently falls below U.S. legal and planning thresholds for armed conflict. We have plans for what we do when someone launches a rocket at an Embassy. There is a graduated, proportional response plan in place for that kind of attack, along with 'off-ramps' for de-escalation after the fact" (Joy. 2020). Joy feels that weaponized information might need to be looked at with an aggregated government methodology with agencies not siloed from each other so information can be shared.

In addition, there are numerous documents targeted at the audience of policymakers. These include *Information Warfare (IW): Issues for Congress*, *Defense Primer; Information Operations, Free Speech and the Regulation of Social Media Content*, prepared by the Congressional Research Service. These documents target the actions of nation-states. Yet domestic terrorism and information warfare have blurred the boundaries of what constitutes a state enemy. Traditional distinctions—public versus private interests, warlike versus criminal behavior—and geographic boundaries, such as those between nations as historically defined, are complicated by the growing interaction and the influence by state actors on alt groups. Given the wide array of possible opponents, weapons, and strategies, it becomes increasingly difficult to distinguish between foreign and domestic sources of IW threats and actions. Roger Moreland of Rand Corporation states,

> "You may not know who's under attack by whom, or who's in charge of the attack. This greatly complicates the traditional role distinction between domestic law enforcement, on the one hand, and national security and intel-

> ligence entities, on the other. Another consequence of this blurring phenomenon is the disappearance of clear distinctions between different levels of anti-state activity, ranging from crime to warfare. Given this blurring, nation-states opposed to U.S. strategic interests could forgo more traditional types of military or terrorist action and instead exploit individuals or transnational criminal organizations (TCOs) to conduct "strategic criminal operations." (Moreland, 1996)

Richard Fomo, from the Center for Internet and Society, has developed an offensive and defensive strategy for countering weaponized information. This strategy includes imposing sanctions and policy responses towards agent provocateurs like Russia and China, especially if they intervene in any democratic processes. This seems straight-forward but a fundamentally tricky recommendation is Fomo's counsel to allow for intelligence transparency between the government and the public. The public needs to understand the context of some of the larger implications of cognitive hacking by knowing the actors and messages. While Fomo acknowledges that this is a difficult balance, he feels countering disinformation is a public policy priority and it is paramount that the government notifies the public and news media of evidence of cognitive hacking. The news media companies that should be given access to this information was not addressed and seems problematic in and of itself given the current challenges of the public authenticating and trusting news sources.

A solid proposal from Fomo was the emulation of the European Union's East StratCom disinformation task force to combat disinformation campaigns. Their biweekly newsletter, the Disinformation Review, published over social media, highlights disinformation. According to *The New York Times*, East Stratcom serves as "Europe's front line against this onslaught of fake news" (Scott, 2017). The newsletter has over 52.9K followers (Rettman, 2017). Unlike the U.S., the European Union (EU) has taken a strategic attack against disinformation and by December 2018, the European Commission launched its Action Plan Against Disinformation, which remains a key pillar of EU policy, granting mandates to several operational arms. The action plan emphasized four areas of work: improving the capabilities of EU institutions to detect, analyze, and expose disinformation; strengthening coordinated and joint responses to disinformation; mobilizing the private sector to tackle disinformation and raising awareness and improving societal resilience. The European Council also made commitments to strengthening the EU's democracy-building capabilities around the world, including promoting instruments created to mitigate the effects of online interference during elections. The Carnegie Endowment for International Peace outlined these strategic proposals that could apply to the U.S. as well (Panameet, 2020). For the East Strat Operational approach, see Figure 9.

