Connect to Divide: Social Media in 21st Century Warfare
Major Eddy Gutierrez

Figure 1: Photo by artisteer/Getty Images and phive2015/Adobe Stock.
Source: An Addictive, Emergent Threat

In the last decade, social media-enabled information warfare (IW) emerged as a clear threat to the United States and liberal democracy. In that time, the US failed to develop an effective national security strategy to counter the threat. This paper will explore this threat and provide recommendations for two key issues: (1) the weaponization of social media against US national instruments of power and (2) the impact of social media platforms (SMP) on US democratic institutions. Open societies like the US possess unique vulnerabilities compared to closed, authoritarian states. For example, Wired reported on Russian and Chinese actions to restrict access rather than engage SMPs like Facebook, Google, and Twitter to remove problematic content. The Research and Development (RAND) Corporation detailed that once access is controlled, these states exploit open societies' vulnerabilities to expand divisions across democratic institutions. In 2016, Russia exploited the American political divide through a coordinated social media campaign to undermine election security and credibility. Driven by the campaign's success, state and non-state actors are seeking to employ similar tactics. However, as

Nate Low argued in Foreign Policy, rather than seizing key terrain, actors exploit the open exchange of information to target attention in order to gain followers.

21st Century IW requires the audience's attention to influence behaviors and habits. This attention is not only a finite resource but also currency. Captivology: The Science of Capturing People's Attention, by Ben Parr, identifies seven triggers to call people to attention: automaticity, framing, disruption, reward, reputation, mystery, and acknowledgment. Gaining attention, however, is not enough; the message must permeate to influence others, a concept that social manipulators refer to as "sticky." In Made to Stick, Chip and Dan Heath describe the idea of permanency as having five principles: simplicity, unexpectedness, concreteness, credibility, and emotions. The combination of these two ideas form the basis for the triggers and principles. The Islamic State of Iraq and Syria (ISIS) combined these two ideas to recruit followers. Russian proxies did so to sow division across multiple democracies.

Social Media Platforms Build the Attention Economy

The attention economy operates off a habit loop. Since the early 2000s, SMP engineers created algorithms and site pages designed to exploit addiction patterns. This loop, described by Charles Duhigg, as a neurological cycle consisting of three elements: cue, routine, and reward. SMPs provide all three elements: (1) alerts and updates cue a user's action, (2) the user establishes a routine to review the alerts and updates, and (3) views, likes, shares, tweets, comments (as detailed by Peter Singer and Emerson Brooking in LikeWar) lead to the reward of social gratification (see Figure 2). The user's brain is trapped in a habit loop-supported cycle and the SMP earns their attention.

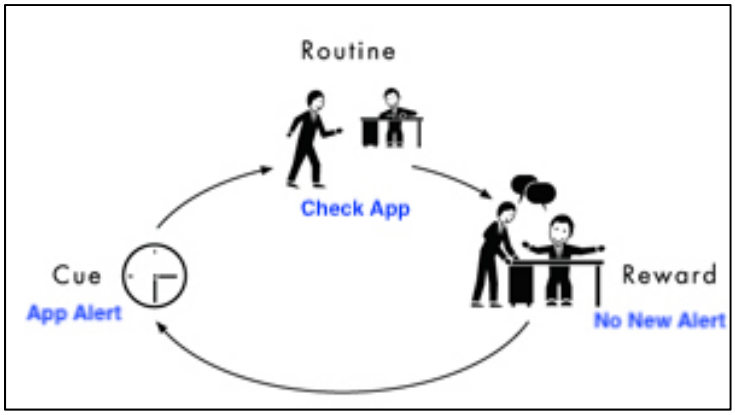


Figure 2: Charles Duhigg's Habit Loop.
Source: Charles Duhigg

This phenomenon is described as "The Rabbit Hole," effect in which SMP algorithms encourage viewers to increase use based on the habits of average users and in some instances triggers actions from the viewer. In doing so, Singer and Brooking argue, SMP algorithms created a market centered on attention and altered social behavior to reward popularity and recognition over facts. In 2019, Facebook employed this loop to generate $67 billion in advertising or for 98.5 percent of its global revenue. By the end of 2020, Facebook is estimated to generate another $82 billion in advertising (see Figure 3).

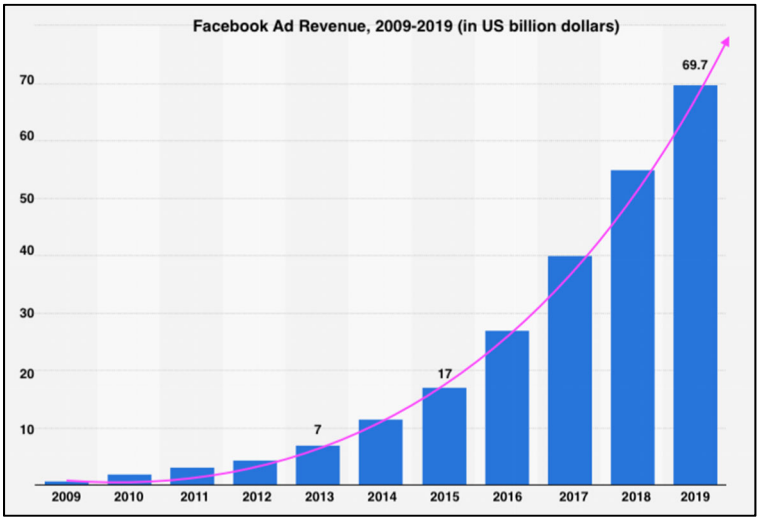


Figure 3: Facebook's Ad Revenue, 2009-2019 (in US billion dollars).
Source: Statista

The Impact of the Attention Economy

Based on Facebook earnings projections, it may appear that the addiction is incurable. The challenge is co-dependence. While SMPs depend on the advertising revenue, users gain not only connection but other important services at the expense of their personal data. Global users remain willing to accept that exchange. Since the turn of the millennium, American consumers quickly adopted new technology at exponential rates without consideration of the unintended effects (see Figure 4).

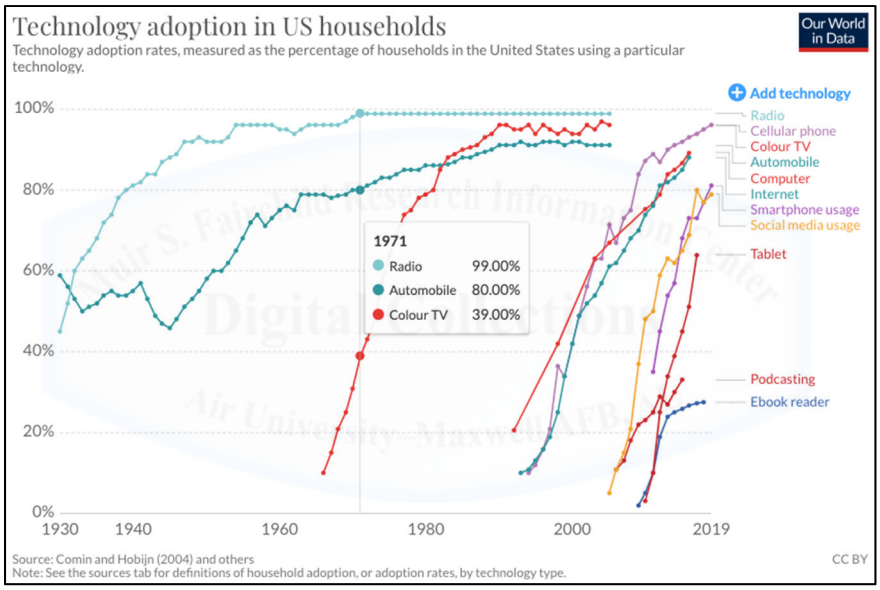


Figure 4: Technology adoption in US households, 1930-2019.
Source: Our World in Data

SMPs are no exception. Social media activity may lead to filtered preference bubbles that reinforce biases exposing the user to targeted group manipulation. Like any tool, SMPs may be used for good or ill. The cue/routine/reward cycle applies equally to "cat videos," election manipulation, and ISIS propaganda. In essence, IW leered from the digital advertising industry to seek followers for its cause.

The addiction created by the SMP industry connected the world to push information to millions with a single-click; however, it created a damaging side-effect to democracy. Critical thinking has taken a back seat. For the Shorenstein Center on Media, Politics and Public, John Wihbey covers two key trends on critical thinking and social media. First, amongst a dataset of 43 million Twitter users, just 20,000 "elite users" (i.e., "influencers") generated half of all the links consumed. Second, users are cornered into fast thinking and cognitive bias to keep pace with the expanse and speed of content sharing. Clint Watts, senior fellow at the Center for Cyber and Homeland Security at George Washington University and author of Messing with the Enemy highlights two trends in addiction and consumption. First, a 2015 study on internet addiction showed that adults spent 2.75 hours per day on the phone and 59 percent of people exhibited dependency on social media (See Figure 5).

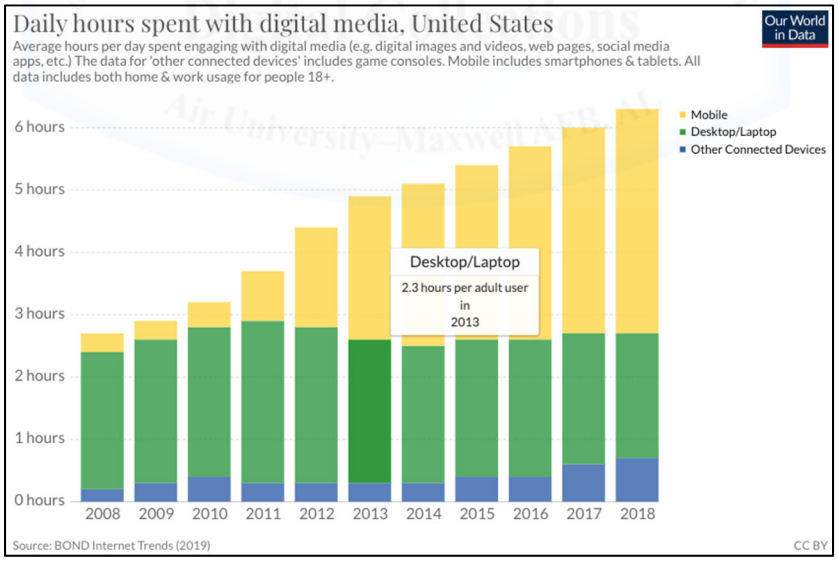


Figure 5: Daily hours spent with digital media in the US, 2008-2018.
Source: Our World in Data

Second, the average human attention fell to 8 seconds, hurting critical thinking skills. For example, Facebook's newsfeed interface enables users to establish time-saving habits by centralizing data as opposed to navigating between apps. These innovations designed to turn

attention into revenue for the SMP and advertisers are the same techniques exploited with hostile intent. As mobile device and SMP use increases, users' attention span and critical thinking decreases: a cognitive environment ripe for social manipulation—the birth of 21st Century IW.

Evolution of 21st Century Information Warfare (IW).

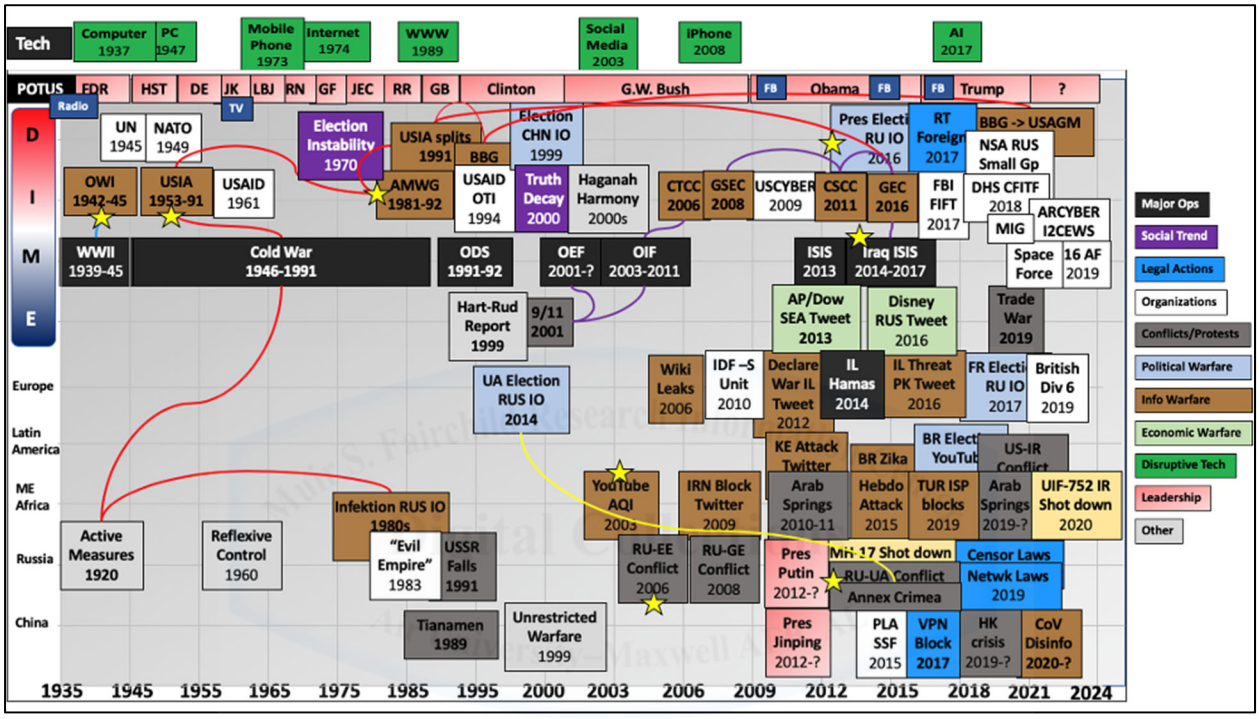


Figure 6: Evolution of Information Warfare toward Social Media.
Source: Author from Multiple Sources

Pre-Social Media Age

IW is not a new method of conflict. In 2009, Admiral Michel Mullen, Chairman of the Joint Chiefs of Staff, opined: "America has lost its way on strategic communications. Most strategic problems are a matter of policy and execution problems." Historically, the US was quick to disband and forget the value of information on the battlefield. After successful IW campaigns, senior leaders often disbanded the group only to reactivate it again after losing positional advantage. Today's positional disadvantage is compounded and complicated by the actor's ability to use social media to influence millions of users across the globe instantly with

low barrier to entry. The speed of the message may be different, but lessons learned during World War II (WWII) are still applicable today. During the war, the US Office of War Information (OWI) developed an information campaign intending to bolster the war effort at home and abroad by using all forms of media, including the nascent Hollywood movie industry. In addition to defending the American public's view of the war, the OWI played a key offensive role by developing efforts such as Operation Annie that utilized a radio-based disinformation campaign ultimately leading Nazi ground forces into a trap. Despite this success, at the end of WWII, the US terminated the OWI.

Thirty years later, during the Cold War, the Soviets used a technique called "selective replay" in print media and radio as part of a coordinated IW campaign. In response, the US established the Active Measures Working Group (AMWG) within the US Information Agency (USIA) to address Soviet IW measures. According to Low, the AMWG's role was crucial in raising public awareness of Soviet disinformation efforts and restricting their effectiveness abroad as evidenced by the Soviets disavowing the 1980s Operation Infection AIDS campaign in its official media outlets originally designed to blame the US. Fletcher Schoen and Christopher Lamb further detailed AMWG's successes at driving Soviets' costs. Ultimately, AMWG hastened the fall of the Soviet Union by exposing its multibillion disinformation effort at much less cost and with a smaller workforce than it took to create it.

Counter IW campaigns must be willing to speak the truth against disinformation as silence allows the enemy to seize the initiative and being first matters. However, like the OWI, AMWG was terminated after the end of the Cold War with its functions divided across new organizations. Watt argues that this reorganization led to the loss of both its expertise and effective interagency collaboration. Low agrees: despite the campaign's success, it became

dormant and enabled Russia to adopt and adapt its tactics, techniques, and procedures (TTP) to bolster its IW capability for the social media age.

Social Media Age

The same IW lessons learned in WWII and the Cold War need to be relearned again. A failure to anticipate the shifting global information environment left the US ill-prepared to combat technology-savvy extremists in the Middle East. In War in 140 Characters, David Patrikarakos cites the rise of Abu Musab al-Zarqawi to become the "Bin Laden of the Internet" as emblematic of the weaponization of social media by nonstate actors. Watts elaborates that Zarqawi's jihadist network, al Qaeda in Iraq (AQI), weaponized YouTube by creating content depicting their successes in killing US soldiers and civilians to a musical soundtrack. Zarqawi's efforts demonstrated how social media can push power down to an individual and away from the institution to create a movement. By 2006, AQI rebranded itself as the Islamic State of Iraq with its own IW/media arm tasked with professionalizing the development of this content with a sticky message of fear, action, and blood to recruit and shape public opinion.

In response to the extremist IW threat, the US established the Counterterrorism Communication Center (CTCC) to counter the spread of Islamic State propaganda on the internet and social media. Despite previous IW success in WWII and the Cold War, this initiative met with varied results. Watts argued that unlike the AMWG, the CTCC failed to defeat extremist propaganda on social media as a result of several reorganizations, renaming, in addition to being underfunded, and overmanaged. In 2016, as a result of this lack of effectiveness, the CTCC became known as the Global Engagement Center (GEC). The GEC assumed some USIA functions under the Countering Foreign Propaganda and Disinformation Act. But, according to Watt, throughout each change, it has taken very few measures against current IW threats.