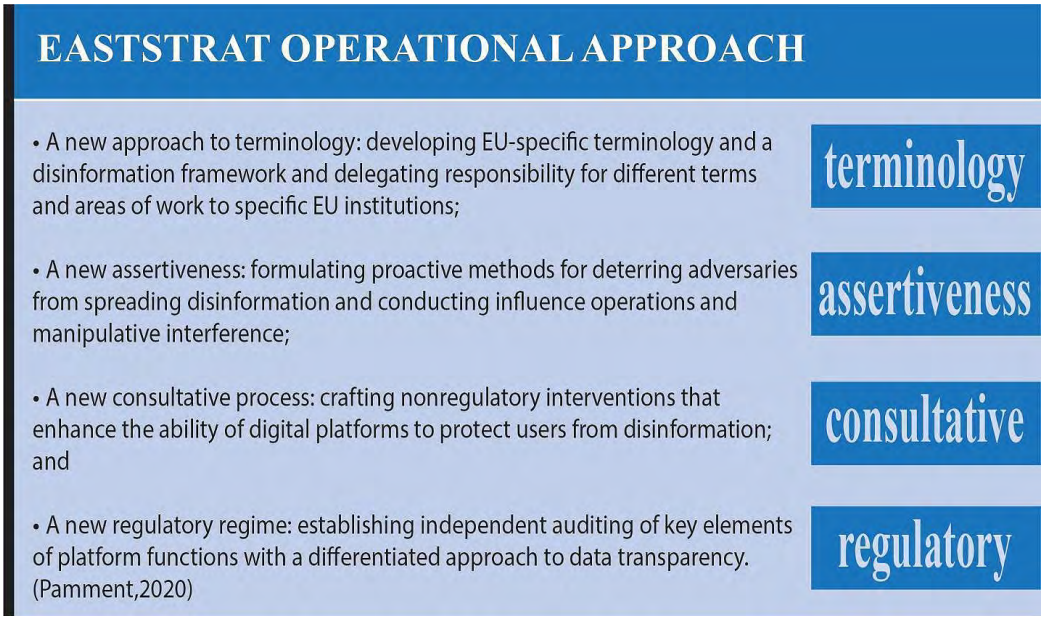

Figure 9.

Perhaps the most significant players, social media corporations, must also be engaged and take action. They cannot stand by wittingly with eyes on profit. Social media companies must become accountable and address the fact that their platforms are being used by foreign governments and nefarious groups to spread deadly disinformation. While Google and Facebook have been slow to take action, it must be noted that they have taken some steps to begin to tackle these issues. They have acknowledged that their platforms have been exploited and they now utilize third-party fact-checking and changing algorithms. Facebook did this for their trending section and Google has started tagging news search results with phrases like mostly true or false. Additional action against fake news includes not displaying ads for sites that include fake news (Fomo, 2020). Recently, Facebook's oversight board in January 2021 directed the company to restore several posts that the social network had removed for breaking its rules on hate speech, harmful misinformation and other matters. The decisions are the first rulings for the board, which Facebook created last year as a kind of supreme court, casting the final votes on the hardest calls the company makes about what it does and does not allow users to post (Bond, 2021).

Another variable is that data privacy legislation for social media companies has not kept pace with the weaponization of information. According to Army General to Cyber Command, Joseph Brendlare states, "A dynamic that started with a purely commercial marketplace is producing technologies that can be weaponized and used for the purposes of influencing the people of the United States to do things other than just buy products . . . some of that

is a good thing . . . the extent to which it might produce a violent outcome, it's a really bad thing. Absent the appropriate forms of regulation, we really have an unregulated arms market here" (Tucker, 2020). In December 2020, the Defense Bill Section 230 was vetoed. The bill, which, among many factors, gives tech companies protections for third-party content posted on their platforms and allows them to make good faith efforts to moderate content. Some claimed that social media firms use the law to unfairly censor conservatives, a claim that has been proven unsubstantiated (Axelrode, 2020).

According to authors Alina Polyakova and Daniel Fried, they feel "[T]hat is a good (and publicly visible) step but does not address bottom issues of content distribution (e.g., micro-targeting), algorithmic bias toward extremes, digital cloning and lack of transparency." They suggest the U.S. government must make several organizational changes to counter foreign disinformation. "While the United States has sometimes acted with strength against purveyors of disinformation, e.g., by indicting IRA-connected individuals, U.S. policy is inconsistent. The U.S. government has no equivalent to the European Commission's Action Plan Against Disinformation and no corresponding Code of Practice on Disinformation, and there remains no one in the U.S. government in overall charge of disinformation policy; this may reflect the baleful U.S. domestic politics and Trump's mixed or worse messages on the problem of Russian-origin disinformation" (Tucker, 2020).

Conclusion

There is a proverb that is sometimes referred to as a curse—may you live in interesting times. First mentioned in British correspondence in 1936 and attributed to Chinese diplomats, the word interesting can certainly apply to the twenty-first century future of fake news and IW. The way forward in these uncharted waters is unmapped, muddy, and difficult to navigate. The denotative meaning of the word interesting implies something cute or curious, but the connotative meaning is something far more ominous. As stated by Craig Temberg, "While we love free speech and we want free speech to be as open as possible, it's also true that my speech can drown out your speech and my lies can drown out your truth" (Davies, 2021). Also, he points out, we are chartering a brave new world or what he refers to as a "science experiment" when it comes to fake information. What he has found is when, "you really eliminate the voice of someone who is pushing a lot of lies . . . It turns out that those lies have a lot less traction. They move around less often" (Davies, 2021). But as social media companies have shared, their hands have been forced to decide who gets to talk and they have not wanted to be the arbitrators of first amendment rights, for that is a lot of power.

Yet how to handle fake news and deliberate disinformation campaigns that are being wielded by state actors is difficult when the lines between state and non-state actors are blurred. Additionally, it begs the question of what

agency is to monitor lies, deceit and deliberately using information as a weapon. Both Michael Hayden and Michael Morell feel the intelligence community should not go down that road, but they are both concerned about the connection between white supremacy groups with ties out of the U.S. (Hayden, 2021). Recently, as both state and non-state actors experience the backlash from January 6, 2021, many social media disinformation campaigns have moved to platforms where the communications are encrypted end-to-end, and cannot be easily monitored, posing another challenge.

Back in the early 1800s, when the internet was the telegraph, Ralph Waldo Emerson and Henry David Thoreau preached self-reliance of the individual in all matters, but especially for people to think for themselves and not follow ideas or institutions blindly. Emerson stated, "Whoso would be a man, must be a nonconformist." Weaponized information removes individualism by targeting the thinking mind with computational propaganda and technology that can mimic legitimate news websites and overloads an individual's ability to decipher fact from fiction. Individualism turns into group think when a brain receives an echo chamber of repetitive information. Because social media has become a tool in dangerous propaganda, doublethink has evolved into an unprecedented threat that must be addressed. The twenty-first century is an interesting time, especially when powerful new technology makes the speed and targeting of misinformation towards people's cognitive biases unmatched in human history. Yet the weaponization of information alerts us to thinking about the very conscious use of information to achieve various goals.

"Words also shoot," noted the Russian Minister of Defense Sergei Shoigu when opening the first military media festival in Russia in 2015, indicating the important role of information in contemporary Russian military thinking runs parallel to Chinese self-preservation information campaigns. The United States needs to be proactive in addressing the weaponization of information by educating its policymakers and public, enacting legislation with and for social media companies and devising counterintelligence measures, because the insurrection on Capitol Hill on January 6, 2021 may be a foreshadowing of a plane hitting the twin towers, and that plane may have already hit its target.

Margaret S. Marangione is a senior researcher for defense contractor, Syntelligent Analytic Solutions. She started her career as an Intelligent Analyst for the CIA and worked as a Security Analyst for Grumman-Northrop. She is a former researcher for the Humanitarian Mine Action Center working directly with the State Department, Department of Defense, United Nations and the Geneva Center. She is the founding editor of the J*ournal of Mine*

Action and her intelligence-related articles have appeared in the International Journal of Intelligence and Counterintelligence, the Global Intelligence Studies Journal and Signal Magazine. The funding for this article was supported by Syntelligent Analytic Solutions. The author can be reached at Margaret.marangione@syntelligent.com

Appendix 1

C/o Xavier Dawson

APPENDIX 1 EXAMPLE OF SOCIAL MEDIA CONSPIRACY THEORIES

December 2, 2020

Seasonal thoughts, feelings; covid-19: statistics, masks, tests, vaccine; rebelling citizenries; US election; imminent changes; unconditional love

With loving greetings from all souls at this station, this is Matthew. How greatly this season of holy days differs from previous years dominates thoughts and feelings around your world. Instead of traditional observances and festivities with family and friends, many are mourning loved ones to whom they were denied goodbyes and are having to forego attending sacred services. We, too, feel sadness that your year 2020 is ending on that solemn note.