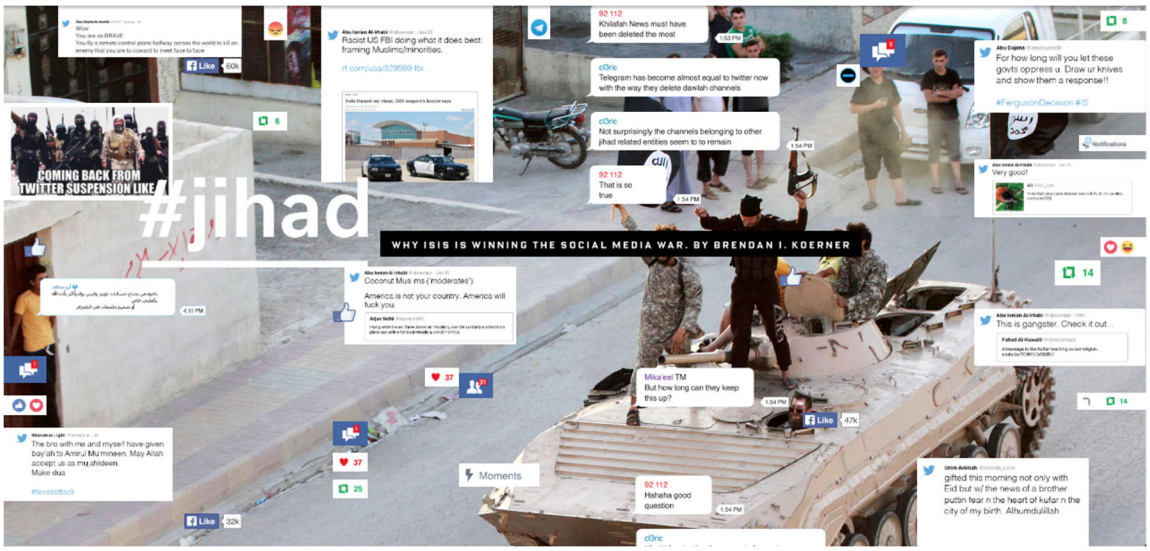


Figure 7: Why ISIS is Winning in Social Media War. Source: Wired

The professionalization of its IW and social media efforts is arguably the reason the Islamic State emerged into a major middle east threat in 2013. As the US used radio broadcasts during *Operation Annie*, ISIS successfully used the internet to convince numerically superior Iraqi forces to abandon posts and weapons out of fear, resulting in the rapid conquer of Mosul and large swaths of territory in Iraq and Syria. To summarize Singer and Brooking's detailed explanation of ISIS' campaign:

> *Using SMPs and tags like #AllEyesOnISIS, ISIS ran its military offensive like a virtual marketing campaign that recruited over 30,000 foreigners from nearly a hundred countries to join its cause. By 2016, Iraqi forces understood the weaponization of SMPs and used ISIS TTPs against them in its SMP-enabled IW efforts with the use of portable cellphone towers and its own #FreeMosul tag. Additionally, the US State and Defense Departments joined Iraqi forces in the online battle mounting an offensive in cyber and social media. As a result, the SMP feeds became surreal for worldwide users to join and "like" whichever post they chose.*

In her report for National Public Radio (NPR), Dina Temple-Raston highlighted US efforts to counter ISIS' IW campaign via a unique IW command structure by the National Security Agency (NSA) and US Cyber Command (USCYBERCOM). This capability was necessary due to the observation that, as Watts stressed, "terrorists have and will continue to

evolve, migrate, and innovate on these technologies and whatever comes next." Before adopting this IW structure, the US faced the reality of being caught out-maneuvered in cyberspace and social media. Unlike the GEC, this IW command structure allowed the US to execute forward into ISIS network to find, fix, and target its key nodes to degrade its command and control.

The Disinformation Chain

While ISIS was forcing the US to restructure for to meet the demands of the 21st Century, Russia was honing its capabilities. In 2007, Russia used IW to sow division in Estonia by amplifying historical angst over efforts to move the historical Bronze Soldier statue, which commemorates both the Soviet defeat of the Nazis but also the oppression of Soviets. In their September 6, 2019 episode of The Weekly, entitled "The Blueprint" the New York Times explained Russian information strategy against Estonia. Russia employed a multi-faceted information operations (IO) approach through (1) timely diplomatic messaging from President Putin against the North Atlantic Treaty Organization (NATO) expansion, (2) social media manipulation to spread disinformation, and (3) malicious cyber-attacks to disrupt its government, media, and banking institutions. RAND's research team refers to this approach as the disinformation chain that is driven by leadership (Putin), proxies (Kremlin-backed hacker), and amplification channels (social media, news outlets) to target the consumer (Estonians) (see Figure 8).

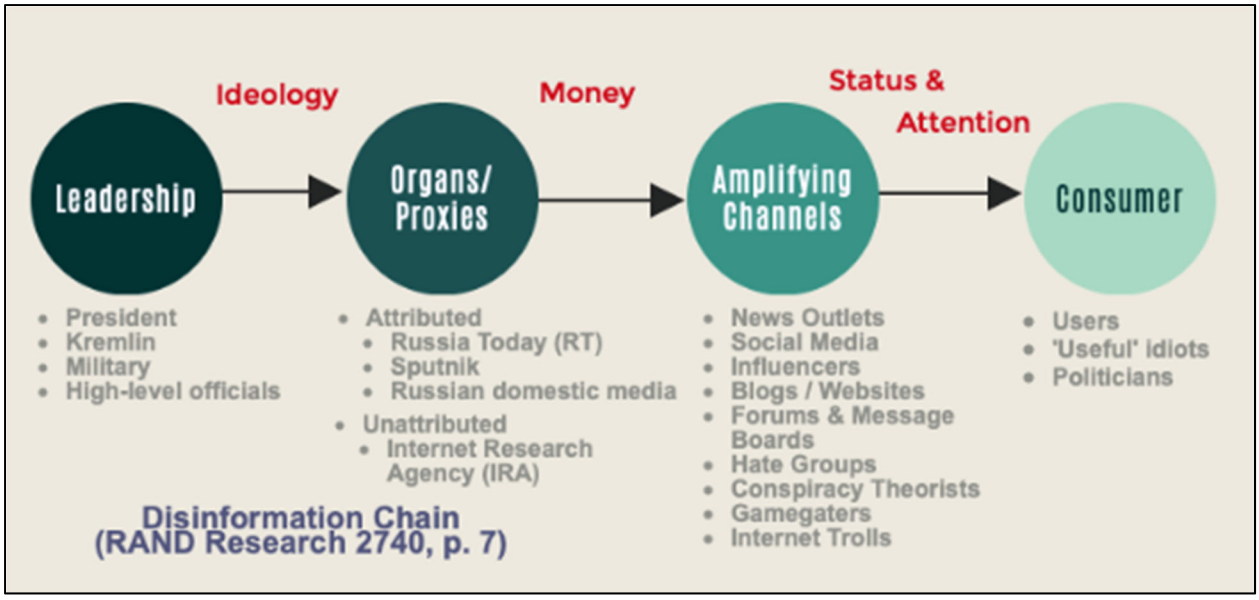
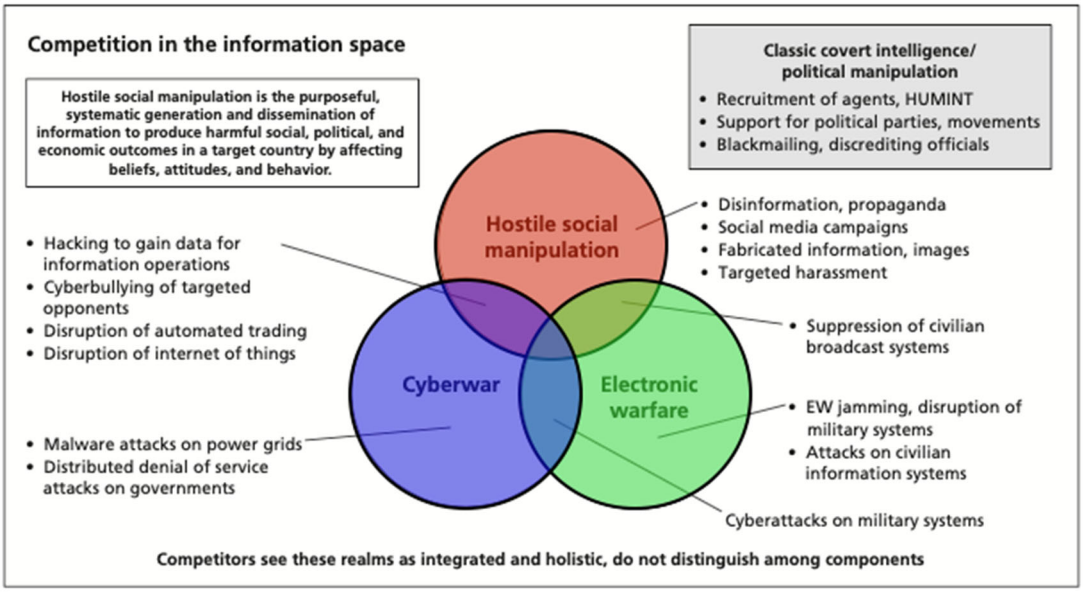


Figure 8: RAND Disinformation Chain. Source: Author from RAND

Despite this demonstration of capability by Russia's IW force, the US failed to pivot to prevent similar actions. The New York Times argued that the US was too distracted in the Middle East and short-sighted to recognize the potential Russian IW threat. The US failed to recognize the parallels between ISIS and Russian employment of disinformation and did not apply their lessons learned and new TTPs. With minimal accountability or international response from the Estonia conflict, Russia continued to improve its TTPs against other nations. During the 2014 Ukraine conflict, Russia integrated cyber warfare, hostile social manipulation (e.g., media outlets and social media), and electronic warfare by gathering indications and warnings on soldiers positioning by sending fake social media posts to their family's page. Russia exploited Ukrainian soldiers' reliance on mobile technology to adjust target sets designed to create fear, confusion, and chaos (see Figure 9). To defeat Russian disinformation, RAND argues that the US must engage all links within the chain as Estonia and Ukraine did; however, in 2016 the US failed to do so.



NOTE: HUMINT = human intelligence.

Figure 9: The Boundaries of Social Manipulation. Source: RAND

Weaponization of Social Media against the US

Singer and Brooking argue that SMP's efforts "to make the world open and connected" are enormously successful financially but present an opportunity to manipulate national instruments of power. The problem is becoming increasingly more complex as SMP use around the world becomes ubiquitous (see Figure 10).

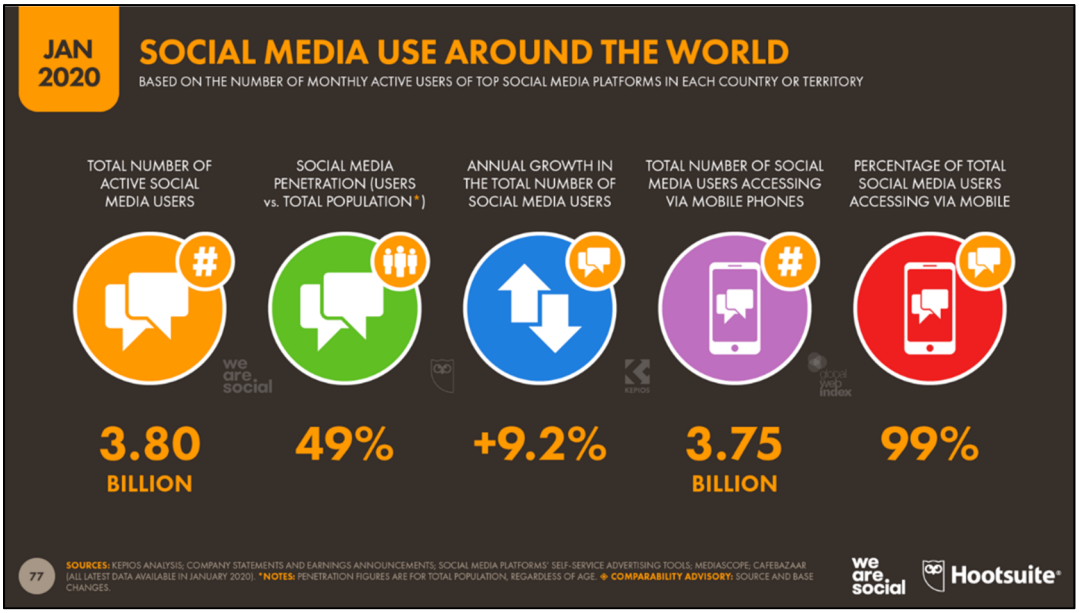


Figure 100: Social Media Use Around the World. Source: Datareportal

As 21st Century IW took root in the Middle East and across European borders, it asymmetrically targeted the US, affecting all its national instruments of power. In Winning Without Fighting, Ross Babbage explains that Russia views the West as a powerful competitor, bitter rival, and greatest military threat. As a result, Russia is leveraging social media warfare to relentlessly attack the US to erode the public's belief in the democratic system in an effort to return to its former status as a Great Power (see Figure 11).

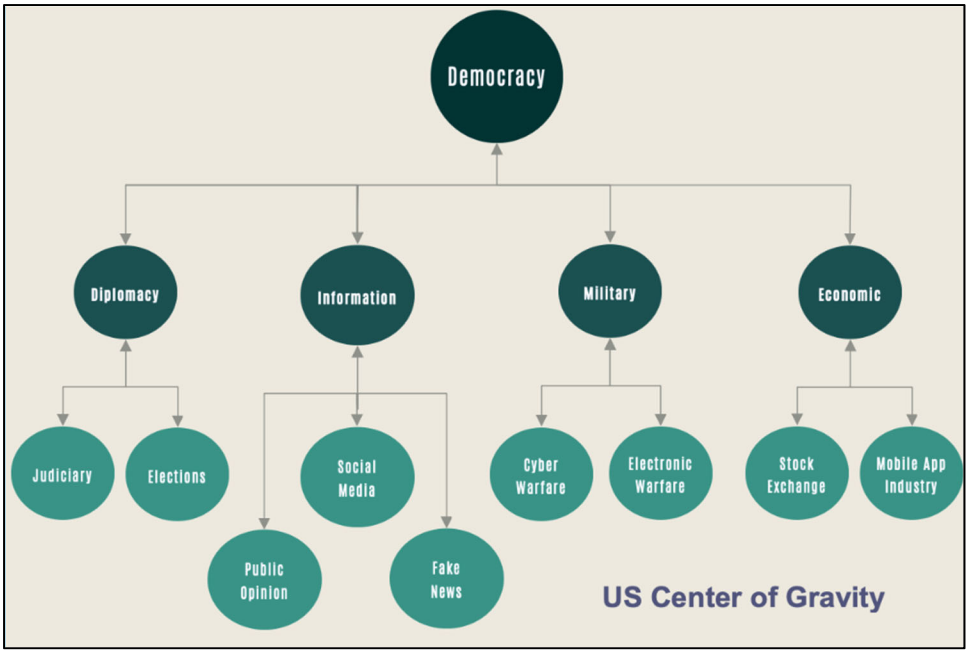


Figure 111: Social Manipulation across US Instruments of Power.
Source: Author from RAND

Hostile Social Manipulation

The RAND Hostile Social Manipulation report provides an excellent representation of the complex scheme of maneuver malicious actors can leverage to best achieve the objective or desired emotion (see Figure 12). In October 2019, Jack Stubbs and Christopher Bing reported on SMPs endeavors to address shortcomings, such as removing Russian Instagram accounts targeting US voters but remain reactive. Another emergent dilemma is the manipulation of online search results. "Reputation Management" companies argue that their purpose is to fix the imbalance of power between clients and online information about them. However, as Rachel Levy reported in the Wall Street Journal, these companies' TTP include the spread of disinformation intended to manipulate SMP's algorithm results, such as Google's search. The NATO Strategic Communications Center of Excellence (StratCom CoE) identified how reputation managers, or manipulative service providers, grow undeterred with Russia dominating

this industry. Critics argue that in manipulating online information, reputation managers prevent the larger audience from making an informed decision.

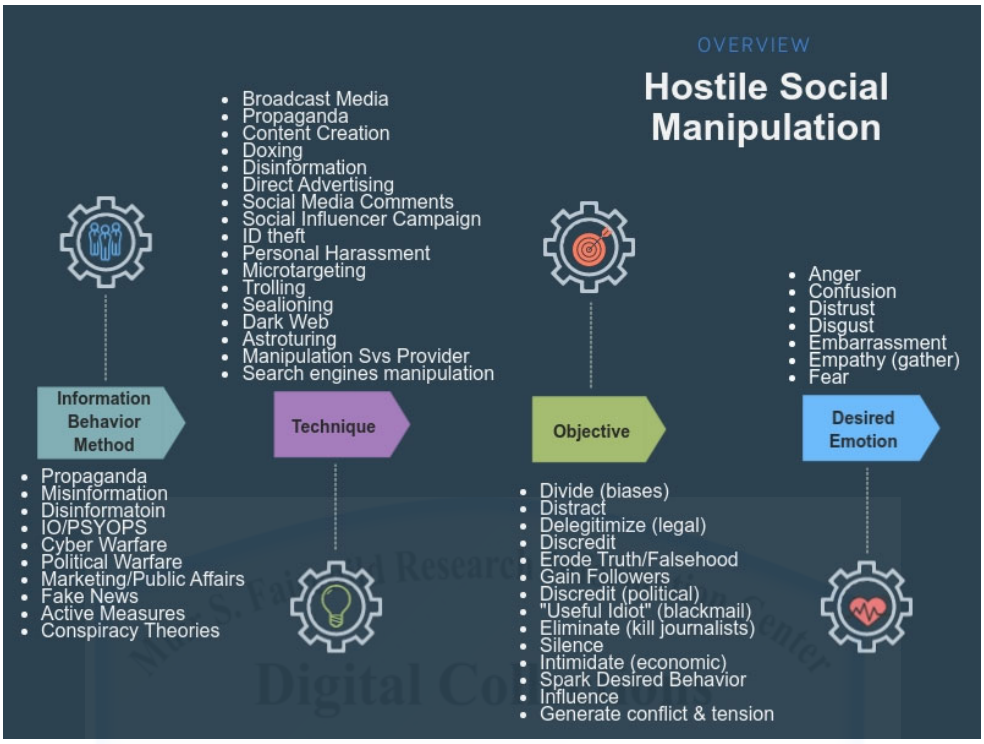


Figure 12: Overview of Hostile Social Manipulation
Source: Author from RAND

According to the Center for Strategic and International Studies (CSIS), Russia views the US judiciary system as dependent upon public acceptance of the legitimacy of its outcomes. Devi Nair, Arthur Nelson, and Suzanne Spaulding highlighted how Russia uses its disinformation chain intentionally to convince readers that the US justice system is broken. Russia's objective is to drive US citizens to question whether the current system supports their values and needs but never to provide answers.