This paragraph in isolation is not brutally fallacious. There's an appeal to tradition in discussing typical holiday celebration, as well as an assumption that this tradition is a good and righteous thing (which will later be used to imply any change to this status quo for any reason is evil). This is mostly setting up for the paragraphs to come, establishing empathy and being, for the most part, reasonable at the start.

Dear ones, you can keep bright the spirit of this season that celebrates love, the goodness in your life and the world, and sharing with those who are in need. As you act upon those sentiments that uplift you and all whom your caring touches, you can revisit joyous holidays in memory. If beloved persons no longer are with you, you can feel happy for them—they are living in a wondrous world of amazing activity and diversity.

Again, not necessarily fallacious yet, but putting forth a great deal of work to create a connection with the reader by calling them "dear ones" and consoling them on potential deaths of close loved ones. This is to build an amount of trust and goodwill, which will later be leveraged.

Earth's energy field of potential also is reflecting the society's other primary thoughts, feelings and actions. They have to do with covid foremost, then unrest in increasing numbers of countries and the United States presidential election. To address those situations, we begin with the reader's questions that are in the minds of all who know what is behind the "pandemic."

This is a sort of de facto thesis statement for the email, covering its topics-to-come of the pandemic and election. Notably, the word "pandemic" is only referred to in this email in quotation marks, a quiet implication of non-legitimacy or lack of pandemic-worthy threat.

"Should lightworkers not wear a mask in public and refuse to be tested for COVID-19 to help spread awareness of the truth about it? Why are cases spiking? What can we do if vaccinations are mandatory when a vaccine is available?" If masks are required by employers or entry into public buildings, never would we suggest that you incur a troublesome situation for yourself by violating that regulation. But as often as you can, lower the mask and breathe naturally.

The questions opening this paragraph are loaded, based in a number of assumptions of an unspoken "truth" about covid, presented as questions from readers which the previous paragraph implies should be the questions all readers are asking. At the end of this paragraph is one of the most blatant deceptions in the email, in which the writer eschews all accountability by advising readers not to "incur a troublesome situation" for themselves by not wearing masks (note the implication that this is merely as a form of conflict avoidance, rather than an agreement with policy). Immediately following this statement, the very antithesis is stated, quote: "as often as you can", readers are encouraged to lower their masks and breathe "naturally" (an appeal to nature as an inherent good, implying that masks are artificial and therefore unhealthy).

Unless your work requires being tested, avoiding that precludes the possibility of being quarantined when you don't have the disease. It is not that cases of covid are surging to record numbers, it is the statistics that are. Tests are part of the massive deception. Some are made to register only positive, others are designed to detect the viruses that cause colds and "standard" flu, and all those positives are declared covid-19. Statistics also include the seriously ill whose deaths are claimed to be caused by "complications due to covid."

This paragraph consists pretty much entirely of statements with no foundation in evidence, completely unfounded claims about covid-19 operations. Notably, these claims are not consistent; a number of claims about how covid-19 tests are fraudulent are given, because the point is not to prove a concrete truth, but to create doubt in the existing truth, in which case multiple disagreeing theories can be utilized as though they were multiple pieces of evidence, dissonance between them being avoided by stating that these fraudulent methods are all being used.

References

Axelrod, Tal. (2020, December 1). "Trump Threatens to Veto Defense Bill over Tech Liability Shield." Text. *The Hill*. https://thehill.com/homenews/administration/528301-trump-threatens-to-veto-defense-bill-over-tech-liability-shield.

Babb, Colin E. (2020, March 17)."Dezinformatsiya and the Cold War." Future Force. https://futureforce.navylive.dodlive.mil/2020/03/dezinformatsiya-and-the-cold-war/.

Bajema, Natasha, and Christine Parthemore. (2020, March 29). "How to Counter China's Coronavirus Disinformation Campaign." *Defense One*.