Unfortunately, SMPs do not agree on how to address threats like Russian hostile social manipulation and instead create their own rules; especially where it intersects with politics. Unlike Twitter, Facebook argued that the technology industry should not be in the position of

fact-checking political ads nor would it ban political advertisements as it gives attention to lesser-known candidates. However, Facebook failed to realize that microtargeting political ads to only specific filtered groups undermines the general public's ability to respond as they are not able to see those ads. Google's political ads policy, on the other hand, is to limit its audience targeting to age, gender, general location, and contextual terms. It does appear that SMPs agree in blocking disinformation by altering its search algorithms and coordinated with third-party fact-checkers to prevent harm to others like in the 2020 China coronavirus crisis. However, this was in the medical sector. Solutions remain evasive at the intersection of social media and politics.

News Media Outlets

According to RAND's Truth Decay study, post-2000, the rise of SMPs and the demands placed on its education system amplified cognitive bias, drastically reshaping American information consumption. "Truth Decay" consists of blurred lines and increased volume of opinions over fact, disagreement of facts and interpretation, and a declining trust in traditional media. Jennifer Kavanaugh described how pre-2000s journalism and cable programming news evolved from academic, abstract reasoning, authority-based, and event-based to a landscape dominated by emotions, arguments, and opinions to persuade and debate. As a result, news outlets favored speed over accuracy to be first to report but also on occasion spread "fake news." Arguably, the US is divided by media bias, distrust, and political ideology. RAND research found that echo chambers and preference bubbles generated by SMPs expand the divide. (see Figures 13 and 14). Singer and Brooking expound on this concept by highlighting that American polarization was exploited by Russia during the 2016 US presidential elections to achieve its objective by fomenting confusion, chaos, and distrust.

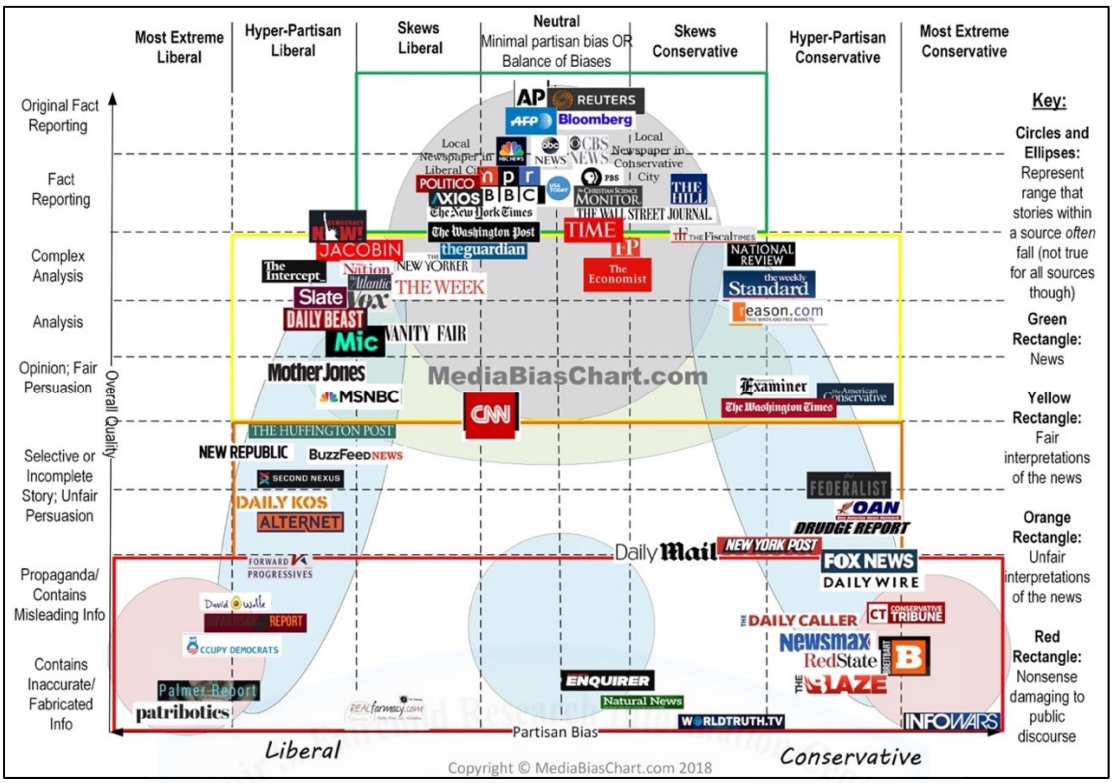


Figure 12: Example of Media Bias.
Source: Media Bias Chart

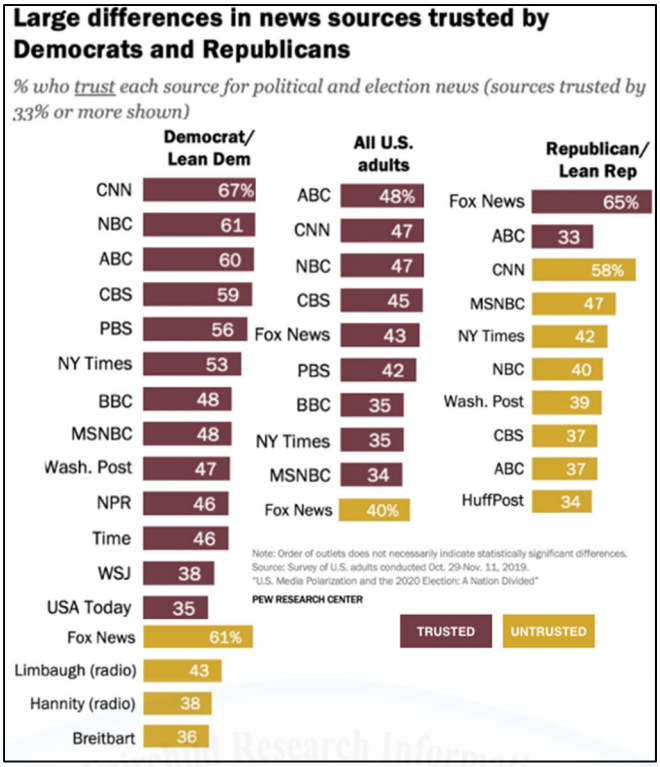


Figure 14: US Media Polarization and the 2020 Election: Trusted & Untrusted Media by Political Party.
Source: Journalism.org

For example, Nieman Lab reported newsrooms will inevitably be forced to shoulder the heavy burden of identifying media created using artificial intelligence (AI) technology (i.e., deepfakes), a task that will require complex forensic techniques and increase costs for news outlets. For trustworthy agencies, the charge of deepfake will be their burden to disprove and in an environment of fast-thinkers and cognitive bias that effort drives further consumer distrust and truth decay. While Facebook banned deepfakes, shallowfakes, the predecessor of deepfakes and defined as manipulated video using non-AI editing tools, are allowed, which can be just as dangerous. The US can look to Finland's disinformation efforts to address the problems of truth decay. Per CNN's Eliza Mackintosh, Finland prioritizes funding for K-12 digital literacy, critical thinking programs, and voter literacy as a whole-of-nation approach.

Election Security

Arguably, Russia's Estonia and Ukraine operations served as a rehearsal for anti-US operations designed to erode public opinion and confidence in selecting its leadership. As detailed by New York Times' The Weekly, unlike the Estonia-Russia conflict, the US was hesitant to blame Russia for its interference leading up to the US 2016 presidential elections to avoid creating public panic and loss of confidence in its election process. Since 2008, Facebook played an increasingly large role in the last three US presidential elections with its Engagement Custom Audience tools designed to apply microtargeting to influence a subset of individuals with common traits. The 2019 Mueller report documented how the IRA paid approximately $100,000 for over 3,500 advertisements that specifically campaigned against some candidates and benefitted others during the 2016 US presidential elections. Between 2015 and 2017, 470 IRA-controlled Facebook accounts made over 80,000 posts resulting in targeted social media manipulation and IW messaging reaching at least 29 million US persons before deactivation. As part of a study, the NATO StratCom CoE purchased similar manipulation service provider capabilities with 300 euros to evaluate the SMPs' response. The NATO StratCom CoE team concluded that SMPs are failing to protect democratic institutions from manipulations and self-regulating SMPs do not work. Sebastian Bay and Rolf Fredheim explain that while SMPs have a vested interest in becoming better at identifying fake and bot accounts during account creation, they still struggle at removing accounts and disinformation even as it was reported.

According to NPR, many US election officials believe "the biggest danger [to election security] is causing enough confusion to undermine public trust in the process" and expect attacks to also come from Iran, China or some domestic player to undermine democracy. After the 2016 US presidential elections, the US government established election security as a top priority. The outcome resulted in several task force elements across bureaucratic hierarchies and

authorities that focuses on a single node rather than synergistic opportunities, such as those demonstrated by the 1980s AMWG (RAND). One unique success story, however, is the stand up of NSA's Russia Small Group in 2018. CBS News' Olivia Gazis reported that the joint election security task force played a pivotal role against IRA activity. The Russia Small Group was successful as a result of the military "defend forward" doctrine change in its 2018 cyber strategy; however, public awareness was absent. The Russia Small Group is not unique. Other entities like the Foreign Influence Elections 2020 group are playing a role in tracking what foreign media outlets are doing to influence the upcoming US presidential elections (see Figure 15).

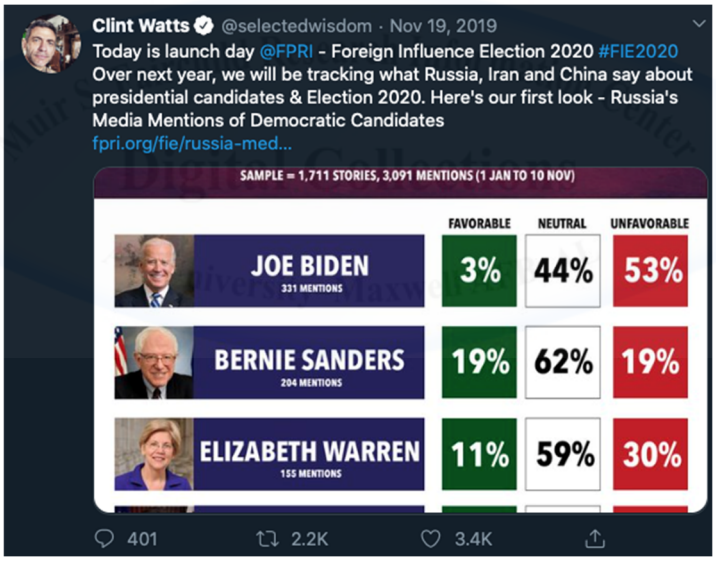


Figure 135: Screenshot of Clint Watts Foreign Influence Election 2020 report tweet. Source: Twitter

In this instance, the Foreign Influence Elections 2020 group are fitting in the OWI and AMWG-like roles to provide public awareness against Russian disinformation. The Russia Small Group's sole focus on the Russian problem reduces flexibility and integration to react to evolving threats. Further, the US task force structures may lead to added costs and delayed responses, unlike the AMWG era that sunk costs on the adversary. Additionally, the US can

leverage academia and other nation's framework to provide solutions. For example, a Mozilla Foundation research team conducted a temporal network analysis on 10 GB of tweets over 10 years from over 11 countries. The results demonstrate a view of how individual networks of social manipulation compare over time to better understand topic trends and habits (see Figure 16).

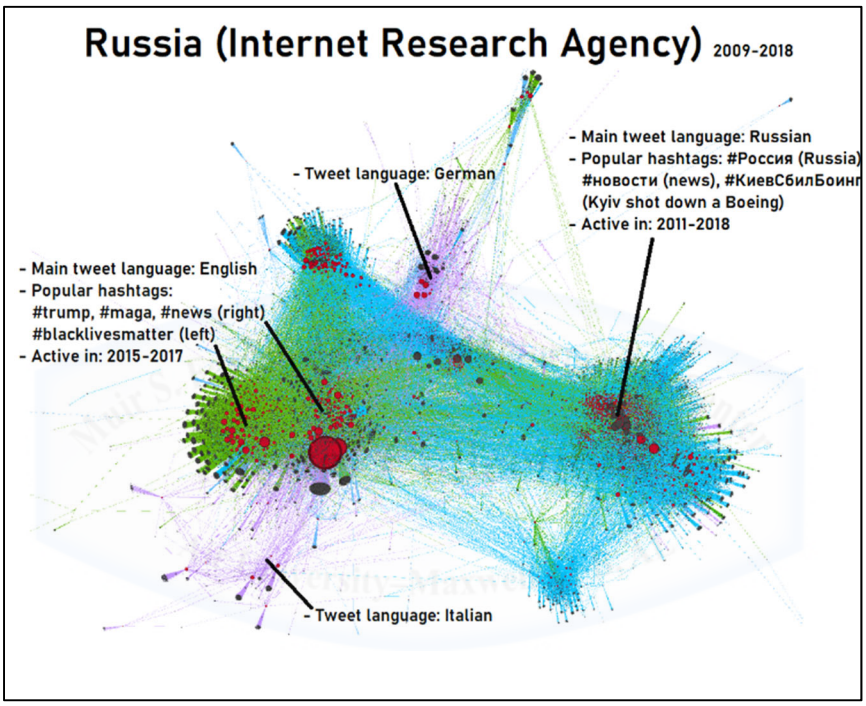


Figure 14: High-level visualizations of Russia disinformation operations on Twitter using temporal network analysis, 2008-2019.
Source: Massachusetts Institute of Technology

Near real-time analyses like these may better serve SMPs and election authorities to best identify and block these influence actors before disinformation spreads too far to do damage control. Additionally, MIT's physics application using the Ising model, which assesses the behavior of ferromagnets, helped explain how US elections transitioned to a period of increasing instability post-1970 as a result of small changes in voter preferences. Furthermore, the US can look at other nation's electoral process to address some of its vulnerability gaps. For example,

unlike the US presidential 10-month voting period, France's final election voters go to the polls two weeks after the final candidates are determined. Watts detailed further that France (like many other countries) also imposed a 2-day media blackout during its 2017 presidential election that had the effect of mitigating Russian interference as demonstrated in the US 2016 presidential election.

Legal Implications of Social Media

Despite the seriousness of the threats, nations remain slow to establish laws and policies at the federal and international levels towards regulating social media. Today's leaders are using SMPs to drive decisions in ways that deviate from formal communicational channels often requiring impromptu damage control. As highlighted by Patrikarakos, in 2012, a tweet from the Israeli Defense Force (IDF) accidentally declared war in 2012. Unsurprisingly, European countries have taken more direct legal approaches, such as France's "fake news" ban and Germany's removal of "illegal" hate speech (see Figure 17).

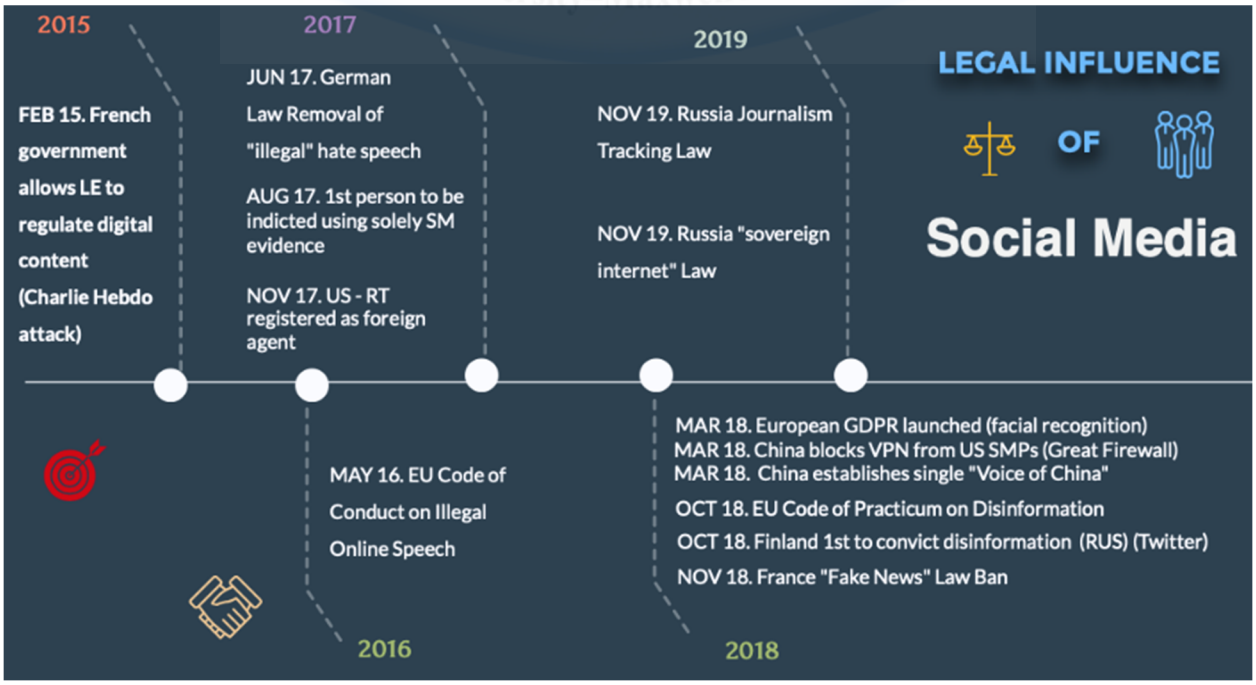


Figure 15: Legal Influence of Social Media.
Source: Author from multiple sources.