Beckett, Lois. (2020, October 16). "QAnon: A Timeline of Violence Linked to the Conspiracy Theory." *The Guardian*. http://www.theguardian.com/us-news/2020/oct/15/qanon-violence-crimes-timeline.

Belkin, Douglas. (2020, June 5). "Exclusive Test Data: Many Colleges Fail to Improve Critical-Thinking Skills." *Wall Street Journal*, sec. U.S. https://www.wsj.com/articles/exclusive-test-data-many-colleges-fail-to-improve-critical-thinking-skills-1496686662.

Bergmann, Max, and Carolyn Kenney. (2017, June 6). "War by Other Means." Center for American Progress. https://www.americanprogress.org/issues/security/reports/2017/06/06/433345/war-by-other-means/.

Brooks, David. "Opinion November 26, 2020. The Rotting of the Republican Mind." *The New York Times*. Opinion. https://www.nytimes.com/2020/11/26/opinion/republican-disinformation.html.

Cadwalladr, Carole. (2018, March 18). "'I Made Steve Bannon's Psychological Warfare Tool': Meet the Data War Whistleblower." *The Guardian*, sec. News. https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump.

Confessore, Nicholas. (2018, April 4). "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far." *The New York Times*. sec. U.S. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

Curto, Justin. (2020, October 16). "Savannah Guthrie Says Trump Can't Act Like 'Someone's Crazy Uncle' on Twitter." *Vulture*. https://www.vulture.com/2020/10/savannah-guthrie-trump-crazy-uncle-babylon-bee.html.

Cybersecurity & Infrastructure Security Agency. (2020, November 12). "Joint Statement from Elections Infrastructure Government Coordinating Council & the Election Infrastructure Sector Coordinating Executive Committees," https://www.cisa.gov/news/2020/11/12/joint-statement-elections-infrastructure-government-coordinating-council-election.

Dawson, Xavier. (2020, November 19).

Deeks, Ashley, Sabrina McCubbin, and Cody M. Poplin. (2017, October 25). "Addressing Russian Influence: What Can We Learn From U.S. Cold War Counter-Propaganda Efforts?" Lawfare. https://www.lawfareblog.com/addressing-russian-influence-what-can-we-learn-us-cold-war-counter-propaganda-efforts.

Doffman, Zak. (2020, March 12). "Chinese Hackers 'Weaponize' Coronavirus Data For New Cyber Attack: Here's What They Did." *Forbes*. https://www.forbes.com/sites/zakdoffman/2020/03/12/chinese-hackers-weaponized-coronavirus-data-to-launch-this-new-cyber-attack/.

Easton, Anthony, and Patrick Franck. (2020, August 23). "Information Warfare on United States' Citizens: How China Weaponized COVID-19." *Over the Horizon*,

Gazis, Olivia. (2020, March 30). "Amid COVID-19 Outbreak, China Shifts to Use 'Russian-Style' Disinformation Tactics." *CBS News*. https://www.cbsnews.com/news/coronavirus-covid-19-outbreak-china-russian-style-disinformation-tactics/.

Geissler, Erhard, and Robert Hunt Sprinkle. (2013). "Disinformation Squared: Was the HIV-from-Fort-Detrick Myth a Stasi Success?" *Politics and the Life Sciences 32*, no. 2 (2013): 2-99. Accessed December 16, 2020. http://www.jstor.org/stable/43287281.

Haber, Jonathan. (2020, March 2). "It's Time to Get Serious About Teaching Critical Thinking." *Inside Higher Ed.* https://www.insidehighered.com/views/2020/03/02/teaching-students-think-critically-opinion.

Haynes, Trevor. (2018, May 1). "Dopamine, Smartphones & You: A Battle for Your Time." Science in the News (blog), http://sitn.hms.harvard.edu/flash/2018/dopamine-smartphones-battle-time/.

Herzstein, Robert E. (1979). *The War That Hitler Won: The Most Infamous Propaganda Campaign in History*. London: Hamilton.

Hutchinson, Andrew. (2020, June 30). "Facebook Announces News Feed Algorithm

Update to Put More Emphasis on Original, Quality News Content." *Social Media Today*. https://www.socialmediatoday.com/news/facebook-announces-news-feed-algorithm-update-to-put-more-emphasis-on-origi/580827/.