However, the west remains at a disadvantage as authoritarian regimes apply countermeasures to censor information within its network to mitigate their own vulnerabilities. For example, Singer and Brooking describe China's Golden Shield Project which provides the capability to censor its intranet by restricting terms and anti-regime historical events (e.g., Tiananmen protest) making it difficult to organize grassroots protests. According to Niall Firth, Russia is pushing its journalism tracking law in response to the US registering RT as a foreign agent and its "sovereign internet" to control internal information flow at lesser costs.

Despite demonstrated hostility in the information space, these acts have not driven a widespread response, as a kinetic attack likely would have, under existing international law and norms. This vulnerability is compounded by United Nation's Article 51, which provides the "inherent right to individual or collective self-defense if an armed attack occurs against a state." Further there is no clear relationship between NATO Article 5 Collective Defense and IW; it was only invoked following the 9/11 attacks where an attack on one member was interpreted as an attack on all. Nations must begin to reconsider its defense policies in the information domain as a result of IW actions by Russia in Estonia and Ukraine. As of September 2019, only 27 countries agreed on the need to impose joint costs on hostile actors in cyberspace. However, the lack of widespread agreement on the appropriate response to cyberspace or information actions presents an easily exploitable gap for state and non-state actors.

Economic Control of Mobile App Industry

Exploitation of SMPs is not the extent of the reach US adversaries are willing to go to defeat democracy. Within the economic instrument of power, they seek to control the mobile app industry to influence the channel of communication. By observing the US employment of

technology in the Iraq War and Russia's IW attacks, China adopted its own "informatized local warfare" doctrine critical to its national security and winning future conflicts. According to then-Federal Bureau of Investigation (FBI) Director, Christopher Wrage, China seeks "to replace the US as the world's leading superpower and influence…while breaking the law along the way…using censorship, propaganda, public diplomacy, economic pressure, and strategic messaging." While China is using similar IW TTPs as the Russian actors, the Center for New American Strategy (CNAS) argued China's mobile app industry has positioned itself to close the gap against the US SMP market since 2011 (see Figure 18).

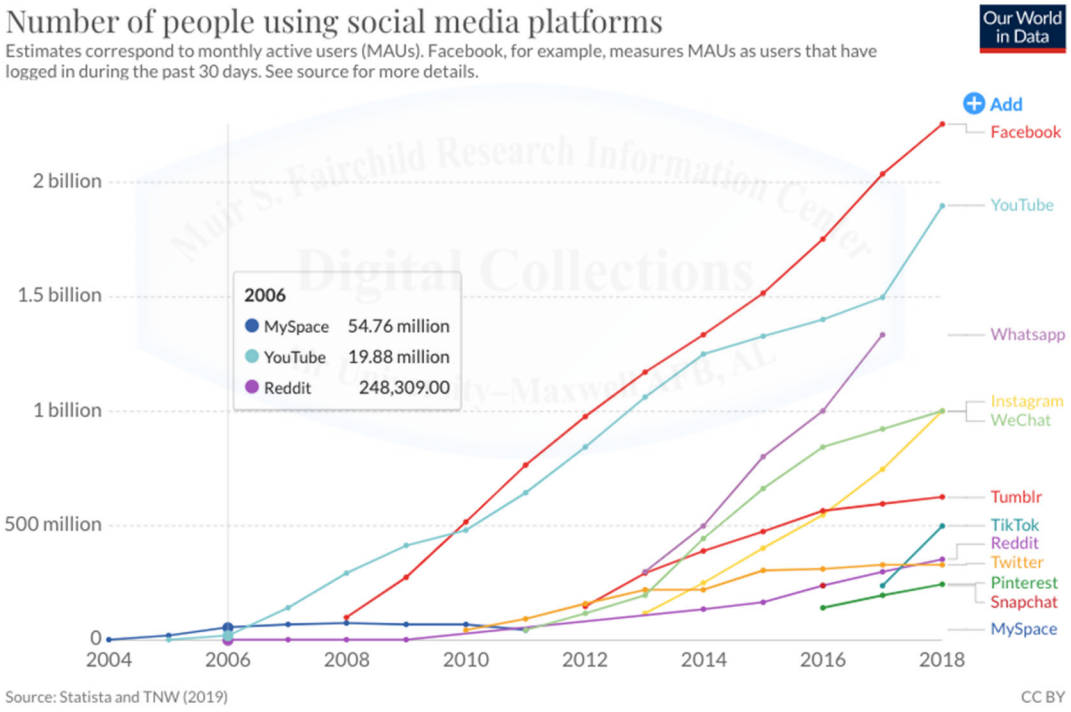


Figure 168: Number of people using social media platforms, 2004-2018.
Source: Our World in Data

The CNAS report highlighted Chinese investments to expand its global social media presence; for example, WeChat Pay's penetration of emerging markets like Malaysia (see Figure 19). In doing so, China quietly exports its surveillance state ideology, as an alternative to

democracy, while collecting data on its users. This includes China's ability to censor social media usage for its users as counter-IW means.

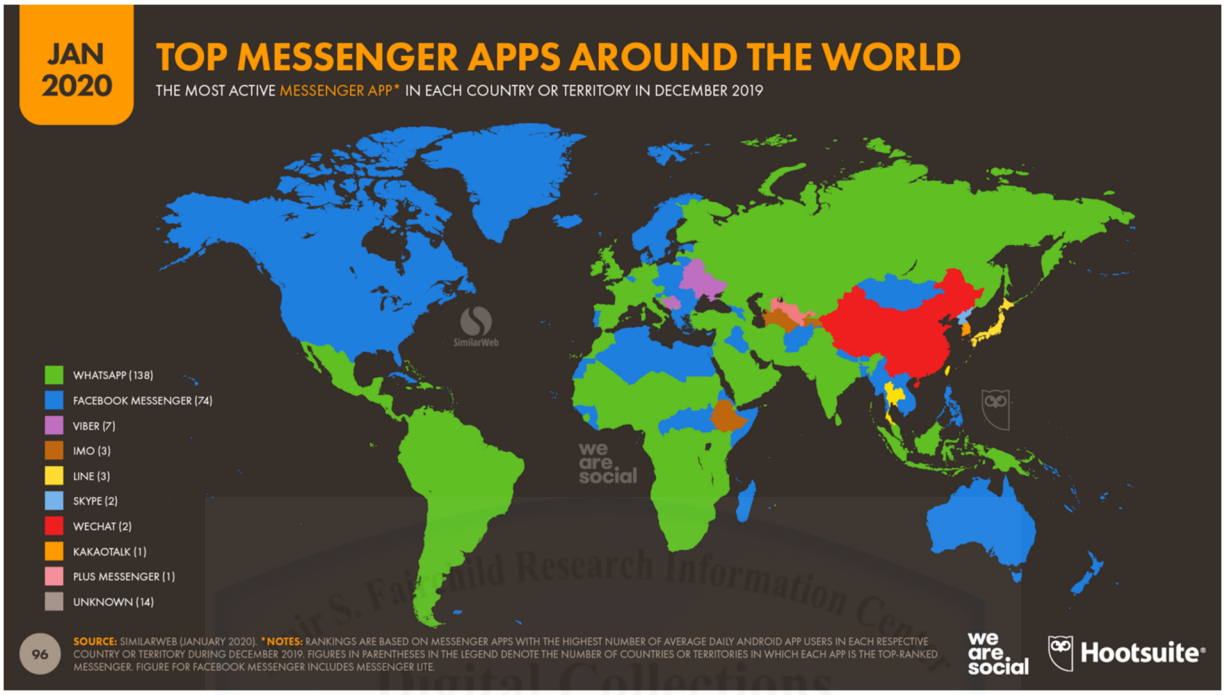


Figure 179: Top Messenger Apps Around the World, Jan 2020.
Source: Datareportal.com

Some nations are beginning to show concern in the security risks posed by China's mobile apps. For example, the Indian Intelligence Bureau directed its troops to uninstall 42 Chinese apps from their phones due to privacy and operations security concerns. Kristen Lee and Karina Barbesino argue that while China seeks to remove US influence from within its border, it still uses Facebook and Twitter to influence US users that allows it to push its narrative when it sees an opportunity to do so.

Economic Instability and Economic Pressure

While 9/11 attacks on the World Trade Center twin towers were directed at disrupting the global economy, social media manipulation may indirectly influence the financial stocks by instilling fear on its followers. Shawn Langlois detailed the 2013 Associated Press Twitter (AP)

hack: the Syrian Electronic Army (SEA) announced a hoax White House attack creating fear and uncertainty resulting in the S&P 500's $136 billion loss of market capital during the six-minute window that the post remained online (see Figure 20).