Ignatidou, Sophia. (2019, August 19). "The Weaponisation of Information Is Mutating at Alarming Speed." *The Guardian*. http://www.theguardian.com/commentisfe/2019/aug/19/weaponisation-of-information-mutating-privacy.

Isaac, Mike, and Daisuke Wakabayashi. (2017, October 30). "Russian Influence Reached 126 Million Through Facebook Alone." *The New York Times*. sec. Technology. https://www.nytimes.com/2017/10/30/technology/facebook-google-russia.html.

Joy, Ronald. (2020, December 18). Interview. E-mail.

Kang, Cecilia, and Sheera Frenkel. (2018 April 4). "Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users" *The New York Times*. sec. Technology. https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html.

Kanno-Youngs, Zolan. (2020, September 17). "F.B.I. Director Warns of Russian Interference and White Supremacist Violence." *The New York Times*, sec. U.S. https://www.nytimes.com/2020/09/17/us/politics/fbi-russia.html.

Lapowsky, Issie. (2018, July 18). "Shadow Politics: Meet the Digital Sleuth Exposing Fake News." *Wired*, https://www.wired.com/story/shadow-politics-meet-the-digital-sleuth-exposing-fake-news/.

Leman, Patrick J., and Marco Cinnirella. (2013, June 27). "Beliefs in Conspiracy Theories and the Need for Cognitive Closure." *Frontiers in Psychology*, https://doi.org/10.3389/fpsyg.2013.00378.

Levitin, Daniel. (2017, March 9). "How to Fight the Weaponization of Fake News | Opinion." *Newsweek*. https://www.newsweek.com/fake-news-critical-thinking-daniel-levin-weaponized-lies-book-564852.

Levy, Steven. (2020, June 5). "Mark Zuckerberg Is an Arbiter of Truth—Whether He Likes It or Not." *Wired*, https://www.wired.com/story/mark-zuckerberg-is-an-arbiter-of-truth-whether-he-likes-it-or-not/.

Lyons, Kim. (2021, January 21). "Facebook's Trump Ban Will Be Reviewed by Its New Oversight Board." *The Verge* https://www.theverge.com/2021/1/21/22242616/facebook-refers-decision-suspend-trump-oversight-board.

Memmott, Mark. (2013, October 30). "75 Years Ago, 'War Of The Worlds' Started A Panic. Or Did It?" *NPR*. https://www.npr.org/sections/thetwo-way/2013/10/30/241797346/75-years-ago-war-of-the-worlds-started-a-panic-or-did-it.

Mitchell, Amy, Mark Jurkowitz, J. Baxter Oliphant, and Elisa Shearer. (2020, May 20). "Americans Who Rely Most on White House for COVID-19 News More Likely to Downplay the Pandemic." *Pew Research Center's Journalism Project* (blog), https://www.journalism.org/2020/05/20/americans-who-rely-most-on-white-house-for-covid-19-news-more-likely-to-downplay-the-pandemic/.

Molander, Roger C., Andrew Riddile, and Peter A. Wilson. (1996). Strategic Information Warfare: A New Face of War. Santa Monica, CA: RAND Corporation, https://www.rand.org/pubs/monograph_reports/MR661.html.

Morell, Michael. (2021, January 26). Assault of Intelligence: After Trump. The Hayden Center.

Posetti, Julie, and Alice Matthews. (2018, July 23). "A Short Guide to the History of 'Fake News' and Disinformation: A New ICFJ Learning Module." International Center for Journalists, https://www.icfj.org/news/short-guide-history-fake-news-and-disinformation-new-icfj-learning-module.

Rand Corporation. (2020). "Information Operations." Rand Corporation. https://www.rand.org/topics/information-operations.html.

Rauch, Jonathan. (2018). "The Constitution of Knowledge." National Affairs, https://www.nationalaffairs.com/publications/detail/the-constitution-of-knowledge.

Rettman, Andrew. (2017, November 28). "EU Diplomats to Get Training on 'Fake News.'" *EUObserver*. https://euobserver.com/foreign/140051.