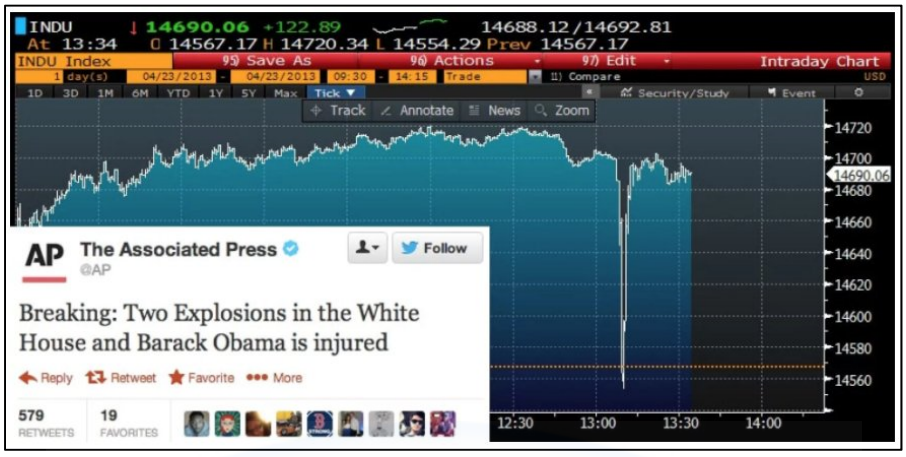


Figure 18: Syria Electronic Army hacks the AP Twitter and sends DOW crashing.
Source: Market Watch

Russia's Internet Research Agency (IRA) achieved a similar objective orchestrating a 2016 Disney stock plunge by creating a bomb hoax that in reality was a mechanical malfunction. Unlike SEA, the IRA used Disney users' social media live posts to build credibility, create its disinformation narrative, and then amplified it through news media outlets (proxies), Russia Today (RT) and Sputnik, to reach other consumers creating confusion and chaos (see Figure 21).

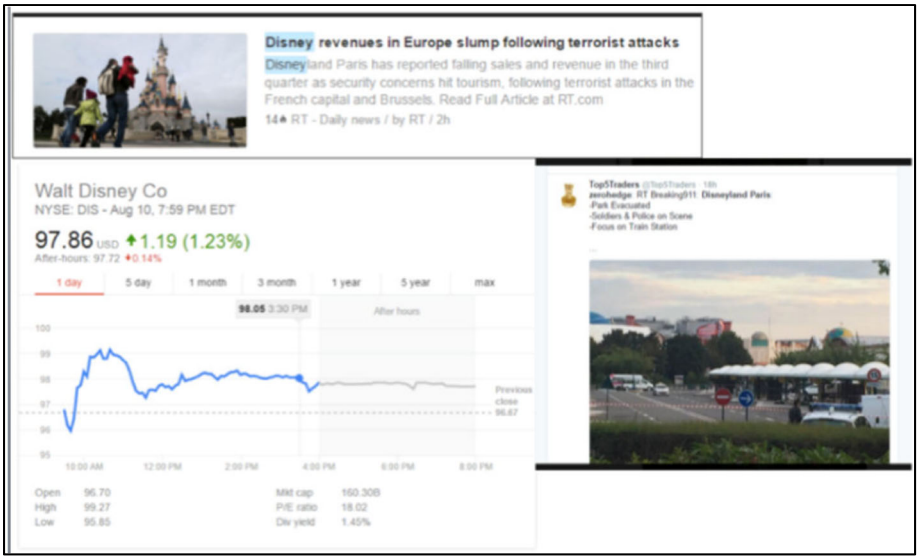


Figure 19: Russia disinformation on Disneyland Paris evacuation, 2016.
Source: War on the Rocks

Furthermore, China demonstrated its ability to apply economic pressure to censor anti-government information on social media during the 2019 Hong Kong protests where it demanded Apple to remove mobile apps that aided in tracking police movements and coordinate protests.

Military IW Structure.

According to RAND, while the OWI and AMWG were created to support the ongoing war, the US Department of Defense (DoD) seeks to do the same in 21st Century warfare although it is limited domestically due to Title 10 and Title 50 authorities. Morgan Dwyer, a CSIS fellow, argued organizations that separate technology and mission inadvertently create bureaucratic barriers and become counterproductive ultimately hampering technical development. In 2015, according to Mark Pomerlau, China centralized space, cyber, electronic warfare, psychological warfare under the Strategic Support Force to prioritize and execute its IW efforts. However, in similar fashion to the US election task force reorganization, the military services established

fragmented IW elements within its structure, whereas psychological operations remain under US Special Operations Command (USSOCOM) and space moved under US Space Force.

The DoD must create the structure to fight the future fight as well as determining how best to integrate IW efforts build upon its successes of the NSA Small Russia Group. Public Affairs is also an important component of IW and must be part of the discussions and solutions. In a joint all-domain operations strategy, there needs to be a consideration to re-designate USCYBERCOM as the US Information Warfare Command. USCYBERCOM is already integrated with NSA and it aligns with the electromagnetic spectrum domain—as information flow drives decision superiority. In doing so, the Defense Department must expand its EW, IO, and social behavior expertise across its services by developing appropriate training programs and simulated environments and not stove-piped solely under USSOCOM—in 21st Century warfare everyone is a participant and vulnerable. In its current structure and within a contested environment, the overall US narrative faces bureaucratic barriers unless supported and directed by a single IW organization. Finally, senior leaders need to reassess the Goldwater-Nichols Act and the Unified Command Plan to determine whether the current command structure meets the needs of the future fight.

Recommendations

In 1988, Charles Wick, then leading the USIA, emphasized: "In responding to disinformation, the US has the tremendous advantage that the truth is inherently more powerful than lies. But if the lie goes unchallenged, then they [sic] can have a damaging effect." In order to seize on that advantage, the US must take the following actions to defend itself from foreign influence. First, per Schoen and Lamb, policymakers need to consider establishing an OWI or AMWG-like organization to lead the US IW efforts. If the GEC is assigned this role, then

policymakers must ensure it has the necessary resources and the scoped responsibility to be effective. Second, the State Department must continue to push for expanded response in NATO Article V as it pertains to cyber and information domains. Third, policymakers must strengthen the democratic SMP branding and competitors in third world markets and build resilience of at-risk populations, such as empowering influencers. Finally, policymakers and the Federal Election Commission should reconsider other nations' electoral security processes to include prohibition of political microtargeting ads. Policymakers and the Federal Trade Commission should also address foreign spending on SMP digital advertising that undermines democracy.

Furthermore, the US must take the following actions to defend itself from the internal flaws exposed by SMPs on its democratic system. First, the US can look to Finland's disinformation efforts to address the problems of the "attention economy" popularity over facts reward system, lack of critical thinking due to fast thinking, and truth decay. Second, in accordance with NATO's StratCom CoE recommendations, policymakers must regulate SMPs using a third-party source, while applying measures of success standards that increase costs on hostile social manipulation activity. Additionally, policymakers must work with SMPs to develop solutions that preserve democracy and promotes accuracy over aggression and popularity. This may include applying a grading-scale to news outlets by a nonpartisan organization. Fourth, the US can also look at academia to provide different perspectives and solutions. Finally, military leaders need determine whether the current command structure meets the needs of the future fight.

Summary

The US needs a consistent IW strategy on how to navigate the new terrain, but the information and social battlespace also allows the adversary freedom of navigation if left uncontested. In 21st Century warfare, the US faces progressive and asymmetrical attacks on its

national instruments of power from foreign weaponization of social media. SMPs create a truth decay amplified by cognitive biases and low levels of critical thinking that makes the US vulnerable to social manipulation. The US needs a consistent strategy to deal with this IW threat by adopting lessons learned from historical success.

OWI and AMWG deserve greater study to modernize their approach to drive sunk costs to adversary attacks in war and peace. Legal gaps to address SMP technology creates a challenge on how to enforce outdated laws that do not address the issue. Fortunately, the US can look at its European allies to adopt best practices and address disruptive SMPs. Additionally, the US must remain engaged in monitoring Russia's IW in the Baltic region and China's influence operations in Hong Kong, Taiwan and Tibet to better understand emerging threats. Policymakers and SMPs must work jointly on possible solutions. SMPs must continue to provide data for academia, science, and technology researchers to analyze and provide unbiased reporting on trends and future recommendations. Policymakers should listen to the CSIS recommendation to prioritize technology in synchronization with existing or new organizations' distinct mission to create more opportunities for engineers to innovate and optimize in pursuit of the mission. Lastly, the US military leaders need to reevaluate whether the current structure is suited to fight future wars. To win the current fight we must respect the fact that in 21st Century warfare, everyone plays a role. Both policymakers, SMPs, and private citizens must step up to secure the vulnerability created by our attention, habits, and influence—the technology that connects us to divide US (United States, that is).