Richelle, McDaniel. (2015). *The Spread of Knowledge Via Print*. Western Oregon University. https://digitalcommons.wou.edu/cgi/viewcontent.cgi?article=1002&context=history_of_book.

Rid, Thomas. (2018). *Disinformation: A Primer in Russian Active Measures and Influence Campaigns.* CreateSpace Independent Publishing Platform.

Rosenberg, Matthew, Nicholas Confessore, and Carole Cadwalladr. (2018, March 17). "How Trump Consultants Exploited the Facebook Data of Millions." *The New York Times*. sec. U.S. https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

Schneider, Christopher, Markus Weinmann, and Jan vom Brocke. (2018, July). "Digital Nudging: Guiding Online User Choices through Interface Design." Communications of the ACM.

Schwartz, A. Brad. (2015, May 6). "The Infamous 'War of the Worlds' Radio Broadcast Was a Magnificent Fluke." *Smithsonian Magazine*. https://www.smithsonianmag.com/history/infamous-war-worlds-radio-broadcast-was-magnificent-fluke-180955180/.

Scott, Mark, and Melissa Eddy. (2017, February 20). "Europe Combats a New Foe of Political Stability: Fake News." *The New York Times*, sec. World. https://www.nytimes.com/2017/02/20/world/europe/europe-combats-a-new-foe-of-political-stability-fake-news.html.

Shane, Scott, and Sheera Frenkel. (2018, December 17). "Russian 2016 Influence Operation Targeted African-Americans on Social Media." *The New York Times*, sec. U.S. https://www.nytimes.com/2018/12/17/us/politics/russia-2016-influence-campaign.html.

Singer, Natasha. (2018, April 11). "What You Don't Know About How Facebook Uses Your Data." *The New York Times*, , sec. Technology. https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html.

Statista Research Department. (2019, August 13). "Topic: Beliefs and Conspiracy Theories in the U.S." *Statista*. https://www.statista.com/topics/5103/beliefs-and-superstition-in-the-us/.

Tierney, Dominic. (2020, September 13). "How Putin Got Into America's Mind." *The Atlantic*, https://www.theatlantic.com/ideas/archive/2020/09/how-putin-got-into-americas-mind/616330/.

Travers, Mark. (2020, March 21). "Facebook Spreads Fake News Faster Than Any Other Social Website, According To New Research." *Forbes*, https://www.forbes.com/sites/traversmark/2020/03/21/facebook-spreads-fake-news-faster-than-any-other-social-website-according-to-new-research/.

Tucker, Patrick. (2020, November 12). "Myths About Vote Tampering Could Persist For Years, Say Experts." *Defense One*. https://www.defenseone.com/technology/2020/11/myths-about-vote-tampering-could-persist-years-say-experts/170017/.

Waltzman, Rand. (2017, April 27). "The Weaponization of Information; Testimony of Rand Waltzman Before the Committee of Armed Services Subcommittee of

Cyber Security U.S Senate." The Rand Corporation.

Watson, Ben, and Bradley Peniston. (2020, November 13). "Today's D Brief: 'The Most Secure' Election; Syria 'Shell Games'; China's New Joint Ops Doctrine; And a Bit More." Defense One, https://www.defenseone.com/threats/2020/11/the-d-brief-november-13-2020/170024/.

Weichart, Brandon. (2020, December 14). "China Weaponized COVID-19 against America." *The Washington Times*, https://www.washingtontimes.com/news/2020/dec/14/china-weaponized-covid-19-against-america/.

Weiner, Tim. (2020). *The Folly and the Glory: America, Russia, and Political Warfare, 1945-2020*. First edition. New York, New York: Henry Holt and Company.

Wolpert, Stuart. (2009, January 27). "Is Technology Producing a Decline in Critical Thinking and Analysis?" UCLA, https://newsroom.ucla.edu/releases/is-technology-producing-a-decline-79127.

Zhong, Raymond, Paul Mozur, Jeff Kao, and Aaron Krolik. (2020, December 19). "No 'Negative' News: How China Censored the Coronavirus." *The New York Times*, sec. Technology. https://www.nytimes.com/2020/12/19/technology/china-coronavirus-censorship.html.